

Security Personal Helper based on Enhanced Reputation, Identity management and Cryptographic data Storage (Project establishment support - PES)Application Number: ES488794 Project Number: 0

Applicant**Project Owner**

Institution / company (Norwegian name)	MOVATION AS
Faculty	
Institute	
Department	
Address	Fridtjof Nansens plass 9
Postal code	0160
City	OSLO
Country	Norge
E-mail	josef.noll@movation.no
Website	www.movation.no
Enterprise number	889497092
eAdministration	

Project administrator

First name	Josef
Last name	Noll
Position/title	Chief Technologist
Phone	90838066
E-mail	josef.noll@movation.no
Confirmation	<input checked="" type="checkbox"/> The application has been approved by the Project Owner

Project manager

First name	Josef
------------	-------

Security Personal Helper based on Enhanced Reputation, Identity management and Cryptographic data Storage (Project establishment support - PES)

Application Number: ES488794 Project Number: 0

Last name	Noll
Institution / company (Norwegian name)	Movation
Faculty	
Institute	
Department	
Address	Fridtjof Nansens plass 9
Postal code	0160
City	Oslo
Country	Norge
Position/title	Dr
Academic degree	Dr
Preferred language	English
Phone	90838066
E-mail	josef.noll@movation.no

Project info

Project title

Project title	Security Personal Helper based on Enhanced Reputation, Identity management and Cryptographic data Storage
---------------	-----------------------------------------------------------------------------------------------------------

Primary and secondary objectives of the project

Primary and secondary objectives	Establish an EU project for FP7, objective 1.4 "trustworthy ICT", deadline 17. Jan 2012
	<p>Primary objective</p> <p>* deliver proposal in Q1.2012</p>
	<p>Secondary Objective</p> <p>* establish an ecosystem of Norwegian partners to find a market for the envisaged technology</p>

Project summary

Security Personal Helper based on Enhanced Reputation, Identity management and Cryptographic data Storage (Project establishment support - PES)

Application Number: ES488794 Project Number: 0

Project summary

SPHERICS aims to bridge the current gap between final end users and Internet service providers, by offering an intermediate element acting as a helper or facilitator. The main aim of this intermediate element, and of SPHERICS, is to provide user-centric security and privacy solutions based on these main pillars:

* Identity management as the key element for the end users to keep under control their authentication information and their attributes. This component is aiming to provide a homogeneous way to access different Internet service providers with almost no user intervention. Issues arising in this particular field are related to the definition of standard interfaces to provide authentication, authorization and access control information to different Internet services solutions. Moreover, the integration of reputation and privacy mechanisms as part of IdM solutions in use for the Internet has to be taken into consideration. The evaluation of assurance information about the identities accessing the services is also an important aspect of this key element.

* Trust and reputation management as the mechanism aiming to help in selecting between different service providers based on their reputation within the community. It will be based on an end user's past experiences of service providers and the reports of other entities on them. By using this approach users are able to make smarter and safer decisions when having to choose a service provider in the Internet. Current challenges in this area include: how to actually compute reputation scores, how to gather and store users' feedback, how to bootstrap the system or how to deal with certain specific security threats such as collusion or Sybil attack, for instance. Another challenge is to investigate the links between identity management and reputation, as indicated above. We could consider the inclusion of a reputation manager within the Identity provider that will allow users to take reputation into account.

Funding scheme

Supplementary info from applicant

Programme/ activity	PES
Application type	Project establishment support
Topics	
Other relevant programmes/ activities/ projects	FP7, objective 1.4, Trustworthy ICT - submission: 17Jan2012
Discipline(s)	ICT, Security

Security Personal Helper based on Enhanced Reputation, Identity management and Cryptographic data Storage (Project establishment support - PES)

Application Number: ES488794 Project Number: 0

If applying for additional funding, specify project number

Have any related applications been submitted to the Research Council and/or any other public funding scheme

No

If yes, please provide further information

Progress plan

Project period

From date (yyyymmdd) 20111207

To date (yyyymmdd) 20120117

Main activities and milestones in the project period (year and quarter)

Milestones throughout the project	From		To	
establish EU FP7 proposal	2011	4	2012	1

Budget

Cost plan (in NOK 1000)

	2011	2012	2013	2014	2015	2016	2017	2018	Sum
Payroll and indirect expenses	120								120
Procurement of R&D services									0
Equipment									0
Other operating expenses									0
<i>Totals</i>	120	0							120

Security Personal Helper based on Enhanced Reputation, Identity management and Cryptographic data Storage (Project establishment support - PES)

Application Number: ES488794 Project Number: 0

Specification

costs are related to writing the proposal

Cost code (in NOK 1000)

	2011	2012	2013	2014	2015	2016	2017	2018	Sum
Trade and industry	120								120
Independent research institute									0
Universities and University Colleges									0
Other sectors									0
Abroad									0
<i>Totals</i>	120	0							120

Funding plan (in NOK 1000)

	2011	2012	2013	2014	2015	2016	2017	2018	Sum
Own financing	60								60
International funding									0
Other public funding									0
Other private funding									0
From Research Council	60								60
<i>Totals</i>	120	0							120

Specification

Movation is main participant, but responsible to build a use-case network consisting of Norwegian industry, Research and SME. Ongoing discussions with Telenor on App-store use-case, with Opera Software on Cloud use case, with FFI on identity and trust measurement and with SMT on context-aware information handling to social networks and the cloud.

