Horizon 2020

Call: H2020-DS-2014-1

Topic: DS-02-2014

Type of action: IA

Proposal number: 653586

Proposal acronym: SpeechXRays

Table of contents

How to fill in the forms

The administrative forms must be filled in for each proposal using the templates available in the submission system. Some data fields in the administrative forms are pre-filled based on the previous steps in the submission wizard.

1 - General information

Topic	DS-02-2014	Type of action	IA
Call identifier	H2020-DS-2014-1	Acronym	SpeechXRays
Proposal title*	Multi-channel biometrics combining acoustic and machine vision analysis of speech, lip movement and face		

Note that for technical reasons, the following characters are not accepted in the Proposal Title and will be removed: < > " &

Duration in months	*36*		
Fixed keyword 1	*Complexity and cryptography, electronic security, privacy, biome*	Add	
Fixed keyword 2	*Security*	Add	Remove
Fixed keyword 3	*Privacy*	Add	Remove
Free keywords	*voice biometrics, face recognition, voice recognition*		

Abstract

The SpeechXRays project will develop and test in real-life environments a user recognition platform based on voice acoustics analysis and audio-visual identity verification. SpeechXRays will outperform state-of-the-art solutions in the following areas:

- *Security: high accuracy solution (cross over accuracy1 of 1/100 ie twice the commercial voice/face solutions)*
- *Privacy: biometric data stored in the device (or in a private cloud under the responsibility of the data subject)*
- *Usability: text-independent speaker identification (no pass phrase), low sensitivity to surrounding noise*
- *Cost-efficiency: use of standard embedded microphone and cameras (smartphones, laptops)*

The project will combine and pilot two proven techniques: acoustic driven voice recognition (using acoustic rather than statistical only models) and multi-channel biometrics incorporating dynamic face recognition (machine vision analysis of speech, lip movement and face).

The vision of the SpeechXRays project is to provide a solution combining the convenience and cost-effectiveness of voice biometrics, achieving better accuracies by combining it with video, and bringing superior anti-spoofing capabilities.

The technology will be deployed on 2000 users in 3 pilots: a workforce use case, an eHealth use case and a consumer use case.

The project lasts 36 months and is coordinated by world leader in digital security solutions for the mobility space.

Remaining characters 563

Has this proposal (or a very similar one) been submitted in the past 2 years in response to a call for proposals under the 7th Framework Programme, Horizon 2020 or any other EU programme(s)? ○ Yes ● No

Declarations

1) The coordinator declares to have the explicit consent of all applicants on their participation and on the content of this proposal.	☒
2) The information contained in this proposal is correct and complete.	☒
3) This proposal complies with ethical principles (including the highest standards of research integrity — as set out, for instance, in the European Code of Conduct for Research Integrity — and including, in particular, avoiding fabrication, falsification, plagiarism or other research misconduct).	☒

4) The coordinator confirms:

- to have carried out the self-check of the financial capacity of the organisation on https://ec.europa.eu/research/participants/portal4/desktop/en/organisations/lfv.html. Where the result was "weak" or "insufficient", the coordinator confirms being aware of the measures that may be imposed in accordance with the H2020 Grants Manual (Chapter on Financial capacity check); or	☒
- is exempt from the financial capacity check being a public body including international organisations, higher or secondary education establishment or a legal entity, whose viability is guaranteed by a Member State or associated country, as defined in the H2020 Grants Manual (Chapter on Financial capacity check); or	☐
- as sole participant in the proposal is exempt from the financial capacity check.	☐

5) The coordinator hereby declares that each applicant has confirmed:

- they are fully eligible in accordance with the criteria set out in the specific call for proposals; and	☒
- they have the financial and operational capacity to carry out the proposed action.	☒

The coordinator is only responsible for the correctness of the information relating to his/her own organisation. Each applicant remains responsible for the correctness of the information related to him and declared above. Where the proposal to be retained for EU funding, the coordinator and each beneficiary applicant will be required to present a formal declaration in this respect.

According to Article 131 of the Financial Regulation of 25 October 2012 on the financial rules applicable to the general budget of the Union (Official Journal L 298 of 26.10.2012, p. 1) and Article 145 of its Rules of Application (Official Journal L 362, 31.12.2012, p.1) applicants found guilty of misrepresentation may be subject to administrative and financial penalties under certain conditions.

Personal data protection

Your reply to the grant application will involve the recording and processing of personal data (such as your name, address and CV), which will be processed pursuant to Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. Unless indicated otherwise, your replies to the questions in this form and any personal data requested are required to assess your grant application in accordance with the specifications of the call for proposals and will be processed solely for that purpose. Details concerning the processing of your personal data are available on the privacy statement. Applicants may lodge a complaint about the processing of their personal data with the European Data Protection Supervisor at any time.

Your personal data may be registered in the Early Warning System (EWS) only or both in the EWS and Central Exclusion Database (CED) by the Accounting Officer of the Commission, should you be in one of the situations mentioned in:
-the Commission Decision 2008/969 of 16.12.2008 on the Early Warning System (for more information see the Privacy Statement), or
-the Commission Regulation 2008/1302 of 17.12.2008 on the Central Exclusion Database (for more information see the Privacy Statement) .

Proposal ID **653586** *Acronym* **SpeechXRays**

2 - Administrative data of participating organisations

PIC	***Legal name***
996570532	*OBERTHUR TECHNOLOGIES SA*

Short name: OT

Address of the organisation

Street RUE D ESTIENNE D ORVES 420

Town COLOMBES

Postcode 92700

Country France

Webpage www.oberthur.com

Legal Status of your organisation

Research and Innovation legal statuses

Public body .... no

Non-profit .... no

International organisation .... no

International organisation of European interest ...... no

Secondary or Higher education establishment .... no

Research organisation .... no

Small and Medium-sized Enterprises (SMEs) .... no

Legal person .... yes

Nace code 30 - Manufact. (office machinery & computers)

Department(s) carrying out the proposed work

Department 1

Department name	Technology & Innovation	
Street	RUE D ESTIENNE D ORVES 420	☒ Same as organisation address
Town	COLOMBES	
Postcode	92700	
Country	France	

Dependencies with other proposal participants

Character of dependence	***Participant***	

Person in charge of the proposal

The name and e-mail of contact persons are read-only in the administrative form, only additional details can be edited here. To give access rights and basic contact details of contact persons, please go back to Step 4 of the submission wizard and save the changes.

Title Mr. Sex ● Male ○ Female

First name **Xavier** Last name **Aubry**

E-Mail **euproject@zazventures.com**

Position in org. Consultant

Department *Please indicate the department of the Contact Point above in the organisation*

Street RUE D ESTIENNE D ORVES 420 ☒ Same as organisation address

Town COLOMBES Post code 92700

Country France

Website

Phone Phone 2 *+xxx xxxxxxxxx* Fax *+xxx xxxxxxxxx*

Other contact persons

First Name	***Last Name***	***E-mail***	***Phone***
Jean-Loup	Depinay	j.depinay@oberthur.com	

PIC	***Legal name***
936862279	*Horowitz Biometrics Limited*

Short name: HB

Address of the organisation

Street 364 a, high road

Town London

Postcode NW102EA

Country United Kingdom

Webpage

Legal Status of your organisation

Research and Innovation legal statuses

Public body .... no

Non-profit .... no

International organisation .... no

International organisation of European interest ...... no

Secondary or Higher education establishment .... no

Research organisation .... no

Small and Medium-sized Enterprises (SMEs) .... no

Legal person .... yes

Nace code

Department(s) carrying out the proposed work

Department 1

Department name	EU Projects
Street	364 a, high road
Town	London
Postcode	NW102EA
Country	United Kingdom

☒ Same as organisation address

Dependencies with other proposal participants

Character of dependence	***Participant***	

Proposal ID **653586** *Acronym* **SpeechXRays**

Person in charge of the proposal

The name and e-mail of contact persons are read-only in the administrative form, only additional details can be edited here. To give access rights and basic contact details of contact persons, please go back to Step 4 of the submission wizard and save the changes.

Title	Dr.	Sex	● Male ○ Female
First name	**David**	Last name	**Horowitz**
E-Mail	**drdavidmhorowitz@gmail.com**		
Position in org.	CTO		
Department	*Please indicate the department of the Contact Point above in the organisation*		
Street	364 a, high road	☒ Same as organisation address	
Town	London	Post code	NW102EA
Country	United Kingdom		
Website			
Phone		Phone 2	*+xxx xxxxxxxxx*
Fax	*+xxx xxxxxxxxx*		

Other contact persons

First Name	***Last Name***	***E-mail***	***Phone***
Hari Krishna	Maganti	maganti.harikrishna@gmail.com	

Proposal ID **653586** *Acronym* **SpeechXRays**

PIC	***Legal name***
997983337	*SIVECO ROMANIA SA*

Short name: SIV

Address of the organisation

Street	SOSEAUA BUCURESTI-PLOIESTI COMPLEX
Town	BUCURESTI
Postcode	013685
Country	Romania
Webpage	www.siveco.ro

Legal Status of your organisation

Research and Innovation legal statuses

Public body	no	Legal person	yes
Non-profit	no		
International organisation	no		
International organisation of European interest	no		
Secondary or Higher education establishment	no		
Research organisation	no		
Small and Medium-sized Enterprises (SMEs)	no		

Nace code 72 - Computer & related activities

Department(s) carrying out the proposed work

Department 1

Department name	European Projects
Street	SOSEAUA BUCURESTI-PLOIESTI COMPLEX VICT
Town	BUCURESTI
Postcode	013685
Country	Romania

☒ Same as organisation address

Dependencies with other proposal participants

Character of dependence	***Participant***	

Person in charge of the proposal

The name and e-mail of contact persons are read-only in the administrative form, only additional details can be edited here. To give access rights and basic contact details of contact persons, please go back to Step 4 of the submission wizard and save the changes.

Title: Dr.

Sex: ○ Male ● Female

First name: **Monica**

Last name: **Florea**

E-Mail: **monica.florea@siveco.ro**

Position in org.: Head of Unit European Projects

Department: European Projects

Street: SOSEAUA BUCURESTI-PLOIESTI COMPLEX VICTORIA PARK CORP CLA

☒ Same as organisation address

Town: BUCURESTI

Post code: 013685

Country: Romania

Website: www.siveco.ro

Phone: +40 730 055 784

Phone 2: +40 (021) 302 3300

Fax: +40 (021) 302 3391

Proposal ID **653586** *Acronym* **SpeechXRays**

PIC	***Legal name***
942469364	*TECH INSPIRE*

Short name: INSP

Address of the organisation

Street 15 Pragnell Road

Town London

Postcode SE12 0LF

Country United Kingdom

Webpage www.techinspire.co.uk

Legal Status of your organisation

Research and Innovation legal statuses

Public body	no	Legal person	yes
Non-profit	no		
International organisation	no		
International organisation of European interest	no		
Secondary or Higher education establishment	no		
Research organisation	no		
Small and Medium-sized Enterprises (SMEs)	yes		

Nace code 7110 -

Proposal ID **653586** *Acronym* **SpeechXRays**

Department(s) carrying out the proposed work

Department 1

Department name	Research Department
Street	15 Pragnell Road
Town	London
Postcode	SE12 0LF
Country	United Kingdom

☒ Same as organisation address

Dependencies with other proposal participants

Character of dependence	***Participant***	

Proposal ID **653586** *Acronym* **SpeechXRays**

Person in charge of the proposal

The name and e-mail of contact persons are read-only in the administrative form, only additional details can be edited here. To give access rights and basic contact details of contact persons, please go back to Step 4 of the submission wizard and save the changes.

Title: Dr.

Sex: ● Male ○ Female

First name: **Talal**

Last name: **Ous**

E-Mail: **talal.ous@techinspire.co.uk**

Position in org.: Research Director

Department: *Please indicate the department of the Contact Point above in the organisation*

Street: 15 Pragnell Road

☒ Same as organisation address

Town: London

Post code: SE12 0LF

Country: United Kingdom

Website:

Phone:

Phone 2: *+xxx xxxxxxxxx*

Fax: *+xxx xxxxxxxxx*

Other contact persons

First Name	***Last Name***	***E-mail***	***Phone***
Raj	Muttukrishnan	r.muttukrishnan@city.ac.uk	

Proposal ID **653586** *Acronym* **SpeechXRays**

PIC	**Legal name**
969630431	REALEYES OU

Short name: EYE

Address of the organisation

Street	VAHE 15
Town	TALLINN
Postcode	11615
Country	Estonia
Webpage	www.realeyesit.com

Legal Status of your organisation

Research and Innovation legal statuses

Public body	no	Legal person	yes
Non-profit	no		
International organisation	no		
International organisation of European interest	no		
Secondary or Higher education establishment	no		
Research organisation	no		
Small and Medium-sized Enterprises (SMEs)	no		

Nace code 72 - Computer & related activities

Proposal ID **653586** *Acronym* **SpeechXRays**

Department(s) carrying out the proposed work

Department 1

Department name	R&D	
Street	24 Tolgyfa utca	□ Same as organisation address
Town	Budapest	
Postcode	1027	
Country	Hungary	

Dependencies with other proposal participants

Character of dependence	***Participant***	

Person in charge of the proposal

The name and e-mail of contact persons are read-only in the administrative form, only additional details can be edited here. To give access rights and basic contact details of contact persons, please go back to Step 4 of the submission wizard and save the changes.

Title	Dr.		Sex	● Male	○ Female
First name	**Elnar**		Last name	**Hajiyev**	
E-Mail	**elnar@realeyesit.com**				
Position in org.	CTO				
Department	R&D				
Street	79 Wardour street		□ Same as organisation address		
Town	London		Post code	W1D 6QB	
Country	United Kingdom				
Website					
Phone		Phone 2	+xxx xxxxxxxxx	Fax	+xxx xxxxxxxxx

Proposal ID	**653586**	*Acronym*	**SpeechXRays**

PIC	***Legal name***
999924695	*Hellenic Telecommunications & Telematics Applications Company*

Short name: FNET

Address of the organisation

Street	Science & Technology Park of Crete, Vassilikia
Town	Heraklion
Postcode	71003
Country	Greece
Webpage	http://www.forthnet.gr

Legal Status of your organisation

Research and Innovation legal statuses

Public body	no	Legal person	yes
Non-profit	no		
International organisation	no		
International organisation of European interest	no		
Secondary or Higher education establishment	no		
Research organisation	no		
Small and Medium-sized Enterprises (SMEs)	no		

Nace code 61 -

Department(s) carrying out the proposed work

Department 1

Department name	Innovation department
Street	Science & Technology Park of Crete, Vass
Town	Heraklion
Postcode	71003
Country	Greece

☒ Same as organisation address

Dependencies with other proposal participants

Character of dependence	***Participant***	

Person in charge of the proposal

The name and e-mail of contact persons are read-only in the administrative form, only additional details can be edited here. To give access rights and basic contact details of contact persons, please go back to Step 4 of the submission wizard and save the changes.

Title	Mr.	Sex	● Male ○ Female
First name	**Manolis**	Last name	**Stratakis**
E-Mail	**mstra@forthnet.gr**		
Position in org.	Resarch Manager		
Department	*Please indicate the department of the Contact Point above in the organisation*		
Street	Science & Technology Park of Crete, Vassilikia Vouton, Innovation	☒	Same as organisation address
Town	Heraklion	Post code	71003
Country	Greece		
Website			
Phone		Phone 2	*+xxx xxxxxxxxx*
Fax	*+xxx xxxxxxxxx*		

Other contact persons

First Name	***Last Name***	***E-mail***	***Phone***
George	Vasilakis	gevas@forthnet.gr	

Proposal ID **653586** *Acronym* **SpeechXRays**

PIC	***Legal name***
999488777	*INSTITUTUL NATIONAL DE CERCETARE -DEZVOLTARE PENTRU FIZICA SI INGINERIE NUCLEA*

Short name: IFIN

Address of the organisation

Street	Atomistilor Street 407
Town	MAGURELE
Postcode	RO 077125
Country	Romania
Webpage	

Legal Status of your organisation

Research and Innovation legal statuses

Public body	yes	Legal person	yes
Non-profit	yes		
International organisation	no		
International organisation of European interest	no		
Secondary or Higher education establishment	no		
Research organisation	yes		
Small and Medium-sized Enterprises (SMEs)	no		

Nace code - Not applicable

Department(s) carrying out the proposed work

Department 1

Department name	Department of Computational Physics and Information Technologies
Street	Atomistilor Street 407
Town	MAGURELE
Postcode	RO 077125
Country	Romania

☒ Same as organisation address

Dependencies with other proposal participants

Character of dependence	***Participant***	

Proposal ID **653586** *Acronym* **SpeechXRays**

Person in charge of the proposal

The name and e-mail of contact persons are read-only in the administrative form, only additional details can be edited here. To give access rights and basic contact details of contact persons, please go back to Step 4 of the submission wizard and save the changes.

Title: Dr.

Sex: ● Male ○ Female

First name: **Alexandru**

Last name: **Nicolin**

E-Mail: **alexandru.nicolin@nipne.ro**

Position in org.: Scientific Researcher

Department: *Please indicate the department of the Contact Point above in the organisation*

Street: Atomistilor Street 407

☒ Same as organisation address

Town: MAGURELE

Post code: RO 077125

Country: Romania

Website:

Phone:

Phone 2: *+xxx xxxxxxxxx*

Fax: *+xxx xxxxxxxxx*

Other contact persons

First Name	***Last Name***	***E-mail***	***Phone***
Nicolae Victor	Zamfir	dirgen@nipne.ro	

Proposal ID	**653586**	*Acronym*	**SpeechXRays**

PIC	***Legal name***
999995893	*FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS*

Short name: FORTH

Address of the organisation

Street	N PLASTIRA STR 100
Town	HERAKLION
Postcode	70013
Country	Greece
Webpage	www.forth.gr

Legal Status of your organisation

Research and Innovation legal statuses

Public body	no	Legal person	yes
Non-profit	yes		
International organisation	no		
International organisation of European interest	no		
Secondary or Higher education establishment	no		
Research organisation	yes		
Small and Medium-sized Enterprises (SMEs)	no		

Nace code 721 -

Proposal ID **653586** *Acronym* **SpeechXRays**

Department(s) carrying out the proposed work

Department 1

Department name	Computational Medicine Laboratory
Street	N PLASTIRA STR 100
Town	HERAKLION
Postcode	70013
Country	Greece

☒ Same as organisation address

Dependencies with other proposal participants

Character of dependence	***Participant***	

Person in charge of the proposal

The name and e-mail of contact persons are read-only in the administrative form, only additional details can be edited here. To give access rights and basic contact details of contact persons, please go back to Step 4 of the submission wizard and save the changes.

Title: Dr.

Sex: ● Male ○ Female

First name: **Kostas**

Last name: **Marias**

E-Mail: **kmarias@ics.forth.gr**

Position in org.: Head

Department: Computational Medicine Laboratory

Street: N PLASTIRA STR 100

☒ Same as organisation address

Town: HERAKLION

Post code: 70013

Country: Greece

Website: http://www.ics.forth.gr/cml

Phone: +302810391672

Phone 2: +xxx xxxxxxxxx

Fax: +302810391428

Other contact persons

First Name	*Last Name*	*E-mail*	*Phone*
Margherita	Antona	antona@ics.foth.gr	+302810391743
Theano	Apostolidi	apost@ics.forth.gr	+302810391453
Emmanouil	Spanakis	spanakis@ics.forth.gr	+302810391446

Proposal ID **653586** *Acronym* **SpeechXRays**

PIC	***Legal name***
999975620	*UNIVERSITY COLLEGE LONDON*

Short name: UCL

Address of the organisation

Street GOWER STREET

Town LONDON

Postcode WC1E 6BT

Country United Kingdom

Webpage http://www.ucl.ac.uk

Legal Status of your organisation

Research and Innovation legal statuses

Public body ....yes

Legal person .... yes

Non-profit ....yes

International organisation ....no

International organisation of European interest ......no

Secondary or Higher education establishment ....yes

Research organisation ....yes

Small and Medium-sized Enterprises (SMEs) ....no

Nace code 853 -

Department(s) carrying out the proposed work

Department 1

Department name	Department of Electronics and Electrical Engineering	
Street	Torrington Place	□ Same as organisation address
Town	London	
Postcode	WC1E 7JE	
Country	United Kingdom	

Dependencies with other proposal participants

Character of dependence	***Participant***	

Person in charge of the proposal

The name and e-mail of contact persons are read-only in the administrative form, only additional details can be edited here. To give access rights and basic contact details of contact persons, please go back to Step 4 of the submission wizard and save the changes.

Title: Dr.

Sex: ● Male ○ Female

First name: **Clayton**

Last name: **Stewart**

E-Mail: **c.stewart@ee.ucl.ac.uk**

Position in org.: Senior Research Associate

Department: *Please indicate the department of the Contact Point above in the organisation*

Street: Torrington Place

□ Same as organisation address

Town: London

Post code: WC1E 7JE

Country: United Kingdom

Website:

Phone:

Phone 2: *+xxx xxxxxxxxx*

Fax: *+xxx xxxxxxxxx*

Proposal ID **653586** *Acronym* **SpeechXRays**

PIC	***Legal name***
999849326	*Institut Mines-Telecom*

Short name: TSP

Address of the organisation

Street RUE BARRAULT 46

Town PARIS 13

Postcode 75634

Country France

Webpage www.institut-telecom.fr

Legal Status of your organisation

Research and Innovation legal statuses

Public body ....yes

Non-profit ....yes

International organisation ....no

International organisation of European interest ......no

Secondary or Higher education establishment ....yes

Research organisation ....yes

Small and Medium-sized Enterprises (SMEs) ....no

Legal person .... yes

Nace code 853 -

Department(s) carrying out the proposed work

Department 1

Department name	Electronics and physics department	
Street	9, Rue Charles Fourier	□ Same as organisation address
Town	Evry Cedex	
Postcode	91011	
Country	France	

Dependencies with other proposal participants

Character of dependence	***Participant***	

Person in charge of the proposal

The name and e-mail of contact persons are read-only in the administrative form, only additional details can be edited here. To give access rights and basic contact details of contact persons, please go back to Step 4 of the submission wizard and save the changes.

Title: Dr.

Sex: ○ Male ● Female

First name: **Dijana**

Last name: **Petrovska**

E-Mail: **dijana.petrovska@telecom-sudparis.eu**

Position in org.: Associate Professor

Department: Electronics and physics department

Street: 9, Rue Charles Fourier

□ Same as organisation address

Town: Evry Cedex

Post code: 91011

Country: France

Website:

Phone:

Phone 2: +xxx xxxxxxxxx

Fax: +xxx xxxxxxxxx

3 - Budget for the proposal

Participant	Country	(A) Direct personnel costs/€ ?	(B) Other direct costs/€ ?	(C) Direct costs of sub-contracting/€ ?	(D) Direct costs of providing financial support to third parties/€ ?	(E) Costs of inkind contributions not used on the beneficiary's premises/€ ?	(F) Indirect Costs / € (=0.25(A+B-E)) ?	(G) Special unit costs covering direct & indirect costs / € ?	(H) Total estimated eligible costs / € (=A+B+C+D+F +G) ?	(I) Reimburse-ment rate (%) ?	(J) Max. grant / € (=H*I) ?	(K) Requested grant / € ?
OT	FR	868 400	44 000	0	0	0	228 100	0	1 140 500	70	798 350	798 350
HB	UK	868 000	39 000	0	0	0	226 750	0	1 133 750	70	793 625	793 625
SIV	RO	482 500	52 715	0	0	0	133 804	0	669 019	70	468 313	468 313
INSP	UK	380 250	50 500	0	0	0	107 688	0	538 438	70	376 907	376 907
EYE	EE	237 250	39 000	0	0	0	69 063	0	345 313	70	241 719	241 719
FNET	EL	178 750	36 000	0	0	0	53 688	0	268 438	70	187 907	187 907
IFIN	RO	87 750	23 000	0	0	0	27 688	0	138 438	100	138 438	138 438
FORTH	EL	222 000	21 000	0	0	0	60 750	0	303 750	100	303 750	303 750
UCL	UK	240 920	21 000	50 000	0	0	65 480	0	377 400	100	377 400	377 400
TSP	FR	311 850	21 000	0	0	0	83 213	0	416 063	100	416 063	416 063

Proposal ID **653586** *Acronym* **SpeechXRays**

Participant	Country	(A) Direct personnel costs/€	(B) Other direct costs/€	(C) Direct costs of sub-contracting/€	(D) Direct costs of providing financial support to third parties/€	(E) Costs of inkind contributions not used on the beneficiary's premises/€	(F) Indirect Costs / € (=0.25(A+B-E))	(G) Special unit costs covering direct & indirect costs / €	(H) Total estimated eligible costs / € (=A+B+C+D+F +G)	(I) Reimburse-ment rate (%)	(J) Max. grant / € (=H*I)	(K) Requested grant / €
		?	?	?	?	?	?	?	?	?	?	?
Total		3 877 670	347 215	50 000	0	0	1 056 224	0	5 331 109		4 102 472	4 102 472

Proposal ID **653586** *Acronym* **SpeechXRays**

4 - Ethics issues table

1. HUMAN EMBRYOS/FOETUSES		Page
Does your research involve Human Embryonic Stem Cells (hESCs)?	○ Yes ● No	
Does your research involve the use of human embryos?	○ Yes ● No	
Does your research involve the use of human foetal tissues / cells?	○ Yes ● No	
2. HUMANS		Page
Does your research involve human participants?	○ Yes ● No	
Does your research involve physical interventions on the study participants?	○ Yes ● No	
Does it involve invasive techniques?	○ Yes ● No	
3. HUMAN CELLS / TISSUES		Page
Does your research involve human cells or tissues (other than from Human Embryos/ Foetuses, i.e. section 1)?	○ Yes ● No	
4. PERSONAL DATA (ii)		Page
Does your research involve personal data collection and/or processing?	● Yes ○ No	21
Does it involve the collection and/or processing of sensitive personal data (e.g.: health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)?	○ Yes ● No	
Does it involve processing of genetic information?	○ Yes ● No	
Does it involve tracking or observation of participants?	○ Yes ● No	
Does your research involve further processing of previously collected personal data (secondary use)?	● Yes ○ No	21
5. ANIMALS (iii)		Page
Does your research involve animals?	○ Yes ● No	

Proposal ID **653586** *Acronym* **SpeechXRays**

6. THIRD COUNTRIES		Page
Does your research involve non-EU countries?	○ Yes ● No	
Do you plan to use local resources (e.g. animal and/or human tissue samples, genetic material, live animals, human remains, materials of historical value, endangered fauna or flora samples, etc.)? (v)	○ Yes ● No	
Do you plan to import any material from non-EU countries into the EU? *For data imports, please fill in also section 4.* *For imports concerning human cells or tissues, fill in also section 3.*	○ Yes ● No	
Do you plan to export any material from the EU to non-EU countries? *For data exports, please fill in also section 4.* *For exports concerning human cells or tissues, fill in also section 3.*	○ Yes ● No	
If your research involves low and/or lower middle income countries, are benefits-sharing measures foreseen? (vii)	○ Yes ● No	
Could the situation in the country put the individuals taking part in the research at risk?	○ Yes ● No	
7. ENVIRONMENT & HEALTH and SAFETY See legal references at the end of the section. (vi)		Page
Does your research involve the use of elements that may cause harm to the environment, to animals or plants? *For research involving animal experiments, please fill in also section 5.*	○ Yes ● No	
Does your research deal with endangered fauna and/or flora and/or protected areas?	○ Yes ● No	
Does your research involve the use of elements that may cause harm to humans, including research staff? *For research involving human participants, please fill in also section 2.*	○ Yes ● No	
8. DUAL USE (vii)		Page
Does your research have the potential for military applications?	○ Yes ● No	
9. MISUSE		Page
Does your research have the potential for malevolent/criminal/terrorist abuse?	○ Yes ● No	
10. OTHER ETHICS ISSUES		Page
Are there any other ethics issues that should be taken into consideration? Please specify	○ Yes ● No	

I confirm that I have taken into account all ethics issues described above and that, if any ethics issues apply, I will complete the ethics self-assessment and attach the required documents. ☒

SpeechXRays

Multi-channel biometrics combining acoustic and machine vision analysis of speech, lip movement and face

Innovation Action - H2020-DS-02-2014
Digital Security: Cybersecurity, Privacy and Trust - Topic: Access Control

List of participants

No	Acronym	Participant legal name	Type	Country
#1	OT	Oberthur Technologies	Industrial	France
#2	HB	Horowitz Biometrics	Industrial/SME	UK
#3	SIV	SIVECO	Industrial	Romania
#4	TEC	Tech Inspire	Industrial/SME	UK
#5	EYE	RealEyes OÜ	Industrial/SME	Estonia
#6	FNET	FORTHNET	Industrial	Greece
#7	IFIN	IFIN-HH	Research	Romania
#8	FORTH	Foundation for Research and Technology - Hellas	Research	Greece
#9	UCL	University College London	Academic	UK
#10	TSP	Institut Mines-Telecom / Telecom SudParis	Academic	France

Terminology and Abbreviations

To aid readability, we have we have followed a policy of providing an expansion of acronyms at many places in the body of the text. But there is a small set of key terms & concepts that are central to the understanding of the project. We provide an explanation of these here, for the benefit of readers who may be unfamiliar with them.

Term/abbreviation	Explanation
FAR (False Acceptance Rate)	The FAR is the probability that the system incorrectly matches the input pattern to a non-matching template in the database (random imposture). A low FAR will increase the level of security of the authentication mechanism.
FRR (False Rejection Rate)	The FRR is the probability that the system fails to detect a match between the input pattern and a matching template in the database. A low FRR will increase the convenience of the authentication mechanism (reducing authentication attempts).
ROC (Receiver Operating Characteristic)	The ROC plot is a visual characterization of the trade-off between the FAR and the FRR. The matching algorithm performs a decision based on a threshold which determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be fewer false non-matches but more false accepts. Conversely, a higher threshold will reduce the FAR but increase the FRR. This means that the FAR/FRR trade-off can be modified for a given system.
EER (Equal Error Rate)	The EER is the rate at which both acceptance and rejection errors are equal, as obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves (better systems have lower EERs)

Table of contents

1. Excellence

1.1 Objectives

The SpeechXRays project will **develop** and **test** in real-life environments a user recognition platform based on voice acoustics analysis and audio-visual identity verification. SpeechXRays will **outperform** state-of-the-art solutions in the following areas:

- **Security**: high accuracy solution (cross over accuracy[1] of 1/100 i.e. twice the commercial voice/face solutions)
- **Privacy**: biometric data stored in the device (or in a private cloud under the responsibility of the data subject)
- **Usability**: text-independent speaker identification (no pass phrase), low sensitivity to surrounding noise
- **Cost-efficiency:** use of standard embedded microphone and cameras (smartphones, laptops)

There are several biometric modalities that may be used for access control purposes. Low cost solutions based on existing embedded sensors (camera-based face recognition) are now provided as standard features of laptops and smartphones but their accuracy is low.

New sensors (fingerprint readers) can be embedded in laptops and smartphones, however they generate additional costs (as they are only used for identification purposes). Iris recognition is a promising technology as it is extremely accurate and is not sensitive to ageing, however it is not easily applicable to mobile devices (all publicly deployed iris recognition systems acquire images of an iris in the near infrared wavelength band of the electromagnetic spectrum and cannot use standard cameras). Worse, all these systems (fingerprint, face, and iris) can be spoofed by fake biometrics as simple as high resolution colour printouts[2].

The most convenient and cost-effective biometric modality is voice, which can be easily captured on a mobile device using its embedded microphone. Voice is noise robust to the human ear. However, today's commercial solutions in voice biometrics fail to deliver the required accuracy levels and are very sensitive to ambient noise, because they rely mostly on machine learning techniques employing statistical analysis and, unlike the human ear, do not consider the acoustic correlates of voice quality. At the 2014 NIST i-vector challenge, the best system performance had a cross-over accuracy of 3%[3], which is not sufficient enough to warrant market adoption.

In order to overcome these limitations, the project will combine and pilot two proven techniques: acoustic driven voice recognition (using acoustic rather than statistical only models) and multi-channel biometrics incorporating dynamic face recognition (machine vision analysis of speech, lip movement and face).

	Accuracy	Spoofing	Convenience	Cost	Sensor size
Fingerprint (capacitive)	4	3	**5**	4	**5**
Fingerprint (optical)	**5**	4	**5**	4	4
Voice	1	3	**5**	**5**	**5**
Face	2	2	3	4	3
Hand	3	4	3	2	2
Iris	**5**	3	2	3	3
SpeechXRays	**5**	**5**	**5**	**5**	**5**

Table 1: Performance comparison of various biometric solutions[4]

[1] The crossover accuracy (also called equal error rate or EER) is the rate at which both acceptance and rejection errors are equal. In currently available commercial system, it is typically around 1/50 for voice recognition, 1/500 for fingerprint recognition and 1/100,000 for iris scan recognition.

[2] Pradnya M. Shende et al (2014). A Survey Based on Fingerprint, Face and Iris Biometric Recognition System, Image Quality Assessment and Fake Biometric. Int. Journal of Computer Science Engineering and Technology (IJCSET) Vol 4, Issue 4,129-132

[3] Greenberg C. S et al., (2014), The NIST 2014 Speaker Recognition i-Vector Machine Learning Challenge, Odyssey 2014, The speaker and language recognition workshop, June 2014, Finland

[4] Data compiled from the evaluation of available commercial systems, on a scale 1 to 5 (5 is the lowest cost and highest accuracy whereas 1 is the highest cost and lowest accuracy). Not that iris recognition accuracy is of an order of magnitude superior to fingerprint recognition, however both are scored at 5 in this table for simplification purposes.

In short, the ambition of the SpeechXRays project is to provide a solution combining the convenience and cost-effectiveness of voice biometrics, achieving better accuracies by combining it with video, and bringing superior anti-spoofing capabilities.

The project's objectives have been structured in 4 key areas (Table 2).

<table>
<tr><td colspan="3"><b>Objective 1: Develop and test a cost effective, convenient, privacy preserving multimodal biometrics solution based on acoustic and machine vision analysis of speech, lip movement and face</b></td></tr>
<tr><td><b>1.1</b></td><td>Acoustic driven voice analysis</td><td>Combine acoustic analysis of the speech spectrogram with classical statistical analysis of the soundwave patterns.</td></tr>
<tr><td><b>1.2</b></td><td>Audio-visual identification</td><td>Combine several biometric modalities: speech, face and synchrony between speech and lips movements</td></tr>
<tr><td colspan="3"><b>Objective 2: Implement the novel biometrics solution in a broadband network, giving access to smart services running over networks with state-of-the-art security, avoiding single points of failure</b></td></tr>
<tr><td><b>2.1</b></td><td>Corporate use case</td><td>Demonstrate a secure information sharing network for corporate users requiring a high level of security, based on the requirement of IFIN-HH[5]</td></tr>
<tr><td><b>2.2</b></td><td>eHealth use case</td><td>Apply the solution to the requirement of hospitals providing telemedicine services, based on the requirement of Greek hospitals recruited by FORTH</td></tr>
<tr><td><b>2.3</b></td><td>Consumer use case</td><td>Apply the solution to the requirement of consumers, based on the requirement of user groups recruited by FNET and OT</td></tr>
<tr><td colspan="3"><b>Objective 3: Guarantee interoperability and portability between systems and services</b></td></tr>
<tr><td><b>3.1</b></td><td>Text-independency</td><td>Compare both text dependent (based on statistical models) and text independent (based on acoustic analysis) solutions.</td></tr>
<tr><td><b>3.2</b></td><td>Device- and network independency</td><td>Develop the client-side implementation of the solution using cross-platform technologies such as HTML5 and network-independent protocols such as SOAP or REST.</td></tr>
<tr><td><b>3.3</b></td><td>Standard compatibility</td><td>Apply existing standards such as ISO/IEC 19784-1 (BioAPI), NIST SP500-288 (WS-BD protocol) and OASIS BIAS SOAP Profile to audio-visual identification</td></tr>
<tr><td colspan="3"><b>Objective 4: Develop a vibrant application and service ecosystem</b></td></tr>
<tr><td><b>4.1</b></td><td>User community</td><td>Stimulate the uptake of the solution by internet and telecom service providers by delivering high quality dissemination and training material, and organizing dedicated workshops</td></tr>
<tr><td><b>4.2</b></td><td>Developer community</td><td>Stimulate the uptake of the solution by application developers by delivering a high quality development SDK, and organizing application development contests</td></tr>
<tr><td><b>4.3</b></td><td>Hacking contest</td><td>Establish credibility by challenging the developer community to try to hack or spoof the solution</td></tr>
</table>

Table 2: Project specific objectives

Table 3 present the project key performance indicators (KPIs) supporting the project objectives, that will be assessed at 3 different points in time: M12 (start of the demonstrators), M24 (at mid-point of the demonstrators) and M36 (end of project).

[5] IFIN-HH, the Romanian Institute of Physics and Nuclear Engineering, handles sensitive research data related to nuclear physics and is engaged in strategic science on behalf of national security.

Objectives				Project KPI	M12	M24	M36	WPs
1	2	3	4					
X				False Reject Rate	10%	5%	2%	WP2
X				False Acceptance Rate[6]	5%	2%	0.5%	WP2
X				Equal Error Rate (cross over accuracy)	1/50	1/75	1/100	WP2
X	X			Sensitivity to surrounding noise	medium	low	low	WP2 WP4
X	X			Sensitivity to individual variations (sickness, ageing, stress)	medium	low	low	WP2 WP4
X			X	Resistance to spoofing	partial	high	high	WP2 WP3
X			X	User convenience[7] (scale 1-5)	3	4	5	WP4 WP6
X			X	Compliance with Data Protection Directive (Directive 95/46/EC)	partial	full	full	WP4
		X		Demonstration of cross-platform compatibility	Android	Android +iOS	Android +iOS +Win8	WP2 WP5
		X		Demonstration of standard compatibility	ISO/IEC 19784-	OASIS BIAS SOAP Profile	NIST SP500-288	WP5 WP9
	X		X	Number of pilot users	50	500	2000	WP6
			X	Number of developers in the ecosystem	0	5	20	WP7
			X	Number of pilot service providers	1	2	5	WP8

Table 3: Project output indicators in relation to project timeline

1.2 Relation to the Work Programme

Table 4 describes how the project contributes to the DS-02 topics and the Secure Societies Work Programme.

DS-02 Topic	Contribution of the Project
The focus is on the development and testing of usable, economic and privacy preserving access control platforms based on the use of biometrics, smart cards, or other devices	The project is focusing on the use of multi-channel biometrics for access control purpose. The choice of audio-visual analysis to perform identity verification can deliver high usability and low cost (based on the use of standard cameras embedded in smartphones, tablets and laptops).
The solutions are to be installed and tested in a broad-band network, giving access to smart services running over networks with state-of-the-art security, avoiding single points of failure	The project will test the solution in 3 real-life use cases requiring various degrees of security: consumer use case (low security), eHealth use case (medium security) and workforce use case (high security). All scenarios will demonstrate an authentication over a secure broadband network giving access to specific services.

[6] Assuming random impostures and not spoofing attempts

[7] Measured by surveying the pilot end-users before, during and after the pilot, taking in account easiness of use, the identification speed and overall user experience

Proposed work should include the management of the access rights in particular for the service providers, ensure the security and privacy of the databases, facilitate a timely breach notification and remediation to the user, and reduce the insider threat.	The project will implement privacy-preserving mechanisms in order to protect the biometric templates, which will be stored encrypted in the mobile device. The solution will include the possibility to revocate biometric templates when spoofing attempts are detected. The solution will also recognize user emotions such as fear (to prevent authentication under duress).
The proposed solutions have to guarantee interoperability and portability between systems and services, sparing the user to have to install a platform, service or country specific technology.	The solution will follow a hybrid architecture combining a native container (for local encrypted of the biometric template) and HTML5 user interfaces (for greater cross-portability across operating systems). The native container can be downloaded from a public app store and will not require any other software installation. The voice biometrics component will be text-independent and therefore language-agnostic.
Proposed work could assist the objective of implementing a secure information sharing network.	The project will implement a secure information network in two of the three use cases: in the workforce scenario, IFIN-HH staff performing research in sensitive fields of research (e.g. nuclear physics) will use the biometrics solution to access a secure information repository; in the eHealth scenario, patients affected by osteoarthritis and medical specialists will be able to interact via a secure collaborative eHealth space.

Secure Societies Work Programme	**Contribution of the Project**
The call will focus on demonstrating the viability and maturity of state-of-the-art security, privacy and trust solutions that have been tested in a laboratory environment. The intention is that after this validation phase they will find a wide up take in the market.	The project takes biometrics modalities (acoustics-driven voice biometrics, audio-visual analysis, privacy frameworks) that have been tested in the lab, and combine them in a robust, low cost, user friendly multi-channel biometrics solution. The biometrics modalities have been chosen for their low cost and high market acceptance potential.
Proving that the security concepts, processes and solutions work in a real life environment, in large scale demonstrators and directly involving end users who would ultimately benefit the most from the outcome, should increase the prospects for an ICT security market and demonstrate the validity and effectiveness of security.	The solution will be validated by industrial partners in large-scale (2000+) real life use cases in order to prepare a solution market launch after the end of the project. The project will demonstrate high accuracy solution (cross over accuracy of 1/100 or more, i.e. twice the commercial voice/face solution)
This call addresses the technology to secure the infrastructure (e.g. networks), hardware (e.g. access devices), services (e.g. cloud computing), components (e.g. RFID), software (e.g. operating systems, web-browsers), etc… against accidental or malevolent use.	The technology developed in the project is versatile and can be used to provide secure access to networks as well as physical locations (the workforce use case will include a physical access control demonstration). The technology is designed to be portable across a wide range of operating systems: the portability will be demonstrated on iOS, Android and Windows.
As cybersecurity is cross-domain the call will provide cybersecurity whatever the application or domain (mobile, eCommerce…), or societal challenge (e.g. health, energy, smart cities …).	The use case scenarios have been selected to cover a wide range of societal challenges: consumer use case (ICT/networks), eHealth use case (health), workforce use case (energy research)

Table 4: Project relation to the Work Programme topic

1.3Concept and approach

1.3.1 Overall concept

The SpeechXRays project applies biometric processes (Figure 1) to audio-visual information captured from the user, as follows:

- Enrolment: audio-visual biometric information from an individual is captured, processed and stored as a biometric template. In subsequent uses, biometric information is captured and compared with the biometric template. SpeechXRays enables convenient enrolment via a smartphone, tablet or laptop equipped with a standard camera.
- Biometric verification mode: one-to-one comparison of the captured biometric sample with a stored biometric template (or model) to verify that the individual is who he claims to be. The result of verification is a yes / no response. SpeechXRays enables robust speaker verification capabilities based on audio-visual information analysis. The generic term of recognition (meaning verification or identification[8]) is also used in this document.
- Authentication: in addition to verifying the identity of a person based on his credentials (such as biometrics or password based), a secure session is opened between the two parties (generally a client and a server). SpeechXRays enables the authentication of a user via a smartphone, tablet or laptop equipped with a standard camera, in order to access specific resources over a wireless broadband network.
- Revocation: ability to cancel specific credentials. SpeechXRays can remediate security issues such as template leakage, spoofing attempts, etc. by cancelling credentials that are deemed at risk.

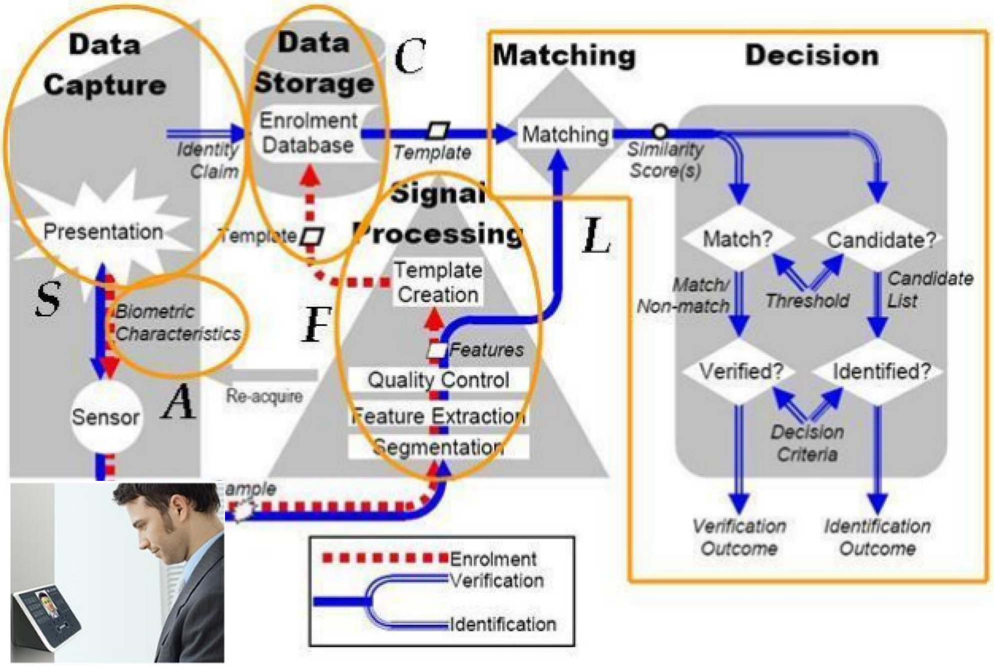


Figure 1: Biometrics Processes

The consortium created for this 36 month project assembles inter-disciplinary skills from 5 industrial/SME partners and 4 research/academic organizations. Please refer to section 3.3 for the consortium as whole and section 4 for partner descriptions.

[8] The biometric identification mode is a one-to-many comparison of the captured biometric sample against a biometric database in an attempt to identify an unknown individual. The result of identification in the closed-set scenario the identity of a user; in an open-set identification scenario the result is either the most probable identity of the identification set, or an probable identity outside this set. SpeechXRays is not focusing on speaker identification, although the technology could be used for law enforcement purposes as part of the (post-project) exploitation activities.

1.3.2 Main project results in relation to Technology Readiness Levels

The project addresses the so-called "implementation gap" (Table 5) between research projects (TRL 1-4) and industrial applications (TRL 9). This bridge requires new styles of consortiums with a strong focus on applied interdisciplinary research, industry-driven requirement (pull) and knowledge/technology transfer.

The results are categorized in 5 main groups:

- A set of algorithms/methods for voice analysis, face analysis and audio-visual analysis
- A security and privacy framework applied to voice/face biometrics
- An end-to-end speaker verification solution, including enrolment, authentication, revocation
- A set of applications implemented in 3 real-life scenarios
- A development environment allowing third party developers to build new applications and service on top of the end to end speaker verification solution (and the related developer ecosystem)

Technical results in relation to the TRLs	Project start	Project end
Voice analysis (acoustic-driven) algorithms	5	8
Face analysis algorithms	6	8
Audio-visual analysis (lip movement) algorithms	5	8
Security framework	7	8
Privacy framework	6	8
End-to-end biometrics solution (including applications and development environment)	5	8

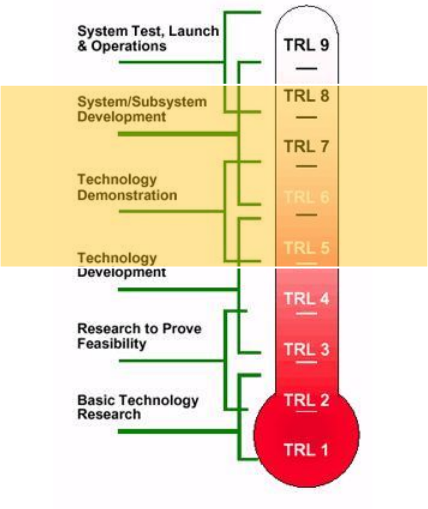

System Test, Launch & Operations
System/Subsystem Development
Technology Demonstration
Technology Development
Research to Prove Feasibility
Basic Technology Research
TRL 9
TRL 8
TRL 7
TRL 6
TRL 5
TRL 4
TRL 3
TRL 2
TRL 1

Table 5: Project focus in relation to Technology Readiness Levels (TRLs)

1.3.3 Linked research & innovation activities

Listed below are national and international research projects where there are already concrete opportunities for synergy, or adoption of project results, because of existing contacts from the consortium.

- BEAT is a Collaborative Project under FP7-SEC (2012-2014) that aims to propose a framework of standard operational evaluations for biometric technologies. This will be achieved by (1) developing an online and open platform to transparently and independently evaluate biometric systems against validated benchmarks, (2) designing protocols and tools for vulnerability analysis, and (3) developing standardization documents for Common Criteria evaluations. **TSP will interface with the BEAT project so the BEAT framework can be used to assess the standard operational characteristics of the SpeechXRays solution.** TSP will combine the achievements of the BioSecure NoE (listed below) with the BEAT and other EU projects. This will allow to re-use already developed and funded work.
- SIIP is a Collaborative Project under FP7-SEC (2014-2018) that aims to develop a break-through Suspect Identification (SI) solution based on a novel SI engine fusing multiple speech analytic algorithms (e.g. voiceprints recognition, Gender/Age/Language/Accent ID, Keyword/ Taxonomy spotting and Voice cloning detection). This Fused Speaker Identification will result in significantly higher true-positive speaker identification, reduced False-Positives/Negatives while increasing reliability and confidence. **HB will interface with the SIIP project in order to understand which of the speech analytic algorithms could be used (if any) in the SpeechXRays project.**
- Tabularasa was a Collaborative Project under FP7-ICT (2010-2013) analysing the effectiveness of direct attacks to a range of biometrics, thus providing an insight as to how vulnerable the different biometric traits are to these attacks. The first line of work proposed to combine multiple biometric traits to build a single

system that is robust to direct attacks and the second line of work proposed to examine novel methods to perform aliveness detection. Finally, novel biometrics which might be inherently robust to direct attacks, such as gait (the manner in which someone walks), vein or electro-physiological signals (such as the heart beat) were explored to determine their advantages and limitations. **HB and TSP will review the output of the Tabularasa project in order to improve the resistance of the SpeechXRays solution to spoofing.**

- MOBIO was a Collaborative Project under FP7-ICT (2008-2010) that aimed to study, develop and evaluate bi-modal (face and voice) biometric technologies in the context of portable and networked devices. The project carried out research on joint bi-modal biometry under various realistic conditions and investigated the following technologies: robust face localisation and speech segmentation in noisy environments, video-based face authentication (in order to avoid replay attacks using pictures of the face we should perform face authentication over the video), speaker authentication, bi-modal authentication (both expert fusion and joint face/speaker authentication to take full advantage of the correlation between modalities) and unsupervised model adaptation thought time. **TSP has already worked with the MOBIO database and protocols, and will evaluate the project speech and face algorithms on this database.** For example, TSP participated to the ICB-2013 speaker challenge on the MOBIO data and obtained the best results with a single system on female speech data.
- BioSecure was a Network of Excellence **led by TSP** under FP6 (2004-2007) providing the biometric R&D community with resources such as evaluation platforms including databases, reference systems (baseline algorithms), assessment protocols for 8 well-established modalities (fingerprints, iris, dynamic signature, hand shape, speech, 2D face, 3D face, and talking faces), educational material (repository of texts and presentations related to different assets of biometrics) and handbook on standards and a guide to biometric reference systems and performance evaluation[9]. **TSP will re-use the NoE resources** as part of the dissemination activities of WP7, in order to stimulate the SpeechXRays ecosystem development.
- SecurePhone was a Collaborative Project under FP6-IST (2002-2004) developing a new mobile communication system (the “SecurePhone”) enabling biometrically authenticated users to deal m-contracts during a mobile phone call in an easy yet highly dependable and secure way. SecurePhone’s biometric recogniser was based on an original combination of non-intrusive, psychologically-neutral biometric methods such as audio-visual and handwritten signature identification techniques. **TSP was a partner** in Securephone and will share the lessons learned from this early project.

More projects (currently about to start but not public yet) will be identified as part of the WP7 activities.

1.3.4 Methodology

The project will take a new scientific approach to voice biometrics by applying the scientific basis of human voice physiology, which produces precise acoustic cues of perceptual salience unique to each individual speaker. The precise vocal tract physiology is directly derived from the feature analysis of the speech spectrogram. The scientific basis that is the foundation of this project is based upon the modelling techniques of human voice quality and characteristics that emulate the manner in which the human auditory system identifies a speaker’s voice. The project will model these acoustic cues of the voice physiology and detects them in the first pass of a speaker (voice) authentication system in a deterministic discrete time signal processing architecture.

In addition, multi-channel biometrics will further enhance the system’s performance. Just like the human being uses all of his or her senses in combination to identify an individual, the project uses multi-channel biometrics to improve the accuracy of human identity performance. The solution will combine voice acoustic analysis with dynamic face recognition (including lip movement and facial analysis)

The technology will be combined into a solution capable of running the speaker recognition process

- either locally on the device (cancellable biometric template created by binding keys with biometric data and securely stored on the device for example on the SIM card)
- or remotely, via a secure cloud connection (cancellable biometric template securely stored on a private cloud under the responsibility of the data subject and not on the service provider’s servers)

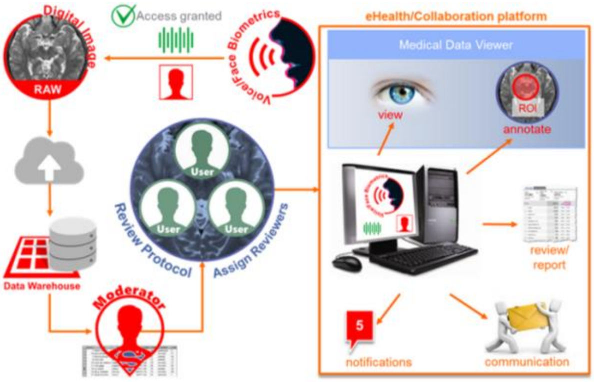
The technology will be piloted in 3 real-life use case scenarios on 2000 users (Table 6

[9] Guide to Biometric Reference Systems and Performance Evaluation; Publisher Springer-Verlag, London, p. 1-394, 2009.

<table>
<tr><th colspan="2">Workforce Pilot</th></tr>
<tr><td>Location</td><td>Horia Hulubei National Institute of Physics and Nuclear Engineering, Bucharest, Romania (IFIN)</td></tr>
<tr><td>Users</td><td><b>689</b> researchers and Ph.D. students</td></tr>
<tr><td>Description</td><td>Scientists working on sensitive nuclear research projects will be able to access the secure information repository of the institute via remote biometrics-based identification through their mobile device. In addition, physical access to the research facility will be tested using the same biometrics-based identification.

The multi-channel biometrics system will be implemented on mobile devices (such as smartphones, tablets and laptops) used to access sensitive data over 3G/4G and WLAN and on-site, on the premises of IFIN-HH, at an access point to one of the data centres. All mobile equipment used for authentication will first be tested for compatibility with the access system (e.g. sufficient quality of sound and video recordings) and all approved equipment will be registered on the access platform. Repeated inconclusive biometrics results the platform will have a user-blocking mechanism.

The on-site access system will implement most of the features of its mobile sibling plus an additional set of protection measures. These extra security measures are enforced to ensure the physical protection of the hardware infrastructure of IFIN-HH and rely on consolidating the above biometrics information with data obtained from the proximity cards (needed to enter the premises of IFIN-HH and each separate building), the perimetral video surveillance system (which can signal, for instance, unusual activities outside the standard working hours), and the Romanian Gendarmerie Detachment which monitors the compound. For repeated negative and/or inconclusive biometrics results the access system should be able to send warning the Gendarmerie Detachment and lock-down the building where the fraudulent entry was forced (e.g., by automatically cancelling the proximity card of the user and blocking all doors). Similarly, in case of hardware failures of the perimetral video surveillance system and that of the proximity cards, both of them constantly monitored by the Gendarmerie Detachment located in the compound, the on-site access system should be automatically/manually blocked.</td></tr>
<tr><td>Focus</td><td>This scenario will test the level of security, threat remediation and adaptability of the solution to various application (online access, physical perimeter access)</td></tr>
<tr><th colspan="2">e-Health Pilot</th></tr>
<tr><td>Location</td><td>3 Greek hospitals working with FORTH and their patients</td></tr>
<tr><td>Users</td><td><b>400</b> medical specialist and patients</td></tr>
<tr><td>Description</td><td>Patients and doctors will use the remote biometrics solution to access a collaboration platform developed by FORTH to support the prevention and management of a chronic condition (osteoarthritis). Patients will be able to remotely and securely report health data such as activity level, pain, etc. while general practitioners and specialists will be able to access the patient journals for decision-support.



Digital Image
RAW
Access granted
Voice/Face Biometrics
eHealth/Collaboration platform
Medical Data Viewer
view
ROI
annotate
User
User
User
Review Protocol
Assign Reviewers
Data Warehouse
Moderator
review/ report
5
notifications
communication

Osteoarthritis is a disabling degenerative joint disease leading to joint pain, stiffness and loss of function predominantly in the knees, hips, hands, and spine that can partially overcome by losing weight and by exercising. Many of the patients have reduced mobility and may live in remote rural areas in Greece. Therefore, they need to exchange remotely information about their health</td></tr>
</table>

	status and level of physical activity, in order for their general practitioner to provide a personalized chronic disease management program. Osteoarthritis management requires interactive multi-scale visualization of heterogeneous data (medical imaging such as MRI/CT scans, physical reports) where different experts visualize the complete data as an ensemble and to navigate between the individual datasets, changing spatial and temporal scale as required, and provide feedback and consultation. Therefore, various medical experts need to access sensitive patient data on their own devices (laptop or tablet).
Focus	This scenario will test the security, privacy, usability and cost-effective features of the security platform. In particular, the scenario will test the context-dependent feature that allows administrators to modify the FAR/FRR trade-off in order to reduce the risk of false reject for low security data (e.g. physical examination) and reduce the risk of false accept for high security data (e.g. MRI/CT scans).
e-Health Pilot	
Location	A triple play internet service provider (FNET) serving customers all around Greece
Users	**1000** customers of FNET
Description	Customers will be able to access e-billing information, user profiling information, user accounts using an authorization service based on remote biometrics-based identification through a secure cloud connection. User of this trial scenario is to demonstrate the use of system in a consumer environment. Such an environment is typically very demanding since it involves interaction with users that are not accustomed to the provided interface while at the same time it provides a very good indication of the system's usability in a real world setting. forthnet In this particular scenario the user verification system developed in the project will be used to enhance the user experience of FNET's customers, while accessing information and services offered by the company. Such services may involve e-billing information, user profiling information, access to the user's account, etc. Users from a selected consumer base, instead of following the typical access control procedure, will be able to use an authorization service based on remote biometrics-based identification through a secure cloud connection. The motivation for using a biometrics-based user identification system in this scenario is twofold: • To provide access control to restricted information through a natural and unobtrusive way. As with other biometric-based approaches, SpeechXRays verification may replace or augment PINs and passwords with something that cannot be forgotten lost or stolen. • To improve user experience by personalizing each user session. Most of FNET's triple play solutions target consumer households (broadband internet based on ADSL technology and PayTV services mainly SAT but OTT as well). The authentication of such services is performed at the router and STB level and not at the individual one. Part of the company's strategic planning involves developing the infrastructure to enable it to target the individual members of each household that use its services. The goal is to be able to provide recommendations and suggestions based on an individual's habits, behaviour, and lifestyle or automatically adjust the interaction device (Web interface, set-top-box, mobile phone) to the user's unique preferences (e.g. enforcing parental control settings).
Focus	This scenario will test ease of use, performance, security and the ability to target the actual user(s) of FNET services. While security is typically the primary consideration when incorporating user recognition technology, in this particular scenario security is necessary but is not as crucial as convenience or ease of use.

Table 6: SpeechXRays pilots

1.3.5 Sex/gender analysis

Base on the biometric technology used in the project (face and voice analysis), the consortium has not identified any sex/gender-related issues related to the type of activities to be carried out, the resulting technology and its potential applications. However, in carrying out the project activities, the consortium will promote gender equality. The project is committed to the strategy of European Commission for equal promotion of women and men.

The SpeechXRays project addresses the cybersecurity sector where the low percentage of women in boardroom or leading positions has been identified as problematic in both academia and industry. The consortium pledges to follow the European strategy for gender equality for getting more women into the labour market and into high decision-making positions.

Specifically, the consortium will include women as technology end-users in leading positions in the demonstrators, as scientists involved in leading research and as prominent speakers actively involved in project dissemination (for example Dijana Petrovska as leading anti-spoofing expert).

Finally, women and men differ in their needs for and experience with technology. Therefore, it is important to include both women and men in technology considerations. Analysing sex and gender as well as including both female and male users in technology development is a planned action of this project that can lead to better designs and improved marketability of SpeechXRays solutions.

1.4 Ambition

Speaker or voice recognition is a biometric modality that uses an individual’s voice for recognition purposes. It is a different technology than “speech recognition”, which recognizes words as they are articulated. The speaker recognition process relies on features influenced by both the physical structure of an individual’s vocal tract and the behavioural characteristics of the individual.

A popular choice for remote authentication due to the availability of devices for collecting speech samples (e.g., telephone network and computer microphones) and its ease of integration, speaker recognition is different from some other biometric methods in that speech samples are captured dynamically or over a period of time, such as a few seconds. Analysis occurs on a model in which changes over time are monitored, which is similar to other behavioural biometrics such as dynamic signature, gait, and keystroke recognition.

Speaker recognition has co-evolved with the technologies of speech recognition and speech synthesis because of the similar characteristics and challenges associated with each. In 1960, Gunnar Fant published a model[10] describing the physiological components of acoustic speech production, based on the analysis of x-rays of individuals making specified phonic sounds (which incidentally provided the inspiration for the project name). In 1969, Dr. Joseph Perkell used motion x-rays[11] and included the tongue and jaw to expand upon the Fant model.

Original speaker recognition systems used the average output of several analogue filters to perform matching, often with the aid of humans “in the loop”. In 1976, Texas Instruments built a prototype system[12] that was tested by the U.S. Air Force and The MITRE Corporation. In the mid-1980s, the National Institute of Standards and Technology (NIST) developed the NIST Speech Group to study and promote the use of speech processing techniques.

Advances in voice biometrics, face biometrics and audio-visual (lip movement) analysis are now making it possible to use a combination of voice and face analysis for speaker recognition purposes, especially as high performance microphones and cameras are nowadays available on commercial smartphones, tablets and personal computers.

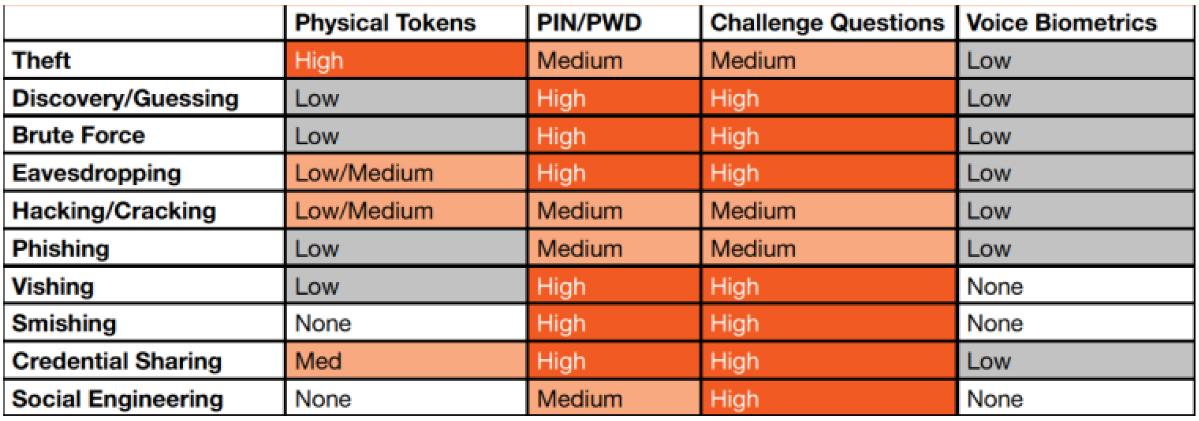
The SpeechXRays project will develop and test a platform based on voice acoustics analysis and audio-visual identity verification. SpeechXRays will outperform state-of-the-art solutions in the following areas:

[10] Fant, Gunnar. *Acoustic theory of speech production: with calculations based on X-ray studies of Russian articulations*. Vol. 2. Walter de Gruyter, 1971.

[11] Perkell, J. S. (1969). *Physiology of speech production: Results and implications of a quantitative cineradiographic study* (No. 53). MIT Press.

[12] Haberman, W., & Fejfar, A. (1976, May). Automatic identification of personnel through speaker and signature verification—system description and testing. In*Proc. 1976 Carnahan Conf. on Crime Countermeasures* (pp. 23-30).

- Security: high accuracy solution (cross over accuracy of 1/100 or better), lower vulnerability to fraud than other methods based on physical tokens, PIN/password or challenge question (Table 7).
- Privacy: biometric data securely stored in the device (or in a private cloud under the responsibility of the data subject)
- Usability: text-independent speaker identification (no pass phrase), low sensitivity to surrounding noise
- Cost-efficiency: use of standard embedded microphone and cameras (smartphones, laptops)



	Physical Tokens	PIN/PWD	Challenge Questions	Voice Biometrics
Theft	High	Medium	Medium	Low
Discovery/Guessing	Low	High	High	Low
Brute Force	Low	High	High	Low
Eavesdropping	Low/Medium	High	High	Low
Hacking/Cracking	Low/Medium	Medium	Medium	Low
Phishing	Low	Medium	Medium	Low
Vishing	Low	High	High	None
Smishing	None	High	High	None
Credential Sharing	Med	High	High	Low
Social Engineering	None	Medium	High	None

Table 7: Vulnerability to fraud of various security methods

1.4.1 Competitive and patent landscape

The consortium analysed 59 patents related to speaker recognition technologies. The most relevant patents are listed in Table 8.

The analysis is used to determine the “freedom to operate” (i.e. avoiding developing technologies or methods which are already protected) and to map the competitive landscape (i.e. refining the exploitation strategy of the project by identifying possible competitors or partners).

Not surprisingly, the patent landscape is dominated by major companies such as AT & T, Google, Apple, Blackberry, MasterCard, etc., A few emerging players such as Speechpro and Auraya have developed specific patents related to voice biometrics. The patents listed in Table 8 mostly rely on machine learning techniques whereas the proposed technique in this project is based on acoustics driven voice biometrics.

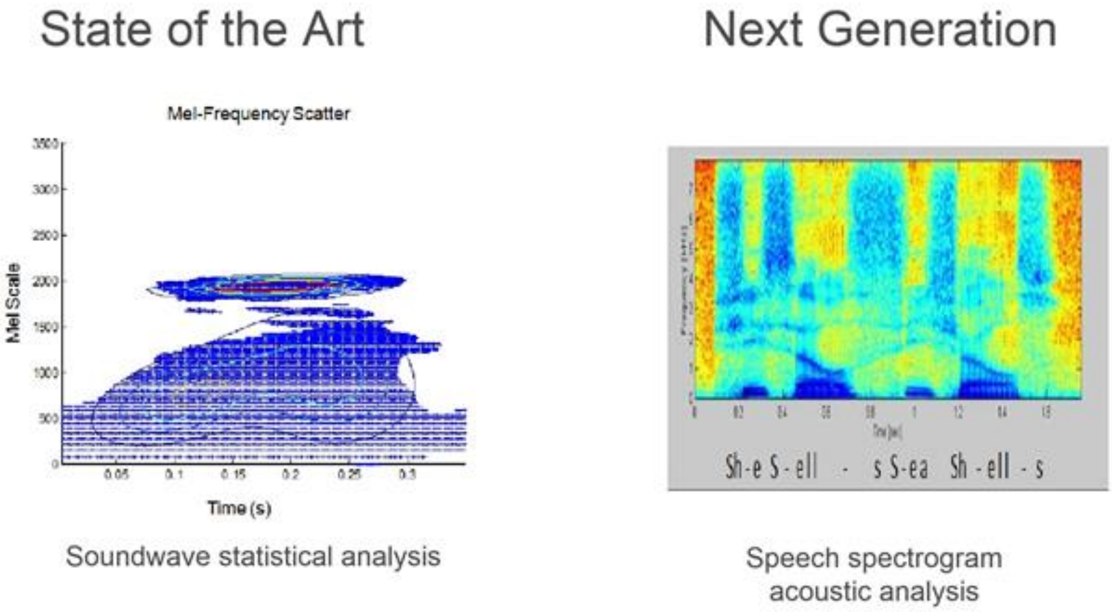
Patent no	Assignee	Subject
US 8,775,187 B2	**Auraya Pty Ltd, Sydney (AU)**	**Voice Authentication System and Methods**
US 8,510,104 B2	Research In Motion Limited, Waterloo (Canada)	System and Method for low overhead frequency domain voice authentication
US 8,555,358 B2	MasterCard International Incorporated, Purchase, N.Y. (US)	System and Method for Secure Telephone and Computer Transactions using Voice Authentication
US 8,543,834 B1	Google Inc., Mountain View, Calif. (US)	Voice authentication and command
US 8,694,314 B2	Yamaha Corporation, Hamamatsu-shi (JP)	Voice authentication apparatus
US 8,676,579 B2	BlackBerry Limited, Waterloo, Ontario (Canada)	Dual microphone voice authentication for mobile device
US 8,571,867 B2	Porticus Technology, Inc., Needham, Mass. (US)	Method and system for bio-metric voice print authentication
US 8,620,666 B1	West Corporation, Omaha, Nebr. (US)	System, method, and computer-readable medium that facilitate voice biometrics user authentication
US 8,615,219 B2	AT&T Intellectual Property I, L.P., Atlanta, Ga. (US)	Voice over IP based biometric authentication

US 8,645,137 B2	Apple Inc., Cupertino, Calif. (US)	Fast, language-independent method for user authentication by voice
US 8,712,790 B1	Robert Bosch GmbH, Stuttgart, Germany	Multi-user remote health monitoring system with biometrics support
US 8,583,498 B2	Face It Corp., San Diego, Calif. (US)	System and method for biometrics-based fraud prevention
US 8,731,251 B2	Precise Biometrics AB, Lund, (SE)	Method of matching, biometric matching apparatus, and computer program
US 8,804,918 B2	International Business Machines Corporation, Armonk, NY (US)	Method and system for using conversational biometrics and speaker identification/verification to filter voice streams

Table 8: Identified patents

To the knowledge of the consortium, there are no available patents for voice biometrics based on acoustic correlates of voice quality as opposed to machine learning techniques. The proposed technique in this project offers major opportunities to own various intellectual properties for European industrial and research organizations.

1.4.2 Voice Analysis



State of the art

Speaker recognition systems work on the principle that every user has a unique set of speech features which can be used to discriminate one user from another. During enrolment or training phase, the speech features are extracted and stored along with speaker's reference. Then during recognition phase the user's speech features are extracted and compared with the stored ones. These systems can be categorised into text dependent (when the same text is spoken during enrolment and recognition phases) and text independent (unconstrained mode). Text-independent systems are more commercially attractive than text-dependent systems because it is harder to mimic an unknown phrase than a known one.

Most “text dependent” speaker verification systems use the concept of Hidden Markov Models (HMMs), random models that provide a statistical representation of the sounds produced by the individual[13]. Most “text independent” applications use the Gaussian Mixture Model (GMM), a state-mapping model closely related to HMM. These methods are often combined with Support Vector Machines (SVM) and Maximum-Likelihood Linear Regression (MLLR) methods. In recent National Institute of Standards and Technology (NIST) 2014

[13] Springer handbook of speech processing, Edt. Jacob Benesty, M. M. Sondhi and Yiteng Huang, Springer – Verlag Berlin 2008, ISBN : 978-3-540-49125-5

speaker recognition challenge, techniques based on i-Vectors (fixed-length feature vector projected into a low-dimensional space) and probabilistic linear discriminant analysis (PLDA) have shown relative improvement of approximately 38% over the baseline system[14]. Despite this small increase, these techniques remain insufficient in accuracy.

These statistical methods compare the similarities and differences between the input speech features and the stored speech features to produce a recognition decision. After enrolment, during the recognition phase, the same quality/duration/loudness/pitch features are extracted from the submitted sample and compared to the model of the claimed or hypothesized identity and to models from other speakers. The other-speaker (or "anti-speaker") models contain the "states" of a variety of individuals, not including that of the claimed or hypothesized identity. The input speech features (freshly acquired during the verification phase) and enrolled models are compared to produce a "likelihood ratio," indicating the likelihood that the input sample came from the claimed or hypothesized speaker. If the voice input belongs to the identity claimed or hypothesized, the score will reflect the sample to be more similar to the claimed or hypothesized identity's model than to the "anti-speaker" model.

The seemingly easy implementation of speaker recognition systems contributes to their process's major weakness: susceptibility to transmission channel and microphone variability and noise. Systems can face problems when end users have enrolled on a clean land line phone and attempt verification using a noisy cellular phone. The inability to control the factors affecting the input system can significantly decrease performance. Speaker verification systems, except those using prompted phrases, are also susceptible to spoofing attacks through the use of recorded voice. Anti-spoofing measures that require the utterance of a specified and random word or phrase are being implemented to combat this weakness. Most of the statistical approaches require huge training data and computational resources for reliable performance.

Innovation 1: Acoustic-driven Voice Biometrics

In this project, an acoustics driven voice biometrics is proposed which enhances the speaker verification performance with minimum training data and is also computationally less intensive. The project will implement auditory models validating a user's claimed identity using the acoustic correlates of human vocal-tract physiology. Whereas conventional approaches "wash out" the acoustics in the system's first pass, the project approach looks in detail at acoustic correlates of vocal tract physiology. Reliance on a specific text for voice authentication is not necessary; rather, the distinctive features of speech and voice quality are identified. Because the project approach measures several more parameters of voice quality than the current state-of-the-art, even imposters are not expected to generate a false accept, as their vocal tracts physiology differ from that of the true speaker. The reason is that the degree of measurable difference in the acoustics of each speaker is greater than the sensitivity of the auditory system.

The project aims to deliver the first voice (speaker) authentication system based on well-proven science of the acoustic correlates of vocal tract physiology, resulting in the ability to better identify individual characteristics of a speaker. These acoustic correlates have been shown to improve accuracy and noise-robustness in up to 77% relative to speech recognition systems based solely on short-term pitch and energy features[15,16]. The application of physiologically-based models of speech acoustics to a voice authentication system is anticipated to have dramatic impact.

Taking account of vocal tract physiology allows advances in these regards. The vocal tract is essentially a tube that changes to produce different speech sounds. The sounds can be modelled as a perfect acoustic tube with perturbations attributed to the articulators along the length of the tube, resulting in a changing area as a function of vocal tract length. Constrictions along the length of the vocal tract correspond to consonants, while an open vocal tract corresponds to vowels. During a vowel, formant frequencies, or resonances, are remarkable. The

[14] Greenberg C. S et al., (2014), The NIST 2014 Speaker Recognition i-Vector Machine Learning Challenge, Odyssey 2014, The speaker and language recognition workshop, June 2014, Finland

[15] Hasegawa-Johnson, M., Cole, J., Shih, C., Chen, K., Cohen, A., Chavarria, S., ... & Choi, J. Y. (2004, May). Speech recognition models of the interdependence among syntax, prosody, and segmental acoustics. In Proceedings of HLT/NAACL (pp. 56-63).