Security Personal Helper based on Enhanced Reputation, Identity management and Cryptographic data Storage (Project establishment support - PES)

Application Number: ES488794 Project Number: 0

Partners

Partners under obligation to provide professional or financial resources for the implementation of the project

1

Institution/ company	Movation
Department/ section	
Address	Fridtjof Nansens plass 9
Postal code	0160
City	Oslo
Country	Norway
Enterprise number	
Contact person	Josef Noll
Contact tel.	90838066
Contact e-mail	josef.noll@movation.no
Partner's role	Financing and Research activity

Attachments

Project description

Filename	Spherics-1_1-Concept-p1-5.pdf
Reference	ES488794_001_1_Projektbeskrivelse_20111207

Other items

Filename	Spherics-2_2-Individual-participants.pdf
----------	------------------------------------------

Security Personal Helper based on Enhanced Reputation, Identity management and Cryptographic data Storage (Project establishment support - PES)

Application Number: ES488794 Project Number: 0

Reference ES488794_010_1_Annet_20111207

B1.1 Concept & objectives

B1.1.1 Concept

Albert has just started up a small business, and needs to rapidly expand his computing resources to exploit his new idea. Outsourcing these to an Internet-based service provider is ideal for him in terms of cost and flexibility, and after a quick search he finds several of these offering what he needs. However, he does not know any of them and therefore their expected behaviour. Since he has to trust the service provider with its intellectual property but has no hint about the secure handling of this, he is worried and decides he cannot risk it. As a result, he feels disappointed that he has to set up the computing infrastructure himself, and concerned that his competitors may get to market first and at a lower cost.

End users are understandably distrustful when their personal, private and sensitive data is externally managed by an entity (possibly unknown) in the Internet, and they would therefore like to have more control over what is happening to their data, how it is actually being managed, which service provider is really having access to it and under what circumstances.

Thus, **SPHERICS (Security Personal Helper based on Enhanced Reputation, Identity management and Cryptographic data Storage)** aims to bridge the current gap between final end users and Internet service providers, by offering an intermediate element acting as a helper or facilitator¹. The main aim of this intermediate element, and of **SPHERICS**, is to provide user-centric security and privacy solutions based on the next three main pillars:

- **Identity management** as the key element for the end users to keep under control their authentication information and their attributes. This component is aiming to provide a homogeneous way to access different Internet service providers with almost no user intervention. Issues arising in this particular field are related to the definition of standard interfaces to provide authentication, authorization and access control information to different Internet services solutions. Moreover, the integration of reputation and privacy mechanisms as part of IdM solutions in use for the Internet has to be taken into consideration. The evaluation of assurance information about the identities accessing the services is also an important aspect of this key element.
- **Trust and reputation management** as the mechanism aiming to help in selecting between different service providers based on their reputation within the community. It will be based on an end user's past experiences of service providers and the reports of other entities on them. By using this approach users are able to make smarter and safer decisions when having to choose a service provider in the Internet. Current challenges in this area include: how to actually compute reputation scores, how to gather and store users' feedback, how to bootstrap the system or how to deal with certain specific security threats such as collusion or Sybil attack, for instance. Another challenge is to investigate the links between identity

¹ Within the scope of **SPHERICS**, we will use indistinctly the terms *helper* and *assistant*, considering them as synonyms in this context.

management and reputation, as indicated above. We could consider the inclusion of a reputation manager within the Identity provider that will allow users to take reputation into account before deciding which Internet service provider (among a certain list) to interact with and exchanging certain personal data identifying themselves.

- **Secure data storage and processing.** Advanced techniques have been recently developed for storing data on potentially untrusted infrastructures owned by untrusted entities without compromising the confidentiality of the data. Such techniques could empower the end users by letting them take control of the security of their data in the Internet, and not having to rely on the service providers to do this for them. In **SPHERICS**, secure data storage by means of advanced cryptography techniques is a key element in the final successful acceptance of Internet applications processing personal or confidential data. Besides providing guarantees for confidentiality, cryptographic data storage can also provide additional resilience against service providers' failures or malware attacks. As a result, the deliberate disruption or accidental failure of a service provider will not compromise the service or the data it is based on. The user will have a choice between different confidentiality and availability guarantees.

All these three major technologies considered in **SPHERICS** will be addressing a certain number of key technical challenges and functionalities as these ones now described:

- **User-centricity and usability** are often aspects that are not fully considered as part of the different solutions that service providers are offering. This is making end users reluctant to widely adopt these solutions. **SPHERICS** is intended to define an intermediate element closer to the user acting as a helper application/middleware that will be easy to use and where security and privacy properties can be directly managed. This project is also intended to create a user model integrating different aspects such as computing skills, domain expertise, usage frequency, etc. so different types of end users can be identified and the different security services can be personalized in the way they are presented to the user.
- **Privacy-awareness** is one of the main concerns of end users when making use of the Internet. Different technical solutions have been defined in order to provide privacy for Internet services, such as the use of trusted computing, searchable encryption, just-in-time encryption, data obfuscation, etc. However, there is no easy way to make these technical solutions closer to the final users, so they can select the particular technology to use depending on the requirements of the data being managed or the security level required at a particular moment. In this project, we will develop mechanisms that enable users to establish customized privacy policies, in a simple and user-friendly way.
- **Seamless data portability** in a secure and reliable manner is a commonly neglected factor when developing Internet services. Yet, it is usually one of the features most frequently demanded by end-users. Their perception about the potential (and nowadays probable) loss of (all or part of) their sensitive and private data, or its uncontrolled disclosure to unauthorized entities, hinders the users from transferring their data between different service providers. **SPHERICS** will provide the mechanisms needed to ensure secure and seamless portability of users' data in the Internet.

The main goal of our approach is to increase the users' security and privacy in the Internet, in order to foster the broad development and acceptance of Internet services solutions.

Solution: A User-Centric Security and Privacy Facilitator based on Enhanced Trust and Reputation, Identity management and Cryptographic data Storage.

By means of a smart integration of the three main technologies abovementioned - Identity management, trust and reputation management and secure data storage and processing - **SPHERICS** aims to provide end-users in the Internet with a simple and friendly security assistant, guiding them in some of the most common interactions with service providers today. Thus for instance, the assistant will allow users to select the most trustworthy services based on the reputation of their providers, as well as to have a tight control over their personal data and how such data is stored, processed and transferred to other providers.

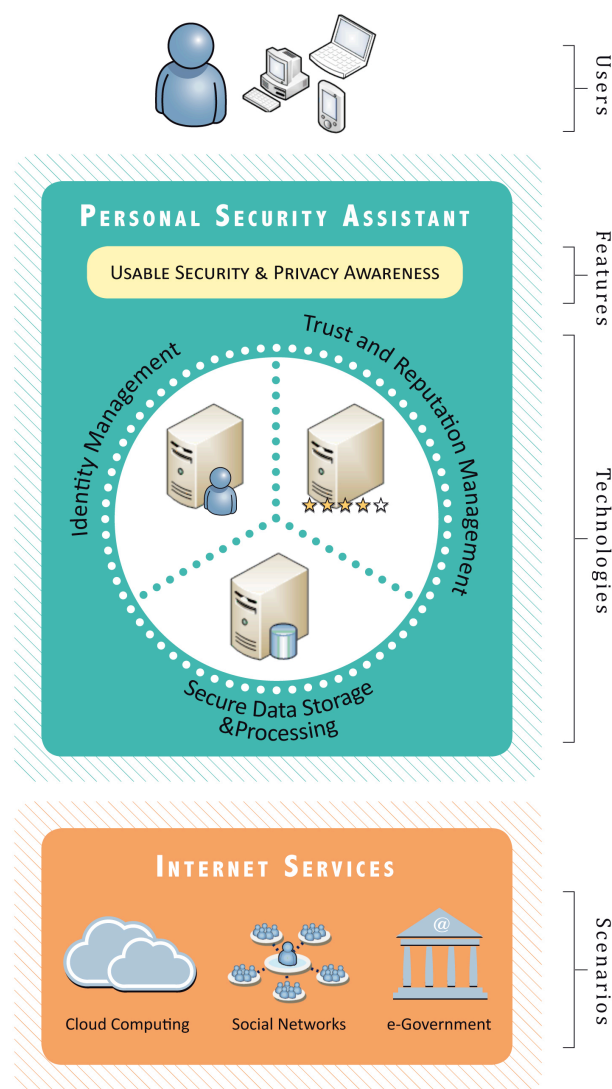


Figure 1: Overall illustration of SPHERICS

Figure 1 shows the overall picture of **SPHERICS**. As it can be observed, the end-users are the focus of this project as well as the entities whose security and security perception is aimed to be improved. They will be given the control over their personal and sensitive data handled in the Internet, by allowing them to select the security level they want to apply for each transaction.

As of scenarios to get the requirements and validate the results, the **SPHERICS** project will be focusing on cloud computing, social networks and e-Government, as shown next. Each of them is having a certain functionality to be considered in particular regarding end user data management, being confidentiality the most relevant in the cloud computing scenario, privacy in the social networks scenario, and accountability in the e-Government scenario.

Use case: Cloud computing

Alice is a businesswoman who just started a small enterprise. Her work requires travelling quite often and she bought both a laptop and a Smartphone, besides her PC. She would like to have access to her business documents wherever she is and through all her devices. Since her enterprise does not own the needed infrastructure, she decides to outsource such data in a cloud provider.

User-centricity and usability

However, she does not feel very comfortable delegating the assets of her company to an unknown entity, without a guarantee of the preservation of the privacy of her business sensitive data.

Privacy-awareness

She does not know any cloud provider offering the service she looks for and starts searching for the most appropriate one. The **SPHERICS** assistant offers her an reputation assessment for each of the cloud providers found, based on a smart aggregation of the feedback provided by previous users of each of those providers.

Trust and reputation management

Once she has selected the cloud provider she wants to interact with, she is required to create a new user account. However, she does not want to create yet another account, but rather benefit from the Single Sign-On advantages of her OpenID one.