[16] Reynolds, D., Andrews, W., Campbell, J., Navratil, J., Peskin, B., Adami, A., ... & Xiang, B. (2003, April). The SuperSID project: Exploiting high-level information for high-accuracy speaker recognition. In Acoustics, Speech, and Signal Processing, 2003. Proceedings.(ICASSP'03). 2003 IEEE International Conference on (Vol. 4, pp. IV-784). IEEE.

shape and location (in the frequency domain) of these resonances (amplitude as a function of frequency) correspond to speech sounds. It is in these patterns that the acoustic attributes corresponding to the speaker's underlying physiology may be found. It has been proven that the ear represents subtlety of these patterns faithfully as high in the auditory processing chain as the auditory nerve, showing that the ear has evolved to detect the subtle changes of voice quality (source).

Sound vibration during speech occurs at the glottis, is composed of two vocal folds that vibrate as air passes through them. Voice quality is primarily due to glottal behaviour and vocal tract characteristics. Moreover, there are subtle changes in how the voice produces a word as a function of time: while voice quality is mistakenly thought to be a perceptual constant, phonation is not. As phonation is the source of voice quality, therefore, voice quality is not a constant attribute. For example the project will examine micro-change in phonation, which can be measured at least 2000 times a second; while a window is applied to allow for variability in timing, the spectral characteristics due to the glottal source are prominent during vowels and consonant vowel transitions[17]. Even professional imposters or voice imitators cannot vary the vocal tract, for example, to a degree that would lead to mistaken authentication of the speaker.

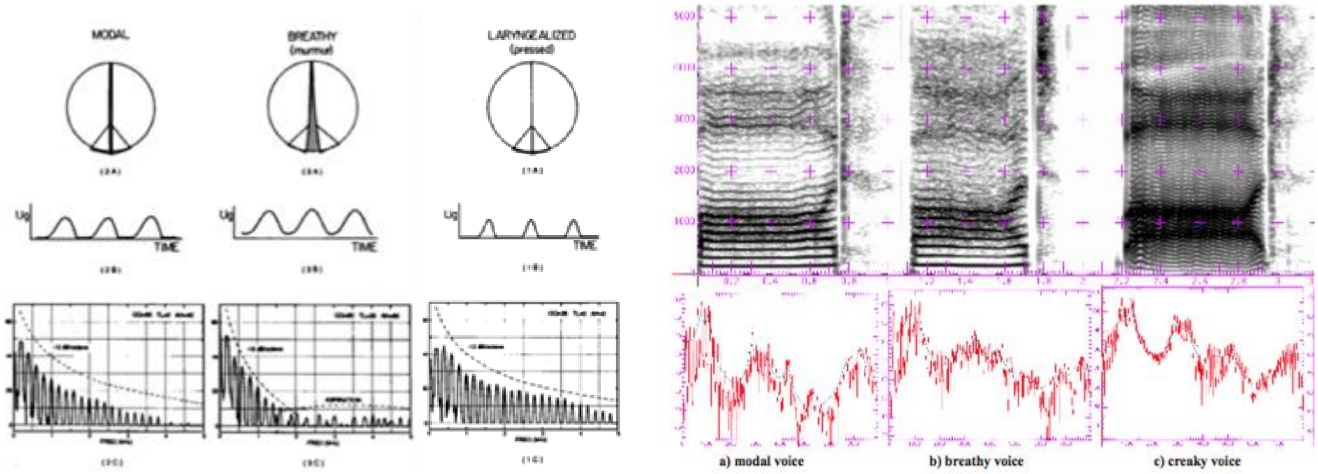


Figure 2: Acoustic data in different glottal configurations (adapted from Klatt and Klatt)

Figure 2 (left) shows as circles three different glottal configurations. Below the glottal configuration is a depiction of the amplitude of airflow through the glottis as a function of time. At the bottom is the short time Fourier transform of the signal, which indicates a slice in time of the spectrum.

Figure 2 (right) show the full acoustic spectrogram in the same three glottal configurations, demonstrating the richness of the acoustic information available (in comparison to the simple statistical analysis of the signal).

The three glottal configurations correspond to modal voice, breathy voice and pressed/creaky voice, three primary voice quality categories that may be used to describe the type of voice a speaker has. These figures are shown to depict the broad categories of speech quality, but there will nonetheless be subtle variations across different metrics corresponding to the speaker's vocal physiology and resultant acoustic signal.

The project will develop novel speech authentication system based on spectro prominences a.k.a formant frequencies and individual discreet harmonics along with a low computational classifier such as polynomial classifier. The acoustic properties based system will improve the accuracy performance and noise robustness while being less computationally intensive to be portable onto the small footprint devices such as tablets and mobile phones.

Another issue is text independence. Voice biometric solutions may be based on the voice modality only and use text-dependent statistical models'. Companies may also be offering text-independent solutions. It seems that text-independence may not necessarily be a desired feature in cases where a text-dependent (and text-prompted) solution may offer better accuracy and anti-spoofing with a shorter speech utterance than a text-independent approach. Detailed voice acoustic quality measures may also use segmental knowledge (for example, which phone is uttered) and that is easier to control with a text-dependent approach. This project will compare both text dependent and text independent solutions.

[17] Klatt, D. H., & Klatt, L. C. (1990). Analysis, synthesis, and perception of voice quality variations among female and male talkers. Journal of the Acoustical Society of America, 87(2), 820-857.

Innovation 2: Context-Dependent Matching Threshold Tuning

Any biometrics system can be described by its ROC (Receiver Operating Characteristics) curve, a visual characterization of the trade-off between the FAR and the FRR, as the matching algorithm performs a decision based on **a threshold** which determines how close to a template the input needs to be for it to be considered a match.

In practice, if the threshold is reduced, there will be fewer false non-matches but more false accepts. Conversely, a higher threshold will reduce the FAR but increase the FRR. This means that the FAR/FRR trade-off can be « tuned » for a given biometrics system.

In order to optimize the convenience of the biometrics system, the project will implement a mechanism in which the matching threshold can adapt to the criticality of the application that the user is trying to access (Figure 3).

- An application with low security requirement will have a lower threshold, in order to reduce the FRR (but therefore increasing the FAR)
- An application with high security requirement will have a higher threshold, in order to reduce the FAR (but therefore increasing the FRR)

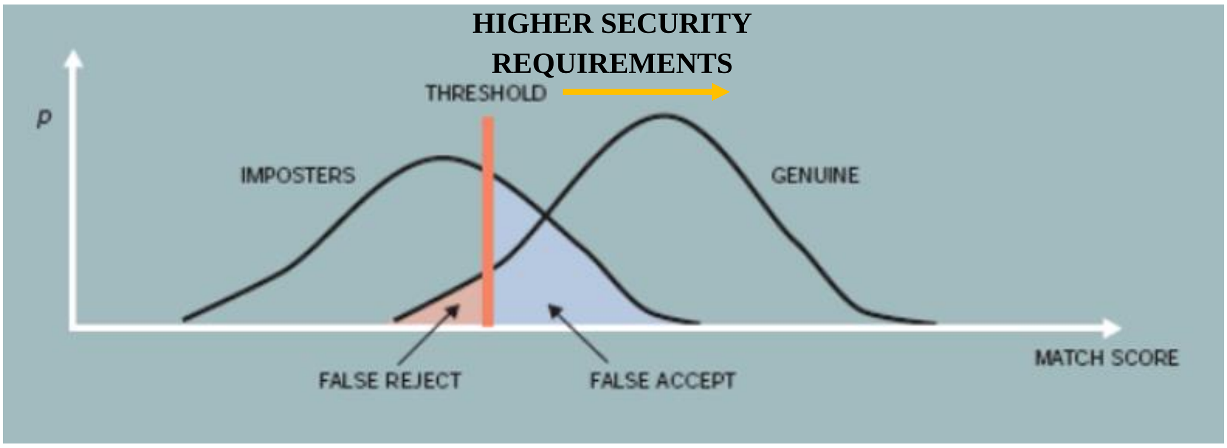


Figure 3: ROC plot and impact of the selected matching threshold on FAR and FRR

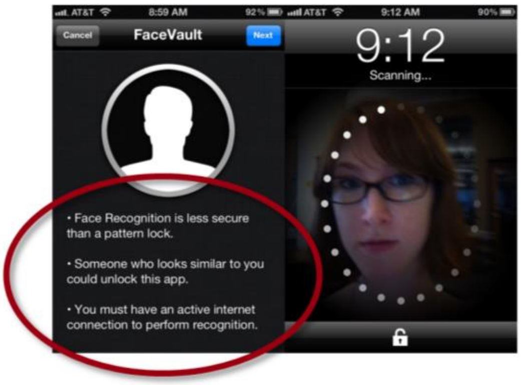
1.4.3 Audio-Visual Identity Verification

Mobile phones, tablets and personal computers are equipped with microphones and cameras. This allows for an economical verification of identity from a talking face. A talking face combines several biometric modalities: speech, face and synchrony between speech and lips movements. This combination makes spoofing attacks quite challenging. Fusion can be achieved at parametric, score and/or decision levels. As the face modality is sensitive to illumination and pose variations, and the voice modality is sensitive to noise, we take the assumption that a talking face offers more robust identity verification than either face or speech alone.

In the context of this project, speech is produced by a user in front of a camera. Such a recording offers an acoustic signal and a sequence of images in synchrony with speech. Verifying the identity of the user can therefore be performed on these two modalities (voice and face). In addition, the *synchronisation* of face movement (primarily lips movements) with the speech signal provides the dual benefit of ascertaining the "aliveness" of the face (preventing spoofing attempts using fake biometrics) and providing an extra set of co-inertial features[18]

[18] Bredin, H., Mayoue, A., & Chollet, G. (2009). Talking-face Verification. In Guide to Biometric Reference Systems and Performance Evaluation (pp. 297-326). Springer London.

State of the Art



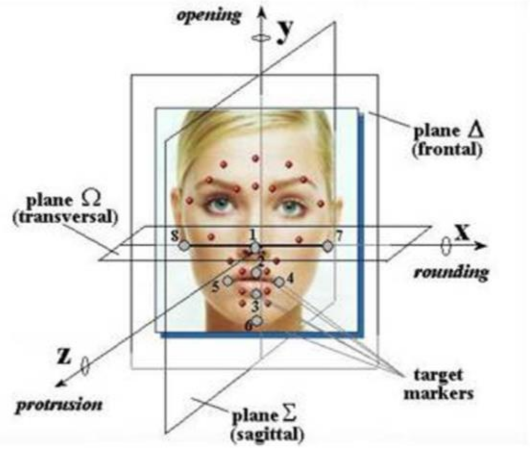
• Face Recognition is less secure than a pattern lock.

• Someone who looks similar to you could unlock this app.

• You must have an active internet connection to perform recognition.

Facial recognition algorithms identify static facial features by extracting landmarks, or features, from an image of the subject's face. They can be spoofed by a presenting a picture to the screen.

Next Generation



Next gen algorithms can identify dynamic lip/face movements and measure the synchrony between voice and audio images

State of the art

Face verification includes two steps: face detection and face identification. In the context of our project, the user is assumed to be cooperative and will position his face at the centre of the image mirrored on the display of the smartphone, tablet or PC. Therefore the focus of this section will be on face identification, rather than face detection. Face identification algorithms can be divided into several categories[19,20]:

- Geometric-feature-based methods are based on human knowledge of the typical human face geometry and facial features arrangement. A related method is the feature invariant approach, that aims to find structural features that exist even when the viewpoint or lighting conditions vary and then use these to locate faces ;
- Template-based methods represent the most popular technique used to recognize and detect faces. Unlike the geometric feature based approaches, they use feature vectors that represent the entire face template rather than the most significant facial features. Template matching methods can also be based on predefined templates are sensitive to scale, shape and pose variations.
- Appearance-based methods are using a pattern classification problem with two classes: “face” and “non-face” and statistical analysis / machine learning to discover the statistical properties or probability distribution function of the pixel brightness patterns of images belonging in the two classes. Numerous algorithms have been developed to support this approach, among which Support Vector Machine (SVM) methods, Karhunen-Loeve expansion based methods (e.g. eigen face approach), neural networks (e.g. fuzzy hybrid learning algorithm), Hidden Markov Models (HMM), etc.

Such approaches can be combined with other methods tracking specific elements of the face, such as lips.

Castrillon-Santana et al[21] (open source framework based on the work of Viola & Jones[22] taking into account the localisation of the eyes, nose, mouth, chin, ears), Werda et al[23] (Automatic Lip Feature Extraction prototype) as

[19] Tsalakanidou, F., Malassiotis, S., & Strintzis, M. G. (2008). Face Recognition. In Encycl. of Multimedia (pp. 239-244). Springer US.

[20] Vijayakumari, V. (2013). Face Recognition Techniques: A Survey. World Journal of Comp. Application and Technology, 1(2), 41-50.

[21] Castrillón-Santana, M., Déniz-Suárez, O., Antón-Canalís, L., & Lorenzo-Navarro, J. (2008). Face and facial feature detection evaluation performance evaluation of public domain haar detectors for face and facial feature detection.

[22] Viola, P., & Jones, M. J. (2004). Robust real-time face detection. International Journal of Computer Vision, 57(2), 137-154.

well as Bregler et al[24] (eigen face approach to lip movement detection dubbed « eigenlips ») have successsfully developed systems focusing on lip movement detection for speech recognition. Sanchez et al[25] demonstrated that a similar approach can be used for speaker recognition. In fact, the synchrony of speech and lips movements can be adequately captured with canonical correlation, co-inertia and/or HMMs [26,27,28,29]

Commercial systems using face recognition are not very secure. Hadid[30] reports that for instance, some laptops of Lenovo, Asus and Toshiba come with built-in webcams and embedded biometric systems that authenticate users by scanning their faces. However, in 2009, the Security and Vulnerability Research Team of the University of Hanoi (Vietnam) demonstrated at Black Hat 2009 conference, the world's premier technical security conference, how to easily spoof and bypass these systems (Lenovo's Veriface III, Asus' SmartLogon V1.0.0005, and Toshiba's Face Recognition 2.0.2.32 - each set to its highest security level) using fake facial images of the legitimate user, thus gaining access to the laptops. This vulnerability is now listed in the National Vulnerability Database of the National Institute of Standards and Technology (NIST) in the US.

Innovation 1: Audio-Visual Synchrony Analysis

The SpeechXRays project will use multi-channel speech and face biometrics and their correlations, in order to provide a secure, privacy preserving (revocable) biometrics and spoofing resistant (anti-spoofing) solution.

The key to this will be the dynamic analysis of the face (in particular lip movements and how they relate to the acoustic data).

One of the major drawbacks of biometrics is that the biometric traits (characteristics) can be faked. In such cases the challenge, called aliveness detection, is to be able to detect if the biometric sample belongs to a “live” person or is an artificial replica (such as a previously recorded speech of a speaker, a 2D photo of a face, etc.). When dealing with uni-modal biometrics systems, the anti-spoofing consists of developing an associated aliveness detection module to the biometric comparison module.

Because it is difficult to find a perfect uni-modal biometrics that can suit different applications, has high accuracy, does not require expensive sensors, is easy to use, and cannot be spoofed, SpeechXRays will combine information from multiple biometric sources, with the following advantages:

- A multi-biometric system will substantially improve the matching accuracy of the system compared to a voice-only or face-only modality.
- When multiple biometric traits are involved, it becomes more difficult for an impostor to spoof the system.

The information fusion can be carried out at different levels of the biometric system, such as sensor, feature, score, decision, or rank level. Most multimodal systems that rely on score fusion in order to combine the unimodal biometric scores unimodal aliveness detection methods for anti-spoofing. Therefore standard audio-visual systems are very vulnerable to spoofing attacks (the presentation of pre-recorded audio clip together with

[23] Werda, S., Mahdi, W., & Hamadou, A. B. (2013). Lip localization and viseme classification for visual speech recognition. arXiv preprint arXiv:1301.4558.

[24] Bregler, C., & Konig, Y. (1994, April). “Eigenlips” for robust speech recognition. In Acoustics, Speech, and Signal Processing, 1994. ICASSP-94., 1994 IEEE International Conference on (Vol. 2, pp. II-669). IEEE.

[25] Sanchez, U. R., & Kittler, J. (2006, May). Fusion of talking face biometric modalities for personal identity verification. In Acoustics, Speech and Signal Processing, 2006. ICASSP 2006 Proceedings. 2006 IEEE International Conference on (Vol. 5, pp. V-V). IEEE.

[26] Chollet, G., Landais, R., Hueber, T., Bredin, H., Mokbel, C., Perrot, P., & Zouari, L. (2007). Some experiments in audio-visual speech processing. In*Advances in Nonlinear Speech Processing* (pp. 28-56). Springer Berlin Heidelberg.

[27] Faraj, M. I., & Bigun, J. (2007). Audio–visual person authentication using lip-motion from orientation maps. *Pattern recognition letters*, *28*(11), 1368-1382.

[28] Abboud, B., Bredin, H., Aversano, G., & Chollet, G. (2007). Audio-visual identity verification: an introductory overview. In *Progress in nonlinear speech processing* (pp. 118-134). Springer Berlin Heidelberg.

[29] Rúa, E. A., Mateo, C. G., Bredin, H., & Chollet, G. (2007). Aliveness detection using coupled hidden markov models. In *Proc. Spanish Workshop on Biometrics*.

[30] Hadid, A. (2014). Face Biometrics under Spoofing Attacks: Vulnerabilities, Countermeasures, Open Issues, and Research Directions. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (pp. 113-118).

a still photograph is enough to fool the system[31])

In contrast, SpeechXRays will exploit the **natural correlation** between speech and face biometrics to improve accuracy and to detect spoofing.

Joint analysis of face and voice biometrics (usually referred to as "talking face"), exploiting the synchronization between the speech signal and the corresponding lip motion, provides a unique advantage over ordinary multi-modal fusion techniques. Hence, this synchronization property can be utilized as a "third cue" in addition to the individual voice and face modalities.

The project will measure the synchrony of speech with lips movements both globally and at the segmental level, using canonical correlation and co-inertia as a global measure[32] and using pseudo-phones and visemes associations at the segmental level[33].

The information fusion can be carried out at different levels of the biometric system, such as sensor, feature, score, decision, or rank level. Most multimodal systems that rely on score fusion in order to combine the unimodal biometric scores unimodal aliveness detection methods for anti-spoofing. Therefore standard audio-visual systems are very vulnerable to spoofing attacks (the presentation of pre-recorded audio clip together with a still photograph is enough to fool the system[34])

Innovation 2: Emotional Analysis

The project will also use the video-based face analysis to perform emotion recognition, using existing technologies provided by consortium partner EYE.

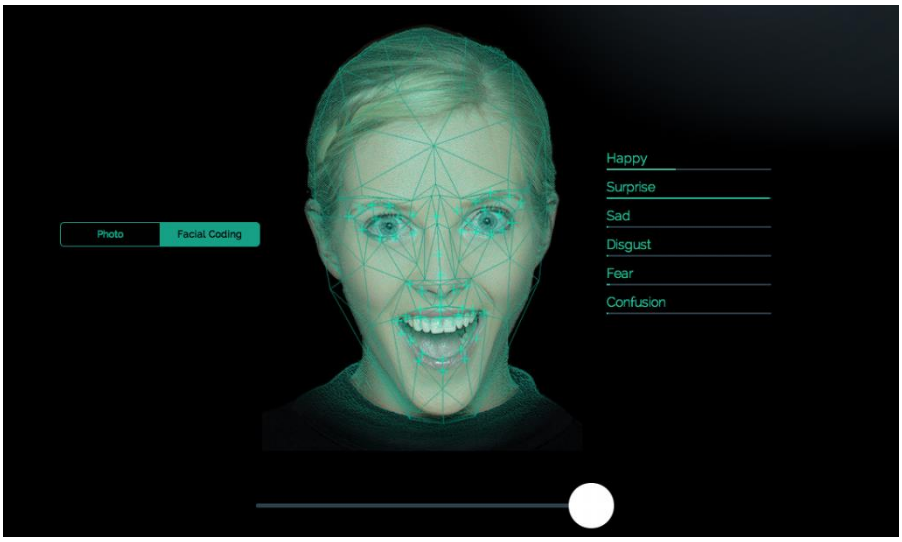


Figure 4: Realeyes emotional analytics solution

The project will develop specific face analytics classifiers as follows:

- Evaluation of the impact of user physiological or behavioural changes on system accuracy : the project will evaluation of impact of different emotional states on accuracy of identification systems used in this project and develop classifiers capable of recognising chewing or face occlusion. This will prevent situations where the user is not able to authenticate because of his emotional state (tired, sad) or behaviour (eating a chewing-gum).
- Duress detection: the project will develop improved emotion classifiers focusing on fear in order to identify if an individual is being « forced » to authenticate against his will. This will make the system even more useful in high security applications scenarios.

[31] Bredin, H., & Chollet, G. (2008, April). Making talking-face authentication robust to deliberate imposture. In ICASSP (pp. 1693-1696).

[32] H. Bredin, G. Chollet Audio-Visual Speech Synchrony Measure for Talking-Face Identity Verification. IEEE-ICASSP (2007)

[33] T.J. Hazen Visual Model Structures and Synchrony Constraints for Audio-Visual Speech Recognition. IEEE Trans on ASLP (2005)

[34] Bredin, H., & Chollet, G. (2008, April). Making talking-face authentication robust to deliberate imposture. In ICASSP (pp. 1693-1696).

- False reject optimization: the project will develop classifiers to detect more complex cognitive states, such as boredom or frustration. This will prevent the scenario where an initial false rejection triggers counterproductive emotional reactions with the user (anger, frustration) that make it even more difficult for the user to be authenticated in subsequent attempts. Therefore, the system could be able to take in account a « frustration factor » for a user not able to authenticate (which is unlikely to be similar in the case of an impostor).

1.4.4 Security and Privacy in Biometric based Authentication

Traditional authentication methods such as passwords and identity documents can be easily forgotten, lost, guessed, stolen, or shared. However, authentication using anatomical traits such as fingerprint, face, palm print, iris and voice are very difficult to forge since they are physically linked to the user. Biometric systems prevent non-repudiation and can also detect whether an individual has multiple identities. Thus, biometric systems impart higher levels of security and seen a rapid proliferation in a wide variety of government and commercial applications around the world in the last two decades[35]. However, various security and privacy challenges deter the public confidence in adopting biometric based authentication systems.

State of the art

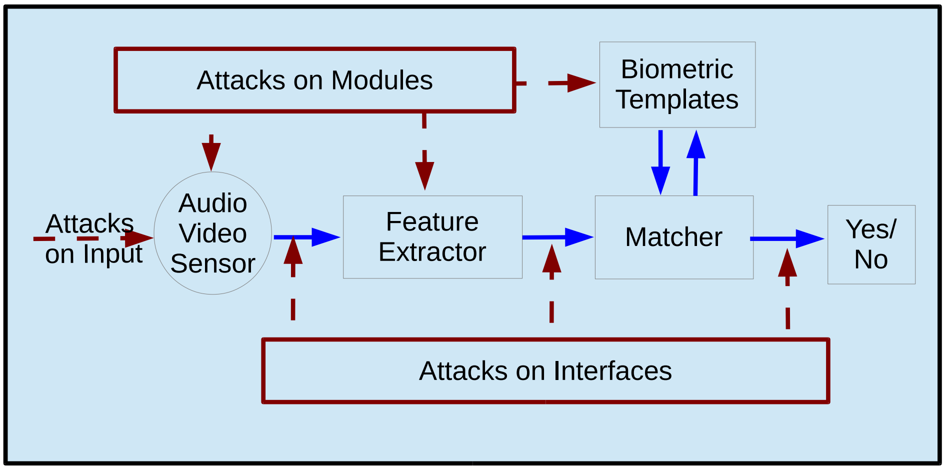


Figure 5: Biometrics points of attacks

A biometric system may fail due to manipulation by adversaries. Such manipulations can be carried out via insiders or by directly attacking the system infrastructure (Figure 5). An adversary can avoid a biometric system by colluding with insiders or fraudulently manipulating the procedures of enrolment and exception processing, originally designed to help authorized users. External adversaries can also cause a biometric system to fail through direct attacks on the user interface (sensor), the feature extractor and matcher modules, the interfaces between the modules, and the template database e.g., Trojan horse, man-in-the-middle, and replay attacks. However, there several countermeasures like cryptography, timestamps, and mutual authentication that are available to minimize their impact.

Adversary scans for vulnerability in inputs, interfaces, and modules. Attack at user interface is mostly due to the presentation of a spoof biometric trait. If the sensor is unable to distinguish between fake and genuine biometric traits, the adversary easily intrudes the system under a false identity. Multimodal biometric systems are robust enough to mitigate spoofing attacks. Aliveness testing (vitality detection) methods have also been suggested among feasible counteractions against spoof attacks. Aliveness testing, which aims to detect whether the submitted biometric trait is live or artificial, is performed by either software module based on signal processing or hardware module embedded into the input device itself. But, so far, the literature review states that no effective method exists yet[36].

[35] Jain, A. K., & Nandakumar, K. (2012). Biometric Authentication: System Security and User Privacy. *IEEE Computer*, *45*(11), 87-92.

[36] Schuckers, S., Hornak, L., Norman, T., Derakhshani, R., & Parthasaradhi, S. (2002). Issues for liveness detection in biometrics. In Proceedings of Biometric Consortium Conference. IEEE, New York.

Otherwise adversary compromises the database of enrolled identities, known as template leakage attack, gains access to the enrolment biometric. This is a major security threat and allows the attacker to use the enrolment biometric to gain repeated access to the system, and to any other biometric systems. This is also a privacy breach where the attacker has gained access to the user's physical identity information and can henceforth illegally impersonate the user. The seriousness of this threat is greatly increased by the fact that biometrics are inherent properties of the human body and cannot be revoked and then re-issued[37]. ISO/IECFCD 24745 standard recommends the following three features in any biometric systems to mitigate template leakage attacks[38] 1) the data stored on the database should provide little or no information about the actual biometric 2) the stored data should not allow an attacker to gain unauthorized access to the system successfully 3) if the user's stored data is known to have been compromised, then it should be possible to revoke it and issue a new set of biometric credential[39]. There are two well-known schemes known as biometric cryptosystems and cancellable biometrics satisfies the three recommendations. Biometric cryptosystems are designed to securely bind a digital key to a biometric. Cancellable biometrics consists of intentional, repeatable distortions of biometric signals based on transforms which provide a comparison of biometric templates in the transformed domain. In contrast to templates protected by standard encryption algorithms, transformed templates are never decrypted since the comparison of biometric templates is performed in transformed space which is the very essence of cancellable biometrics[40].

Project innovations

Innovation of the project in terms of security and privacy is on development and implementation of secure template and revocable biometric techniques to preserve the privacy of user's unique anatomical traits used for combined voice acoustic analysis with dynamic face recognition. When people use biometric services for authentication, they must allow the service to have access to their biometrics credentials. This exposes the user to abuse, with security, privacy and economic implications. For instance, the service could extract information such as gender, ethnicity, and even the emotional state of the user from the recording – factors not intended to be exposed by the user – and use them for undesired purposes. Moreover, due to the recent trends toward Cloud computing, it is imaginable that the biometric authentication systems will also be outsourced to potentially untrusted servers in the Internet. These servers could be malicious itself or vulnerable to passive and active attacks by intruders. Hence it is crucial to preserve the privacy of the user's biometric data without compromising or altering the system performance. Any private information that can be gleaned by inspecting a user's interaction with a system must be protected from prying eyes.

Innovation 1: Cryptobiometrics

The system should enable voice and dynamic face recognition processing tasks subject to no party, including the users, the system, or a snooper, can derive undesired or unintended information from the transaction. This would imply, for instance, that a user may enrol for authentication without fear that an intruder or even the system itself could capture and abuse his voice or statistical models derived from it. This will be achieved by incorporating biometric cryptosystem and cancellable biometrics technologies[41].

We will develop and implement a one-way cryptographic function tailored for voice acoustic and dynamic face recognition to transform the user biometric data into a template with the following features:

- the template used for the authentication, generated from the biometric data, cannot be reverse engineered to reveal the true biometric data
- the user will be able to generate different ‘‘templates’’ for different applications with the same biometric data, whilst ensuring that these different identities cannot be linked to each other

[37] Wang, Y., Rane, S., Draper, S. C., & Ishwar, P. (2012). A theoretical analysis of authentication, privacy, and reusability across secure biometric systems. Information Forensics and Security, IEEE Transactions on, 7(6), 1825-1840.

[38] Simoens, K., Bringer, J., Chabanne, H., & Seys, S. (2012). A framework for analyzing template security and privacy in biometric authentication systems. Information Forensics and Security, IEEE Transactions on, 7(2), 833-841.

[39] Breebaart, J., Yang, B., Buhan-Dulman, I., & Busch, C. (2009). Biometric template protection. Datenschutz und Datensicherheit-DuD, 33(5), 299-304.

[40] Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. IBM systems Journal, 40(3), 614-634.

[41] Jain, A. K., Nandakumar, K., & Nagar, A. (2008). Biometric template security. EURASIP Journal on Advances in Signal Processing, 2008, 113.

This will preserve the privacy of the user's biometric data from template leakage. In case of leakage, the system could simply revoke the enrolled template with freshly generated template. In general the following four different types of cryptographic techniques are used to protect the template: 1. salting (e.g. biohashing) 2. noninvertible transform (e.g. robust hashing) 3. key binding (e.g. fuzzy vault, fuzzy commitment) 4. key generation (e.g. secure sketch, fuzzy extractor)[42]. Each technique has its own advantages and disadvantages and have been exploited in several biometric authentication systems in the past. However, a single technique cannot be used to satisfy all the security and privacy requirements. Moreover, these techniques have only been implemented and tested on traditional biometrics such as fingerprints, Iris and face based authentication systems. This project will implement and investigate the cryptographic techniques for combined voice acoustic and lip based face authentication system individually and jointly. Each scheme will be evaluated in terms of false acceptance rate and false rejection rate.

Innovation 2: Homomorphic public-key encryption scheme

We develop an end-to-end privacy-preserving biometric authentication system to protect users vocal tract physiology derived from the feature analysis of the speech spectrogram and dynamic face features such as lip movement during the authentication from the authentication server as well as passive eavesdroppers. The end-to-end anonymous protocol is crucial when the biometric system is outsourced to third party such as cloud computing paradigm. In literature, there have been several privacy preserving biometric recognition systems such as the face recognition that are developed based on the cryptographic primitives such as homomorphic encryption, secure multiparty computation and oblivious transfer. However, developing a private tool to analyse the speech spectrogram and dynamic face recognition in encrypted domain in order to derive the precise vocal tract physiology and lip movement have not been done to-date. Moreover, the model of the acoustic cues of the voice physiology combined with lip movement of face for an individual is unique like his fingerprint. Hence it is crucial to keep it secure during transmission and storage. We will achieve this by implementing secure two-party protocol using Paillier cryptography to perform authentication in the encrypted domain. The Paillier cryptosystem is an additively homomorphic public-key encryption scheme, whose provable semantic security is based on the decisional composite residuosity problem. Additive homomorphic property supports addition and scaling operations in the encrypted domain. Hence the user's biometric inputs will be encrypted using the Paillier cryptography and the authentication will be performed by the server in the encrypted domain[43, 44, 45].

[42] Rathgeb, C., & Uhl, A. (2011). A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security, 2011(1), 1-25.

[43] Luo, Y., Cheung, S. C. S., & Ye, S. (2009, June). Anonymous biometric access control based on homomorphic encryption. In Multimedia and Expo, 2009. ICME 2009. IEEE International Conference on (pp. 1046-1049). IEEE.

[44] Upmanyu, M., Namboodiri, A. M., Srinathan, K., & Jawahar, C. V. (2009). Efficient biometric verification in encrypted domain. In Advances in Biometrics (pp. 899-908). Springer Berlin Heidelberg.

[45] Rahulamathavan Y, Phan R, Veluru S, Cumanan K and Rajarajan M, Privacy preserving multi-class support vector machine for outsourcing the data classification in cloud, IEEE Transactions in Dependable and Secure Computing, 10.1109/TDSC.2013.51, 2014.

2. Impact

2.1 Expected impacts

2.1.1 Results, impact and KPIs

Table 9 describes how the project results outlined in Section 1 support the expected impact of the call.

DS-02 expected impact	Relationships between project results and expected impact
Impact 1: *actions will deliver secure, but user-friendly, access to ICT systems, services and infrastructures, resulting in a consumerisation of devices for access control.*	The SpeechXRays algorithms and methods for speaker recognition and audio-visual recognition can be used in a variety of consumer devices (smartphones, tablets, laptops). The sensors used (camera and microphone) in the context of the project are already embedded in these devices, facilitating the consumerisation of these biometric methods. The modalities used (voice and face) make the system extremely user-friendly, and the multi-channel approach increases its security (accuracy, resistance to spoofing)
Impact 2: *The level of security of online services and critical infrastructures protected by these access systems should be demonstratably higher than by the state-of-the-art approach.*	The level of security achieved by the SpeechXRays solution will be higher than existing commercial systems based on voice or face recognition (or both). The analysis of the synchrony between face (lips) and voice will provide aliveness assessment (to avoid spoofing) and increased recognition accuracy. In addition the system will use cancellable (revocable) templates and cryptobiometrics for increased security and privacy.
Impact 3: *The proposed solutions are expected to support the creation of commercial services making use of electronic identification and authentication.*	The SpeechXRays solution will be deployed to support real-life authentication services in 3 use case scenarios: workforce, e-health and consumer. The solution will include development environment allowing third party developers to build new applications and service on top of the core technology. The consortium partners will dedicate efforts to the development of a developer community.

Table 9: Project contribution to the call topic's expected impacts

Table 10 presents the project key performance indicators (KPIs) related to the project expected impacts, at project end, as well as 5 years after project end and 10 years after project end.

Impact			Project impact indicator (Europe-wide)	End of project	End + 5 years	End + 10 years
1	2	3				
X			Biometric solution cost (software cost per user)	2 EUR	1 EUR	0.5 EUR
X			Biometric solution reach (total addressable market)	1M+[46]	10M+	50M+
X		X	Biometric solution user-friendliness	high	very high	very high
	X		Biometric solution performance (equal error rate)	1/100	1/150	1/200
	X		Biometric solution performance (resistance to spoofing)	high	high	high
	X		Biometric solution performance (template leakage)	none	none	none
X	X	X	Number of application developers or device suppliers	10	80	200
X	X	X	Number of commercial services	5	40	100
X		X	Number of users	2,000	5M	35M

Table 10: Project outcome indicators in relation to project timeline

[46] Based on the 3 project trials (Forthnet alone has 1.08M subscribers that could use the SpeechXRays solution)

2.1.2 Market analysis

The total biometric market is expected to grow to $23.54 billion by 2020 at an estimated CAGR of 17.6%[47] and include a wide variety of biometric modalities (fingerprint, palm, face, iris, vein, voice & signature). Leading companies include 3M (U.S.), Cross Match Technologies (U.S.), Facebanx (U.K.), Fingerprint Cards AB (Sweden), Fujitsu Ltd (Japan), Fulcrum Biometrics (U.S.), NEC Corporation (Japan), RCG Holdings LTD. (Hong Kong), Safran SA (France), Siemens Ag (Germany), Suprema Inc. (South Korea), Thales Group SA (France), Validsoft (U.K.). However, it is important to differentiate the consumer products (e.g. capacitive fingerprint reader embedded in an iPhone) from the industrial-grade products (e.g. high resolution optical fingerprint reader used in law enforcement).

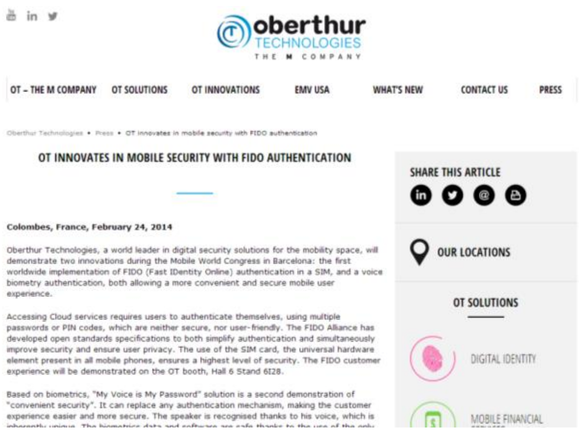
SpeechXRays is clearly addressing the consumer-side of the market, in alignment with the call objectives.

According to Goode Intelligence[48], growth in the consumer market will initially be driven by the integration of fingerprint sensors in high-end smartphones and tablets. Growth will then be rapidly followed by other innovative biometric technologies deployed as part of either FIDO (Fast Identity Online)-enabled solutions, proprietary-device OEM led initiatives such as Touch ID, and integration into multi-factor authentication platforms.

Biometrics Group[49] projects that the inclusion of biometrics in mobile devices will generate about 7.2Bn EUR worth of revenue by 2018 for the biometrics industry, not just through unlocking mobile devices through security applications, but also through multi-factor authentication services and the approval of instant electronic payments. Surveys analysed by this research firm have found that consumers prefer voice recognition technology. According to a survey conducted by IT provider Unisys, the biometric modalities ranked by consumer preference are: voice recognition (32 percent), fingerprints (27 percent), facial scan (20 percent), hand geometry (12 percent), and iris scan (10 percent). As a result, the firm projects that voice recognition will be widely adopted.

The voice verification segment of this market is in its nascent stages of development, but growth is anticipated as voice biometrics and speech recognition become more widely used. The major end-user segments of voice biometrics is in verticals such as financial services, healthcare, telecommunications, and government (three of which are represented in the SpeechXRays pilots). The major applications include transactional authentication and verification systems, wireless security device, computer/network security and physical access control.
Early leaders in voice biometrics included Diaphonics (acquired by Ivrnet in 2010) and Persay (acquired by Nuance in 2011). Newcomers include Sensory, Victrio, Agnitio, among other. Nuance is the current market leader with 35M voiceprints in use by their customers.