Identity management

The selected cloud provider supports several alternatives for securing the stored data. Alice selects the most appropriate for her business, depending on its necessities on data protection, resilience and availability. It can be also the case where Alice does not trust the Cloud Provider and wishes to protect her data before storing it. Also, if she does not trust the Cloud Provider to have a high enough availability she might wish to store the data across several providers to add redundancy. **SPHERICS** allows her to develop any of these

Secure data storage and processing

three options to protect her data.

After one year, her business has successfully grown and she needs to move all her company sensitive data to another cloud provider offering a better quality service. The **SPHERICS** assistant helps her to move all this data in a seamless, transparent and secure way.

**Seamless data
portability**

Use case: Social networks

Bob wants to share his personal information and data (photos, videos, etc.) with his family, friends and acquaintances. Moreover, he wants to retain the control over his data at every moment and to be capable to easily adjust by himself the policies that govern the access to his data.

**User-centricity and
usability**

However, he does not want certain videos to be available to all of his contacts.

Privacy-awareness

There exist several social network providers, but Bob has no previous experience with them.

**Trust and
reputation
management**

He wants his profile to be linked with his identities and associated profiles in other social networks

**Identity
management**

Once Bob has made a decision, aided by the **SPHERICS** assistant, he would like that the provider that stores his data does not have access to the content. However, he would expect that the provider still be able to process the data, for example, to perform searches.

**Secure data
storage and
processing**

Due to a change on the privacy policies of his current social network provider, Bob wants to move his personal information to another social network, which has a more appropriate privacy policy for him. The **SPHERICS** assistant should make the process of portability easy.

**Seamless data
portability**

2.2 Individual participants

2.2.1 NEC Europe Ltd. (NEC)

NEC Corporation produces tailored solutions in the core technologies and services required in a networked world, ranging from advanced semiconductor solutions, to large-scale mission critical systems, systems integration, and broadband and mobile technologies. The NEC group employs more than 100,000 people worldwide with a multi-billion dollar sales volume world-wide. NEC began business in Europe in the early 1970s. Since then, NEC's activities have steadily increased to include sales, manufacturing and R&D functions.

NEC Europe Ltd., which is wholly owned by NEC Corporation, was established in London in 1993. The NEC Network Laboratories in Heidelberg, Germany, have been established in 1997 as NEC's second European research facility. A special emphasis here lies on solutions that meet the needs of NEC's European customers, focusing on software-oriented research and development for the next-generation Internet, such as new communication architectures and protocols to support multimedia delivery and mobility together with intelligent Internet services. NEC Network Laboratories have had specific focus on security, privacy, identity, network management, transport and routing and mobility.

NEC Laboratories Europe has participated in many projects focusing on security and trust in the future Internet. This includes the topics of securing critical infrastructures (WSAN4CIP), a trustworthy Internet of Things (SENSEI), network security and inter-domain monitoring (DEMONS), and in Identity Management (SWIFT).

Innovative role in the project

NEC will bring in his extensive experience in trust and reputation management as well as secure data storage and processing. In particular, NEC will contribute with his expertise in the areas of trust and reputation management integration in Identity management systems. In addition, NEC will focus on the application of multi-party computation in order to preserve the privacy of sensitive users' data.

Main tasks NEC is involved in

WP2: NEC will work on the overall architecture of the security assistant and on defining the interfaces for the integration of trust and reputation management and secure storage and processing methods.

WP4: NEC will strongly contribute to the trust and reputation management components, working on the interoperability of trust management systems and the protection of user input.

WP5: NEC will strongly contribute to the secure storage and processing architecture. NEC's focus is on advanced cryptographic solutions for secure data storage and methods for flexible data processing using multi-party computation and functional encryption.

WP6: NEC is leader of this Work Package and will lead the specification of the security assistant contribute to the implementation and integration of enablers developed in WP4 and WP5 into the security assistant. NEC will work on the demonstrator for the cloud computing scenario.

WP7: NEC will actively work on the dissemination and exploitation of project results. Dissemination will aim for high-visibility publications at workshops, conferences and in Journals. Demonstrators will be shown at internal and external events. NEC targets exploiting project results in following business unit projects.

Profile of key staff members

Dr. Félix Gómez Mármol is a research scientist in the security group at NEC Laboratories Europe, Heidelberg, Germany. His research interests include authorisation, authentication and trust management in distributed and heterogeneous systems, security management in mobile devices and design and implementation of security solutions for mobile and heterogeneous environments. He received an MSc and PhD in computer engineering from the University of Murcia, Spain.

Dr. Jens-Matthias Bohli received a master's degree in 2003 and doctorate degree in 2007, both in Computer Science from the University of Karlsruhe. Currently, he is a senior researcher in the security group at NEC Laboratories Europe which he joined in 2007. He worked on the European projects UbiSec&Sense, WSAN4CIP, SENSEI, and DEMONS and has experience in leading Work Packages and Tasks. During winter 2009/2010 Jens-Matthias was at the University of Sussex teaching a course on Security Engineering. His research interests include cryptography, wireless security, and privacy and trust in the Future Internet.

2.2.2 Universidad de Málaga (UMA)

The Network, Information and Computer Security (NICS) Lab at University of Malaga is an international leading Security research group headed by Javier Lopez, Full Professor of the Computer Science Department. NICS is composed of 20 persons, including faculty members, post-docs researchers, top PhD students, and technical and management staff, being distributed on two different locations, the university premises at Andalusian Scientific Park and the Computer Science Department at Campus Teatinos.

NICS members have participated in more than 40 security research projects at international and national level, funded by V, VI and VII European Frameworks Programmes as well as by different Ministries in Spain, Japan, Norway and Singapore. Additionally, NICS members have published over 200 publications, among them more than 40 journal publications with impact factor (ISI-ranked).

NICS Lab actively participates in international committees and Working Groups in the Security area, as well as in the organization of multiple international conferences and workshops. Moreover, NICS is particularly dynamic in the exchange of researchers with other research institutions, having signed official scientific and technical cooperation agreements in US with NIST (Information Technology Laboratory, Computer Security Division), and in Singapore with I2R (Cryptography & Security Department).

Over the years, NICS members have been especially active in technology transfer to companies like ATOS Origin, HP Labs, Telefonica, France Telecom, Siemens, Indra, Banesto, Orange, Endesa, Sermepa and Telvent, as well as to public entities like the Spanish Ministry of Defense, the Andalusian Government, and RedIRIS (Spanish advanced communications network for academic and R+D Centres).

Innovative role in the project

The NICS Lab at UMA will provide its expertise in Network and Information Security, and particularly, in Trust and Reputation Management.

Main tasks UMA is involved in

WP2: UMA will collaborate both in T2.1, especially in the requirements derived from the social networks usage case, and T2.2, that will define the architecture of the system.

WP3: UMA will participate in the analysis of the state of the art on Identity Management (T3.1) and in the design of the Identity component of SPHERICS (T3.2)

WP4: UMA will lead this work package, providing its expertise in Trust and Reputation Management systems, and will take part in all the associated tasks (T4.1, T4.2 and T4.3)

WP5: UMA will lead the analysis of the state of the art on Secure Storage and Processing (T5.1) and will participate in the design of its associated component (T5.2)

WP6: UMA will collaborate in the integration of the different components into a single prototype (T6.1) and in the validation process of the Social Network usage case (T6.3)

WP7: UMA will take part in both the dissemination and standardisation activities within the project (T7.1 and T7.2)

Profile of key staff members

Prof Javier Lopez received his MSc and PhD degrees in Computer Science in 1992 and 2000, respectively, from University of Malaga. He, is currently Head of Department, where he, and during last ten years has developed part of his research in USA, Japan and Australia. His activities are mainly focused on network security and critical information infrastructures, leading a number of national and international research projects in those areas, including projects in FP5, FP6 and FP7 European Programmes. He is steering committee member of ERCIM WG on Security and Trust Management, and has been the Chair of IFIP Trust Management WG from June 2006 to May 2009.

Dr Isaac Agudo is Associate Professor at the Computer Science Department of the University of Málaga. He has been involved in different European (PICOS, SPIKE and, most recently, PASSIVE) and national research projects since 2002, when we obtained his Master Degree in Mathematics. He received his PhD in Computer Science in 2008 by the University of Málaga. His publications focus in the area of identity management and access control. He has participated in the organization of international conferences and in the editorial board of journals in the field of information security.

Dr Carmen Fernández-Gago is a Postdoctoral researcher at the department of Computer Science of the University of Málaga. She holds a PhD, in Computer Science from the University of Liverpool (United Kingdom), and has worked there on Verification Techniques for non-monodic First-order Temporal Logics. In January 2006 she joined the group NICS at University of Málaga, where she works since then as a postdoctoral researcher. Her main interests are in the area of trust and reputation management systems. She has published many research papers in the area and is a member of several program

committees. She has also worked in several European projects such as SERENITY, GREDIA, SPIKE and currently NESSoS.

David Nuñez received a M.Sc., in Computer Science from University of Málaga in 2010, and currently he is working on his Ph.D. in Information Security. His research interests include cloud computing, identity managements and cryptography. He is currently participating in the FP7 project PASSIVE, focusing in the area of identity management, authentication and authorization.

2.2.3 Portugal Telecom Inovação, SA

Portugal Telecom Inovação, SA develops innovative and competitive services and solutions for the telecommunications market. Our success has been built and sustained on the competences we can call on in applied research, technology integration, services and solutions development, telecommunications engineering and training services. Major products include systems and solutions for intelligent networks (IMS - next generation/convergence approach), Access Networks (both copper and optical), Multimedia and IP Solutions, Mobile Networks, Services and Platforms, Network Management, Business Intelligence, IT Systems and Software Engineering, as well as Telecommunications Business Processes, Support and Training. With operations spread over three continents and its headquarters in Aveiro, PT Inovação also has branches in Oporto and Lisbon. In Latin America, the company has a subsidiary in São Paulo and, more recently, has set up a software development centre in Salvador, both in Brazil. Since last year, the operation in Africa has been centered on a subsidiary company in Luanda, Angola. PT Inovação promotes R&D cooperation and has privileged partnerships with major universities and centres of innovation, at both the national and international level. The company holds several certifications: Quality Management Certification System that complies with ISO 9001 standards, the ISO 14001 Environment Management Certification and the NP 4457 Management System for Research, Development and Innovation.