Oberthur has started to develop a voice biometrics offering under the tagline "My Voice is My Password" based on technologies from Agnitio (Figure 6). However, the technologies developed by Agnitio are based on voice modality only and use text-dependent statistical models. Oberthur plans to incorporate the multichannel biometric solution developed by the consortium in their voice biometrics product line, in order to bring more advanced audio-visual recognition models to consumer devices.



OT INNOVATES IN MOBILE SECURITY WITH FIDO AUTHENTICATION

Colombes, France, February 24, 2014

Oberthur Technologies, a world leader in digital security solutions for the mobility space, will demonstrate two innovations during the Mobile World Congress in Barcelona: the first worldwide implementation of FIDO (Fast IDentity Online) authentication in a SIM, and a voice biometry authentication, both allowing a more convenient and secure mobile user experience.

Accessing Cloud services requires users to authenticate themselves, using multiple passwords or PIN codes, which are neither secure, nor user-friendly. The FIDO Alliance has developed open standards specifications to both simplify authentication and simultaneously improve security and ensure user privacy. The use of the SIM card, the universal hardware element present in all mobile phones, ensures a highest level of security. The FIDO customer experience will be demonstrated on the OT booth, Hall 6 Stand 6I28.

Based on biometrics, "My Voice is My Password" solution is a second demonstration of "convenient security". It can replace any authentication mechanism, making the customer experience easier and more secure. The speaker is recognised thanks to his voice, which is inherently unique. The biometrics data and software are safe thanks to the use of the only

Figure 6: Oberthur launched "My Voice is My Password" at the Mobile World Congress 2014

[47] Next Generation Biometric Market by Technology (Fingerprint, Palm, Face, Iris, Vein, Voice & Signature), Function, Application (Government, Defense, Travel & Immigration, Home Security, Banking, Consumer Electronics & so on) & by Geography - Forecasts & Analysis 2014 – 2020. Markets & Markets (2014).

[48] Mobile and Wearable Biometric Authentication Market Analysis and Forecasts (2014-2019). Goode Intelligence. June 2014

[49] "Special Report: Mobile Biometric Authentication". Biometrics Research Group Inc, June 2014. Accessed at http://www.biometricupdate.com/201408/special-report-mobile-biometric-authentication

2.1.3 Barriers / obstacles and activities required to achieve the expected impacts

The drivers in the voice biometric market includes the increasing popularity of voice verification in mobile phone solutions, no dependency on infrastructure, easy implementation and low initial investment. However factors posing a challenge to the growth of this market are a lack of standards, lack of awareness among end-user industries and regulatory bodies and confusion created between voice biometrics and speech recognition. Table 11 lists the barriers/obstacles to impact and required activities in order to achieve the expected impacts.

Expected impact	**Barriers / obstacles**	**Steps needed to achieve the impact**	**WPs**
Consumerisation of devices for access control	Sensor size and cost can limit the incorporation of biometric technologies in consumer devices	The project takes an approach focusing on voice and face modalities, both of which can be captured by existing sensors embedded in consumer devices	WP2
	Privacy concerns may lead consumer to disregards biometrics solutions that required a voice or face recording	The solution will generate cancellable biometric templates created by binding keys with biometric data and securely storing them on the device	WP3
	Confusion between voice biometrics and speech recognition may lead consumers to question the accuracy of speaker identification	The project dissemination activities will place an emphasis on end-user awareness, clearly making a difference between speech recognition and speaker recognition (and the difference in performance/accuracy)	WP7
	Lack of standards for voice biometrics	The consortium will dedicate substantial effort to standardization activities	WP9
Higher security than state-of-the-art	High sensitivity to background noise or low-light conditions may render the authentication inoperable	The project technology will use acoustic driven approaches to voice biometrics (which are not sensitive to noise) and audio-visual synchronization analysis (which is not sensitive to lighting conditions)	WP2
	Spoofing	The project multichannel approach makes spoofing more difficult.	WP2
Creation of commercial services	Lack of awareness among end-user industries	The project dissemination activities will target early adopter verticals such as banking who have successfully adopted voice biometrics.	WP8
	Lack of awareness among regulatory bodies	The project will target regulatory authorities in new segments such as healthcare, where biometrics is needed to curb healthcare fraud and to provide increase patient care while protecting patient privacy	WP8

Table 11: Barriers/obstacles to impact and activities required to overcome them

2.1.4 Industrial, scientific and societal impact

The project industrial impact is driven by industrial partners (OT, SIV) and end-users (IFIN, FNET) that will allocate substantial resources (50 PM) to community building, exploitation and activities. The call will focus on demonstrating the viability and maturity of state-of-the-art security, privacy and trust solutions that have been tested in a laboratory environment. The intention is that after this validation phase they will find a wide up take in the market. The project will develop an industrial ecosystem of end-user and application developers deriving benefits from the use of the platform. The SpeechXrays solution will allow third party application developers to build new applications based on the technologies developed in the project. The project industrial impact will be measured by the number of third party developers (or device suppliers) relying on the SpeechXrays solution for authentication.

The project scientific impact is driven by 3 research partners (FORTH, TSP, UCL) and 3 research-performing SMEs (HB, EYE, TEC) and rests on a rich set of scientific dissemination activities described in Section 2.2.7. The project will influence the biometrics community by focusing attention on the use of acoustic-driven voice recognition and audio-visual synchronization analysis. Proving that the security concepts, processes and solutions work in a real life environment, in large scale demonstrators and directly involving end users who would ultimately benefit the most from the outcome, should increase the prospects for an ICT security market and demonstrate the validity and effectiveness of the scientific foundations of the project. However, the lack of long-lasting cooperation between industry and research (whose timelines and objectives are rarely aligned) is a serious obstacle to the scientific impact of a project where industrial partners and SMEs are dominant. In order to prevent the project to focus too heavily on short-term industrial impact and not enough on longer-term scientific impact, the project coordinator will enforce a simple rule: any peer-reviewed article develop in the course of the project will have to include at least one industrial partner or end-user. The project scientific impact will therefore be measured by the number of peer-reviewed articles published *in collaboration* between industry and research.

The project societal impact results from addressing specific challenges listed in the Secure Societies Work Programme. As cybersecurity is cross-domain, the project is able to provide benefits to many application domains supporting various societal challenges. Therefore the project societal impact will be measured by the flexibility of the solution and its applicability to various industrial domains. The workforce pilot will have impact on industries with high security requirements such as energy, transportation, military/law enforcement. The eHealth pilot will have an impact on healthcare sector where biometrics is needed to curb healthcare fraud and to provide increase patient care while protecting patient privacy. The consumer pilot will have an impact on other sectors such as banking, e-commerce, etc.

2.1.5 Contribution to European innovation capacity and integration of new knowledge

The challenge-based third pillar of Horizon 2020 emphasizes the need to take the societal problems themselves as a starting point for corporate and university research and innovation work. The technical work of the project involves a wide range of challenging task and the interdisciplinary approach of the project (voice acoustics, face recognition, audio-visual analysis, biometrics, security, privacy) requires a unique combination of skills that can only be provided by the best European scientists (France, Estonia, Greece, Romania, UK)

One of the main purposes of the project is to create a developer community and a user community that can support innovative biometric applications supported by a knowledge triangle of education, research and business inspired from the EIT ICT Labs model (Figure 7).

Several concepts have emerged in recent decades to interpret and illustrate the process of knowledge creation, in particular the non-linear nature of innovation and the multiple input and feedback loops required between the actors in an innovation system. For example, new knowledge on voice acoustic-driven recognition created by the SpeechXRays research is the source of improvement for all voice biometrics commercial providers and in return, new market prospects for innovation identified by SpeechXRays end-users can point towards new avenues for audio-visual analysis.

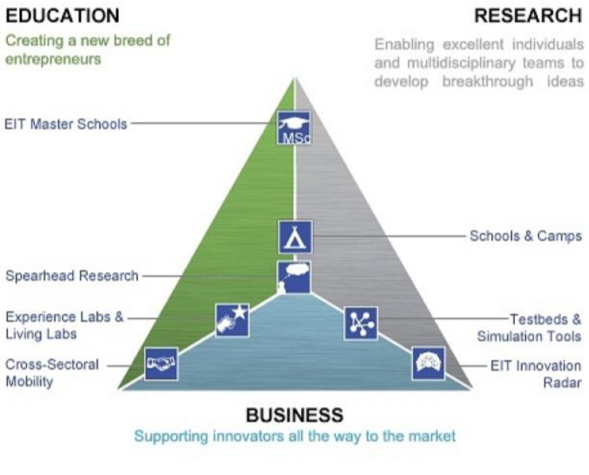

EDUCATION
Creating a new breed of entrepreneurs
RESEARCH
Enabling excellent individuals and multidisciplinary teams to develop breakthrough ideas
EIT Master Schools
MSc
Schools & Camps
Spearhead Research
Experience Labs & Living Labs
Testbeds & Simulation Tools
Cross-Sectoral Mobility
EIT Innovation Radar
BUSINESS
Supporting innovators all the way to the market

Figure 7: The EIT ICT Labs knowledge triangle

In particular, since the project will use cancellable and unleakable templates (biometrics cryptosystems), it will be possible to release such databases for the research community. **It will be the first time that such biometric databases are made publicly available for further research evaluation.**

2.1.6 Contribution to standards

As part of the standardization activities of WP9, The SpeechXRays consortium will interface with the standardization bodies that have been the most active in the area of voice biometrics and face biometrics, specifically the NIST Information Technology Laboratory (ITL) and the ISO/IEC Joint Technical Committee 1, Subcommittee 37- Biometrics (Figure 8).

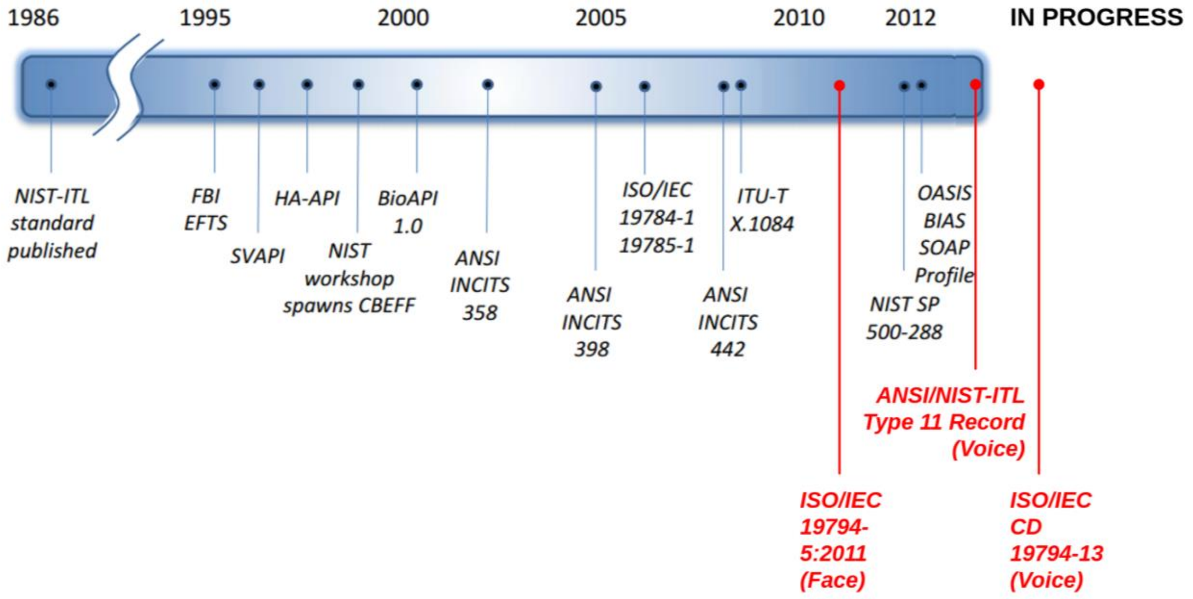


Figure 8: Development timeline of the biometrics standards

The domain of face biometrics has been addressed by recent standard updates, therefore the consortium will develop the solution in accordance with published standards such as ISO/IEC 19794-5:2011 and ANSI/NIST-ITL 1-2011.

There are renewed efforts to develop standards supporting secure access to the Web and Web services using biometric, speaker identification and verification (SIV). Interest in SIV is growing in both the private and public sector. That interest is motivated by a variety of factors, primarily cost and labour issues; convenience; and the growing number of regulations/laws governing data privacy and security that have been put in place exist at international, national, local, and industry levels.

Despite the growing interest in SIV, the lack of standards is a market and technology barrier

Unlike other biometric technologies (and unlike speech recognition and speech synthesis), there are no standards specifically governing the use of SIV. ISO/IEC 19784-1 (called “BioAPI”) is a generic, biometric application programming language that was designed to support SIV in non-telephony deployments. Its utility for SIV Web-services applications has not yet been fully explored. The other SIV standards projects (IETF MRCP V2; INCITS 1821-D Speaker Recognition Format for Raw Data Interchange, NIST-ITL Type-11 Record and ISO/IEC 1.37.19794-13) are all still under development.

The consortium therefore intends to make contributions to the development of the ISO/IEC 19794-13 standard, currently in Committee Draft status with target publication date 2016-01-04 (Table 12). However,

Published Standards	**Description**
ANSI/NIST-ITL 1-2011	Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information. In addition to the exchange of fingerprint, latent, face, and iris biometric data, the 2011 version of the standard includes new modalities such as forensic image mark-ups for **face** and iris; images of all body parts, new metadata fields such as geoposition of sample collection; biometric data hashing and information assurance; and data handling logs.
NIST SP500-288	New protocol, called WS-Biometric Devices (WS-BD), allowing desktops, laptops, tablets and smartphones to access sensors that capture biometric data such as fingerprints, iris images and **face images** using web services. The WS-Biometric Devices protocol enables interoperability by adding a device-independent web-services layer in the communication protocol between biometric devices and systems.
ISO/IEC 19784-1	Biometric application programming interface -- Part 1: **BioAPI** spec.
ISO/IEC 19794-5:2011	Biometric data interchange formats -- Part 5: **Face image** data
ISO/IEC 29109-5:2014	Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 -- Part 5: **Face image** data
ISO/IEC TR 29794-5:2010	Biometric sample quality -- Part 5: **Face image** data
OASIS BIAS SOAP Profile	The Biometric Identity Assurance Services (BIAS) profile specifies how to use the eXtensible Markup Language (**XML**) defined in ANSI INCITS 442-2010 – Biometric Identity Assurance Services to invoke Simple Object Access Protocol (**SOAP**) -based services that implement BIAS operations. These SOAP-based services enable an application to invoke biometric identity assurance operations remotely in a Services Oriented Architecture (SOA) infrastructure.
Standards in development	**Description**
IETF Media Resource Control Protocol Version 2 (MRCPv2)	Protocol allowing client hosts to control media service resources such as speech synthesizers, **recognizers, verifiers and identifiers residing in servers on the network**. MRCPv2 is not a "stand-alone" protocol - it relies on other protocols, such as Session Initiation Protocol (SIP) to rendezvous MRCPv2 clients and servers and manage sessions between them, and the Session Description Protocol (SDP) to describe, discover and exchange capabilities.
INCITS 456-2010, Information technology - Speaker Recognition Format for Raw Data Interchange (SIVR-1)	This standard specifies a concept and data format for **representation of the human voice at the raw-data level** with optional inclusion of non-standardized extended data. It does not address handling of data that has been processed to the feature or voice model levels. This standard contains definitions of relevant terms, a description of the basic speaker-recognition session, a data format for containing the data, and conformance information.
Draft Voice Supplement to the ANSI/NIST-ITL 1-2011	Joint effort between FBI and NIST to conduct research supporting the creation of **voice** biometric standards for the U.S. Government. The Investigatory Voice Biometrics Committee worked to produce a functional draft of the Type-11 Record aimed to seed a Voice Supplement to the ANSI/NIST-ITL 1-2011 standard. However, the focus of this document is on speaker identification for **law enforcement purposes** (and not access control).
ISO/IEC CD 19794-13	Biometric data interchange formats -- Part 13: **Voice** Data

Table 12: List of relevant standards

2.2 Measures to maximize impact

2.2.1 Joint Dissemination Plan

In order for SpeechXRays to have a far-reaching impact on the development of voice biometrics consumers systems, the dissemination strategy will encompass all stakeholders of value chain (Table 13).

Category	**Target Audience**	**Why them?**	**What's in it for them?**
Industry	Service providers (consumers)	They want to provide remote authentication services to decrease their costs and increase their level of service	SpeechXRays will provide them with a secure and convenient alternative to PIN/password, tokens and challenge questions.
	IT managers (workforce)	They want high security solutions that are adopted by their users (i.e. convenient)	
	Software developers	They need robust authentication modules for their applications	SpeechXRays will provide them with core services that can be re-used to develop their solutions
	Mobile device manufacturers (OEMs)	They ship devices carrying biometric sensors	SpeechXRays will provide them with a secure alternative to low-cost capacitive sensors
	Biometrics solutions suppliers	They develop biometrics solution for OEMs, service providers and consumers	SpeechXRays will provide new technology foundation for voice biometrics
Research	Biometrics researchers	They develop the next generation authentication methods	SpeechXRays will advance the state of the art in voice biometrics
	IT security and privacy researchers	They develop the next generation IT security and privacy frameworks	SpeechXRays will advance the state of the art in crypto-biometrics
Individuals	Consumers	They want convenient authentication solutions that preserve their privacy	SpeechXRays will use cancellable biometrics templates securely stored on the user device
	Workers	They want convenient authentication solutions that provide high security	SpeechXRays will provide them with a secure and convenient alternative to PIN/password, tokens and challenge questions.

Table 13: Targeted audience of the SpeechXRays project

2.2.2 Exploitation Plan Outline

WP8 Leader OT will use a specific exploitation methodology for EU-funded collaborative projects that will be the cornerstone of the project exploitation strategy. The method (Figure 9) is particularly well suited for Horizon 2020, as it has a major focus on market impact and is fully integrated with the compulsory periodic reviews, milestones, deliverables defined in the project

.

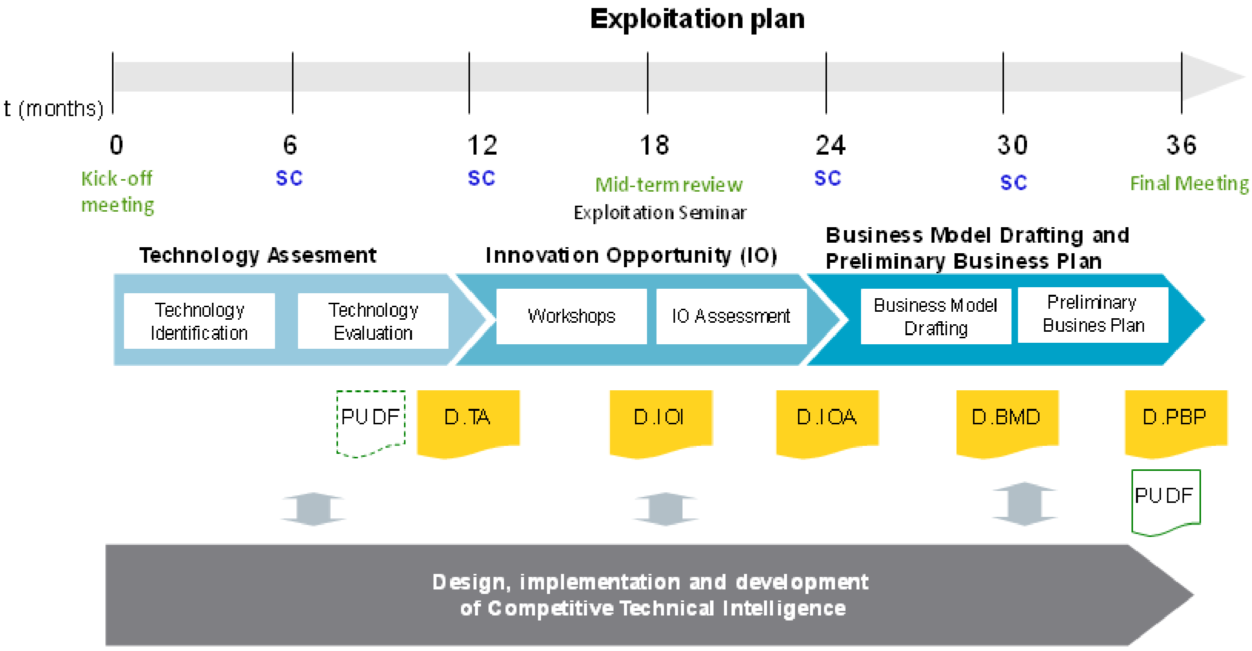


Figure 9: Overview of the exploitation methodology

The method is organized along two tracks. The first track is the elaboration process of a successful exploitation plan based on 3 discrete modules: Technology Assessment (TA), Innovation Opportunities (IO) and Business Plan (BP). The second track, running in parallel, is the development of a Competitive Technical Intelligence (CTI) that will interact with the 3 modules at all stages of the process.

The SpeechXRays Exploitation Manager is responsible for developing the exploitation plan and implementing the methodology, with the support of all project partners.

Technology Assessment (TA) Module

The module starts with the identification of technologies described in the DoW and extends it with in-depth technology evaluations including alternative technologies, markets, competitors, IPRs and related information.

Innovation Opportunities (IO) Module

The module defines the market segments targeted by the technologies listed at the previous stage. Therefore it must explore the applications and potential uses meeting the needs of a particular customer segment. This approach requires structured workshops where cross-domain expertise is required. It also includes interactions (focus groups, one to one meetings, and tradeshows) with target customer customers and industry experts.

Business Model Draft (BMD) and Business Plan (PBP) Module

The module start with generating a Business Model Canvas, a visual chart with elements describing the value proposition, infrastructure, customers, and financial elements of each Innovation Opportunity identified at the previous stage. The module also identifies the best exploitation form based on the nature of the results and its ownership structure (creation of spin-offs, products producing and sailing, licensing of products/services, patenting, etc.). IPR management is of crucial importance in this stage. Once the best Business Model Canvas have been selected, a Preliminary Business Plan is developed.

Depending on project result type, the partners foresee different exploitation strategies listed in Table 14.

Exploitation Strategy[50]	Voice recognition models	Face recognition models	Audio-visual synchrony models	Revocable encrypted templates	End-to-end Biometrics solution	Applications
OT	M,U,L,P	M,U,L,P	M,U,L,P	M,U,L,P	M,U,L,P	U,P
HB	M,U,L,P	M,U,L,P	M,U,L,P	M,U,L,P	M,U,L,P	U,P
SIV	U,P	U,P	U,P	U,P	U,P	U,P
TEC	U,P	U,P	U,P	M,U,L,P	U,P	U,P
EYE	U	M,U,L,P	M,U,L,P	U	U	U
FNET	M,U	M,U	M,U	M,U	M,U,L,P	U,P
IFIN	U,P	U,P	U,P	U,P	U,P	U,P
FORTH	U,P	M,U,L,P	M,U,L,P	U,P	U,P	M,U,L,P
UCL	U,L,P	U,L,P	U,L,P	U,L,P	U,P	U,P
TSP	U,L,P	U,L,P	U,L,P	U,L,P	U,P	U,P

Table 14: Exploitation strategy by partner in relation to the project result type

The SpeechXRays consortium has carefully selected industrial pilots that provide opportunities for technical and business *cross-fertilization*, either via business development activities, project dissemination or synergies with other research projects. Industries targeted for the pilots are not only interesting for their technical relevance, they also constitute springboards for a wider deployment and use of the technology:

- The pilots address large markets therefore the pilots have the potential to generate significant *interest from other stakeholders of these industries:* for example the e-Health pilot is focusing on a collaboration platform to manage osteoarthritis but can generate interest to support the patient-doctor interaction in any other healthcare domain.
- The industrial partners have significant international network therefore the pilots have the potential *to address other geographies* with the support of the relevant consortium member: for example OT is a market leader in security solutions for mobile devices and already serves 5,000 banks, 300 mobile operators and more than 100 governments, which will become prospects for the SpeechXRays technology.
- UCL is the Demonstrator leader allowing for more efficient *cross-fertilization* between the demonstrators.

2.2.3 Business Plan Outline

Preliminary business-plans have already been developed for the SpeechXRays technology (Table 15). Since voice biometrics solutions are not widely deployed in the industry targeted by the pilots, the consortium has analysed data from other industries where voice biometrics has already been deployed: banking.

The following data is extracted from a case study on Barclays supplied by Nuance[51]. Prior to the deployment of voice biometrics, more than 10% of legitimate clients were failing and 25% of fraudulent attempts were successful, using the legacy authentication process (PIN + security questions). Once voice biometrics was introduced, no fraudulent attempts were successful (note that transactions above 10,000 GBP still required security question in addition to the voice authentication). The successful authentication rate with passive voice biometrics was 95%, generating a 15% reduction in call times and a 3-4% reduction in operating costs for the bank.

SpeechXRays technologies can provide even higher benefits, with a successful authentication rate of 98% and no security question required due to a higher accuracy (EER of 1/100 or better)

[50] M=Making and selling results, U=Using results internally, L=Licensing results to third parties, P=Providing Services, Consultancy

[51] Barclays' voice biometrics case study accessed at http://www.nuance.com/for-business/by-solution/customer-service-solutions/solutions-services/customer-success/barclays-infographic/index.htm

GENERIC BUSINESS PLAN	
Products The solution will be declined in 3 variations • An end to end solution for turnkey implementation with customers • A development environment for customized implementation • A white label version for OEMs	**Product positioning** The solution will be positioned as an alternative to consumer-grade biometrics solutions embedded in mobile devices (face, voice, low-resolution fingerprint). It will not compete with industrial-grade biometrics used for law enforcement, border control (high-resolution fingerprint, iris, palm veins, etc.)
Market size and segmentation Goode Intelligence predicts that by 2017, there will be more than 990 M mobile devices shipped with fingerprint sensors, and 5.5 Bn users of mobile and wearable biometric technology around the globe (including other technologies than fingerprint sensors). The market for SpeechXRays is therefore comprised between 2Bn Euros (size of the consumer fingerprint biometrics) and 11Bn Euros (size of the total consumer biometrics market), with banking applications representing the largest category, and new applications emerging such as e-health.	**Go to market** The SpeechXRays solution will be marketed via three main channels: • Direct sales: technology providers (e.g. HB) will sell a turnkey end to end solutions to small and medium size customers • Channel sales: system integrators (e.g. SIV) will propose a customize solutions (and additional service) to large service providers and corporate customers • OEM sales: industrial partners (e.g. OT) will propose an OEM version of the solutions to mobile device manufacturers and telecom service providers
Competition Market leader: Nuance Emerging players: Sensory, Victrio, Agnitio	**Revenue forecast** The solution should be available at a cost of 2 EUR per user per year and reach 35M users within 10 years of project end, i.e. a turnover of 70M Euros per year, representing 4% of the size of the consumer fingerprint biometrics and 1% of the total consumer biometrics market.

Table 15: Generic (joint) business-plan for SpeechXRays

SPECIFIC BUSINESS PLAN FOR OTRTHUR TECHNOLOGIES	
Exploitable result description	Mobile Biometric Secure Authentication including: • Secure Element (eSE, SIM) • Biometric software for secure element • Biometric software for mobile • Credential management solutions.
Target market	Identity and Access Management (IAM) market, starting with • eHealth • Corporate Access Control • Government applications
Market size	The Identity and Access Management (IAM) market reached $4.4 billion in 2012, up from $4 billion in 2011 IDC anticipates that the overall market will increase to $6.9 billion in 2017, representing a 2012 – 2017 CAGR of 9.4%,
List of activities ad timetable for commercial use	End of project + 1 year: launch at “Cartes” or “Mobile World Congress”
	End of project + 2 years: early adoption by large customers and OEMs
	End of project + 5 years: mass market selling
Patents, trademarks	Support the branding of “My Voice is My Password”

Table 16: Specific (individual) business-plan for SpeechXRays

2.2.4 Knowledge Management and IPR

Dissemination and use of knowledge generated in the project is governed by the terms of the Grant Agreement and the terms of the Consortium Agreement. In order to make sure that these terms are followed, to avoid disputes and to facilitate business planning, the Steering Committee will maintain an IPR Directory throughout the lifetime of the project. This document will list all items of knowledge relating to the work of the project (both background know-how and results developed in the project), and make explicit for each item its owner, nature, status and dissemination and protection measures. The directory will be regularly updated, and distributed to all partners. It will form a key tool to enable knowledge management.

An initial version of the IPR directory will be created at the start of the project. However, at the stage of producing the proposal, the consortium has already considered what kind of strategy should be followed concerning IPR issues for the main results of the project, and reached preliminary agreement on this. The basic principle on which we are agreed is that research and development results must be available to a large audience to facilitate wide adoption of project results, while in the meantime having options in place for rewarding those that invested. The consortium's preliminary agreement is described in Table 17.

Initial agreement on IP and use rights	**Contributing partners**	**Consortium partners**
Encrypted biometric template database	Public (open access)	
Security and privacy mechanisms	Public (open access)	
Voice recognition models	IPR	Use rights
Face recognition models	IPR	Use rights
Audio-visual synchrony models	IPR	Use rights
End-to-end biometrics solution	IPR	Use rights

Table 17: IPR strategy related to result type

2.2.5 Open Access Strategy

SpeechXRays will fully embrace the open access policy of Horizon 2020 by providing on-line access to scientific information that is free of charge to the end-user and that is re-usable. In the context of this project, scientific information refers to peer-reviewed scientific research articles (published in scholarly journals) and research data (data underlying publications, curated data and/or raw data).

Open access to scientific peer reviewed publications has been anchored as an underlying principle in the Horizon 2020 and is explained in the Regulation and the Rules of Participation as well as through the relevant provisions in the grant agreement. The SpeechXRays consortium will use the OpenAire repository for peer-reviewed articles published by the consortium will ensure the largest possible impact among researchers, policy-makers and businesses. AS of March 2014, OpenAire already hosts over 19,000 open access publications, including 1147 for FP7-ICT and 73 for FP7-SECURITY, and is currently visited by over 1000 researchers per day.

Each consortium partner commits to deposit as soon as possible and at the latest on publication. Each partner will ensure open access to the deposited publication (via the repository) at the latest on publication, if an electronic version is available for free via the publisher, or within six months of publication (twelve months for publications in the social sciences and humanities) in any other case. Partner will also ensure access to the bibliographic metadata that identify the deposited publication (including the terms European Union (EU) and Horizon 2020; the name of the action, acronym and grant number; the publication date, and length of embargo period if applicable, and a persistent identifier). However, the partners will retain their copyright and grant adequate licences to publishers, based on Creative Commons licenses.

The project is not participating to the Pilot on Open Data, however, in the context of the digital era, the notion of publication increasingly includes the data underpinning the publication and results presented, also referred to as "underlying data". Partners will aim to deposit at the same time the research data needed to validate the results presented in the deposited scientific publications, into a data repository, and aim to make open access to this data. The SpeechXRays consortium will publish on already publicly available databases (such as Mobio, BioSecure, and NIST speaker data). Since the project will use cancellable and unleakable templates (biometrics cryptosystems), it will be possible to release such databases for the research community. **It will be the first time that such biometric databases are made publicly available for further research evaluation.**

2.2.6 Individual Dissemination & Exploitation Activities

To complement the join dissemination plan (section 2.2.1) and the join exploitation plan (section 2.2.2), Table 18 provides a **non-exhaustive list** of the **individual activities** planned by each partner.

Partner	Activities during project phase	Activities after project completion
OT	Present the project output at Cartes or Mobile World Congress where OT is exhibiting. Promote and evangelize during technical or scientific conference like the WorldID Congress. Support the standardization efforts towards ETSI or FIDO.	Sell the solutions to OT customers proving the efficiency of a model based on an end to end security reinforced by a management system allowing openness to other services. Build close commercial relationship between SpeechXRays partners and OT and act as an integrator or reseller for the consortium partners, leveraging OT's global presence.
HB	Publish 1 journal paper per year, and 2 conference papers or presentations per year for example in IEEE Transactions on Signal Processing and IEEE Transactions on Pattern Analysis and Machine Intelligence	Develop and sell a productized version of the SpeechXRays prototype to various end-users. Build close relationship with OT in order to leverage their worldwide network of customers and partners.
SIV	Present the project results to national cyber-security event such as DefCamp (annual event in Romania). Organize executive meetings with key Central European public authorities to evaluate their commercial interest.	Provide integration services for the SpeechXRays turnkey solution and develop a portfolio of public government customers in Central Europe. Establish a concept showroom for Central Europe at IFIN-HH.
TEC	Publish 1 Journal paper per year in top IEEE/Elsevier journal such as IEEE Knowledge and Data Engineering and 2 conference papers in major IEEE/ACM conferences. Involve at least 1 PhD and 1 MSc student.	Including the project findings in a book (to be published). Incorporate the project results in case studies presented in the Under Graduate and Post Graduate modules of City University London, where TEC personnel is teaching. Build a specific consultancy offering around the project results.
EYE	Involve 1 PhD candidate in the project. Publish 1 conference paper, for example at Mobile World Congress. Publish one article in relevant online industrial magazine per year, for example Multimedia tools and applications Journal.	Broaden academic presence of Realeyes as an industrial researcher in the field of emotion recognition. Include new improved emotion and cognitive state classifiers in main business product. Draw additional insights of advertisement performance from the newly developed classifiers and improve the business proposition for existing customers.
FNET	Disseminate the project results internally within FNET, as well as externally towards FNET customer (1.08M subscribers). Present the project results are relevant industry tradeshows, such as Digital Service Congress.	Investigate mid- and long- term commercial exploitation of the integrated platform will be investigated, as well as the exploitation of the individual software modules. Surveys selected subset of existing customers to refine go to market.
IFIN	Publish one journal paper during the period of the project and one conference paper per year. Involve at least one PhD student and one Master student in the project. Publish project news on IFIN website and websites of all projects which benefit directly from the improved security access system.	Depending on the results of the testing and calibration, roll-out the solution permanently within IFIN-HH for an installation with stringent security requirements. Serve as a demonstration environments towards other government organizations.
FORTH	Publish 1 journal paper per year, and 2 conference papers or presentations per year in	Evaluate spin-off possibilities for the commercial exploitation of the technology as

Partner	Activities during project phase	Activities after project completion
	relevant ICT/health open access (or hybrid) publications such as Journal of Medical Internet Research, Healthcare — Open Access Journal, International Journal of Health, Wellness and Society, International Journal of Medical Informatics.	part of the family of innovative products from FORTH (the Integrated Care Solutions - ICS) which are today in the process of commercialization and exploitation through participation in a number of National competitive tenders from Health and Social Care authorities in Greece.
UCL	Publish 1 journal paper per year, and 2 conference papers or presentations per year. Involve at least 1 PhD candidate in the project. Present at IEEE International Conference on Acoustics, Speech, and Signal Processing. This annual conference has about 1000 attendees.	Incorporate the project results in the training cursus of UCL and the Defence Academy of Cranfield University.
TSP	Publish 1 journal paper per year, and 2 conference papers or presentations per year, for example in Pattern Recognition and Machine Learning. IET Biometrics. Involve at least 1 PhD candidate in the project.	Include the project results in the institute's Master education programme (reaching 100 students per year)

Table 18: Individual dissemination and exploitation activity examples

2.2.7 List of communication and collaboration activities

The project will encourage the uptake of project results and the development of a partner ecosystem based on the communication and collaboration activities described below.

Academic dissemination

The dissemination of the project results to the scientific and academic audience will be done by publications in technical journals. The research project partners (FORTH, UCL, TSP) and some of the industrial partners (OT, HB) to publish articles in major open access technical journals related to signal processing (e.g. IEEE Transactions on Signal Processing biometrics. IEEE Transactions on Pattern Analysis and Machine Intelligence) and biometrics (e.g. IET Biometrics, International Journal of Biometrics). Peer-reviewed articles will be deposited within 6 months of their publication in European open access databases such as OpenAire (www.openaire.eu) and national open access databases such as Fraunhofer-Publica. The consortium will also favour journals part of the Directory of Open Access Journals. In total the project aims to publish 15 quality journal papers documenting the key project innovations and submit them to major open access scientific journals. An effective and natural way for academic dissemination is the use of project results in teaching and in the material of courses in universities. The project will generate course material regarding biometrics. The project will also provide subjects for thesis (Ph.D. and M.Sc.) at the research institutes involved.

Collaboration with other research projects or working groups

The project will seek cross fertilization with other European research projects. Please refer to section 1.3.3 for a list of national and international projects where there are already concrete opportunities for synergy, or adoption of project results, because of existing contacts from the consortium.

Industry events and scientific conferences

The outputs of the project will be also introduced to industry conferences as speaking engagements or booth exhibits, for example at World e-ID Congress Identity Services for Government, Mobility & Entreprise, Salon Cartes or Mobile World Congress where consortium partners have already scheduled activities (or concrete plans to do so). The consortium will also submit papers at various scientific conferences, such as IEEE International Conference on Acoustics, Speech, and Signal Processing, IEEE Global Conference on Signal and Information Processing (GlobalSIP), International Conference on Information Fusion, International Biometric Conference, IEEE International Conference of the Biometrics Special Interest Group (BIOSIG) and the Odyssey Speaker

Industry associations

The partners of the project belong to several industry associations (for example OT is part of the FIDO Alliance) and will be able to use them to disseminate the project results via newsletters, magazines and presence in international conferences not covered by the consortium partners. FIDO Alliance (Fast IDentity Online) is a non-profit organization formed in July 2012 to address the lack of interoperability among strong authentication devices as well as the problems users face with creating and remembering multiple usernames and passwords.

Specific activities targeting infrastructure operators

A further useful way forward to overcome these barriers is to encourage interest groups for the ecosystem who can share knowledge/ know-how and give information on support required. The consortium intends to pursue a series of activities focusing on ecosystem dissemination: online webinars organized to raise the awareness of various industries about the applications of the project results, and **industry-specific workshops** that will present the demonstrators and emphasize the various alternatives to access/license technology and knowhow develop in the project. In organizing these workshops and conferences, gender balance will be taken into account when selecting speakers, as we believe that this is an excellent means to reach out to both female and male participants.

Internet and social media

A project web site hosted at www.speechxrays.eu [52] will be developed where all public reports, project deliverables, events and articles will be published in order to stimulate dissemination. A specific area of the website will be dedicated to white papers. The project will leverage social medias (LinkedIn, twitter, other) to communicate the project results and will also target popular science programs and publications and mass media (TV, radio and newspapers) to present the project progress and results in a didactic way, in order to facilitate their publishing in the technology sections of general-interest media. The consortium will set up a dedicated LinkedIn Group and Twitter account for the project, in addition to the accounts already managed by the consortium partners.

Dissemination to the broader public

The project will also target the mainstream media as it is especially important to raise the public awareness around resource-efficient manufacturing. The consortium will also issue regular press releases at key milestones of the project and will make use of the CORDIS Wire service for major project result announcements.

[52] The domain names speechxrays.eu has been reserved on behalf of the consortium

3. Implementation

3.1 Work plan — Work packages, deliverables and milestones

3.1.1 Overall work plan structure

The work plan will be implemented by a multidisciplinary, gender-balanced team of scientists and entrepreneurs. Figure 10 summarizes the project structure, showing the names of the work packages (rounded rectangles) and key items exchanged between them (rectangles).

- **Technical Foundations (WP1-4):** conceive, design, implement and test the core technological components of the SpeechXRays approach.
- **Enabling Industrial Acceptance (WP5-6):** transform core technical results to a state suitable for deployment in an operational environment.
- **Exploitation, Dissemination, Standardization (WP7-9):** Carry out activities during the project, and planning activities beyond the project, to prepare for and bring about the promised impact (the use of separate WPs for different aspects of this reflects the importance placed on these activities; they will of course be carefully coordinated).

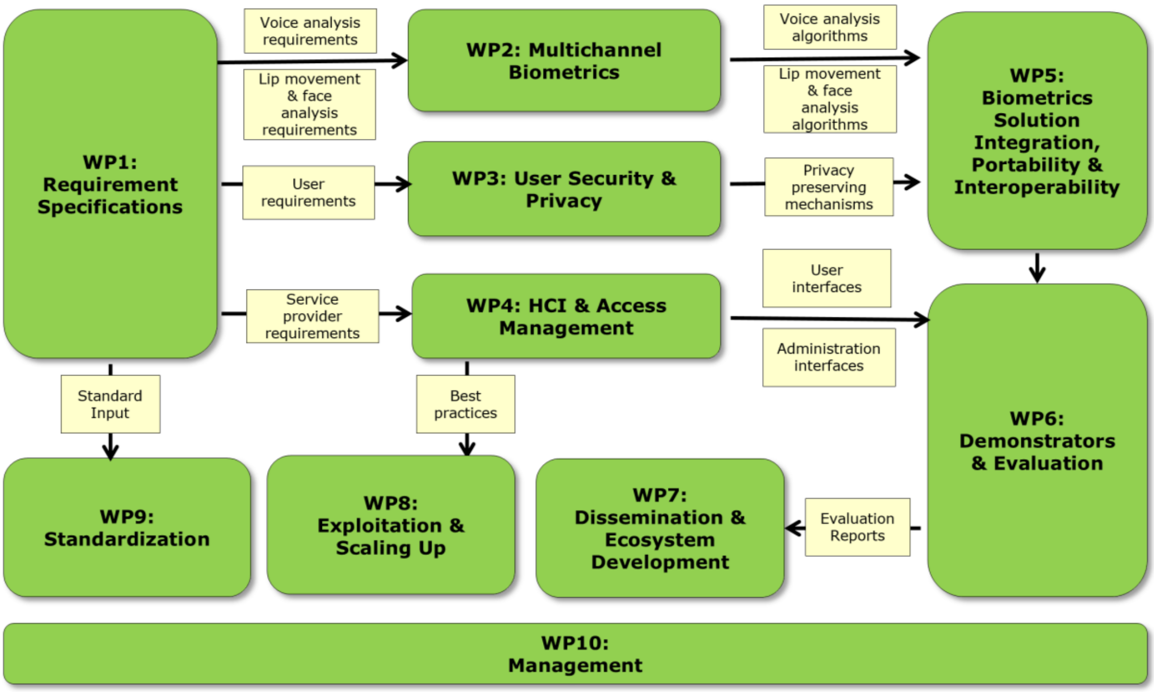

WP1: Requirement Specifications
Voice analysis requirements
Lip movement & face analysis requirements
User requirements
Service provider requirements
WP2: Multichannel Biometrics
WP3: User Security & Privacy
WP4: HCI & Access Management
Voice analysis algorithms
Lip movement & face analysis algorithms
Privacy preserving mechanisms
User interfaces
Administration interfaces
WP5: Biometrics Solution Integration, Portability & Interoperability
WP6: Demonstrators & Evaluation
Standard Input
Best practices
Evaluation Reports
WP9: Standardization
WP8: Exploitation & Scaling Up
WP7: Dissemination & Ecosystem Development
WP10: Management

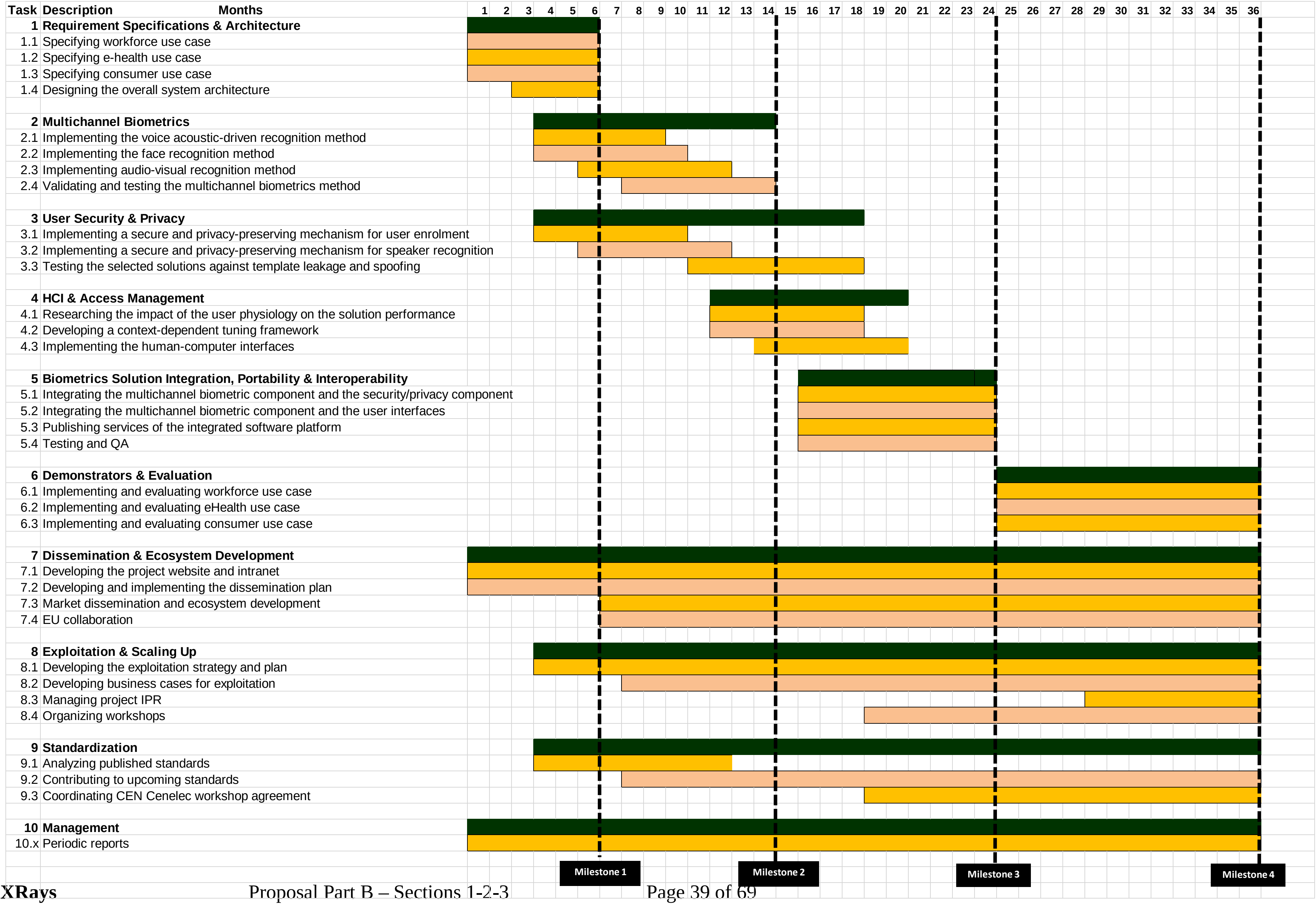
Figure 10: Project Overview PERT Chart

The GANTT chart (Figure 11) includes all tasks described in the WP

- The project duration will be 36 months.
- There are 4 main milestones cutting across all work packages
- Work breakdown into work packages is based on gathering related work, rather than on gathering tasks that occur at around the same time, therefore, some of the work packages run in parallel throughout the project.

3.1.2 Detailed work description

Figure 11: Gantt Chart



Work package nb	1				**Start month**	1				
Work package title	Requirement Specifications & Architecture									
Participant number	1	2	**3**	4	5	6	7	8	9	10
Short name of participant	OT	HB	**SIV**	TEC	EYE	FNET	IFIN	FORTH	UCL	TSP
Person-months per participant	4		**12**			6	4	4		4

Objectives

This work package covers the specification requirements for each of the use cases.

The objectives of this work package are:

- To specify the workforce use case (task 1.1)
- To specify the e-health use case (task 1.2)
- To specify the consumer use case (task 1.3)
- To design a flexible, modular system architecture that can support the 3 pilot scenarios (task 1.4)

Description of work

Task 1.1: Specifying workforce use case (lead: IFIN)

The task will specify the requirements in the context of a research worker accessing sensitive scientific data (nuclear physics) over 3G/4G or WLAN, from a mobile device (laptop, tablet or smartphone). Scientists working on sensitive nuclear research projects will be able to access the secure information repository of the institute via remote biometrics-based identification through their mobile device. In addition, physical access to the research facility will be tested using the same biometrics-based identification.

Task 1.2: Specifying e-health use case (lead: FORTH)
The task will specify the requirements in the context of a patient (or a medical expert) accessing personal health data over 3G/4G or WLAN, from a mobile device (laptop, tablet or smartphone). Patients and doctors will use the remote biometrics solution to access a collaboration platform developed by FORTH to support the prevention and management of a chronic condition (osteoarthritis). Patients will be able to remotely and securely report health data such as activity level, pain, etc. while general practitioners and specialists will be able to access the patient journals for decision-support.

Task 1.3: Specifying consumer use case (lead: FNET)
The task will specify the requirements in the context of a consumer accessing his internet service provider billing data over 3G/4G or WLAN, from a mobile device (laptop, tablet or smartphone). Customers will be able to access e-billing information, user profiling information, user accounts using an authorization service based on remote biometrics-based identification through a secure cloud connection.

Task 1.4: Designing the overall system architecture (lead: SIV)
The task will specify the information flow between the different system components and the integration requirements. The selected architecture will be flexible, so it can accommodate various types of networks and devices, and various authentication situations. The architecture will also be designed to support the latest security and privacy frameworks, and minimize the points of attack.

Task 1.1-1.3 will be implemented based on a user-centric innovation process. Each of the end-users (IFIN-HH, FORTH, FNET) will select super-users (users selected for their interest in new technologies and their communication skills) that will provide initial requirements in WP1 and iterative feedback during the development of the solution (in particular the user interfaces) in WP2-3-4.

SIV will lead this work package as it is in charge of the final integration and needs the most detailed level of knowledge of the use cases. SIV will be supported by consortium members in various parts of the work package:

- IFIN for the workforce use case
- FORTH for the eHealth use case
- FNET, OT for the consumer use case
- OT, TSP for the overall system architecture and TEC for latest security and privacy frameworks

Deliverables

From task	ID	Name	Lead	Main contributors	Diss. level	Delivery month
1.1	D1.1	Workforce use case specifications	IFIN	SIV	CO	6
1.2	D1.2	eHealth use case specifications	FORTH	SIV	CO	6
1.3	D1.3	Consumer use case specifications	FNET	SIV, OT	CO	6
1.4	D1.4	System architecture	SIV	OT, TSP	PU	4

Work package nb	2				**Start month**			4		
Work package title	Multichannel Biometrics									
Participant number	1	**2**	3	4	5	6	7	8	9	10
Short name of participant	OT	**HB**	SIV	TEC	EYE	FNET	IFIN	FORTH	UCL	TSP
Person-months per participant	22	**48**		12					14	14

Objectives

This work package covers the implementation of the individual biometric modalities (voice, face, lip movement) and their combination (multi-channel speaker identification and verification).

The objectives of this work package are:

- To implement a speaker recognition method based on voice acoustics filtering and analysis (task 2.1)
- To implement a face recognition method based on feature extraction and statistical analysis (task 2.2)
- To implement an audio-visual analysis method based on lip movement and audio-visual synchrony analysis (task 2.2)
- To test a multichannel biometrics solution combining all of the above (task 2.3)

Description of work

Given the nature of the project (Innovation Action bringing components from TRL 5-6 to TRL8), the consortium does not aim to redevelop novel biometric modalities, but instead to use proven methods (voice, face), improve them (using acoustic analysis for voice and lip movement for face) and combine them (multi-channel biometrics) to deliver a solution that can outperform existing individual biometric modalities.

Task 2.1: Implementing voice acoustic-driven identification model (lead: HB)

The task will measure the acoustic correlates of voice quality and create a feature vector containing acoustic correlates of voice quality. Key issues will be to a) examine how the acoustic correlates of voice quality vary as a function of placement in the syllable nucleus paying particular attention to consonant (C) vowel (V) and VC transitions, b) pay particular attention to aspiration noise, and c) examine voice quality at the syllable nucleus, mid-stream in the vowel where there is less changes in the acoustics. The task will also evaluate low cost classifiers (dynamic threshholding, vector quantization and polynomial classifiers) and classical GMMs. Low cost classifiers are being evaluated because it has been shown that acoustic correlates of voice quality is robust (see section 1.4.2). GMMs are evaluated to as they are widely used in voice biometrics today.

Task 2.2: Implementing face recognition model (lead: HB)

The BioSecure face recognition reference system[53] and its improvements[54] will be used initially. These algorithms will be compared with other successful algorithms such as 'Local Binary Patterns'[55], SIFT[56] and Active Shape and Appearance Models[57]. Scores of these algorithms will be experimented in task 2.4. A 3D

[53] D. Petrovska-Delacretaz, G. Chollet, B. Dorizzi (2009) Guide to Biometric Reference Systems and Performance Evaluation. Springer

[54] M.A. Mellakh, A. Chaari, S. Guerfi, J. D'Hose, J. Colineau, S. Lelandais, D. Petrovska-Delacrétaz, B. Dorizzi (2009) 2D Face Recognition in the IV2 Evaluation Campaign. ACIVS, pp 24-32.

[55] T. Ahonen, A. Hadid, M. Pietikäinen (2004) Face Recognition with Local Binary Patterns. ECCV(1), pp. 469-481

[56] D.G. Lowe (2004) Distinctive Image Features from Scale-Invariant Keypoints. IJCV 60 :2, pp. 91-110

[57] G.J. Edwards, C.J. Taylor, T.F. Cootes (1998) Interpreting face images using active appearance models. Proc. of the third Int. Conf. on Automatic Face and Gesture Recognition.

active shape model[58] will be exploited for facial landmark tracking in the video sequence. In particular, the lips will be localized and modelled for task 2.3.

Task 2.3: Implementing audio-visual analysis model (lead: HB)

Features from the lips will be obtained by global descriptors such as eigenlips and DCT coefficients. These descriptors will be interpolated to match the speech spectrum sampling rate (100 Hz). Canonical correlation and co-inertia coefficients[59] will be computed to capture the synchrony of speech and lips movements. In the text-dependent case, a measure of the correlation between the observed and the expected visemes for all the phone sequence will also be transmitted to the fusion module of task 2.4. Multi-stream HMMs will also be implemented if sufficient data is available for model adaptation.

Task 2.4: Validating and testing the multichannel biometrics solution (lead: UCL)

Validating and testing the multichannel biometrics solution will require a fusion engine which must, in some near optimal fashion, integrate the information from the two biometrics modules to make a decision of whether or not the user is who they claim to be. The fundamental approach that is being proposed is to incorporate as much of the discriminatory power of the underlying physical acoustics and face data as possible. The weakness of conventional machine learning approaches to the voice biometrics problem is that they do not capture the physical acoustics of the problem. They very early in the processing stream fundamentally cast the problem into a statistical classifier in a large dimensional vector space. We believe a simple Bayesian based decision rule can be employed, likely thresholding on Mahalanobis distance from the mean of the training set. We will select the most robust, highest performance approach to incorporate into our final design.

HB will lead this work package and will be responsible for all the software developments. HB will be supported by consortium members in various parts of the work package:

- TSP for anti-spoofing methods
- OT for the scalability and commercial feasibility of the selected solutions
- TEC for the security and privacy implications of the selected solutions
- UCL, TSP, OT for the validation and testing of the combined solution

Deliverables

From task	ID	Name	Lead	Main contributors	Diss. level	Delivery month
2.1	D2.1	Voice acoustics recognition method	HB	TSP, OT, TEC	PU	9
2.2	D2.2	Face identification method	HB	TSP, OT, TEC	PU	10
2.3	D2.3	Audio-visual analysis method	HB	TSP, OT, TEC	PU	12
2.4	D2.4	Validation report	UCL	HB, TSP, OT	PU	14

[58] D. Zhou, D. Petrovska-Delacrétaz, B. Dorizzi (2010) 3D Active Shape Model for Automatic Facial Landmark Location Trained with Automatically Generated Landmarl Points. ICPR, pp. 3801-3805

[59] H. Bredin, G. Chollet (2007) Audio-Visual Speech Synchrony Measure for Talking-Face Identity Verification. ICASSP

Work package nb	3				**Start month**			10		
Work package title	User Security & Privacy									
Participant number	1	2	3	**4**	5	6	7	8	9	10
Short name of participant	OT	HB	SIV	**TEC**	EYE	FNET	IFIN	FORTH	UCL	TSP
Person-months per participant	2	18		**35**		5	2	2		8

Objectives

This work package covers the implementation of security and privacy mechanisms for the target multichannel biometric solution.

The objectives of this work package are:

- To implement a secure and privacy-preserving mechanism for user enrolment (task 3.1)
- To implement an end-to-end secure and privacy-preserving mechanism for speaker identification and verification (task 3.2)
- To test the strength of the solutions against template leakage and spoofing (task 3.3)

Description of work

Task 3.1: Implementing a secure and privacy-preserving mechanism for user enrolment (leader: TEC)

The task will implement a one-way cryptographic function to mitigate template leakage attacks on biometric module. In particular biometric cryptosystem and cancellable biometrics will be implemented and evaluated. Biometric features such as vocal tract physiology and lib movements are transformed into pseudo random values by cryptographic schemes such as biohashing, robust hashing, key binding, and key generation techniques. Each technique has its own merit and demerit and combining these techniques serially and in parallel will enhance the accuracy and security. Each of the combination will be evaluated in the following category:

- Diversity: the secure template must not allow cross matching across databases, thereby ensuring the user's privacy
- Revocability: it should be straightforward to revoke a compromised template and reissue a new one based on the same biometric data
- Security: it must be computationally hard to obtain the original biometric template from the secure template. This property prevents an adversary from creating a physical spoof of the biometric trait from a stolen template.
- Performance: the biometric template protection scheme should not degrade the recognition performance of the biometric system

Task 3.2 : Implementing secure and privacy-preserving mechanisms for speaker recognition (leader: TEC)

The task will implement end-to-end anonymous privacy-preserving authentication scheme in order to protect the user's biometric data during transmission and storage. This scheme is crucial when applications or organizations outsource the biometric authentication systems to third party such as cloud providers. A novel scheme will be developed to hide the biometric data from active eavesdroppers and malicious server who performs the matching process. This task will exploit cryptographic primitives such as Paillier Homomorphic encryption, secure multi-party computation and oblivious transfer to build a secure scheme to archive user privacy. Paillier cryptography is public-key cryptography and supports additive homomorphism. The user device will generate public key and secret key. The public key will be used to encrypt the user biometric data before transmission. The user device keeps the secret key and sends the encrypted biometrical data and public key to the matching server. Since the secret key resides at user end, no one including the matching server could be able to decrypt the user's biometric data to compromise the user's privacy. However, the matching server exploits the Homomorphic property of Paillier encryption to perform linear operation associated with authentication process. Any non-linear operations will be performed using secure multi-party computation between user and server. Oblivious transfer and privacy-preserving scalar multiplication will be exploited to reduce computational and communication overheads.

Task 3.3: Testing the selected solutions against template leakage and spoofing (leader: TSP)
The task will provide the evaluation frameworks related to template leakage and spoofing. Besides the classical biometric evaluation metrics (such as False acceptance, False Rejection) we will address the issues related to spoofing. We will propose evaluation schemes that will allow testing the biometric solutions developed during the SpeechXRays project for various spoofing attacks. In relation to cancellable biometrics, template diversity and template leakage will be tested. In order to prove that a cancellable biometric system adds template diversity, the task will propose a specific test. In this test, one biometric feature vector is transformed with 100,001 (or even more) transformation parameters. This results in 100,001 different templates from a single feature vector. The first such cancellable template is compared with the remaining 100,000 cancellable templates. If the Hamming distance (or whichever distance is applicable) distribution of these comparisons is close to the impostor Hamming distance distribution, it indicates that a large number of independent templates can be obtained from a single biometric feature vector using the cancellable biometric system in consideration. The task will also address the biometric data protection issue, known also as template leakage, or how much the biometric cryptosystem templates are able to hide the biometric data that they represent. It will test if it is not computationally feasible to recover the original biometric feature vector from the biometric cryptosystem templates created in the context of SpeechXRays project.

TEC will lead this work package and will be responsible for the implementation of the security and privacy frameworks. TEC will be supported by consortium members in various parts of the work package:

- TSP, HB for the testing of the solution against template leakage and spoofing
- IFIN, FORTH, FNET, OT for the user validation of the privacy-preserving framework

Deliverables

From task	ID	Name	Lead	Main contributors	Diss. level	Delivery month
3.1	D3.1	Enrolment security and privacy implementation report	TEC	IFIN, FORTH, FNET, OT	CO	15
3.2	D3.2	Speaker recognition security and privacy recognition report	TEC	IFIN, FORTH, FNET, OT	CO	15
3.3	D3.3	Security and privacy test reports	TSP	TEC, HB	CO	18

Work package nb	4				**Start month**		6			
Work package title	HCI & Access Management									
Participant number	1	2	3	4	5	6	7	**8**	9	10
Short name of participant	OT	HB	SIV	TEC	EYE	FNET	IFIN	**FORTH**	UCL	TSP
Person-months per participant		18	15	14	19			**30**		

Objectives

This work package covers the implementation of user interfaces of the biometrics solution (user enrolment, user identification and verification, user management including template revocation)

The objectives of this work package are:

- To research the impact of the user physiology on the solution performance (task 4.1)
- To develop a context-dependent framework in order to tune the solution performance to the criticality of the application accessed (task 4.2)
- To implement ergonomic human-computer interfaces (HCI) for end-users and administrators (task 4.3)

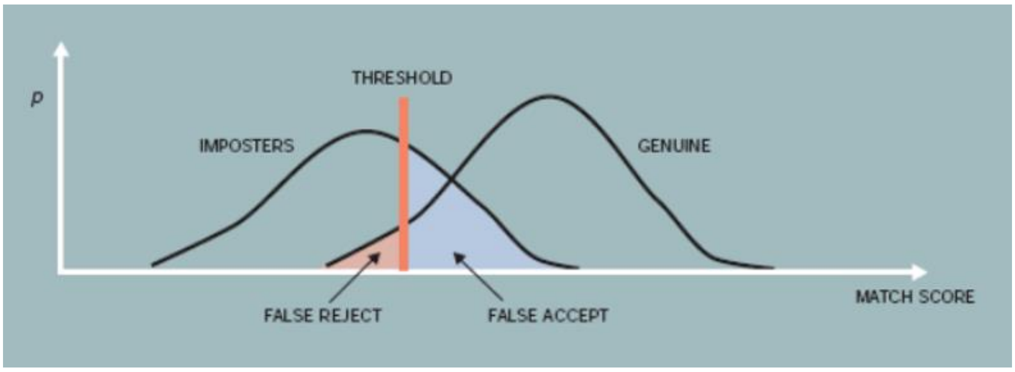
Description of work

Task 4.1: Researching the impact of the user physiology on the solution performance (lead: EYE)

Biometrics systems have different level of tolerance to individual physiological variations. Physical ageing (or sickness) is an important issue for practical biometrics, since it is known that the associated physiological changes can impair performance for most modalities. Similarly, the emotional state of the user may impair the performance of the audio-visual modalities. Understanding the effects of emotion is necessary, therefore both to optimise attainable performance but also to understand how to manage biometric templates. The impact of emotional status on speaker identification and verification may be a benefit in some cases. For example, a system that could identify a user that is attempting to authenticate under duress (threat) would be very useful. The task will define if emotional cues can be reliably gathered in order to prevent false reject or to authentication under duress (e.g. the system would authenticate a user that “looks” tired or sad, but reject a user that looks “stressed” or “under threat”).

Task 4.2: Developing a context-dependent tuning framework (lead: FORTH)

The performance of biometric systems can be described by the Receiver Operating Characteristics (ROC) curve, a visual characterization of the trade-off between the False Acceptance Rate (FAR) and the False Rejection Rate (FRR). The matching algorithm performs a decision based on a threshold which determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be fewer false non-matches but more false accepts. Conversely, a higher threshold will reduce the FAR but increase the FRR. In general, high-security applications will favour a low FAR, at the expense of a high FRR (as it is better to deny access and ask for re-authentication if the system has any doubt). Conversely, low-security applications will favour a low FRR, at the expense of a high FAR (as it is more convenient to authenticate at the first attempt, even if there is a risk it was not a legitimate authentication). However, the level of security required by a user may change over time. The eHealth scenario highlights this well: a patient that is about to access his latest data about blood pressure and temperature may not require a high level of security to do so. However, the same user attempting to access the results of a HIV test would require a much higher level of security to ensure he is the legitimate owner of the data. The task will develop a framework in which the matching threshold can be adapted based on the level of security required by the service that the user is attempting to access.



Task 4.3: Implementing the human-computer interfaces (lead: FORTH)
This task will carry out the design, formative evaluation and implementation of the system's user interfaces, for both and users and administrators, following a user-centred design approach, based on the holistic consideration of the user experience and taking into account the outcomes of tasks 4.1 and 4.2. In order to achieve this, the use cases elaborated in WP1 will be analysed to extract user experience requirements. Based on this analysis several UI prototypes will be designed and assessed following a formative usability evaluation approach, in order to identify appropriate feedback modalities combinations and iteratively refine the designs. The user interface implementation will include an adaptation mechanism to support UI adaptations as required by the context-dependent tuning framework.

FORTH will lead this work package and will be responsible for the development of the context-dependent framework and the human-computer interfaces. FORTH will be supported by consortium members in various parts of the work package:

- EYE and HB for the emotional analysis
- HB and TEC for the context-dependent tuning framework
- SIV for the implementation of the human-computer interfaces

Deliverables

From task	ID	Name	Lead	Main contributors	Diss. level	Delivery month
4.1	D4.1	User physiology impact report	EYE	FORTH, HB	PU	18
4.2	D4.2	Context-dependent tuning framework	FORTH	TEC, HB	PU	18
4.3	D4.3	User interface implementation report	FORTH	SIV	PU	20

Work package nb	5				**Start month**	14				
Work package title	Biometrics Solution Integration, Portability & Interoperability									
Participant number	1	2	**3**	4	5	6	7	8	9	10
Short name of participant	OT	HB	**SIV**	TEC	EYE	FNET	IFIN	FORTH	UCL	TSP
Person-months per participant	4	4	**55**	4				4		

Objectives

This work package integrates the components developed in WP2, WP3 and WP4. It is running at the end of the development period. The system integration will be done in two steps: a short 3 month (M16-M18, 1 iteration) integration phase overlapping with component development in order to generate iterative feedback to the component developers and a longer 6 month (M19-M24, 2 iterations) integration phase to make the system ready for full scale tests.

The objectives of this work package are:

- To integrate the multichannel biometric component and the security/privacy component in a coherent service (task 5.1)
- To integrate the multichannel biometric component and the user interfaces in a coherent service (task 5.2)
- To publish services of the integrated software platform (task 5.3)
- To test the system (task 5.4)

Description of work

Task 5.1: Integrating multichannel biometric component and security/privacy component (lead: SIV)

The aim of this task is to integrate the developed multichannel biometric component and the security/privacy component into a common software platform. This software platform will serve as the liaison between work that will be carried out during this project and future software systems that will be using the outcomes of this project. The activities carried out in order to develop the software integration platform refer to combining the individually developed and tested components (multichannel biometric component and the security/privacy component) into an integrated whole that will deliver added value for the entire software system. In this respect, independent capabilities of the individual software components will deliver cross-functional functionalities, enabling this way the deployment of the state of the art work carried out through the project. Therefore, the outcome of this task will refer to the following:

- Individual core assets developed in the project (such as multichannel biometric component and the security/privacy component) are integrated into the common core asset base of the project;
- Common core assets will enable cut-off, innovative, state of the art results that are linked to this project and beyond.

All carried out activities in other work packages that have delivered output such as requirements, architecture, processes and testing will serve as an input for this task and will contribute to the construction of the integrated software platform.

Task 5.2: Integrating multichannel biometric component and user interfaces (lead: SIV)

The aim of this task is to develop the capability of the integrated software platform to be visible and to create value to the outside world. The visibility to the outside world refers to users of the software platform and its services and other software systems that use certain functionalities of the platform. While the users of the software platform will access its functionalities trough a properly designed (usable) Graphical User Interface (GUI), other software systems may access functions trough software interface languages. In this respect, the integrated software platform will use SOA technology (Service Oriented Architecture) as means of communication to other software systems. As such, services that can be offered by the platform to other software systems will be visible through well-defined software interfaces, called services. This way, an outside software system will access functionalities delivered by the platform trough visible protocols.

Therefore, the results of this task focus on two outcomes: developing a usable GUI to the end users and deploying SOA technology that will be used as a communication channel to/from software systems.

Task 5.3: Publishing services of the integrated software platform (lead: SIV)
This task aims at having the integrated software platform interoperable with other software systems and/or external data sources. The developed services based on SOA technology will need to be discoverable by appointed software systems that need to user various functionalities. During this task, platform services will be deployed and tested individually in order to establish compliance and efficiency with needed standards of service. The interoperability infrastructure deployed during this task addresses the automation of flow between the source system (integrated software platform) and other software systems, or vice versa.

Task 5.4: Testing and QA (lead: SIV)
The aim of this task is to ensure that the developed software integration platform is fulfilling stakeholders' expectations. Moreover, the platform needs to be compliant with requirements as stated by requirements documentation. A testing specification document will be issued based on user requirements documentation. This testing specification documentation will aim to stress out platform capabilities in relation with the three use cases (workforce use case, e-health use case and consumer use case). In order to be able to fulfil stakeholders' expectations and to meet up with users standards a strict quality assurance methodology will be enforced. This QA methodology will ensure that defects in the software product (platform) are prevented and/or addressed in a timely manner. This way, possible shortcomings, mistakes or defects that may occur in the developed product (integrated software platform) may not only be prevented but also properly addressed may these occur.

SIV will lead this work package and will be responsible for the integration, testing and QA of all components. SIV will be supported by consortium members in various parts of the work package:

- HB, TEC, FORTH for the component integration
- HB, TEC, FORTH and OT for the system test & QA

Deliverables

From task	ID	Name	Lead	Main contributors	Diss. level	Delivery month
5.1-5.2	D5.1.1	System release v1	SIV	HB, TEC, FORTH	PU	18
5.1-5.2	D5.1.2	System release v2	SIV	HB, TEC, FORTH	PU	20
5.1-5.2	D5.1.3	System release v3	SIV	HB, TEC, FORTH	PU	24
5.3	D5.3	System interoperability report	SIV	HB, TEC, FORTH	PU	24
5.4	D5.4	Test/QA report	SIV	HB, TEC, FORTH, OT	PU	24

Work package nb	6				**Start month**	18				
Work package title	Demonstrators & Evaluation									
Participant number	1	2	3	4	5	6	7	8	**9**	10
Short name of participant	OT	HB	SIV	TEC	EYE	FNET	IFIN	FORTH	**UCL**	TSP
Person-months per participant	3		9			17	10	10	**18**	

Objectives

This work package deploys the SpeechXRays platform on 2000 users in order to demonstrate the impact of the technologies developed in the course of the project on 3 different use cases.
The objectives of this work package are:

- To implement and evaluate the workforce pilot – 600 users (task 6.1)
- To implement and evaluate the eHealth pilot – 400 users (task 6.2)
- To implement and evaluate the consumer pilot – 1000 users (task 6.3)

Description of work

Task 6.1: Implementing and evaluating workforce use case (lead: IFIN-HH)
The task will implement the solution on over 600 users of mobile devices (such as smartphones, tablets and laptops) used to access sensitive data over 3G/4G and WLAN and on-site, and on a physical access control device. All mobile equipment used for authentication will first be tested for compatibility with the access system (e.g. sufficient quality of sound and video recordings) and all approved equipment will be registered on the access platform. The on-site access system will implement most of the features of its mobile sibling plus an additional set of protection measures. These extra security measures are enforced to ensure the physical protection of the hardware infrastructure of IFIN-HH and rely on consolidating the above biometrics information with data obtained from the proximity cards (needed to enter the premises of IFIN-HH and each separate building), the perimetral video surveillance system (which can signal, for instance, unusual activities outside the standard working hours), and the Romanian Gendarmerie Detachment which monitors the compound. This scenario will test the level of security, threat remediation and adaptability of the solution to various application (online access, physical perimeter access).

Task 6.2: Implementing and evaluating eHealth use case (lead: FORTH)
This task will recruit 400 participants, perform the assessments, do the data entry and run the eHealth use case pilot. SpeechXRays will provide the required user identification services for secure access to the eHealth collaboration platform for all different stakeholder, to allow patients/citizens monitoring and medical expert collaboration. The secure collaboration platform enable by SpeechXRays will allow citizen to be informed if a high risk of developing exist, based on the available datasets and on the predictive models which are based on pattern recognition from the heterogeneous group of quantitative imaging data. It will also provide added value to the doctors/medical experts, with all the necessary information, properly visualized using multi-scale visualization techniques, to provide diagnostic collaboration opinions for better treatment. This scenario will test the security, privacy, usability and cost-effective features of the security platform. In particular, the scenario will test the context-dependent feature that allows administrators to modify the FAR/FRR trade-off in order to reduce the risk of false reject for low security data (e.g. physical examination) and reduce the risk of false accept for high security data (e.g. MRI/CT scans).

Task 6.3: Implementing and evaluating consumer use case (lead: FNET)
This trial will demonstrate the use of system on 1000 customers. Such an environment is typically very demanding since it involves interaction with users that are not accustomed to the provided interface while at the same time it provides a very good indication of the system’s usability in a real world setting.
In this particular scenario the user verification system developed in the project will be used to enhance the user experience of FNET’s customers, while accessing information and services offered by the company. Such services may involve e-billing information, user profiling information, access to the user’s account,

etc. Users from a selected consumer base, instead of following the typical access control procedure, will be able to use an authorization service based on remote biometrics-based identification through a secure cloud connection. This scenario will test ease of use, performance, security and the ability to target the actual user(s) of FNET services. While security is typically the primary consideration when incorporating user recognition technology, in this particular scenario security is necessary but is not as crucial as convenience or ease of use.

UCL will coordinate this work package and will be responsible of the evaluation of each use cases. UCL will be supported by consortium members in various parts of the work package:

- IFIN-HH for the workforce use case
- FORTH for the eHealth use case
- FNET and OT for the consumer use case
- SIV for all use cases

Deliverables

From task	ID	Name	Lead	Main contributors	Diss. level	Delivery month
6.1	D6.1	Workforce pilot implementation report	IFIN-HH	SIV, UCL	PU	34
6.2	D6.2	eHealth pilot implementation report	FORTH	SIV, UCL	PU	34
6.3	D6.3	Consumer pilot implementation report	FNET	SIV, UCL, OT,	PU	34
6.1-6.3	D6.4	Pilot evaluation reports	UCL	IFIN-HH, FORTH, FNET, OT	PU	36

Work package nb	7				**Start month**			1		
Work package title	Dissemination & Ecosystem Development									
Participant number	1	2	3	4	5	6	7	8	9	**10**
Short name of participant	OT	HB	SIV	TEC	EYE	FNET	IFIN	FORTH	UCL	**TSP**
Person-months per participant	16	4	2	2	2	1	1	2	2	**8**

Objectives

This work package focuses in on the dissemination of project results and the development of an ecosystem of partners along the ATI value chain, in order to guarantee a sustainable impact to the project, once it is completed.

The objectives of this work package are:

- To develop the project communication infrastructure (task 7.1)
- To elaborate a successful dissemination plan, taken into account gender balance and open access (task 7.2)
- To conduct market dissemination and SpeechXRays ecosystem development (task 7.3)
- To collaborate with other EU projects (task 7.4)

Description of work

Task 7.1: Development of project website and intranet (OT)

This task will focus on the development of an external project website hosted at www.speechxrays.eu. The website will include a description of the project, the consortium and the industrial demonstrators. It will also contain a list of public deliverables from the project, together with relevant technology and industry related news. A mirror site will be included in the OT website. The traffic to the OT website will be a substantial means of driving attention to the project results. A partner-restricted information repository will be hosted at OT for project internal communication and collaboration.