As the main R&D branch of the larger Portugal Telecom group, its role is to search and develop innovate technical solutions that enable the launch of new and advanced services. PTIN has been involved for many years in several European research projects in different areas from Network to Services and Experimentation/Pilots. In those projects, PTIN played different roles like management, technical contributions and leadership. Examples of such projects are DAIDALOS, AROMA, MUSE, 4WARD, SWIFT and more recently MEDIEVAL, Cloud4SOA, SAIL and SEMIRAMIS, just too few some of them. PTIN has deep knowledge and instantiation experience in terms of IMS and Next Generation Networks (NGN) as well. Lately PTIN was involved in the development of several context and privacy aware IPTV applications for PT IPTV commercial service.

Innovative role in the project

As an operator PTIN will bring their expertise in network (infrastructure), service and business domains. PTIN will mostly contribute to the research, development and instantiation of the solution in the areas of identity, privacy and trust.

Main tasks PTIN is involved in

WP2: PTIN will lead this work package. It will define some usage scenarios for Spherics and identify the requirements for each one. In this work package PTIN will collaborate in the system architecture definition.

WP3: PTIN will participate contributing with the already acquired know-how in what concerns Identity management. PTIN will do the Identity Management State of the Art analysis and capture the Identity Management requirements of the IdM system component.

WP7: PTIN will participate in the dissemination tasks with some promotion initiatives internal to the company's group. PTIN will participate in the exploitation task promoting the tools and techniques developed in Spherics scope, to the PT group companies.

Profile of key staff members

Ricardo Azevedo Pereira received his diploma in Computer and Telematics from the University of Aveiro, in 2003 and his MSc degree in Internet Computing from the Queen Mary College, University of London, in 2006. From 2004 to 2005 worked at Institute of Telecommunications, in Aveiro in the QoS and Mobility areas. In 2005 he joined PT Inovação, in Aveiro, where he currently occupies a project and product manager position and technically leads the Identity and Context Management teams. Moreover he has been responsible for close to product projects, mainly in QoS and IdM. He has been involved in several European projects (DAIDALOS, AROMA, MUSE, SWIFT, SEMIRAMIS) and Eurescom studies. He holds the vice-chairman of the ETSI ISG "Identity and Access Management for Networks and Services" group.

Sónia Pinho concluded her degree in Systems and Informatics Engineering in the year 2000 from Minho University in Braga, Portugal. She joined PT Inovação (PTIN) in Aveiro as a trainee in March 2000, and worked in the Internet Protocol Area, with special focus on the routing protocols evaluation and statistics. Since 2001 she worked as internal network, accesses and network security administrator, in PT Inovação. Furthermore, she was involved in the design and implementation of the security solutions for PTIN LAN and Wireless LAN, as VPN for remote access, LAN-to-LAN VPN, perimeter security, proxying, DNS, DHCP, Certification Authority, WLAN authentication (based on a Radius Server integration with

Microsoft Active Directory). She has many specializations on the network and security area: CCNA certification, ITIL v3 Foundation certification and many courses taken on Cisco Routing, Switching and Security Solutions. Since June 2010 she is working as a researcher in European CIP Projects and as instructor in IP and Network Security area. She is now involved in some FP7 projects and Eurescom studies in the Identity Management, Trust, Privacy and Security area like SEMIRAMIS and Eurescom P2057.

Telma Mota has a degree in Electrical and Computing Engineer and a master degree in Telecommunications both from the Engineer University of Porto. She has been a project manager at PT Inovação for more than 15 years and her main area of expertise is Service and Network Management, specification and design of open and distributed architectures.

She started in the Planning Department of the Portuguese Telephone Company and in 1994 she joined PT Inovação (the research center of Portugal Telecom) where she got expertise in the most relevant service and network architectures such as IN, IN evolution, TINA, Parlay, IMS, TISPAN and MBMS. Since then she has been responsible for PTI participation in several ACTS/IST and EURESCOM projects. Currently, she is the head of the “Platforms and Multiservice Networks” group in PTIN.

2.2.4 Universidad de Murcia (UMU)

The University of Murcia is a large University with approximately 30.000 students and 3.000 staff members. For the Faculty of Computer Science, the Intelligent Systems and Telematics Group, from the Department of Communications and Information Engineering will be participating in this project. This group has experience in security in network infrastructure and at the service and application level. UMU has been collaborating in different national and international research projects, and establishing collaborations with important international research institutions. Relevant to this project UMU has been participating in SEINIT, POSITIF and DESEREC IST projects, working in different aspects as public key infrastructures, key management, secure signaling, policy languages, policy and semantic-based based network and service management and access control and secure services based on SOA. Additionally, UMU is currently working on the SEMIRAMIS IST project directly related to the provision of advance services based on identity in cross-border and cross-domain scenarios.

Innovative role in the project

The UMU team will be providing its expertise in the deployment of real scenarios, in particular those related with cloud computing, and the provision of identity management solutions.

Main tasks UMU is involved in

WP2: UMU will be contributing with the definition of requirements for the cloud computing scenario.

WP3: UMU will be leading this WP and contributing with the design of the identity module.

WP4: UMU will contribute to the integration of the identity and reputation modules.

WP6: UMU will contribute to the implementation of the identity management component and the integration of the whole architecture.

WP7: UMU will participate in the dissemination tasks.