Task 7.2: Development and implementation of a dissemination plan (TSP)

This task will implement the dissemination of project results through a variety of channels. At the beginning of this task, the project consortium will specify a dissemination plan which will be re-assessed and refined periodically, including individual and joint dissemination or communication activities. The efforts will start at project kick off with mentions on the partner website and a dedicated press release. During the course of the project, regular communications will be made towards the industry via newsletters or presence at industry events. Once the trials have been implemented, case studies will be created and published on the partner websites, as well as on industry and technology websites. In addition, the project will publish articles or white paper and make presentations at industry conferences etc. Peer-reviewed articles will be deposited within 6 months of their publication in open access databases. These will not constitute separate project deliverables (they are in any case public information), but regular progress reports produced in WP10 Management will list articles published.

Task 7.3: Market dissemination and ecosystem development (OT)

This task is to actively promote the project technologies and innovations to the market, and to create an ecosystem around the SpeechXRays solution. Various market dissemination activities will be organised such as an application development contest and a spoofing contest. In these contests, the developer (and hacker) community will be asked to develop new application ideas based on SpeechXRays or to attempt to spoof the system.

Task 7.4: EU collaboration (TSP)

The project aims to develop cross-fertilization activities with ongoing FP7-ICT or FP7-SECURITY projects and new Horizon 2020 projects focusing on similar challenges, based on TSP's experience leading the BioSecure NoE.

Although OT will provide a large effort in this WP, it will formally be led by TSP, who will be responsible for the dissemination and collaboration activities, supported by OT for the project website, communication infrastructure and ecosystem development, and generally by all partners.

Deliverables

From task	ID	Name	Lead	Main contributors	Diss. level	Delivery month
7.1	D7.1.1	Internal project repository	OT	All partners	CO	1
7.1	D7.1.2	External project website	OT	All partners	PU	2
7.2	D7.2.1	Dissemination plan	TSP	All partners	CO	6
7.2	D7.2.2	Dissemination report	TSP	All partners	PU	36
7.3	D7.3.1	Developer contest report	OT	All partners	PU	36
7.3	D7.3.2	Spoofing contest report	TSP	All partners	PU	36
7.3	D7.3.3	Ecosystem report	OT	All partners	PU	36
7.4	D7.4	Collaboration report	TSP	All partners	PU	36

Work package nb	8				**Start month**		1			
Work package title	Exploitation & Scaling Up									
Participant number	**1**	2	3	4	5	6	7	8	9	10
Short name of participant	**OT**	HB	SIV	TEC	EYE	FNET	IFIN	FORTH	UCL	TSP
Person-months per participant	**24**	12	2	2	2	2	1	2	2	2

Objectives

This work package will effectively support the exploitation of the project results. Its objectives are:

- To develop an effective exploitation strategy for the (post-project) market replication of project results (task 8.1)
- To create business cases and develop a business plan (task 8.2)
- To manage the IPR resulting from the project (task 8.3)
- To organise industry-specific workshops (task 8.4)

Description of work

Task 8.1: Developing the exploitation strategy and plan (OT)
This task focuses on the development of appropriate exploitation strategy and plan of the project results. The core strategy is to use the extensive contact network of each consortium members as a starting point to get in touch with new potential users of the project solutions. OT will lead this task with support from all project partners. The partners will also develop their own individual exploitation plans based on their contributions to the project and their business development strategy. This task will also be responsible to monitor similar development by third parties (competitive landscape analysis and monitoring).

Task 8.2: Developing business cases for exploitation (OT)

This task focuses on industrial business cases development for the targeted applications, including return on investment (ROI) and cost-benefit analyses (CBA). The data of these cases will be used to build a cost-benefit analysis for each targeted industry cluster.

Task 8.3: Managing project IPR (HB)
HB will document all project results in an IPR directory in order to clearly assign the ownership of the various pieces of software developed in the course of the project, and set up cross-licensing schemes between partners to be able to reuse non-public parts of the projects. This work will be coordinated with the development of industrial business cases to ensure that such activities can proceed without hindrances regarding disputes about ownership and exploitation rights.

Task 8.4: Organizing workshops (OT)
This task will also promote the project results to companies external to the consortium, by arranging 3 workshops in relation with the 3 pilots. The workshops will be full day events promoted at international level and specifically targeting SMEs (i.e. small and medium size organizations that could become customers or partners).

OT will lead this work package and all deliverables except the IPR registry (led by HB)
OT will be supported by all consortium members to maximize the exploitation outputs, and by the pilot leaders (IFIN-HH, FORTH, FNET) in order to build the business cases.

Deliverables

From task	ID	Name	Lead	Main contributors	Diss. level	Delivery month

8.1	D8.1.x	Exploitation plan	OT	All partners	CO	6/18/36
8.2	D8.2	Business cases	OT	IFIN-HH, FORTH, FNET,	PU	24
8.3	D8.3	IPR registry	HB	All partners	CO	36
8.4	D8.4	Reports on industry workshops	OT	All partners	PU	36

Work package nb	9				**Start month**	1				
Work package title	Standardization									
Participant number	1	2	3	4	5	6	7	8	**9**	10
Short name of participant	OT	HB	SIV	TEC	EYE	FNET	IFIN	FORTH	**UCL**	TSP
Person-months per participant	5	3							**10**	3

Objectives

Despite the growing interest in speaker identification and verification, the lack of standards is a market and technology barrier. Therefore, the consortium has elected to dedicate a full work package to certification and standardization activities. The objectives for this work package are:

- To analyse and re-use relevant published standards (task 9.1)
- To contribute to the development of ongoing standard drafts (task 9.2)
- To coordinate a CEN Cenelec workshop agreement (task 9.3)

Description of work

Task 9.1: Analysing published standards (UCL)

The domain of face biometrics has been addressed by recent standard updates, therefore the consortium will analyse, and develop the solution in accordance with, published standards such as ISO/IEC 19794-5:2011 and ANSI/NIST-ITL 1-2011.

Task 9.2: Contributing to upcoming standards (OT)

Unlike other biometric technologies (and unlike speech recognition and speech synthesis), there are no standards specifically governing the use of SIV. ISO/IEC 19784-1 (called “BioAPI”) is a generic, biometric application programming language that was designed to support SIV in non-telephony deployments. Its utility for SIV Web-services applications has not yet been fully explored. The other SIV standards projects (IETF MRCP V2; INCITS 1821-D Speaker Recognition Format for Raw Data Interchange, NIST-ITL Type-11 Record and ISO/IEC 1.37.19794-13) are all still under development. The consortium therefore intends to make contributions to the development of the ISO/IEC 19794-13 standard, currently in Committee Draft status with target publication date 2016-01-04 (Table 12).

Task 9.3: Coordinating CEN Cenelec workshop agreement (UCL)

UCL will subcontract CEN Cenelec to develop a Workshop Agreement (also known as CWA) in the area of multichannel biometrics combining dynamic voice and face identification. The CWA will operate as a pre-standard which tests the applicability and value of standardization to rapidly changing and highly innovative sectors, that may see standardization as a hindrance to innovation and the topics that come under consideration are often ones in which it is unlikely that full consensus could be achieved in an acceptable timeframe. The CWA process will also be a key process to engage with new stakeholder communities. This process will be launched at the end of year 1 and will be open to other members outside of the consortium.

UCL will lead this work package and will be responsible for the analysis of existing standards and the coordination of the CEN Cenelec workshop agreement. UCL will be supported by OT, HB, TSP.

Deliverables

From task	ID	Name	Lead	Main contributors	Diss. level	Delivery month
9.1	D9.1	Report on published standards	UCL	HB, TSP	PU	12
9.2	D9.2	Compilation of standard contributions	OT	HB, TSP, UCL	PU	36
9.3	D9.3	CEN Cenelec workshop agreement	UCL	OT, HB, TSP	PU	36

Work package nb	10	**Start month**	1						
Work package title	Management									

Participant number	**1**	2	3	4	5	6	7	8	9	10
Short name of participant	**OT**	HB	SIV	TEC	EYE	FNET	IFIN	FORTH	UCL	TSP
Person-months per participant	**24**	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5	1.5

Objectives

To carry out the management, co-ordination and reporting activities necessary to:

- Implement the project management principles described in the Project Management section
- Ensure effective implementation of the project in line with guidelines from the Commission, the Project Contract and the Consortium Agreement.

Description of work

This work package covers the activities of the Project Coordinator (OT) in managing the consortium. Management activities must be adapted to the needs of the project as it evolves, but will include at least:

- Organize communication between the Consortium and the Commission concerning project progress and execution of the Contract.
- Set up and run financial accounting and budget reporting processes within the Consortium, and between the Consortium and the Commission.
- Coordinate progress reporting within the Consortium by Work package Leaders, and between the Coordinator and the Commission (see D10.1– D10.3).
- Monitor the progress of individual work packages, in terms of production of deliverables according to schedule, and other key indicators of progress.
- Continuously monitor significant project risks: identify, assess probability and consequences, and devise mitigation strategies.
- Deal with any conflicts which may arise between project participants (in accordance with the principles defined in the Project Management section
- Propose any modifications in the project plan which might be necessary in the light of experience in actually running the project, or due to factors external to the project. Carry out the formal steps needed to obtain approval by Consortium members and the Commission.
- Constitute and run the project management bodies defined in the Project Management section
- Organize and run Project Reviews.
- Monitor and ensure the gender balance in the consortium
- Ensure compliance with, and manage any changes to, the Consortium Agreement.

OT will be the primary contributor (and leader) of this work package and be responsible for producing the periodic reports and final report. OT will also be in charge of developing the project quality handbook. All other partners will allocate at least 1PM to the management activities required.

Deliverables

From task	ID	Name	Lead	Main contributors	Dissemination level	Delivery month
N/A	D10.1	First Periodic Report	OT	All partners	CO	18
N/A	D10.2	Second Periodic Report	OT	All partners	CO	36
N/A	D10.3	Final (Public) Report	OT	All partners	PU	36
N/A	D10.4	Project Quality Handbook	OT	All partners	CO	3

3.1.4 List of Work Packages

WP No.	Work package Title	Lead No.	Short name	Work package Leader(s)	Total PM	Start Month	End Month
WP 1	Requirement Specifications & Architecture	#3	SIV	Monica Florea	34	1	6
WP 2	Multichannel Biometrics	#2	HB	David Horowitz	110	4	14
WP 3	User Security & Privacy	#4	TEC	Muttukrishnan Rajarajan	72	4	18
WP 4	HCI & Access Management	#8	FORTH	Margherita Antona	96	12	20
WP 5	Biometrics Solution Integration, Portability & Interoperability	#3	SIV	Ionut Arsene	71	16	24
WP 6	Demonstrators & Evaluation	#9	UCL	Hugh Griffiths	67	25	36
WP 7	Dissemination & Ecosystem Development	#10	TSP	Dijana Petrovska-Delacrétaz	40	1	36
WP 8	Exploitation & Scaling Up	#1	OT	Emmanuelle Dottax	51	4	36
WP 9	Standardization	#9	UCL	Clayton Stewart	21	4	36
WP10	Management	#1	OT	Jean-Loup Depinay	37.5	1	36
Total					**599.5**		

Table 19: List of Work Packages

3.1.5 List of deliverables

Table 20 lists all deliverables in chronological order. Table 21 lists (as requested) the formal deliverables in a separate table.

The following numbering scheme is used:

- Dw.t: Indicates that this is a deliverable from work package w, task t.
  Ex: D4.1 is from work package 4, task 1.

- Dw.t.s : Indicates that work package w task t produces several deliverables the final s provides a sequence number.
  Ex: D2.1.1 and D2.1.2 are two deliverables from work package 2, task 1.

The deliverables list is sorted according to delivery date (as required).

No	Name	WP No.	Lead	Type [60]	Dissem. level [61]	Deliv. date
D7.1.1	Internal project repository	WP7	OT		CO	1
D7.1.2	External project website	WP7	OT		PU	2
D1.4	System architecture	WP1	SIV		PU	4
D1.1	Workforce use case specifications	WP1	IFIN		CO	6
D1.2	eHealth use case specifications	WP1	FORTH		CO	6
D1.3	Consumer use case specifications	WP1	FNET		CO	6
D7.2.1	Dissemination plan	WP7	TSP		CO	6
D8.1.1	Exploitation plan - initial	WP8	OT		CO	6
D2.1	Voice acoustics recognition method	WP2	HB		PU	9
D2.2	Face identification method	WP2	HB		PU	10
D2.3	Audio-visual analysis method	WP2	HB		PU	12
D9.1	Report on published standards	WP9	UCL		PU	12
D2.4	Validation report	WP2	UCL		PU	14
D3.1	Enrolment security and privacy implementation report	WP3	TEC		CO	15
D3.2	Speaker recognition security and privacy recognition report	WP3	TEC		CO	15
D3.3	Security and privacy test reports	WP3	TSP		CO	18
D4.1	User physiology impact report	WP4	EYE		PU	18
D4.2	Context-dependent tuning framework	WP4	FORTH		PU	18
D5.1.1	System release v1	WP5	SIV		PU	18
D8.1.2	Exploitation plan - intermediate	WP8	OT		CO	18
D4.3	User interface implementation report	WP4	FORTH		PU	20
D5.1.2	System release v2	WP5	SIV		PU	20
D5.1.3	System release v3	WP5	SIV		PU	24
D5.3	System interoperability report	WP5	SIV		PU	24
D5.4	Test/QA report	WP5	SIV		PU	24
D8.2	Business cases	WP8	OT		PU	24
D6.1	Workforce pilot implementation report	WP6	IFIN		PU	34
D6.2	eHealth pilot implementation report	WP6	FORTH		PU	34

[60] R = Document, Report (excluding periodic and final reports); DEM = Demonstrator, Pilot, Prototype, Plan Designs, DEC= Website, Patent Filing, Press & Media Actions, Video, OTHER: Software, Technical Diagram

[61] PU = Public, fully opne, e.g. web; CO = Confidential, restricted under conditions set out in Model Grant Agreement; CI= Classified, information as referred to in Commission Decision 2001/844/EC

D6.3	Consumer pilot implementation report	WP6	FNET		PU	34
D6.4	Pilot evaluation reports	WP6	UCL		PU	36
D7.2.2	Dissemination report	WP7	TSP		PU	36
D7.3.1	Developer contest report	WP7	OT		PU	36
D7.3.2	Spoofing contest report	WP7	TSP		PU	36
D7.3.3	Ecosystem report	WP7	OT		PU	36
D7.4	Collaboration report	WP7	TSP		PU	36
D8.1.3	Exploitation plan -final	WP8	OT		CO	36
D8.3	IPR registry	WP8	HB		CO	36
D8.4	Reports on industry workshops	WP8	OT		PU	36
D9.2	Compilation of standard contributions	WP9	OT		PU	36
D9.3	CEN Cenelec workshop agreement	WP9	UCL		PU	36

Table 20: Chronological list of project deliverables

No	Name	WP No.	Lead	Type [62]	Dissem. level [63]	Deliv. date
D1.1	First Periodic Report	WP1	OT	R	CO	M18
D1.2	Second Periodic Report	WP1	OT	R	CO	M36
D1.4	Final (Public) Report	WP1	OT	R	PU	M36

Table 21: List of formal project reports

[62] R = Document, Report (excluding periodic and final reports); DEM = Demonstrator, Pilot, Prototype, Plan Designs, DEC= Website, Patent Filing, Press & Media Actions, Video, OTHER: Software, Technical Diagram

[63] PU = Public, fully opne, e.g. web; CO = Confidential, restricted under conditions set out in Model Grant Agreement; CI= Classified, information as referred to in Commission Decision 2001/844/EC

3.2Management structure and procedures

3.2.1 Organizational structure, milestones and decision-making

This project will be carried out by a Consortium of 10 partners from 5 different EU Member States. The project work is divided into 10 work packages. These constitute the work breakdown structure of the project, gathering together the major groups of activities to be carried out. The overall management structure is depicted in Figure 12, with roles and responsibilities identified and summarised below.

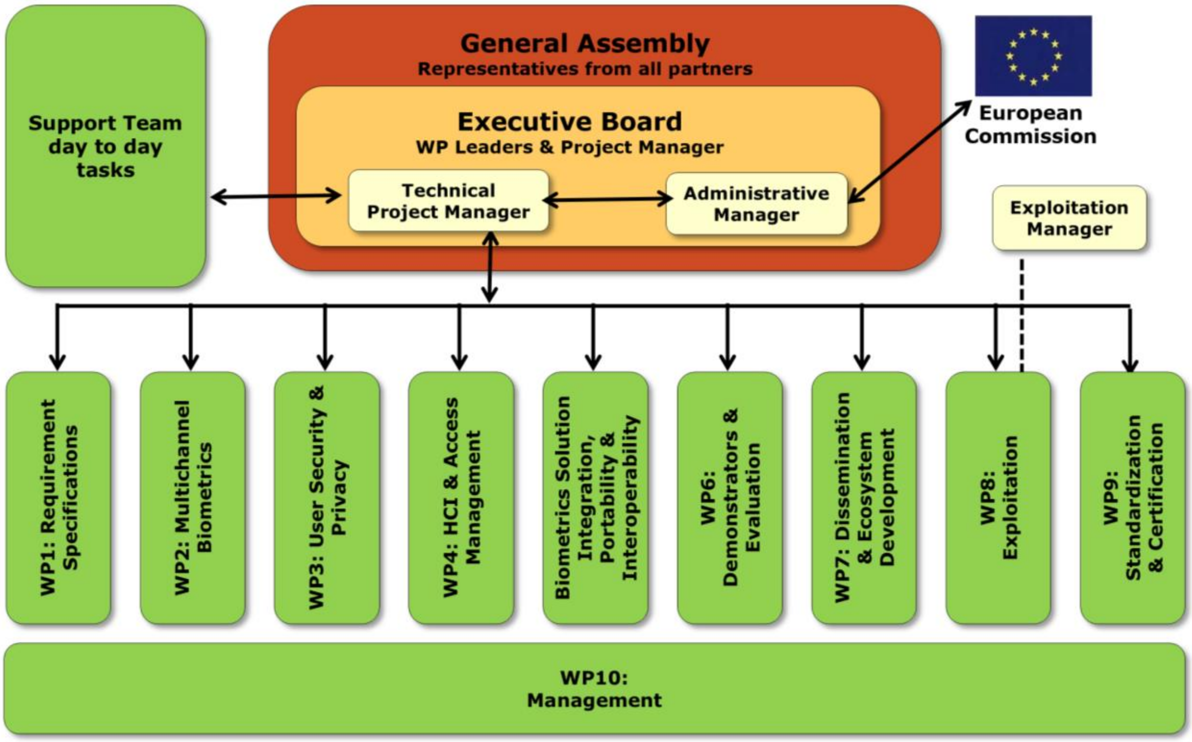

Support Team day to day tasks
General Assembly
Representatives from all partners
Executive Board
WP Leaders & Project Manager
Technical Project Manager
Administrative Manager
European Commission
Exploitation Manager
WP1: Requirement Specifications
WP2: Multichannel Biometrics
WP3: User Security & Privacy
WP4: HCI & Access Management
Biometrics Solution Integration, Portability & Interoperability
WP6: Demonstrators & Evaluation
WP7: Dissemination & Ecosystem Development
WP8: Exploitation
WP9: Standardization & Certification
WP10: Management

Figure 12: Project organizational structure

Milestone number	Milestone name	WP	Leade r	Expected month	Means of verification
MS1	Use cases ready	WP1	SIV	M6	All use cases documented
MS2	Core modules ready	WP2 WP3	HB	M14	Biometrics module ready and validated.
MS3	Solution ready	WP4 WP5 WP6	SIV	M24	All components ready. Solution integration complete. Solution ready for trial deployment.
MS4	Pilots completed	WP7	UCL	M36	All pilots and evaluation reports completed

Table 22: List of project milestones

Decision-making

This section describes the most important mechanisms for reaching decisions (Table 23), in a Consortium with multiple partners, each with their own goals. The general principle will be to try to achieve decisions by informal means and consensus, using formal procedures such as voting only when essential. Nevertheless: *all* decisions which can have an impact on project progress (whether reached formally or not) will be documented, for visibility within the Consortium. Precise details of the remit of the various management bodies, and of voting procedures etc. are carefully defined in the *Consortium Agreement*.

Level	**Decision mechanism**	**Escalate if:**
Project	Verbal consensus only *Meetings*: regular; as needed	No consensus reached
Executive Board	Verbal consensus; vote if necessary Simple majority *Meetings:* Every 12 weeks	One partner insists
General Assembly	Voting mandatory; simple majority. *Meetings:* Every 12 months,	Intervention by the Commission, or legal action, is the only escalation possible; decision on this up to individual partners

Table 23: Decision-making mechanisms

Conflict management

Identification of any conflicts which arise in the project is the responsibility of all project participants. Any signs of disagreement between project participants should be notified to the work package leader or project manager (as appropriate), who should then instigate the conflict resolution procedure, escalating to higher levels only if necessary:

1. The manager should *separately* contact all parties either in person or by *telephone*, to identify the different viewpoints (it is important not to use email: that medium very often leads to a rapid escalation of disagreements). Based on a clarification of viewpoints, the manager should try to propose a solution. If one is achieved, it should be recorded in a short report; if not, no documents should be produced, and the problem escalated.
2. If level 1 fails, the matter should be taken up by the Executive Board (at a special meeting, if need be). At this level, all work should be in writing. If conflicts relate to matters which would normally be assessed as part of the annual reviews by the Commission, the views of the Commission should be sought.
3. If level 2 fails, a special meeting of the General Assembly should be called. Partner representatives will then be required to vote on the issue.

Project re-planning and change management

In an ambitious and dynamic project of this kind, changes to customer requirements are expected and will generate changes to the project plans. Handling changes in project plans will therefore be regarded as a normal part of project management, to be carried out without undue formalities.

Project progress will be continuously monitored, and where discrepancies between plans and progress are observed (or predicted), corrective actions will be initiated. In particular, the Executive Board will carry out *risk assessment* at their regular meetings. This involves identifying project risks and assessing their probability and the nature of the consequences should the risk be incurred. If the risk level is judged to be high, changes in project planning may be necessary. A set of project risks has already been identified (see Section 3.2.3). It will serve as the basis for risk assessment at the first meeting of the Executive Board, and will be continuously updated thereafter.

Decisions on any necessary re-planning of detailed tasks at the *work package level* will be made by the Work Package Leader, in consultation with all partners involved in the work package. Results should be reported to the Project Coordinator. *Project level* changes will be the responsibility of the Executive Board (except in the case of *major* changes). In addition to any reviews arising from regular risk assessment, the detailed project plan will be reviewed at least once per year, and revised if necessary. Certain types of re-planning may require the approval of the Commission, according to the terms of the *Grant Agreement*. It will be the responsibility of the Project Coordinator to contact the Commission regarding the matters.

Project re-planning which results in changes deemed to be *major* must be handled by the General Assembly, using voting procedures. Changes will be deemed to be major if any one partner protests about a proposed change, or automatically if the change involves:

- Modifications to the Consortium Agreement or to the management structures and principles
- Problems with the performance of any partner, or partner request to leave the Consortium
- Re-allocation of budget between work packages and/or partners

Implementation of major changes may necessitate a change in the overall project plan, detailed project plans or the work breakdown structure of the project. As explained above, the management structure of the project essentially follows the work breakdown structure of the project. The management structure can therefore adapt to changes in the work breakdown structure.

Innovation management

Innovation management is a process which requires an understanding of both market and the technical problems of the project, with a goal of successfully implementing appropriate creative ideas. The consortium will establish a task force to be led by WP9 Leader on innovation management with the duties below:

- Monitor and collect market needs and customer requirements on resource-efficient machining solutions
- Observe additional added-value which may be created during the project implementation.
- Identify any mismatch between the project values and market/customer needs.
- Bring necessary attentions to the Executive Board for decisions so as to respond to an external or internal opportunity.
- Implement the decisions into exploitation activities to seize the opportunity.

The innovation management of the project is both combined with the exploitation activities such as the 4 industry specific workshops, and scheduled as a standing agenda item of the regular Executive Board meetings. The consortium consists of both end-users and suppliers who will be actively involved in this task force of innovation management.

Quality assurance

The project will employ the following mechanisms for quality assurance in the project:

- A *Project Quality Handbook*, derived from experience in earlier projects, customized for this project and updated as required.
- Feedback from annual Commission reviews. Project management will foster an attitude where these reviews are treated as part of the project's QA, rather than as an adversarial assessment.

3.2.2 Management bodies and management skills within the project

Level	Management Body	Composition	Principal Responsibilities
WP	WP leader	One person, from partner leading the WP.	• Co-ordinate and report on progress of detailed work in the WP.
Project	Executive Board	Leaders + Project Manager.	• Make strategic decisions concerning project co-ordination, direction, and overall management and planning. • Project Risk Management.
	Project Management Team	Project Manager + Support Team (see details below).	• Implement decisions of the executive board and general assembly. • Assist all other management bodies. • Overall day-to-day project management.
	General Assembly	One representative of each partner.	• Strategic decisions on major changes. • Resolution of any major conflicts.

Table 24: Project governance bodies

OT will have the role of *coordinator* and have overall responsibility for management of the project, and for all liaisons with the Commission. OT has already been involved in a number of R&I projects under the national or EC frameworks, either as coordinator or contributor (Table 25).

Project acronym	Description	RTD programme	Role
IDEA4SWIFT	Automatic Border Control for Frequent Traveler	ITEA3	coordinator
SIMPATIC	Anonymous security function implementation on mobile	ANR (FR)	partner
LYRICS	Anonymous security function design	ANR (FR)	partner
MAS	Nanoelectronics for eHealth	ENIAC	partner

Table 25: Coordinator project experience

The administrative manager of SpeechXRays will be Jean-Loup Dépinay who has been involved in FP6 and FP7 EC-funded projects where he has been leading and managing several research work packages. The technical project manager of SpeechXRays will be David Horowitz from Horowitz Biometrics, who has vast domain experience in the field of biometrics in particular, and security and identity in general. Jean-Loup Dépinay and David Horowitz will be assisted by a support team, so they can concentrate on the real content of the tasks. The duties of the support team will include:

- Follow-up: check that progress reports, deliverables etc. are produced according to plan; alert the relevant managerial bodies to any discrepancies which arise.
- Advise project participants on the details of administrative and other data required in reports.
- Take care of all practical arrangements in connection with arrangements for meetings etc.
- Maintain an electronic infrastructure for ease of communication within the Consortium, and for controlled, shared access to project documents.

3.2.3 Risk management

This project implementation plan, produced at the start of the project, is subject to revision in the course of the project, in accordance with the procedures for project re-planning outlined in this section.

One of the main reasons that project re-planning may be necessary is as a result of regular risk assessment in the project (Figure 13). The initial list of risks here presented in Table 26 is a start to this process; more detailed assessment of risks will be carried out regularly, based on practical experiences in running the project.

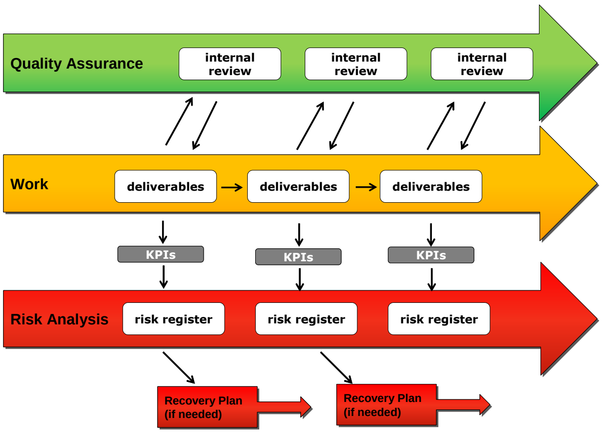


Figure 13: Risk management process

<table>
<tr><th colspan="7">Risks</th></tr>
<tr><th>Cat.</th><th>Code</th><th>Description</th><th>WP involved</th><th>Prob 1-10</th><th>Severity 1-10</th><th>Milestone concerned</th></tr>
<tr><td><b>Mgt</b></td><td><b>R1</b></td><td>A pilot is not completed, because of lack of resources and/or personnel changes at a project partner.</td><td>WP6</td><td>4</td><td>8</td><td>MS4</td></tr>
<tr><td colspan="7"><i>The coordinator will use the mechanisms described in section 2.1.8 and raise the issue urgently with the management in the partner organization, as losing one of the industrial pilot projects may decrease the quality of the outcome of the project. If no alternative pilot can be found within the company, in consultation with the commission, the consortium will consider whether a replacement partner (and pilot) can be sought.</i></td></tr>
<tr><td><b>Mgt</b></td><td><b>R2</b></td><td>A research, industrial or software development partner exits the consortium.</td><td>WP10</td><td>2</td><td>8</td><td>MS1</td></tr>
<tr><td colspan="7"><i>As the consortium was carefully assembled to represent complementary skills and expertise, exit of one of the partners would be a serious setback. Project management will undertake immediate acquisition actions to find a replacement partner. Potential candidates have been already been discussed as part of contingency planning.</i></td></tr>
<tr><td><b>Tech</b></td><td><b>R3</b></td><td>Insufficient performance of voice acoustic-driven recognition models</td><td>WP2</td><td>3</td><td>8</td><td>MS2</td></tr>
<tr><td colspan="7"><i>If the voice acoustic-driven models do not deliver the performance observed in the lab, they will be complemented by classical statistical methods (e.g. GMM) and possibly, text-dependent approaches. The combination of acoustic-driven and classical methods will still deliver marked improvements, notably in terms of usability (low sensitivity to surrounding noise).</i></td></tr>
<tr><td><b>Tech</b></td><td><b>R4</b></td><td>The results of the demonstrators are not as previously envisioned.</td><td>WP6</td><td>4</td><td>7</td><td>MS4</td></tr>
<tr><td colspan="7"><i>The requirements established early in the project should provide guidance on biometrics implementation strategy. The development of the pilots will be monitored throughout the project to ensure that decisions that may have a negative impact on the project outcome are registered and discussed, and where possible, amended.</i></td></tr>
<tr><td><b>Tech</b></td><td><b>R5</b></td><td>Solution too complex to be scaled up in real-life settings. This would severely limit the uptake of the project’s results.</td><td>WP6
WP7
WP8</td><td>2</td><td>9</td><td>MS4</td></tr>
<tr><td colspan="7"><i>The partners will monitor the development of the platform continuously, to detect industrialization problems in an early phase. The experience of the partners X and Y with the development of successful commercial solutions will minimise this risk.</i></td></tr>
<tr><td><b>Tech</b></td><td><b>R6</b></td><td>Launch of a similar concept by third parties</td><td>WP9</td><td>2</td><td>5</td><td>MS3-MS4</td></tr>
<tr><td colspan="7"><i>The project partners are well networked and will be aware of similar developments in time to discuss potential collaboration or explore other synergies with third parties. Nevertheless, the partners will continuously screen the market and should an unexpected development occur, will adapt their exploitation plans as needed.</i></td></tr>
</table>

Table 26: Preliminary risk register

3.3 Consortium as a whole

The consortium was formed to put together a group of 10 organisations that complement each other in terms of background knowledge, technical competence, capability of new knowledge creation, business and market experience, and expertise in end-user domains where the project technologies and innovations can be readily exploited. The consortium consists of academic/research organisations, technology suppliers and end-users (Table 27). The partners have been selected that they can contribute most effectively to different work packages. The most competent partner in the core area of each work package has been chosen as the WP Leader, taking the geographical distribution of the partners into account.

Most partners also possess extensive knowledge and hands-on experience regarding the dissemination and exploitation of the project results:

- FORTH, UCL, TSP have experience using Open Access (e.g. deposit of peer-reviewed articles in the OpenAIRE repository, https://www.openaire.eu/) for wide dissemination of project results.
- OT, HB, SIV are experienced in industry-oriented research and technology development at TRL 6-8 Moreover, they all possess time-tested experience of commercialisation.
- OT has worldwide customers that can reach to the target industries globally for exploitation of the project results.
- OT, via its corporate communication team, has a strong project exploitation capability through face to face contact at presentations, industrial seminars and trade shows.

Category	**Partner Name**	**Profile**	**Main Roles**
Research	FORTH	Leading Greek research institute with expertise in Human Computer Interaction	WP4 Leader
	UCL	British university with expertise in image/video coding and signal processing	WP6 and WP9 Leader
	TSP	French research institute with expertise in biometrics and anti-spoofing	WP7 Leader WP2 and WP3 Support
Industrial Suppliers	OT	World leader in digital security solutions for the mobility space serving 5,000 banks, 300 mobile operators and more than 100 governments	Coordinator (WP10) Exploitation Manager (WP8)
	HB	British SME, early leader in acoustic driven voice feature based biometrics	WP2 Leader Technical Project Leader
	SIV	Romanian system integrator with an extensive EC project track record	WP1 and WP5 Leader
	TEC	British SME consultancy with expertise in IT security and privacy	WP3 Leader
	EYE	Estonian SME specialized in emotion recognition based on face video analysis	WP2 and WP4 Support
Industrial End users	FNET	Leading Greek triple-play ISP with over 1M customers	Consumer Pilot Leader
	IFIN	Romanian nuclear physics research centre	Workforce Pilot Leader
	FORTH	Leading Greek research institute serving as end-user with it Computational Medicine Lab	eHealth Pilot Leader

Table 27: Partner list

Table 28 highlight the complementarity and interdisciplinarity of the consortium

Skill/expertise/technology	**OBE**	**HB**	**SIV**	**TEC**	**EYE**	**FNET**	**IFIN**	**FORTH**	**UCL**	**TSP**
Acoustics		**X**							**X**	
Emotion recognition					**X**			**X**		
Signal processing		**X**							**X**	
Voice recognition	**X**	**X**							**X**	
Face recognition	**X**	**X**			**X**			**X**	**X**	**X**
Audio-visual analysis		**X**								**X**
Anti-spoofing										**X**
Revocable biometrics				**X**						**X**
Cryptobiometrics				**X**					**X**	
Privacy-preserving mechanisms	**X**			**X**					**X**	
Secure mobile applications	**X**									
Workforce applications			**X**				**X**			
eHealth applications			**X**					**X**		
Consumer applications					**X**	**X**				

Table 28: Illustration of the interdisciplinary character of the consortium

3.4 Resources to be committed

The allocation of person-month effort amongst the partners is summarised in Table 29, according to their responsibilities and the resources estimated for achieving their assigned tasks. The staff effort in each WP is estimated based on the complexity of the tasks, complementarity of partner skills, inter-WP relationships and integration schedule between WPs. Project risk **R2** on "a research, industrial or software development partner exits the consortium" (Section 3.2.3) has been taken into account when assigning partners to WPs so that no single WP or task will be left incomplete. The overall effort of the project is **599.5 person months** over the 4 project years. The details of cost allocation per partner are summarised in Table 30.

Nb	Short name	WP1	WP2	WP3	WP4	WP5	WP6	WP7	WP8	WP9	WP10	Total person months
1	OT	4	22	2		4	3	16	24	5	24	**104.0**
2	HB		48	18	18	4		4	12	3	1.5	**108.5**
3	SIV	12			15	55	9	2	2		1.5	**96.5**
4	TEC			35	14	4		2	2		1.5	**58.5**
5	EYE		12		19			2	2		1.5	**36.5**
6	FNET	6		5			17	1	2		1.5	**32.5**
7	IFIN	4		2			10	1	1		1.5	**19.5**
8	FORTH	4		2	30	4	10	2	2		1.5	**55.5**
9	UCL		14				18	2	2	10	1.5	**47.5**
10	TSP	4	14	8				8	2	3	1.5	**40.5**
Total		**34**	**110**	**72**	**96**	**71**	**67**	**40**	**51**	**21**	**37.5**	**599.5**

Table 29: Project effort breakdown by workpackage and partner

Effort and Cost Allocation per Partner (Euros)										
	Effort		Costs							
Partner	Total person-months	Partner share of the total effort	**Direct cost of one person-month**	Direct personnel costs	Travel, equipment & other direct costs	Indirect costs	Sub-contracting	**Total costs**	Partner share of the budget	EC contri-bution
OT	104	17%	**8,350**	868,400	44,000	228,100	-	**1,140,500**	21%	798,350
HB	109	18%	**8,000**	868,000	39,000	226,750	-	**1,133,750**	21%	793,625
SIV	97	16%	**5,000**	482,500	52,715	133,804	-	**669,019**	13%	468,313
TEC	59	10%	**6,500**	380,250	50,500	107,688	-	**538,438**	10%	376,906
EYE	37	6%	**6,500**	237,250	39,000	69,063	-	**345,313**	6%	241,719
FNET	33	5%	**5,500**	178,750	36,000	53,688	-	**268,438**	5%	187,906
IFIN	20	3%	**4,500**	87,750	23,000	27,688	-	**138,438**	3%	138,438
FORTH	56	9%	**4,000**	222,000	21,000	60,750	-	**303,750**	6%	303,750
UCL	48	8%	**5,072**	240,920	21,000	65,480	50,000	**377,400**	7%	377,400
TSP	41	7%	**7,700**	311,850	21,000	83,213	-	**416,063**	8%	416,063
TOTAL	599.5	100%		3,877,670	347,215	1,056,221	50,000	**5,331,106**		4,102,469
% by cat				72.74%	6.51%	19.81%	0.94%		SME	29%

Table 30: Project effort breakdown by cost type and partner

The resources are described in the following main categories:

- *Direct personnel cost.*
- *Other direct cost.* This category includes travel, equipment and other goods and services.
  - Travel budget is reserved for each partner to attend project meetings, workshops, setting up demonstrators, and other dissemination and exploitation events over the 3-year project period. The average expense for one 3-day trip in Europe costs has been estimated between 1500 and 1750 Euros depending on the partner with 4 person-trips per year for a regular partner, 6 person-trips per year for a WP leader and 8 person-trips per year for the coordinator.
  - A equipment budget between 5,000 and 25,000 Euros has been allocated to partners for sourcing hardware and software equipment required (additional details are provided in Table 31 when “other direct cost” exceed 15% of the “personnel cost”)
  - A budget of 15,000 Euros has been reserved to FNET to purchase small gifts that will be given to FNET users involved in the pilot (although the unit cost of the gift is small – 15 Euros per user for 1000 users, it will be sufficient to get people motivated to try the new authentication service)
  - A budget of 3000 Euros for the financial audit is are reserved for those partners whose requested fund from EU is over 325,000 Euros.
- *Sub-contracting:* A subcontracting budget of 50,000 Euros has been allocated to UCL for CEN CENELEC, in order to support the CEN CENELEC Workshop Agreement.