Profile of key staff members

Gregorio Martinez Perez received a M.S. and Ph.D. degrees in Computer Science at the University of Murcia (Spain). In 1997 he started to work in the Computer Service of the same University on various projects related to security and networking. In 1999 he started as research staff in the Department of Information and Communications Engineering of the University of Murcia. In 2001 and 2007, he was appointed lecturer and associate professor in the same department, respectively. Recently he has been approved for promotion as a full professor. His scientific activity is mainly devoted to security and the distributed management of IP based communications networks. He is also working on open source models and real-time and critical applications and systems. He is working on different national and European IST research projects related to these topics. As part of these projects he is collaborating with different universities, companies and research centers across Europe. He has been doing several research internships as visiting professor in the Department of Computer Science of the University College London (UCL-CS) and the Département Informatique et Réseaux of the École Nationale Supérieure des Télécommunications (ENST-INFRES) in Paris. He has published more than 100 papers in national and international conference proceedings, magazines and journals. Gregorio has been guest editing several special issues in different journals and magazines. He is member of the editorial board of 12 journals and member of the review board of more than 20 high level journals and magazines.

Felix J. Garcia Clemente received a M.S. and Ph.D. degrees in Computer Science at the University of Murcia (Spain). In 1999 he started to work on national and European IST research projects related to security and networking as research staff in the Department of Information and Communications Engineering of the University of Murcia. In 2002 and 2011, he was appointed lecturer and associate professor in the Department of Computer Engineering, respectively. His scientific activity is mainly devoted to security and the distributed management of IP based communications networks. Currently he is working on different national and European research projects related to these topics. As part of these projects he is collaborating with different Spanish and European universities, companies and research centers. He has published more than 40 papers in national and international conference proceedings, magazines and journals.

2.2.5 Thales UK Research and Technology (TRT)

Thales UK Research and Technology (TRT) is the UK research and innovation centre for the Thales Group of companies. The Thales Group is a major player in civil and commercial markets around the

world and is a leading defence contractor. Thales shares advanced technologies and draws on complementary capabilities across the Group to meet the specific requirements of each customer. TRT undertakes research programmes of interest to the Divisions of the Thales Group to provide technologies and processes in support of the development of new products and services. We also provide a range of consultancy and support services to Thales companies. We have around 100 Engineers, Scientists and Mathematicians at our Reading site with a wide range of knowledge and experience. Our main areas of expertise are Radio Communication Products, Precise Positioning and Navigation, Video Image Processing, Signal Processing, Information Security and Secure Communications. TRT has been involved in Information Security related activities since the mid 1980's and have skills ranging from encryption algorithm implementation through security architecture development to software evaluation.

We work closely with the Thales Business Lines at all stages of their programmes delivering research, proof of concept demonstrators, advanced development and consultancy. TRT has been involved in many successful collaborative research projects funded by the EC and the UK Technology Strategy Board. Among those completed within the last five years, are: EC FP7 project INTERSECTION developing a distributed security architecture for heterogeneous interconnected networks, EC FP6 project ENTHRONE implementing an MPEG21 end to end multimedia distribution chain, EC FP7 project SENSEI developing a service based infrastructure for Internet connected sensor networks and actuators, EC PASR project SOBCAH demonstrating an integrated port security system, We are also involved in the following "live" projects: EC FP7 project PASSIVE developing techniques for using computing virtual machines in high assurance environments, FI-WARE a part of the FI-PPP future internet programme, EC FP7 project CONTAIN developing a secure information infrastructure for cargo container security.

Innovative role in the project

TRT will use its strong background in information security to develop techniques and technologies for secure data storage and processing. A particular focus for TRT will be applying our industrial experience to making the use of such techniques practical in the context of this project.

Main tasks TRT is involved in

WP2: TRT will participate in the scenario development and requirements capture with a particular emphasis on the secure storage and operations on encrypted data. It will also contribute to designing the architecture of the Personal Security Assistant.

WP5: TRT will lead this work package and will develop techniques and technologies to secure data stored and processed by online service providers. It will also contribute to designing and implementing the secure data storage and processing enabler.

WP6: TRT will contribute to the specification, integration and validation of mechanisms for secure data storage and processing. It will also contribute validating the Personal Security Assistant for the e-government scenario.

WP7: TRT will contribute to the dissemination activities of the project through the production of publicity material and academic papers. We will also participate in the exploitation activities of the

project including promotion to the appropriate companies in the Thales Group of the tools and techniques developed by the project.

Profile of key staff members

Dr. Adrian Waller joined Thales UK Research and Technology in 1997 after completing his PhD at Royal Holloway University of London and a one-year spell as a post-doctoral researcher at the University of Ljubljana in Slovenia. He is now a Technical Consultant in Information Security responsible for providing consultancy and research expertise on a wide variety of projects. Adrian has a strong track record in security research and innovation, and has published numerous papers and is the holder of several patents. He has presented at many international conferences, including being a keynote speaker, and acts on several programme committees. Adrian has significant experience in international collaborations, especially on EC research projects including SEINIT, ESSTRT, e-SENSE, SENSEI, PASSIVE and FIWARE. He has also been a Work Package leader. He has developed good relationships with leading UK Universities in Information Security - including Surrey, RHUL and Liverpool John Moores – and acts as a PhD industrial supervisor, presents seminars for MSc courses, and gets involved in course assessment and advisory board activities.