Finally, Table 31 shows other direct costs and provides specific details when they exceed 15% of the personnel costs (as per H2020 rules).

Partner	Equipment	Travel	Other	Sub contracting	Comments for other costs >15%
OBE	5,000	36,000	3,000		
HB		36,000	3,000		
SIV	22,715	27,000	3,000		
TEC	16,000	31,500	3,000		
EYE	18,000	21,000			12 trips @1750 EUR, cloud computing capacity for emotion analysis computation @0.5k EUR per month for 36 months
FNET		21,000	15,000		12 trips @1750 EUR, corporate gifts for trial users @15 EUR per unit
IFIN	5,000	18,000			12 trips @1500 EUR, equipment required for physical access control trial (secure door @4500 EUR + embedded tablet/camera @500 EUR)
FORTH		21,000			
UCL		18,000	3,000	50,000	
TSP		18,000	3,000		
Total	**66,715**	**247,500**	**33,000**	**50,000**	

Table 31: Other cost breakdown by partner

4 Members of the Consortium

Nb	Acronym	Participant legal name	Type	Country
#1	OT	Oberthur Technologies	Industrial	France
#2	HB	Horowitz Biometrics	Industrial/SME	UK
#3	SIV	SIVECO	Industrial	Romania
#4	TEC	Tech Inspire	Industrial/SME	UK
#5	EYE	RealEyes OÜ	Industrial/SME	Estonia
#6	FNET	FORTHNET	Industrial	Greece
#7	IFIN	IFIN-HH	Research	Romania
#8	FORTH	Foundation for Research and Technology - Hellas	Research	Greece
#9	UCL	University College London	Academic	UK
#10	TSP	Institut Mines-Telecom / Telecom SudParis	Academic	France

Partner 1: Oberthur Technologies SA (OT)

The organization

OT is a world leader in digital security solutions for the mobility space. OT has always been at the heart of mobility, from the first smart cards to the latest contactless payment technologies which equip millions of smartphones. Present in the Payment, Telecommunications and Identity markets, OT offers end-to-end solutions in the Smart Transactions, Mobile Financial Services, Machine-to-Machine, Digital Identity and Transport & Access Control fields. With 6000 collaborators worldwide, OT is a recognized and highly regarded global leader in digital security solutions.

Relevant skills/experience/technologies

OT has technical expertise in the development of embedded secure software, secure devices and identity documents, and associated server based solution operated by clients in-house or in managed services. OT brings a unique industry positioning serving 5,000 banks, 300 mobile operators and more than 100 goverments. OT's new initiative "My Voice is My Password", recently launched at the Mobile World Congress 2014, will be one of the key exploitation tracks for the SpeechXRays project.

Role in the project

OT is the project coordinator and will lead WP8 Exploitation & Scaling Up and WP10 Management

Key personnel

Jean-Loup Dépinay (M) is program manager in charge of the collaborative R&D projects of Oberthur Technologies and he has coordinated or participated to 15 projects funded by French or European programs (FUI, ANR, Eniac...) As Java Card OpenPlatform Architect, he has architected and managed several Java Card platforms which have been deployed worldwide. He was also responsible for developing Java Card security improvements. Mr. Dépinay is currently a member of the Java Card Forum. Mr. Dépinay has been an active participant in the GlobalPlatform Card Committee since the very beginning of GlobalPlatform and was elected to the Board of Directors in 2008

Emmanuelle Dottax (F) has been working in the field of cryptography and secure implementations for more than ten years. She holds a MSc in Cryptography and Discrete Mathematics, and was first involved in the NESSIE European project with Ecole Normale Supérieure, where she took an interest in embedded implementations and physical attacks. She then continued studying security of implementations as a member of the Security Team of Morpho. She has been managing the Crypto Group of Oberthur Technologies for 5 years before becoming a Security Architect. She holds a strong expertise in embedded security, cryptographic protocols and implementation of cryptographic algorithms. She has published several scientific papers in international conferences and is co-inventor of more than 20 patents

Nicolas Bousquet (M) has been working for 7 years for smart card industry in software design and development. In Oberthur Technologies, he is an embedded developer engineer. He has been involved in the development of Java Card 3.0 Connected Edition, and participated to the definition of its specification. He also handles internals projects such as prototyping innovative devices. He is now involved in mobile security dealing with emerging technologies such as Trusted Execution Environment. He participated to some funded collaborative projects closely linked to Java Card: Inspired, Mecanos, and is currently involved VEADISTA funded projects.

Relevant publications/patents/products/services

OT Digital Identity Solutions: with more than 100 customer applications worldwide, backed by extensive experience of smart card production and high-security printing, OT offers a broad range of identity solutions for all types of traditional and electronic document, from passports and national identity cards to driving licences, access badges, health cards, residency permits and visas. OT envisions and designs the products for tomorrow’s identity market: simpler and more secure for users, these identity documents are developed in response to the needs and expectations of citizens for mobility and data protection.
Dottax, E., Giraud, C., Rivain, M., & Sierra, Y. (2009). On second-order fault analysis resistance for CRT-RSA implementations. In Information Security Theory and Practice. Smart Devices, Pervasive Systems, and Ubiquitous Networks (pp. 68-83). Springer Berlin Heidelberg.
Rivain, M., **Dottax, E.,** & Prouff, E. (2008, January). Block ciphers implementations provably secure against second order side channel analysis. In Fast Software Encryption (pp. 127-143). Springer Berlin Heidelberg.
Bringer, J., Chabanne, H., & **Dottax, E.** (2006, June). HB^+^+: a Lightweight Authentication Protocol Secure against Some Attacks. In Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2006. SecPerU 2006. Second International Workshop on (pp. 28-33). IEEE.
Dottax, E. (2002). Fault attacks on NESSIE signature and identification schemes. Public report, NESSIE, 284-285.

Relevant research projects
IDEA4SWIFT is and ITEA3 project focusing on identity management, secure documents, interoperable exchange and citizens authentication for worldwide interconnection of frequent travellers.
SIMPATIC is a national French research project funded by ANR providing the most possible efficient and secure hardware/software implementation of a bilinear pairing in a SIM card.
LYRICS is a national French research project funded by ANR focusing on lightweight privacy-enhancing cryptography for mobile contactless services.
MAS is an ENIAC project developing a secure communication platform and nanoelectronics circuits for health and wellness applications to support the development of flexible, robust, safe and inexpensive mobile AAL systems, to improve the quality of human life and improve the well-being of people.

Existing infrastructure
OT has 50+ sales offices and 35+ service centers, supported by 10 R&D centers.

Does the participant plan to subcontract certain tasks	N
Does the participant envisage that part of its work is performed by linked third parties	N
Does the participant envisage the use of contributions in kind provided by third parties	N

Partner 2: Horowitz Biometrics (HB)

HOROWITZ
BIOMETRICS

The organization

Horowitz Biometrics is an early leader in acoustic driven voice feature based biometrics. The voice biometrics technology is based on 20 years of research and development. The unique solutions are a ground-breaking development of voice acoustic analysis for user authentication and identification within a flexible multichannel framework. The unique proposition provides reliable and state of the art biometric solutions enhancing user experience and solving the identity assurance crisis. The company’s mission is to harness the power of voice acoustics to transform the voice biometrics technology.

Relevant skills/experience/technologies

The team has with strong technical expertise and research and development experience with background in voice technologies, and specifically speaker identification and automatic speech recognition. The company has also directed several research projects in the field of voice biometrics, such as VoiceID, a project funded by the US Office of Naval Research (ONR), during which the company was able to mature the technologies used in SpeechXRays from TRL3 to TRL6.

Role in the project

Horowitz Biometrics is the technical project leader and will lead WP2 Multichannel Biometrics

Key personnel

Dr David Horowitz (M), Founder and CTO, has led a career as a C-Level Manager, Entrepreneur and Scientist. He is an industry expert in multi-channel biometrics, voice identification (speaker recognition), conversational personal assistants and biometrics solutions architecture. Dr. Horowitz has worked with U.K. start-up companies on the full product development life cycle. He has been instrumental helping companies transform their ideas and concepts into usable technology and working deployed products. As a scientist, Dr. Horowitz is an often cited leader in the field of Artificial Intelligence methods based on Brain Science and Cognition; as well as the human perception of sound, acoustics and signal processing.
He has won the approval of $26M of contracts for auditory cognition and computer science research, including €6.3M from the European Union in 2001. His research in voice biometrics began while he was a graduate student at the Massachusetts Institute of Technology (M.I.T.) where he held several roles over nearly a 9 year period. Dr. Horowitz is the author of 28 first rate peer reviewed publications and either the principal or co-inventor of 9 patents (8 awarded; one pending).

Dr. Hari Krishna Maganti (M), CIO, brings over 15 years of technical expertise and experience in voice technologies. Prior to Horowitz Biometrics, Hari has been responsible for leading the development of S-voice (Samsung personal voice assistant) at Samsung Electronics. He had been a active researcher engaged in four major EC projects working across premier research institutes in the world including the Indian Institute of Science (Bangalore, India), the IDIAP Research Institute (Switzerland), University of Ulm (Germany) and Fondazione Bruno Kessler (Italy) resulting in several international patents, publications including a best paper award. He is an active member of IEEE, IETE, CMI and program committee member and reviewer of several international conferences and journals. Hari has excellent industry experience which includes working across different application domains and significant contributions in the areas of algorithm design, software development and hardware implementation. His strong technical and management skills enable him to drive a strong product development lifecycle, including design, implementation, integration, and testing on various platforms.

Dr Gérard Chollet (M), CSO, studied Linguistics, Electrical Engineering and Computer Science at the University of California, Santa Barbara where he was granted a PhD in Computer Science and Linguistics. He taught at Memphis State University and University of Florida before joining CNRS. In 1981, he was asked to take in charge the speech research group of Alcatel. In 1983, he joined a newly created CNRS research unit at ENST. The group contributed to a number of European projects such as SAM, ARS, FreeTel as well as national projects. In 1992, he was asked to participate to the development of IDIAP, a new research laboratory of the `Fondation Dalle Molle' in Martigny, Switzerland. IDIAP contributed to SpeechDat, M2VTS and other European projects. From 1996 to 2012, he was full time at ENST, managing research projects and supervising doctoral work. Funding was secured from such projects as Eureka-Majordome and MajorCall, NoE-BioSecure, Strep-SecurePhone, IP-Companion@ble, AAL-vAssist, FET-ILHAIRE. CNRS decided in july 2012 to grant him an emeritus status. He has supervised over forty doctoral thesis.

Relevant publications/patents/products/services
“The Quantal Speech Recogniser”, Sole Inventor, **Horowitz, D.M.** (May 22, 2011) – pending.
Hueber, T., Benaroya, E. L., **Chollet, G.,** Denby, B., Dreyfus, G., & Stone, M. (2010). Development of a silent speech interface driven by ultrasound and optical images of the tongue and lips. Speech Communication, 52(4), 288-300.
Horowitz, D.M. and Hodges, J.: Short Proceedings and Monograph **-** Towards a Research Agenda for the Next Decade on Speech and Multimodality. July, 2007. This project involves an international workshop and a survey of the current state of the art in multimodal technology and speech recognition.
Koreman, J., A. C. Morris, D. Wu, S. Jassim, H. Sellahewa, J. Ehlers, **G. Chollet** et al. "Multi-modal biometric authentication on the SecurePhone PDA." (2006).
“Automatic prosody markup for TTS”, Co-Inventor **Horowitz, D.M.**, Vox Generation Ltd, July, 2001. Applies traditional speech science (formant bandwidth and open quotient) as well as Natural Language Processing (word chunking, ToBI tone prediction at phrase boundaries).

Relevant research projects
VoiceID: an early stage research project funded by the **US Office of Naval Research** focusing on Human Identity Verification from Voice Identification based upon the Individual Characteristics of the Human Vocal Tract.

Existing infrastructure
IT infrastructure including hardware workstations and software licenses required for software development.

Does the participant plan to subcontract certain tasks	N
Does the participant envisage that part of its work is performed by linked third parties	N
Does the participant envisage the use of contributions in kind provided by third parties	N

Partner 3: SIVECO Romania SA (SIV)	SIVECO Project: Progress™

The organization

SIVECO Romania SA is a private shareholder company, established in 1992, with over 1000 employees, located in Bucharest, Romania. During its twenty years of existence, SIVECO has become one of the most important Romanian providers and software integrators of Enterprise Resource Management License and Maintenance, eLearning, eGovernment, eHealth, eBusiness, eAgriculture, eCustoms solutions and turnkey projects acting both on the internal and international markets. Moreover, SIVECO has gained a solid reputation on international markets by developing successful projects together with several international companies, collaboration that has blossomed into genuine partnership over the years. SIVECO provides all services on the whole life cycle of the information projects: analysis of users' requirements, design, development, testing, implementation, end-users training and technical assistance, system maintenance. SIVECO has developed and currently are running some of the largest and most complex, national-wide information systems in Romania, in different domains: Education, Agriculture, Health Insurance, Customs, Nuclear and Social Security. Throughout the time, the company's activity and the solutions developed have been awarded with over 180 national and international prizes.

Relevant skills/experience/technologies

SIVECO Romania SA offers a new approach in computer based education for both educational and enterprise sectors, by leveraging the power and flexibility of its eLearning solutions. Their successful references include very complex projects, as for example, the introduction of the AeL eLearning platform in the Romanian pre-university education; providing an integrated information system for large national companies, etc. SIVECO is also a member of Health Level Seven, that is one of several American National Standards Institute (ANSI) - accredited Standards Developing Organizations (SDOs) operating in the healthcare arena. SIVECO has developed and implemented solutions for large government customers: The National Health Insurance House (CNAS) in Romania; The Ministry of Health in Bulgaria; Nepenthes Group France; The Ministry of Health in Croatia (HZZO).

Role in the project

SIVECO will lead WP1 Requirement Specifications & Architecture and WP5 Biometrics Solution Integration, Portability & Interoperability

Key personnel

Ms. Monica FLOREA, PhD (F) currently acts as Head of the European Projects Department and has been leading SIVECO participation in FP6 projects (ALIS, LD-CAST, P. Cezanne), FP7 (TERENCE, Eurocancercoms), ITEA2 (GUARANTEE; TWIRL) and LLP (RENOVA, COMAVET). Her duties include the coordination of SIVECO projects co-financed by European Commission and collaboration with national and international bodies in the framework of European Union programs. She has two degrees from University "Al.I Cuza" of Iasi, Computer Science and Finance and Banks, an MSc - University Aix Marseille II and a PMP certification. She is coordinating the NESSI Romania initiative. She is also Project Manager in many European projects, responsible for the management, Quality Assurance and Risk Management Strategy.

Prof. univ. Traian IONESCU (M) is currently a Research and Development Manager and CEO's Adviser in SIVECO Romania. He holds a Ph.D. in Systems Science. His professional experience is covering the fields of eSecurity, eHealth, and eLearning. He demonstrates a high level of expertise in security of information and person, based on biometric characteristics (algorithms for optimising the relation between False Acception Rate (FAR) and False Rejection Rate, depending on the application type) and also in the production and management of passports and drivers licenses (CTO in projects for Ethiopia and The Ivory Coast). He has collaborated with The Ministry of Defence from Israel by developing and implementing a monitoring surveillance systems for flying objects and also for increasing the security in high sensitive areas (i.e. Tel Aviv diamond stock exchange). He has also collaborated with International Aviation Safety Assessment Program – IASA in the field of security boarding pass. He has high teaching and research qualification, having more than 20 years experience of working as a research

manager. He has chaired the Department of Control and Industrial Informatics, Faculty of Control and Computer Science, UPB, for 18 years (from 1990 till 2008). He has also occupied the position of project team member in over 60 research projects, and Project Manager in most of them (around 50). He has been involved in many national and European R&D projects developed by SIVECO, such as Linked2Safety– A Next Generation, Secure Linked Data Medical Information Space For Semantically – Interconnecting Electronic Health Records and Clinical Trials Systems Advancing Patients Safety in Clinical research (FP7), ASPECT (ICT PSP), EduTubePlus (ICT PSP), RENOVA (LLP).
Ionut ARSENE (M) is currently Project Manager for Customized Applications Department. He has a Diploma of Engineer in Biotechnical and Ecological systems from the Faculty of Engineering of Biotechnical Systems – University “Politehnica” Bucharest, a Master Diploma in Machines Structure and Integration from the Faculty of Engineering and Management of Technological Systems – University “Politehnica” Bucharest, and a Long Postgraduate Ph.D. from the Faculty of Engineering of Biotechnical Systems – University “Politehnica” Bucharest. He also attended many training courses like: “Business process modelling, analysis and design”, “Business Analysis”, “Presentation Skills”, “Project Management Basics and Advanced Seminar”. His main activities and responsabilities include coordinating of implementation projects for SIVADOC product - Document management system and workflow, programming / developing, consultancy, technical assistance and maintenance services for software applications and web design and programming.

Relevant publications/patents/products/services
Anca Daniela Ionita, Monica Florea, and Lucian Jelea. Correspondence between Multiple Views in a SOA Trans-National Business System, Proceedings of the World Congress on Engineering. Vol. 1, pp. 493-498, 2009.
Anca Daniela Ionita, Alessandra Catapano, Stelian Giuroiu and Monica Florea. Service oriented system for business cooperation, Proceedings of the 2nd International Workshop on Systems Development in SOA Environments, ACM Press, pp13-18, 2008
Lloyd Kamara, Brendan Neville, Jeremy Pitt and Daniel Ramirez-Cano, Rares Chiriacescu, Liliana Dobrica, Monica Florea and Alexandru Szoke. Regulatory Compliance and Alternative Dispute Resolution in e-Societies. IADIS International Conference e-Society, pp321-328, 2008.
Alexandru Szoke, Sorin Portase, Rares Chiriacescu and Monica Florea. Web Service Execution and Monitoring in Integrated Applications in Support of Business Communities (SEMA2B), Proceedings of the 17th International Conference on Information Systems Development, Paphos, Cypru, pp48-50 (ISD 2008).

Relevant research projects
Linked2Safety (FP7-HEALTH) A Next-Generation, Secure Linked Data Medical Information Space For Semantically- Interconnecting Electronic Health Records and Clinical Trials Systems Advancing Patients Safety In Clinical Research.

Existing infrastructure
SC SIVECO Romania SA has a strong ICT Research Infrastructure: a network and optical fiber high speed Internet connection, a data centre (routing servers, storage servers, database servers), network infrastructure and wireless transmission systems, desktop PCs (Intel®CoreTM i3-3240 3.40GHz, 4GB, 1TB, nVidia GeForce GT620 2GB, Free DOS), laptops (HP EliteBook 8540w, Intel Core i7: i7-620M / 2.66 GHz, 8GB RAM DDR3, 500GB HDD / 7200rpm, 1GB Nvidia Quadra FX 1800M).

Does the participant plan to subcontract certain tasks	N
Does the participant envisage that part of its work is performed by linked third parties	N
Does the participant envisage the use of contributions in kind provided by third parties	N

Partner 4: Tech Inspire Ltd (TEC)

Tech Inspire
Inspire for innovation

The organization

Tech Inspire offer technical support in both Engineering and Information Technology (IT) disciplines on the basis of short projects (consultancy) and longer term research collaboration. The experience gained by our team; working actively in a wide range of research and commercialisation projects in the last fifteen years and jointly with key industries and research organisations, is the main asset of our business.

Currently, Tech Inspire employs six researchers from different computer science backgrounds focusing mainly on the security and privacy aspects of information infrastructure, mobile computing and Cloud computing. The researchers are internationally known in the area of identity management and privacy preserving data classification in the encrypted domain. The company has recently been focusing on developing novel techniques for mobile phone user authentication based on the mobile behavioural attributes. The researchers are also actively using novel data fusion techniques to correlate similar mobile user behavioural features for authentication. The researchers have expertise in privacy preserving data mining techniques which are critical in today's online marketplace. Our support starts from early stage of developments ranging from technical consultation for the proof of concept to the development of new software and hardware systems.

Relevant skills/experience/technologies

Tech Inspire has expertise in the areas of information security, mobile data privacy and data fusion, cloud computing service optimisation based on trust and risk. Tech Inspire has pioneered hormormophic encryption techniques to analyse biometric features in the encrypted domain. Tech Inspire will provide the project with (i) Security Management (ii) Privacy preserving authentication techniques (iii) Multi-modal data fusion

Role in the project

Tech Inspire will lead WP3 User Security & Privacy.

Key personnel

Professor Muttukrishnan Rajarajan (M) founded the Mobile Networks and Security Research Group in 2003 at Tech Inspire UK. He has led several research projects in the area of security and privacy in mobile networks, cloud computing, social media analytics, identity management and healthcare. He is currently leading a UK Government's digital government activity in the area of identity management where he is defining the required personal biometric attributes for different levels of security. In addition to this he is leading a major UK-India research project in the area of mobile healthcare management for depression and obesity management where he is exploiting the possibility of using voice biometrics. He was also part of the OPTIMIS FP7 project on Optimised Cloud Services. He is currently working with Blackberry to protect the app space using blackberry emulators in the Cloud. He regularly advises British Telecom on security and privacy issues in the mobile and cloud environments. He has published more than 200 scientific journal and conference papers and an author of 2 books on mobile security and privacy.

Dr. Suresh Babu Veluru (M), Research Fellow worked previously in the Faculty of Computer Science at the University of New Brunswick (Canada), and in the Artificial Intelligence Group, Department of Computer Science at the University of York (UK). Dr. Veluru has been working heavily on the development of fuzzy node weighted tree based similarity algorithm for e-Health Environment. His main expertise and publications in the last 10 years are in the areas of Pattern Recognition and Data Mining, Natural Language Processing and text mining and Artificial Intelligence and Privacy Preserving Data Mining.

Dr Rahul Yogachandran (M) is an expert in the area of privacy preserving data analytics. He has recently developed a new privacy model based on the attribute based encryption techniques whereby t he

users can upload the data to a central server on a privacy protected manner for disease diagnosis. He has published more than 15 papers in the area of e-health and recently has been working with Blackberry UK to understand the malware apps in the Android and Blackberry market place. He will contribute to the privacy preserving data analytics part of the project. He has also unique expertise in analysing for emotional patterns within encrypted facial images. Identified at Rahulamathavan Y. in publications.

Relevant publications/patents/products/services
Rahulamathavan Y, Veluru S, Phan R, Chambers J and **Rajarajan M** (2014), Privacy-Preserving Clinical Decision Support System using Gaussian Kernel based Classification, IEEE Journal of Biomedical and Health Informatics.
Li, F., **Rahulamathavan, Y**. and **Rajarajan, M.** (Sep 2014). Lightweight Static and Dynamic Attributes Based Access Control Scheme for Secure Data Access in Mobile Environment. 39th IEEE Conference on Local Computer Networks, Sep 2014, Edmonton, Canada
Rahulamathavan, Y., Moonsamy, V., Batten, L., Shunliang, S. and Rajarajan, M. (Jul 2014). An Analysis of Tracking Service Settings in Blackberry 10 and Windows Phone 8 Smartphones. 19th Australasian Conference on Information Security and Privacy (ACISP), Jul 2014, Wollongong, Australia
Fahad, L.G., Tahir, S.F. and **Rajarajan, M.** (Aug 2014). Activity Recognition in Smart Homes using Clustering based Classification. 22nd IEEE International Conference on Pattern Recognition (ICPR), Aug 2014, Stockholm, Sweden.
Shittu, R., Healing, A., Ghanea-Hercock, R., Bloomfiled, R. and **Rajarajan, M.** (Sep 2014). A New Metric for Prioritising Intrusion Alerts Using Correlation and Outlier Analysis. 39th IEEE Conference on Local Computer Networks, Sep 2014, Edmonton, Canada

Relevant research projects
OPTIMIS is an FP7-ICT project aimed at enabling organizations to automatically externalize services and applications to trustworthy and auditable cloud providers in the hybrid model.
TRUMP is a collaborative UK-India project, investigating mobile technology as a trusted platform for deploying innovative, healthcare interventions in rural areas.
UID is national research project funded by the UK Engineering and Physical Sciences Research Council (EPSRC) funded project that links information pertaining to human characteristics in real and virtual worlds in order to better understand and manage the uncertainties inherent in establishing human identity in different geographic locations.
Future of Identity is a Network of Excellence project funded by the UK Engineering and Physical Sciences Research Council (EPSRC)
Identifying and Modelling Victim, Business, Regulatory and Malware Behaviours in a Changing Cyberthreat Landscape is a research project funded by the UK Engineering and Physical Sciences Research Council (EPSRC)

Existing infrastructure
Cloud setup, mobile Security test bed, in-house data mining tools, Android lab

Does the participant plan to subcontract certain tasks	N
Does the participant envisage that part of its work is performed by linked third parties	N
Does the participant envisage the use of contributions in kind provided by third parties	N

Partner 5: Real Eyes OÜ (EYE)

The organization

Realeyes specialises in the quantitative collection of emotional response data online via conventional webcams. Based on Paul Ekman’s theory of the cross-cultural universality of emotions and their corresponding facial expressions, our software can measure and analyse respondent’s reactions to a variety of stimuli using cutting-edge facial coding technology, and providing crucial consumer insight. Thanks to the technological advances of cloud computing and the popularity of webcams, we’ve constructed an online coding system, which can collect and process data and report results from all over the world in seconds, dramatically improving the viability of the emotion tracking techniques and scaling their potential.

Relevant skills/experience/technologies

We are a research driven and client focused European company, with offices in Estonia, Hungary, the UK and the USA and over 5 years of operating experience across 11 different countries. The company currently employs 42 specialists in different areas, such as research, development, sales and operations, most of whom work in the European economic area. Thanks to continuing support by the EU through Eurostars and FP7 grant schemes Realeyes has one of the strongest industrial R&D teams in the field in Europe, which consists of 9 machine learning and computer vision researchers, data scientists and engineers. Technology built by Realeyes is patent protected with 7 pending EU patent applications. As a commercial services provider Realeyes is trusted by some of the world biggest brands, publishers and agencies alike, such as AOL, IPSOS, Danone, Mars, Walt Disney and many more.

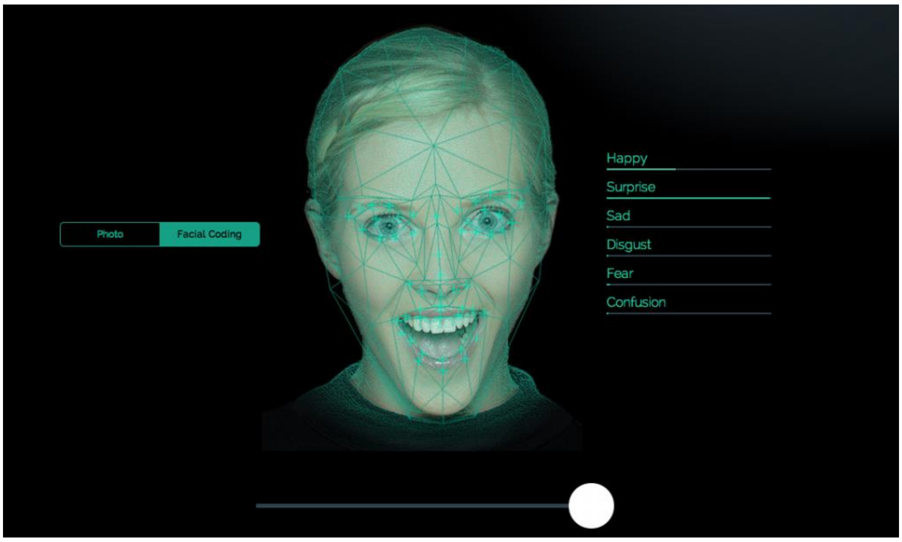
Role in the project

Realeyes will support WP2 Multichannel biometrics and WP4 HCI & Access Management with its emotion recognition technology and expertise.

Key personnel

Dr Gabor Szirtes (M), Head of Research, has previously worked on computational problems of biological learning and memory from machine learning perspective. His interest in functional modelling of the hippocampal formation led him to dynamical (neural Kalman-filter strategies) and structural (random graph simulations, small world architectures) questions. While functional modelling can be defined in many ways, reality imposes different constraints on both structure and dynamics. To get a better understanding of these constraints and thus the encoding/decoding processes, he studied early visual processing and the statistical analysis of single- and multi-unit recordings using maximum likelihood methods (Columbia University, New York) and second and higher order statistical methods (Department of Psychophysiology, Eötvös University, Budapest). Beside single cell level analysis he got involved in research on higher order cognitive behaviour by analysing gaze tracking and fMRI data (PERCEPT project within EU FP6). Central to decoding/encoding processes is the notion of representations, so he studied factors that make neural representations and early sensory processing extremely efficient in terms of computational speed, energy and noise tolerance. The results about linking the theory of Compressive Sampling (a revolutionary idea in signal processing) to the functioning of early visual system have been published in PLoS in 2012. Prior to joining Realeyes, he worked in the neurophysiology lab of Dr Anton Sirota at the University of Tuebingen, Germany, where his main task was to implement novel statistical methods to analyse large-scale data, improve conventional signal processing methods and to model the complex correlations between animal behaviour (recorded by high speed motion capture system) and in vivo neural recordings. In addition, he is an active member of EUCog - European Network for the Advancement of Artificial Cognitive Systems, Interaction and Robotics; and a reviewer of PloS ONE, PloS Computational Biology, Neural Networks, Journal of Computational Neuroscience and Neurocomputing.

Dr Elnar Hajiyev (M), CTO is leading the development of the webcam eye-tracking project and gaze database. He holds BSc (first class) in Information and Media Technology from Brandenburg Univer- sity of Technology, Germany and MSc (distinction) in Computer Science from University of Oxford, UK. His DPhil in Computer Science from the Programming Tools Group, University of Oxford, focused on semantics of aspect oriented programming languages and logic programming in the context of modern relational databases. During his education he received numerous excellency awards, including an Overseas Research Student award, scholarships from Shell and DAAD. Elnar has significant experience working in high-technology companies, including the largest Internet Service Provider of Azerbaijan, Siemens Magnet Technology and his previous technology startup, Semmle, who specialise in on-demand software analytics. He has published more than ten peer-reviewed papers in international journals and conference proceedings.

Relevant publications/patents/products/services	
Szirtes, Gábor, et al. "Facing reality: an industrial view on large scale use of facial expression analysis." Proceedings of the 2013 on Emotion recognition in the wild challenge and workshop. ACM, 2013.	
Jeni, L. A., Lőrincz, A., Nagy, T., Palotai, Z., Sebők, J., Szabó, Z., & Takács, D. (2012). 3D shape estimation in video sequences provides high precision evaluation of facial expressions. Image and Vision Computing, 30(10), 785-795.	
Realeyes Emotion Analytics Platform measuring people's emotional response to media content via standard webcams	 Photo Facial Coding Happy Surprise Sad Disgust Fear Confusion

Relevant research projects
CARP, an FP7-ICT project designing high-level programming formalisms geared towards accelerators, writing highly optimizing compilers to compile high-level code into efficient OpenCL, verifying correctness of accelerator kernels, and employing intensive symbolic testing techniques to find bugs.
European Regional Development Fund Grant

Existing infrastructure
Scalable cloud infrastructure on Amazon Cloud for online data collection and analytics, as well as training and testing of next generation emotion tracking algorithms. Existing emotion recognition technology and database of emotion data.

Does the participant plan to subcontract certain tasks	N
Does the participant envisage that part of its work is performed by linked third parties	N
Does the participant envisage the use of contributions in kind provided by third parties	N

Partner 6: Forthnet S.A. – Hellenic Telecommunications and Telematics Applications Company (FNET)

The organization

Forthnet S.A. is a leading provider of broadband network services in Greece. The company was the first commercial Internet Service Provider in Greece, established in November 1995. Forthnet has entered both the telecommunications and network services business, being a convergent services provider offering from voice telephony to Internet and value-added services over its private broadband network. The company has more than 270.000 enterprise customers using leased lines and broadband access services; more than 320.000 voice telephony lines and 500 data center customers. Forthnet customer base comprises a major part of the Greek Internet community and the market of alternate voice telephony & network providers. The sales volume for 2005, 2006, 2007 and 2008 was 88 MEuro; 93 MEuro; 114 MEuro; 136 MEuro respectively. Forthnet has a full-time staff of 880 persons. The company launched in 2005 an investment plan of 253 million Euro, comprising mainly of fibre infrastructure for over 600 km of MAN, long distance and international connectivity, development investments for broadband network and services infrastructure, EDP infrastructure and market expansion activities. Forthnet operates 75 Points of Presence (PoPs) in respective towns of Greece, interconnected over a high-speed backbone. Forthnet group of companies recently acquired Netmed S.A., the leading satellite TV platform provider with more than 300.000 customers in Greece and Cyprus, and launched a major integration project towards converged broadband access and entertainment media services.

Relevant skills/experience/technologies

Forthnet utilizes and integrates technological solutions on the basis of the latest telecommunications prototypes to develop and provide new services on the Network. It also utilizes various software technologies (Java/J2EE, .Net, Linux, open source, database systems) for the development of information systems for the SMEs and for the realization and provision of eServices. Main interests of R&D department include Broadband communications, Next-Generation networks, Wireless & Ad-Hoc networks, E-Content & Networked Media management & distribution, eTourism, eHealth, eLearning, eGovernment, Advanced Messaging Systems and EWS, User mobility and Mobile Internet. System & network technology and software engineering are within the technological skills and know-how of the R&D team, based upon object-oriented development with C++, Java/J2EE on various operating platforms. Forthnet R&D department has participated in several European research projects in the past, related to synthesis and interoperability of services, mobile application and personalized services within the eHealth domain. Forthnet S.A. has a strong previous participation in EC funded projects in the areas of eHealth, such as HEARTFAID (STREP – IST FP6), which aimed at the development of a knowledge based decision support system for improving the medical-clinical management of heart failure within the elderly population. Forthnet has also participated in FP7 IP REACTION project, where it was mainly involved in the implementation and provision of server and network infrastructure and integrates advanced network and edge communication technologies, as well as contributing to the underlying security modules.

Role in the project

FNET will lead the Consumer Pilot in WP6 Demonstrators & Evaluation.

Key personnel

Manolis Stratakis (M) holds an MSc by research in Computer Networks and Digital Communications and a BSc in Electronic Computer Systems, both from the University of Salford, UK. He is currently the Head of Research Projects in the R&D department of Forthnet S.A., where he is managing several European and National research projects, primarily related to Internet and web applications and the development of Value Added Services in the areas of Mobile Internet, Advanced Messaging Systems, mobile Learning, Electronic Commerce, Teleworking, eHealth, Telemedicine and 3G Technologies. He has worked from 1992 to 1997 at the Institute of Computer Science, Foundation for Research and Technology - Hellas (FORTH), where he was mainly involved in the design and development of digital computer systems. He has also worked as a visiting professor in the Technological Education Institute of Heraklion, School of Technological Applications, from 1993 to 2000. Since 1994 he has delivered a number of Internet related courses in the Cyprus International Institute of Management and several other academic establishments. His research interests include integrated services computer networks, new technologies and applications over the Internet, mobile Internet, intelligent and personalised messaging services, real life links with advanced technology and regional development.

Stylianos A. Louloudakis (M) holds a BSc in Computer Science of the University of Essex, England, and an MSc in Internet and Database Systems of the Southbank University of London, England. He was employed by the Department. of Applied Mathematics and Computer Science, at the Foundation for Research and Technology - Hellas (FORTH) as a computer programs' analyst, where he was mainly involved in the development of applications based on the Java programming language. He was employed by the R&D Department of Forthnet S.A. on January 2005 and since then he has been involved in the development of a number of European and National projects, in the areas of eHealth, Mobile Internet Communications, Mobile Applications, Advanced Messaging Systems, as well as in Computer and Sensor Networks.

Antonis Miliarakis (M) holds an MPhil degree by the Systems Engineering Department, at BRUNEL University, UK. He graduated with honors from the Electrical Engineering Department of the Technological Educational Institute of Crete, Greece, in 2002. Since October 2000 he has worked at Forthnet S.A. where his main responsibility is the technical management of ICT research projects and the design of mobile service platforms and wireless networks. During his activities at the research and development department he has participated in the implementation of many European and national IT projects. Since September 2004 he has been lecturing Computer Systems Architecture, Medical Informatics and Microprocessors at the Applied Informatics and Multimedia department of Technological Education Institute of Crete. As a web services designer, he has designed and implemented applications for desktop and mobile platforms like Pocket PC and Palm OS, using a variety of tools like C, VB6.0, eVB3.0, eVC++, VB.NET and ASP.