Sarah Pennington joined Thales UK Research and Technology in 2007, and is now a Senior Engineer. Her research interests include techniques for operating on encrypted data, identity management and access control. She has worked on the UK Technology Strategy Board project PAL and on EC networking and security projects including e-SENSE, I3CON and SENSEI. Sarah received her BA in Engineering and MEng with distinction from Emmanuel College, University of Cambridge in 2007. Sarah is a member of the IET.

Glyn Jones has been with Thales UK Research and Technology (TRT) since 1997. He is currently responsible for Cyber and Information Security research projects. He has previously led research programmes in Military Network Technology and in Last Mile fixed and mobile telecommunications. He has co-ordinated and participated in the TRT contributions to EC security and networking projects including SEINIT, SUPHICE, SOBCAH, INTERSECTION and PASSIVE and the UK Technology Strategy Board projects SIBIS, TEASE and PAL. He has also taken the role of work package leader on EC projects. Glyn is leading the TEASE project, researching the use of information provenance as a measure of trustworthiness. He is Industrial Steering Group Chair for the Mobile VCE Instant Knowledge Programme and a member of the NATO MSG-080 Collective Mission Simulation Working Group. Prior to joining TRT, Glyn was employed by GEC on telecommunications research at the Hirst Research Centre. Glyn gained his BSc from Durham University in 1978 and is a Chartered Engineer and a member of the IET.

2.2.4 Movation (MOV)

Movation is the leading independent resource center for open innovation in the Nordic. Movation helps start-ups and established companies to expand, extend and excel in their innovation activities. Movation was founded in 2006 by seven Norwegian companies, and was in 2009 transferred into an SME. Through Movation the partners created an arena where experts with different professional backgrounds and expertise exploited their knowledge in new ways to foster innovation.

The seven partners who started Movation are among the leading ICT companies in Norway including Fast Search & Transfer (FAST), Opera Software, and Telenor. Since then partners like Statoil, Sintef, DnB, Nets and Microsoft have joined to foster the innovation through the Movation Ecosystem. The main component is the Innovation Stock Exchange (<http://innobors.eu>), where ideas meet competent capital and challenging customers. The InnoBors has fostered several use-cases in the Future Internet and IoT, a.o. the first interactive electrical motorbike from ESIS.

Movation's expertise and partner network in IoT is widely acknowledged. Movation is administrative project leader of the EU Artemis pSHIELD project, where a.o. sensors systems have been installed on the measurement locomotive Roger from the Norwegian Railway Authority and integrated into the Telenor Shepherd platform.

Innovative role in the project

In SPHERICS Movation will use their knowledge in collaborative research to include cloud companies like Opera Software, App providers like Telenor¹ and communities like Mobile Monday. Movation will also disseminate the project results towards targeted partners in order to create an economic impact for the result of SPHERICS

Main tasks Movation is involved in

WP2: MOV will provide real-world requirements based on the InnoBors ecosystem of SMEs and Inner Circle partners.

WP3: MOV will contribute to the advanced identity management, based on experiences from our cloud solution.

WP4: MOV will lead the implementation of the Trust and Reputation Management (T4.3), and link the reputation to social network activities and professional relations.

WP6: MOV will lead the social networking scenario validation (T6.3), and will relate this work to business opportunities as seen for the InnoBors.

WP7: MOV will lead the workpackage and the dissemination task (T7.1). Besides the scientific dissemination coming from our academic partners and the exploitation from all industrial partners, the focus will be on targeted dissemination and business workshops to create an ecosystem for piloting the outcome of SPHERICS.

Profile of key staff members

¹ Telenor and Google have announced a common App-Store

Dr Josef Noll is Chief Technologist in Movation and leader of the InnoResearch unit. In the area of Internet of Things he is project leader of the Artemis pSHIELD project. Previously he was Senior Advisor at Telenor R&I in the Products and Markets group, and project leader of Eurescom's 'Broadband services in the Intelligent Home' and use-case leader in the EU FP6 'Adaptive Services Grid (ASG)' projects, and has initiated a.o. the EU's 6th FP ePerSpace and several Eurescom projects.

He is reviewer of the EU FP6/FP7 projects HYDRA, Pobicos, and Genesi, and evaluator of the EU's framework programme FP7, the Dutch IOP, the Austrian FIT, and the Cyprus research programmes. He is steering board member of Den Norske Dataforening (DND) "Semantic Web" and the "Mobile strategy" Special Interest Groups (SIG), co- editor of the Working Group 2 (WG2) White Paper "Semantic Services" and the cross-WP Outview User Profiles/Profiling for the Wireless World Research Forum (WWRF).

Truls Berg is a Norwegian entrepreneur, CEO and author, with more than 20 years experience in the IT industry. He holds a number of boards, is a frequently used speaker and is fixed chronicler of Computer World. He has so far helped to start up 10 enterprises, including the Component Software, Integrate and Comperio. In addition, he has assisted a number of other startup companies. Truls is the author of the book: Information Sea - a survival guide for tomorrow's knowledge workers. He is also the leader of the Innovation Forum Norway, where the leading 50+ Norwegian companies are presented. He will contribute with targeting dissemination and contacts towards specific use-case partners.