Relevant publications/patents/products/services
Service portfolio: Forthnet provides Internet access services, Internet news services, website hosting services, and telecommunications services such as voice transmission. Forthnet's network covers mainland Greece, Crete, and the major Greek islands.
Asanin, Stefan, Peter Rosengren, Tobias Brodén, Ivo Ramos Maia Martins, Carlos Cavero Barca, Manuel Marcelino Pérez Pérez, Lydia Montandon, Manolis Stratakis, and Stelios Louloudakis. "Adopting Rule-Based Executions in SOA-Oriented Remote Patient Monitoring Platform with an Alarm and Alert Subsystem." In Wireless Mobile Communication and Healthcare, pp. 437-444. Springer Berlin Heidelberg, 2013.
Validation of a Flexible and Innovative Platform for the Home Monitoring of Heart Failure Patients: Preliminary Results – Forthnet S.A.: Manolis Stratakis, Stelios Louloudakis - Computers in Cardiology 2009

Relevant research projects
The HEARTFAID project (ISST-2004-027107) for the development of innovative computerized systems and services that improve medical knowledge, diagnosis, prognosis, treatment and personalization of elderly patients with Heart Failure.
The REACTION project (FP7-ICT-2009-4) for developing an integrated approach to improved long term management of diabetes; continuous blood glucose monitoring, clinical monitoring and intervention strategies, monitoring and predicting related disease indicators, complemented by education on life style factors such as obesity and exercise and, ultimately, automated closed-loop delivery of insulin.
The SEMEOTICONS project (FP7-ICT-2013-10), for designing and constructing an innovative multisensory system integrated into a hardware platform, collecting Bio-data for extracting biometric, colorimetric, morphometric and compositional descriptors measuring an individual's facial signs. The

integration of such descriptors will provide a Vitrual's Individual Model, for computing, tracing and analyzing the daily evolution of an individual's "wellness index".
The GUARANTEE project (ITEA2 – Call 6) provides a technical solution for personal safety in the home environment. GUARANTEE introduces local and network-supported decision making for safety applications on the basis of sensor input and with immediate response and feedback to the people concerned.

Existing infrastructure
Forthnet's broadband infrastructure network and existing customer base (1.08M subscribers).

Does the participant plan to subcontract certain tasks	N
Does the participant envisage that part of its work is performed by linked third parties	N
Does the participant envisage the use of contributions in kind provided by third parties	N

Partner 7: Horia Hulubei National Institute for Physics and Nuclear Engineering (IFIN-HH)

The organization

IFIN-HH is one of the most important R&D organizations in Romania. In the period 2008-2010 the scientists at IFIN-HH published 946 articles in peer-reviewed Thomson-Reuters-indexed journals and 272 articles in journals not indexed by Thomson Reuters. In the same period the scientists at IFIN-HH organized 20 international conferences at 16 national ones. IFIN-HH is a member of Joint Institute for Nuclear Research – JINR (Dubna, Russia, http://www.jinr.ru), Facility for Antiproton and Ion Research – FAIR (Darmstadt, Germany, http://www.fair-center.eu) and CERN (Geneva, Switzerland, http://home.web.cern.ch). IFIN-HH takes part in large international physics experiments such as ATLAS, ALICE, LHC-b, DIRAC, FOPI, LCG, GASP, KASCADE, SPIRAL 2, and large international projects such as the Real-Time On-Line Decision Support – RODOS, European Nuclear Structure Integrated Structure Initiative – EURONS, and European Isotope Separation On-Line Radioactive Ion Beam Facility – EURISOL. IFIN-HH collaborates with more than 50 universities and research institutes in Europe, 11 in the USA and Canada and 3 from Asia.

Relevant skills/experience/technologies

The most important infrastructure of IFIN-HH is the Nuclear Physics Pillar of the Extreme-Light Infrastructure, ELI-NP (http://www.eli-np.ro), which is currently being built within the premises of IFIN-HH. IFIN-HH is in charge of numerous Installations of National Interest (in Romanian: Instalatii de Interes National) of which we mention here the VVR-S Nuclear Reactor for Research and Production of Radioisotopes, The National Deposit of Radioactive Waste – DNDR, the Tandem Van de Graaff linear accelerator, the Cyclotron U120 accelerator, and the Multipurpose Irradiation Installation – IRASM. IFIN-HH also host one of the largest distributed and parallel computing infrastructure in the country which amounts to 6000 computer cores and 2 PB of storage. The mission of IFIN-HH is focused on advanced scientific research in atomic and subatomic physics.

Role in the project

IFIN will lead the Workforce Pilot in WP6 Demonstrators & Evaluation.

Key personnel

Mitica Dragusin (M), Nuclear Safety Director, has been employed at the Horia Hulubei National Institute for Physics and Nuclear Engineering (IFIN-HH) for 31 years. He has worked for 19 years in the radiation processing of the water-soluble polymers with high activity radiation sources Co-60 and 12 years in the decommissioning of the nuclear facilities. He is Nuclear Safety Director in IFIN-HH from 2006, is the project manager of the decommissioning the nuclear research reactor type VVR-S from institute, which started in 2010 and will be finalized in 2020. From 2013 is also project manager of the cross-border project Romania-Bulgaria – Emersys – “Toward an integrated, joint cross-border detection system and harmonized rapid responses procedures to chemical, biological, radiological and nuclear emergencies”, scheduled to be finished in July 2015, founded by European Regional Development Fund and co-financed by Romanian and Bulgarian Government

Constantin Ivan (M), Technical-Administrative Director, has been employed at the Horia Hulubei National Institute for Physics and Nuclear Engineering (IFIN-HH) in 1985 and has then worked on radiation detectors and associated electronics, as well as radionuclide metrology, namely the development of new equipment and measurements methods for radioactivity. Starting 2004 Dr. Ivan serves at Technical-Administrative Director of IFIN-HH.

Mihnea Dulea (M), Head of the Department of Computational Physics and Information Technologies is a Senior Researcher working on Grid computing, High-Performance Computing and computational biophysics and is the incumbent Head of the Department of Computational Physics and Information Technologies of IFIN-HH. He is also the President of the Romanian Association for the

Promotion of Advanced Computational Methods in Scientific Research, which now represents Romania in PRACE, and has served as coordinator and work package coordinator for more than a dozen national and international projects on Grid infrastructures and High-Performance Computers. Dr. DULEA coordinates the Romanian Tier 2 Federation RO-LCG which represents Romania in WLCG collaboration.
Alexandru Nicolin (M), Senior Researcher II, Department of Computational Physics and Information Technologies, works on numerical and symbolic computing applications for condensed mater physics. Following his graduate studies at the Niels Bohr Institute of the University of Copenhagen, Dr. Nicolin has joined IFIN-HH in 2009 and his currents effort are focused on expanding the Computing Centre of IFIN-HH.

Relevant publications/patents/products/services
Dulea, M., Constantinescu, S., Ciubancan, M. (2012). Support for multiple virtual organizations in the Romanian LCG Federation, 5th Romanian Tier-2 Federation Grid, Cloud & High-Performance Computing Science (RO-LCG), 59-62.
Dulea, M. (2012). National and regional organization of collaborations in advanced computing, 5th Romanian Tier-2 Federation Grid, Cloud & High-Performance Computing Science (RO-LCG), 63-66.
Dima, M., **Dulea M.** (2010). Classical and quantum communications in Grid computing, Optoelectronics and advanced materials – Rapid Communications, 4, 1840-1843.
Dima, M., **Dulea,** M., et al. (2009). The QUANTGRID project (RO) – Quantum security in Grid computing applications, AIP Conference Proceedings, 1203, 461-465.

Relevant research projects
CONDEGRID (PN2-Capacities-M3 CERN): National contribution to the development of the LCG computing grid for elementary particle physics (08EU/2012) – Director: M. Dulea, Period: 2012-2014
IDEI-25(PN-II-ID-PCE-2011-3-0323): High-performance computing for nuclear and particle physics– Director: M.O. Dima, Period: 2011 – 2015
HP-SEE (FP7-RI-261499): High-Performance Computing Infrastructure for South East Europe's Research Communities – Leader Romanian JRU: M. Dulea, Period: 2010-2013
GRICEFCO (SOPIEC-A2-O2.2.3-2008-3 EU structural funds 209): Grid system for physics research and related areas – Director: M. Dulea, Period: 2009 – 2011

Existing infrastructure
The existing infrastructure of IFIN-HH has a two-fold relevance for the project: on one hand, IFIN-HH has a broad set of infrastructures which can be used to test the security system which will be developed in the project, while on the other hand it has an state-of-the art ITC infrastructure which insures excellent real-time communications with the other partners in the project which can constantly monitor the security system.

Does the participant plan to subcontract certain tasks	N
Does the participant envisage that part of its work is performed by linked third parties	N
Does the participant envisage the use of contributions in kind provided by third parties	N

Partner 8: Computational Medicine Laboratory (CML) & Human Computer Interaction Laboratory, Institute of Computer Science (ICS) Foundation for Research and Technology-Hellas (FORTH)

The organization

The Foundation for Research and Technology – Hellas (FORTH) is one of the largest research centres of Greece with well-organized facilities and highly qualified staff. It functions under the supervision of the General Secretariat for Research and Technology of the Hellenic Ministry of Development. The Foundation, with its high quality research results as well as its valuable socioeconomic contribution, makes it one of the top research centres internationally. The Institute of Computer Science (FORTH-ICS), one of the six institutes of FORTH, has a relatively long history and recognized tradition, since its establishment in 1983, in conducting basic and applied research, developing applications and products, providing services, and playing a leading role in Greece and internationally, in the fields of Information and Communication Technologies. Our activities cover important research and development areas, taking into consideration new perspectives, emerging fields of research and technological challenges worldwide.

Relevant skills/experience/technologies

The Human Computer Interaction Laboratory (HCI) of ICS-FORTH, established in 1989, is an internationally recognized centre of excellence in the design and development of adaptable and accessible interactive applications and services for various platforms, such as personal computers, mobile phones, smart appliances and furniture, and other computational devices distributed in the environment. The Laboratory has participated in more than 50 R&D projects in the field of HCI.

The Computational Medicine Laboratory (CML) at FORTH-ICS has established a tradition of internationally acknowledged excellence in conducting high-level R&D work and in developing innovative systems and services. Its research activities focus on the development of innovative computer methods and tools in the area of medical and biomedical informatics, computational medicine, ehealth, m-Health, medical imaging and bioinformatics. The mission of the Computational Medicine Laboratory (CML) is to develop novel ICT technologies in the wider context of personalized, predictive and preventive medicine.

Role in the project

FORTH-HCI will lead WP4 HCI & Access Management.
FORTH-CML will lead the eHealth Pilot in WP6 Demonstrators & Evaluation.

Key personnel

Dr. Kostas Marias (M) holds a Principal Researcher position in the Institute of Computer Science (ICS-FORTH), and since 2010 he is the Head and Founder of the Computational Medicine Laboratory at FORTH-ICS. During 2001-2003, he worked as a Researcher at the University of Oxford and from 2003-2006 as Associated Researcher at FORTH-ICS. He was the coordinator two EC projects on cancer modelling (www.contracancrum.eu and www.tumor-project.eu), and during 2006-2013 worked in several EC funded projects developing ICT technology for personalized medicine. He coordinated the development of a wide range of image analysis and modelling tools (biomodeling.ics.forth.gr) designed for the clinical setting within the wider Virtual Physiological Human (VPH) EC initiative. He has published more than 100 papers in international journals, books and conference proceedings focusing on medical image analysis, biomedical informatics and modelling for personalized medicine.

Dr. Margherita Antona (F) is a Principal Researcher at ICS-FORTH. She is member of the Human Computer Interaction Laboratory of ICS-FORTH, Coordinator of the Centre for Universal Access & Assistive Technologies, and Coordinator of the AmI Classroom activity of the ICS-FORTH AmI Programme. Her research interests include adaptive and intelligent interfaces, computer-supported user interface design, design for all and assistive technologies, eLearning and Ambient Intelligence. She has participated in more than 20 European and national R&D projects. She is Deputy Coordinator of the KRIPIS National Project “Quality of life”, and the scientific responsible for the participation of ICS-

FORTH in the projects AAL-REMOTE and FP7-ICT-VERITAS. She has coauthored more than 90 scientific publications. She is Co-Chair of the International Conference on Universal Access in Human-Computer Interaction (UAHCI) and member of the Editorial Board of the Universal Access in the Information Society International Journal. She is member of Program Committee and Paper Review Committee in various international conferences and workshops.
Dr. Vangelis Sakkalis (M) holds a Principal Researcher position in the Institute of Computer Science – Foundation for Research and Technology (ICS - FORTH). He received his PhD in Electronic and Computer Engineering after completing his Master's degree at Imperial College of Science, Technology and Medicine, UK. His background falls in Biomedical Engineering, Atomic-Molecular Physics, Optoelectronics and Laser. His research interests include biosignal and image analysis, visualization, classification algorithms and biostatistics applied in computational medicine, cognitive neuroscience and biomedical informatics. He is currently coordinating 2 projects (EU and national) related to cancer research. He has published more than 100 papers in scientific archival journals, proceedings of international conferences & workshops and scientific newsletters, related to his fields of expertise. He has given numerous invited lectures worldwide and his research has been funded by numerous funding agencies and companies.
Dr. Emmanouil G. Spanakis (M) is a Collaborating Researcher at the CML of FORTH-ICS. He is also a visiting lecturer at the Computer Science Department, University of Crete. He holds a Ph.D., a M.Sc. and a B.Sc. in Computer Science from the University of Crete, Heraklion, Greece. His expertise, specialization and research lie in the wider scientific domain of computational medicine and wireless communication networks, and in particular on biomedical informatics; wireless medical sensors; ambient intelligence services and smart surroundings; eHealth and mHealth related services; as well as in cross-layer design in wireless ad-hoc networks; wireless interference channel under Signal to Interference Plus Noise Ratio (SINR) constraints; performance and analysis of mobile ad-hoc routing protocols; and wireless network measurements analysis.
George Margetis (M) holds a degree in Computer Science and M.Sc. in "Computer Networks and Digital Communications" and "Information Systems". He is a member of the Human-Computer Interaction Laboratory of FORTH-ICS since 2005. His past work includes network traffic measurement and analysis in high-speed networks, resource control and service differentiation in wired networks. His current work focuses on interaction design, Ambient Intelligence and Smart Spaces, Universal Access and Design for All. He has participated as a technical coordinator or implementation member in a number of European and National research projects. His recent work includes the analysis and investigation of tools and interaction techniques for multimodal interaction in Ambient Intelligence environments, mainly in the fields of education, independent living, tourism and culture.

Relevant publications/patents/products/services
Spanakis, E.G.; Sakkalis, V.; Marias, K.; Traganitis, A. Cross Layer Interference Management in Wireless Biomedical Networks. Entropy 2014, 16, 2085-2104.
Leonidis, A., **Antona, M**., & Stephanidis, C. (2012). Rapid Prototyping of Adaptable User Interfaces. International Journal of Human-Computer Interaction, 28 (4), 213-235.
Margetis, G., Zabulis, X., Koutlemanis, P., **Antona, M.,** and Stephanidis, C. (2013). Augmented interaction with physical books in an Ambient Intelligence learning environment. Multimedia Tools and Applications, 67 (2), 473-495.
Tsiknakis, M.N., Sfakianakis, S.G., **Marias, K**., & Graf, N. (2012). A technical infrastructure to support personalized medicine. IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE), 2012.
Sakkalis, V., Sfakianakis, S.G., & **Marias, K**. (2012). Bridging social media technologies and scientific research: an exemplary platform for VPH modellings. 3rd International ICST Conference on Wireless Mobile Communication and Healthcare (MobiHealth 2012), Workshop on Advances in Personalized Healthcare Services, Wearable Mobile Monitoring, and Social Media Pervasive Technologies (APHS 2012), Paris, France, November 21-23, 2012.

Relevant research projects
MyHealthAvatar is a proof of concept for the digital representation of patient health status. It is designed as a lifetime companion for individual citizens that will facilitate the collection of, and access to, long-term health-status information. This will be extremely valuable for clinical decisions and offer a promising approach to acquire population data to support clinical research, leading to strengthened multidisciplinary research excellence in supporting innovative medical care. MyHealthAvatar will be built on the latest ICT technology with an aim of engaging public interest to achieve its targeted outcomes. In addition to data access, it is also an interface to access integrative models and analysis tools, utilizing resources already created by the VPH community.
HOBBIT sets out to study a future robot that will make older persons feel safe at home. It will pick up objects from the floor, can learn objects and bring objects, and it is equipped with easy-to-use entertainment functions. HOBBIT will offer tools to stay socially connected, keep active with playing games and exercise, and enjoy your time checking out now films, music and books. HOBBIT will detect emergency situations and trigger an appropriate alarm. The focus of HOBBIT is on the development of the mutual care concept: building a relationship between the human and the robot in which both take care for each other. Like when a person learns what an animal understands and can do; similar to building a bond with a pet. The main task of the robot is fall prevention and detection. To achieve this, the robot will clean the floor from all objects and thus reduce the risk of falling. It will detect emergency situations such that help can be called in time. The purpose of the Mutual Care approach is to increase the acceptance of the home robot.
SEMEOTICONS will design and construct an innovative multisensory system integrated into a hardware platform having the exterior aspect of a mirror: the so-called “Wize Mirror”. This will easily fit into users’ home or other sites of their daily life (e.g. fitness and nutritional centres, pharmacies, schools and so on). The Wize Mirror will collect data mainly in the form of videos, images and gas concentration signals. These will be processed by advanced dedicated methods to extract biometric, morphometric, colorimetric, and compositional descriptors measuring individual’s facial signs. The integration of such descriptors will provide a Virtual Individual’s Model, which will be used to compute and trace the daily evolution of an individual’s “wellness index”.
VERITAS (Virtual and augmented environments and realistic user interactions to achieve embedded accessibility design) aims to develop, validate and assess tools for built-in accessibility support at all stages of ICT and non-ICT product development, including specification, design, and development and testing. The goal is to introduce simulation-based and virtual reality testing at all stages of assistive technologies product design and development into the automotive, smart living spaces, (buildings & construction, domotics), workplace and infotainment applications areas.
REMOTE is a pan-European research project concerned with the needs of elderly and individuals with chronic conditions. The focus is to support independent living with the aid of AmI technologies and tele-healthcare with various kinds of monitoring and automation services for tracing activity, fall detection and health condition, as well as detecting risks or critical situations of citizens.

Existing infrastructure
IT infrastructure – hardware, software, development and design tools needed for the project

Does the participant plan to subcontract certain tasks	N
Does the participant envisage that part of its work is performed by linked third parties	N
Does the participant envisage the use of contributions in kind provided by third parties	N

Partner 9: University College London (UCL)

The organization

UCL's main campus is located in the Bloomsbury area of central London, with a number of institutes and teaching hospitals located elsewhere in central London, and satellite campuses in Adelaide, Australia and Doha, Qatar. UCL is organised into 10 constituent faculties, within which there are over 100 departments, institutes and research centres. UCL has around 26,700 students and 11,025 staff and had a total income of £937 million in 2012/13, of which £335 million was from research grants and contracts. UCL has around 4,000 academic and research staff and 650 full professors, the highest number of any British university.

Relevant skills/experience/technologies

The UCL team has expertise in image and video coding, approximate signal processing, incremental refinement of computation for signal transforms and multimedia processing algorithms, intelligent signal processing, including the application of array signal processing techniques to a variety of problems , information processing and information fusion.

Role in the project

UCL will lead WP6 Demonstrators & Evaluation and WP9 Standardization.

Key personnel

Dr Hugh Griffiths (M) was educated at Hardye's School, Dorchester, and Keble College, Oxford University, where he received the MA degree in Physics. He also received the PhD (1986) and DSc(Eng) (2000) degrees from the University of London. In 2006 he was appointed Principal of the Defence College of Management and Technology, Shrivenham (part of Cranfield University). From 1982 to 2006 he was with University College London, serving as Head of the Department of Electronic and Electrical Engineering from 2001 to 2006. His research interests include radar sensor systems and signal processing (particularly synthetic aperture radar and bistatic and multistatic radar and sonar) as well as antennas and antenna measurement techniques. He has published over 300 papers and technical articles on these subjects. He received the IERE Lord Brabazon Premium in 1984, the IEE Mountbatten and Maxwell Premiums in 1996, and the IEEE Nathanson Award in 1996. He serves on the IEEE AESS Board of Governors and as Chairman of the IEEE AESS Radar Systems Panel, and as Editor-in-Chief of IEE Proceedings on Radar, Sonar and Navigation. Also, he was Chairman of the IEE International Radar Conference RADAR 2002 in Edinburgh, UK. He is also a member of the Defence Scientific Advisory Council for the UK Ministry of Defence, and of the Supervisory Board for the UK Ministry of Defence's Defence Technology Centre in ElectroMagnetic Remote Sensing. He is a Fellow of the IEE, Fellow of the IEEE, and in 1997 he was elected to Fellowship of the Royal Academy of Engineering.

Dr Clayton Stewart (M) is currently Visiting Professor, Department of Electronic and Electrical Engineering, University College London and consultant on international S&T engagement with clients including DARPA. He has served as Technical Director Office of Naval Research Global, providing technical direction to a staff of engineers/scientists involved in monitoring, assessing, and sponsoring world-wide S&T; Corporate Vice President/Manager SAIC Reconnaissance/Surveillance Operation; Associate Professor of ECE and Associate Director, Center of Excellence in Command, Control, Communications, and Intelligence at George Mason University, Fairfax, V; Sperry Corporation and ARCO Power Technologies, Inc.. He has been a director in Air Force Studies & Analyses at the Pentagon, an Air Force Academy Associate Professor of EE and an Electronic Warfare Officer/Engineer who flew various tactical aircrafts. He graduated from University of Redlands, BS in Engineering Science and received his MSEE and PhDEE from the Air Force Institute of Technology.

Prof Karl Woodbridge (M) obtained a BSc in Physics in 1976 and a D.Phil in Materials Science in 1979. He joined University College London in 1990 after 11 years working for Philips Electronics in the area of Molecular Beam Epitaxial (MBE) growth of III-V compounds for device applications. He worked initially at UCL in the semiconductor device area before moving to the RF sensors field. He was seconded part time to DERA/QinetiQ Malvern during 2003-2004 working on radar and air traffic management system. He is currently a member of the academic staff in the Sensors Systems and Circuits group and current research has centered on radar systems for a number of applications. He is currently leading a major activity on the development of a pervasive wireless detection system. He has also recently become involved in the setting up of a new departmental III-V MBE facility.

Relevant publications/patents/products/services
Robert D. Henderson ; Robert Short and Clayton V. Stewart. "Tactical multisensor fusion (TMSF)", Proc. SPIE 3720, Signal Processing, Sensor Fusion, and Target Recognition VIII, 460 (July 27, 1999); doi:10.1117/12.357186;
Stewart, Clayton, Yi-Chuan Lu, and Victor Larson. "A Neural Clustering Approach for Waveform Classification." Pattern Recognition, Vol. 27, No. 4, April 1994, pp. 503-513.
Liu, Jun and Clayton Stewart. "Detection of Linear Features in Images Using Radon and Hough Transforms," OE/Aerospace Sensing '94 The Society of Photo Optical Instrumentation Engineers, Orlando, FL, April, 1994. 1 citation.
Kuo-Chu Chang and Clayton V. Stewart, "Application of Bayes nets in sensor fusion", Proc. SPIE 2093, 644 (1994)
Chang, K.C. and Clayton Stewart. "Bayes Nets for Sensor Fusion." SPIE EUROPTO, Innsbruck, Austria, October 4-8, 1993.

Relevant research projects
Sensing and Fusion Testbed, George Mason University, 1992-94, Dr Clayton Stewart
Classification of Aircraft from their Acoustic Signatures, George Mason University, 1992-94, Dr Clayton Stewart

Existing infrastructure
UCL laboratories and IT infrastructure.

Does the participant plan to subcontract certain tasks	N
Does the participant envisage that part of its work is performed by linked third parties	N
Does the participant envisage the use of contributions in kind provided by third parties	N

Partner 10: Institut Mines Telecom / Telecom Sud Paris, Electronics and Physics Departement, Intermedia Lab (TSP)

The organization

Institut Mines-Télécom (IMT) is an umbrella entity integrating six major Grandes Ecoles (French higher education establishments) in the field of information and communication technology (ICT), including the Mines-Télécom SudParis (TSP) school. IMT is under the authority of the French Ministry of Industry. Its mission is to provide education programs for engineers and managers, to conduct research in ICT and to contribute to the industrial development of ICT in close collaboration with industry. IMT is one of the major French players in the R&D Framework Programs supported by the European Commission (more than 40 FP6/IST and 16 FP7 ICT projects). Telecom SudParis developed a vast experience in all major biometric areas such as speech-, face-, handwritten signature- and iris-based authentication, and also in the new field of combining cryptography and biometrics. The Télécom SudParis biometric group with the INTERMEDIA Research Group was the coordinator of the BioSecure FP6 NoE and is also a member of the BEST network.

Relevant skills/experience/technologies

Telecom SudParis developed a vast experience in all major biometric areas such as speech-, face-, handwritten signature- and iris-based recognition, and also in the new field of combining cryptography and biometrics. The research activities of the Intermedia Group are oriented towards pattern recognition, signal processing, and data-driven machine learning methods, that are exploited for different applications such as speech, speaker and language recognition, very low-bit speech coding, biometrics (2D and 3D face, and voice), and crypto-biometrics (including privacy preserving biometrics). D. Petrovska initiated the recordings of the POLYCOST database, the first European telephonic database for Speaker Recognition, available through ELRA. The originality of the speaker recognition research conducted in the Intermedia group is the introduction of high-level features extracted with Automated Language Independent Speech Processing (ALISP) methods, as complementary sources for speaker verification. In such a way idiolectal characteristics of the speakers can be acquired. The advantage of ALSIP-based methods is that they are easily deployable for new languages.

Role in the project

Telecom SudParis will support WP2 Multichannel Biometrics and WP3 User Security & Privacy. Telecom SudParis will lead WP7 Dissemination & Ecosystem Development.

Key personnel

Dijana Petrovska-Delacrétaz (F) (PhD EPFL 1990) She obtained her degree in Physics and PhD from the Swiss Federal Institute of Technology (EPFL) in Lausanne. She was working as a Consultant at AT&T Speech Research Laboratories and was as a Senior Scientist for four years at the Informatics Department of Fribourg University, Switzerland. Since 2004 she is an associate professor within Mines-Télécom SudParis Intermedia group. She participated actively to the coordination of the FP6 NoE BioSecure (related to Multimodal Biometrics), and co-organized in 2005 the 1st BioSecure Residential Workshop of a one month duration with more than 100 participants.

Bernadette Dorizzi (F) is a Professor at Télécom SudParis since September 1989, and has been head of the Electronics and Physics department until December 2009. She is in charge of the Intermedia (Interaction for Multimedia) research team. B. Dorizzi has been coordinating the BioSecure European Network of Excellence and is president of the Association BioSecure (see section on research projects).

Jérôme Boudy (M) (PhD 1988, HDR 2013) is professor in Signal processing for the Electronic & Physics Department: he has led the RNTS-TelePat project on remote Healthcare vigilance (2003-06) and participated actively on ANR-Tandem and IST-FP7 CompanionAble projects. His research area, as member of INTERMEDIA, is on medical, actimetric signal processing and data fusion process for health distress detection, and speech processing. He has co-directed five PhDs on Biomedical and Health distress detection processing and is codirecting presently two theses on speech processing. He is also currently co-animator of the Digital Health network at IMT**.**

Relevant publications/patents/products/services
Bimbot, F., Bonastre, J. F., Fredouille, C., Gravier, G., Magrin-Chagnolleau, I., Meignier, S., Ortega-García J. , **Petrovska-Delacrétaz, D**., Reynolds, D. A. (2004). A tutorial on text-independent speaker verification. EURASIP journal on applied signal processing, 2004, 430-451.
Petrovska-Delacrétaz, D., Chollet, G., & **Dorizzi, B**. (2009). Guide to biometric reference systems and performance evaluation. Springer.
Tistarelli, M., Bicego, M., Alba-Castro, J. L., Gonzàlez-Jiménez, D., Mellakh, M. A., Salah, A. A., **Petrovska-Delacrétaz, D., Dorizzi, B.** (2009). 2D Face Recognition. In Guide to Biometric Reference Systems and Performance Evaluation (pp. 213-262). Springer London.
Khoury, E., Vesnicer, B., Franco-Pedroso, J., Violato, R., Boulkcnafet, Z., Mazaira Fernandez, L. M., ... Chollet G., **Petrovska-Delacretaz, D.** Marcel, S. (2013, June). The 2013 speaker recognition evaluation in mobile environment. In Biometrics (ICB), 2013 International Conference on (pp. 1-8). IEEE
Simonnet, T., Chollet, G., Caon, D., & **Boudy, J.** (2012, March). Automated Audio-visual Dialogs over Internet to Assist Dependant People. In ICNS 2012, The Eighth International Conference on Networking and Services (pp. 105-110).
Kanade, S. G., **Petrovska-Delacrétaz, D., & Dorizzi, B.** (2012). Enhancing Information Security and Privacy by Combining Biometrics with Cryptography. Synthesis Lectures on Information Security, Privacy, and Trust, 3(1), 1-140.

Relevant research projects
SecurePhone was a European co-funded project (FP6-IST-2002-506883) with the aims to realising a new mobile communication system (the "SecurePhone") enabling biometrically authenticated users to deal m-contracts during a mobile phone call in an easy yet highly dependable and secure way. The SecurePhone, based on an prototypal 3G/B3G-enabled handheld computer platform (a smartphone), will provide users with a number of innovative functionalities, such as the possibility to securely authenticate themselves by means of a "biometric recogniser", mutually recognise each other in initiating a phone call, exchange and modify in real time audio and/or text files and eventually e-sign and securely transmit significant parts of their phone conversation. The solution proposed by this project was to realise an innovative prototypal 3G/B3G enabled PDA (the "SecurePhone") enhanced with a "biometric recogniser" in order to permit to users to mutually recognise each other and securely authenticate.
BioSecure (2004-2007) was an FP6 Network of Excellence (NoE) aiming, through integrating multidisciplinary research efforts and facilitating objective evaluations, to address a range of challenging issues in the field of biometrics, with 30 core partners, representing a critical mass of expertise. The mainly academic organizations involved in BioSecure covered a wide range of research activities in the area of multimodal biometrics with extensive experience in database acquisition and performance evaluation campaigns. The project addressed scientific, technical and interoperability challenges as well as standardization and regulatory questions which are critical issues for the future of biometrics and its use in every day's life.
3COST (2012-2016) De-Identification for Privacy Protection in Multimedia Content: De-identification in multimedia content can be defined as the process of concealing the identities of individuals captured in a given set of data (images, video, audio, text), for the purpose of protecting their privacy. This will provide an effective means for supporting the EU's Data Protection Directive (95/46/EC), which is concerned with the introduction of appropriate measures for the protection of personal data. The fact that a person can be

identified by such features as face, voice, silhouette and gait, indicates the de-identification process as an interdisciplinary challenge, involving such scientific areas as image processing, speech analysis, video tracking and biometrics. This Action aims to facilitate coordinated interdisciplinary efforts (related to scientific, legal, ethical and societal aspects) in the introduction of person de-identification and reversible de-identification in multimedia content by networking relevant European experts and organisations.

BioSecure Foundation: The major role of "Association BioSecure" is to maintain and distribute the major outcomes of the BioSecure FP6 Network of Excellence that lasted from June 2004 to September 2007. It provides to the biometric R&D community, resources such as:

- Evaluation platforms including databases, reference systems (baseline algorithms), assessment protocols for a variety of well-established modalities (speech, face, on-line signature, fingerprints, hand shape, iris).
- Educational material (repository of texts and presentations related to different assets of biometrics)
- Handbook on Standards providing updated information on standardisation activities

Existing infrastructure
TSP will update the already available biometric reference systems (including algorithms, and all the relevant material to reproduce baseline results for eight biometric modalities) with developments relevant to the SpeechXRays project. TSP will provide the materials available from the BioSecure Foundation (databases, evaluations protocols, reference-baseline algorithms). TSP will provide the possibility to use its computing resources (including a computer cluster for evaluations of algorithms that will need to be run on large databases).

Does the participant plan to subcontract certain tasks	N
Does the participant envisage that part of its work is performed by linked third parties	N
Does the participant envisage the use of contributions in kind provided by third parties	N

5 Ethics and Security

5.1 Ethics

Specific Issue: Biometric Template Storage

When people use biometric services for authentication, they must allow the service to have access to their biometrics credentials. This exposes the user to abuse, with security, privacy and economic implications. For instance, the service could extract information such as gender, ethnicity, and even the emotional state of the user from the recording – factors not intended to be exposed by the user – and use them for undesired purposes. Moreover, due to the recent trends toward Cloud computing, it is imaginable that the biometric authentication systems will also be outsourced to potentially untrusted servers in the Internet. These servers could be malicious itself or vulnerable to passive and active attacks by intruders. Hence it is crucial to preserve the privacy of the user's biometric data without compromising or altering the system performance. Any private information that can be gleaned by inspecting a user's interaction with a system must be protected from prying eyes.

The system will allow voice and dynamic face recognition processing tasks subject to no party, including the users, the system, or a snooper, can derive undesired or unintended information from the transaction. This implies, for instance, that a user may enrol for authentication without fear that an intruder or even the system itself could capture and abuse his voice or statistical models derived from it. This will be achieved by incorporating biometric cryptosystem and cancellable biometrics technologies.

We will develop and implement a one-way cryptographic function tailored for voice accoustic and dynamic face recognition to transform the user biometric data into a template with the following features:

- the template used for the authentication, generated from the biometric data, cannot be reverse engineered to reveal the true biometric data
- the user will be able to generate different ''templates'' for different applications with the same biometric data, whilst ensuring that these different identities cannot be linked to each other

This will preserve the privacy of the user's biometric data from template leakage. In case of leakage, the system will simply revoke the enrolled template with freshly generated template. In general the following four different types of cryptographic techniques are used to protect the template: 1. salting (e.g. biohashing) 2. noninvertible transform (e.g. robust hashing) 3. key binding (e.g. fuzzy vault, fuzzy commitment) 4. key generation (e.g. secure sketch, fuzzy extractor). Each technique has its own advantages and disadvantages and have been exploited in several biometric authentication systems in the past. However, a single technique cannot be used to satisfy all the security and privacy requirements. Moreover, these techniques have only been implemented and tested on traditional biometrics such as fingerprints, Iris and face based authentication systems. This project will implement and investigate the cryptographic techniques for combined voice acoustic and lip based face authentication system individually and jointly. Each scheme will be evaluated in terms of false acceptance rate and false rejection rate.

The project will develop an end-to-end privacy-preserving biometric authentication system to protect users vocal tract physiology derived from the feature analysis of the speech spectrogram and dynamic face features such as lip movement during the authentication from the authentication server as well as passive eavesdroppers. The end-to-end anonymous protocol is crucial when the biomtric system is outsourced to third party such as cloud computing paradigm. In literature, there have been several privacy preserving biometric recognition systems such as the face recognition that are developed based on the cryptographic primitives such as homomorphic encryption, secure multiparty computation and oblivious transfer. However, developing a private tool to analyse the speech spectrogram and dynamic face recognition in encrypted domain in order to derive the precise vocal tract physiology and lip movement have not been done to-date. Moreover, the model of the acoustic cues of the voice physiology combined with lip movement of face for an individual is unique like his fingerprint. Hence it is crucial to keep it secure during transmission and storage. We will achieve this by implementing secure two-party protocol using Paillier cryptography to perform authentication in the encrypted domain. The Paillier cryptosystem is an additively homomorphic public-key encryption scheme, whose provable semantic security is based on the decisional composite residuosity problem. Additive homomorphic property supports addition and scaling operations in the encrypted domain. Hence the user's biometric inputs will be encrypted using the Paillier cryptography and the authentication will be performed by the server in the encrypted domain.

Overall Approach to Ethics

The project coordinator, OT, applies high standards when it comes to ethics, in all projects in which we are involved. We take the view that ethics in research is not only about answering *yes*, or *no* to questions in a questionnaire, but about taking responsibility for the research one conducts; it is important for the SpeechXRays consortium to show that ethics is given the attention it deserves in the research we propose.

Nothing in this proposal/project shall be deemed to require a party to breach any mandatory statutory law under which the party is operating, including any national or European regulations, rules and norms regarding ethics in conducting research. The SpeechXRays project, as an applicant and potential participant in H2020, confirms that the proposed research and consortium participants fully comply with the principles of the European Charter for Researchers and the European Code of Conduct for Research Integrity of ALLEA (All European Academics) and ESF (European Science Foundation).

The coordinator of the SpeechXRays project, OT, follows ethical guidelines in its work. The ethical guidelines are based on the vision of using science and technology to create a better society and are reviewed every year to ensure they stay up to date with developments in society and the challenges of today. They generally fall into these categories: research ethics, business ethics, and ethics in interpersonal relationships.

All OT's employees (including employees participating in projects led by OT) are expected to act in accordance with the ethical guidelines and principles. As coordinator of the SpeechXRays project, OT will ensure that any ethical issues that may arise during the project (even if not originally anticipated) will be handled appropriately and in a transparent and fair manner.

5.2 Security: N/A

European Commission

RESEARCH AND INNOVATION PARTICIPANT PORTAL E-RECEIPT

Digitally signed by sealingservice.grants.ec.europa.eu
Date: 2014.08.29 07:10:18 CEST
Reason: Acknowledgment of Receipt

This electronic receipt is a digitally signed version of the document submitted by your organisation. Both the content of the document and a set of metadata have been digitally sealed.

This digital signature mechanism, using a public-private key pair mechanism, uniquely binds this eReceipt to the modules of the Participant Portal of the European Commission, to the transaction for which it was generated and ensures its full integrity. Therefore a complete digitally signed trail of the transaction is available both for your organisation and for the issuer of the eReceipt.

Any attempt to modify the content will lead to a break of the integrity of the electronic signature, which can be verified at any time by clicking on the eReceipt validation symbol.

More info about eReceipts can be found in the FAQ page of the Participant Portal. (http://ec.europa.eu/research/participants/portal/page/faq)