Small or medium-scale focused research project (STREP)

ICT Call 8

FP7-ICT-2011-8

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

S · P · H · E · R · I · C · S

Work programme topic addressed
Objective ICT-2011.1.4 Trustworthy ICT
Target outcome: b) Trust, eIdentity and Privacy management infrastructures

Proposal ID: 318126

Name of the coordinating person: Mario Hoffmann
e-mail: mario.hoffmann@aisec.fraunhofer.de
fax: +49 89 3229986-177

Participant no. *	Participant organisation name	Part. short name	Country
1 (Coordinator)	Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V.	Fraunhofer	Germany
2	NEC Europe Ltd.	NEC	United Kingdom
3	Universidad de Murcia	UMU	Spain
4	Universidad de Málaga	UMA	Spain
5	Thales UK Research and Technology	TRT	United Kingdom
6	Portugal Telecom Inovação, SA	PTIN	Portugal
7	Movation	MOV	Norway

PROPOSAL ABSTRACT

Many recent incidents have shown that users' data at service providers is insecure when the providers are attacked or exposed by malicious insiders. In addition, user accounts are not secure when it comes to targeted hacking or social engineering attacks, due to widespread existence of weak passwords or password reuse. The rapidly increasing number of Internet services makes it impossible for users to judge the trustworthiness of those services or providers.

The goal of **SPHERICS** is to significantly increase the users' security and privacy in the Internet by offering an intermediate element, called the Security Personal Assistant, which empowers users to control their sensitive data in a unified way. In particular, the assistant will be based on a unifying approach of integrating trust and reputation management, identity management, as well as cryptographic data protection. **SPHERICS** will apply the assistant to today's most discussed use-cases from cloud computing, social networking and e-government, which are challenging the current state-of-the-art technology.

SPHERICS will use identity management as the key element for enabling end users to maintain control of their authentication information and their personal attributes. This creates a homogeneous way to access different Internet service providers with minimal user intervention. The identity management will link to an easily accessible trust and reputation management system that allows selection of different service providers either by the user or automatically. It will be based on end users' past experiences with service providers and reports about the service providers from other entities. Secure data storage and processing allows sensitive information to be released in a way that is secure against compromised Internet services. Such techniques empower end users by letting them take control of the security of their data in the Internet, without having to rely on the service providers' integrity.

TABLE OF CONTENTS

Section 1: Scientific and/or technical quality, relevant to the topics addressed by the call 4
1.1 Concept and objectives.....4
1.1.1 Concept.....4
1.1.2 Objectives 10
1.2 Progress beyond the state-of-the-art 13
1.2.1 Identity Management 13
1.2.2 Trust and Reputation Management 14
1.2.3 Secure data Storage and Processing..... 15
1.2.4 Related EU projects 16
1.2.5 User interface design of identity and reputation management tools..... 18
1.3 S/T methodology and associated work plan..... 20
1.3.1 Overall strategy and general description 20
1.3.2 Work package interdependencies and timing..... 21
1.3.3 Detailed work package description 23
1.3.4 Risks and contingency plans 50
Section 2: Implementation.....53
2.1 Management structure and procedures..... 53
2.1.1 Management Structure 53
2.1.2 Committees 55
2.1.3 The Work Package Leaders..... 56
2.1.4 Management Procedure Tools 56
2.1.5 Communication Flow..... 57
2.1.6 Conflict Management 57
2.1.7 Consortium Agreement 57
2.2 Individual participants 58
2.2.1 Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)..... 58
2.2.2 NEC Europe Ltd. (NEC) 60
2.2.3 Universidad de Murcia (UMU)..... 62
2.2.4 Universidad de Málaga (UMA) 63
2.2.5 Thales UK Research and Technology (TRT)..... 65
2.2.6 Portugal Telecom Inovação, SA (PTIN) 67
2.2.7 Movation (MOV)..... 68
2.3 Consortium as a whole 70
2.4 Resources to be committed..... 73
Section 3: Impact.....74
3.1 Expected impacts listed in the work programme 74
3.1.1 Target outcomes of Objective ICT-2011.1.4 74
3.1.2 Expected impact of Objective ICT-2011.1.4 77
3.2 Dissemination and/or exploitation of project results, and management of intellectual property.. 80
3.2.1 Dissemination 80
3.2.2 Standardisation..... 82
3.2.3 Exploitation..... 83
Section 4: Ethical Issues 87
Annex: References.....88

Section 1: Scientific and/or technical quality, relevant to the topics addressed by the call

1.1 Concept and objectives

1.1.1 Concept

Consider the following fictitious, but realistic, motivating use case scenario. 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 facilitator[1]. 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** (IdM) 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 minimal 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 end users' 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

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

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 the ones described below:

- **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 adapt to users' models 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. They expect that a system takes care of their data, including sensitive, private and context data, and the disclosure of such data to unauthorized entities, non-trusted connections and unknown service providers. This lack of control hinders the users from transferring their data between different service providers. **SPHERICS** will provide the mechanisms needed to ensure the publishing of user data according to his very personal preferences to services in the Internet.

<u>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.</u>

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.

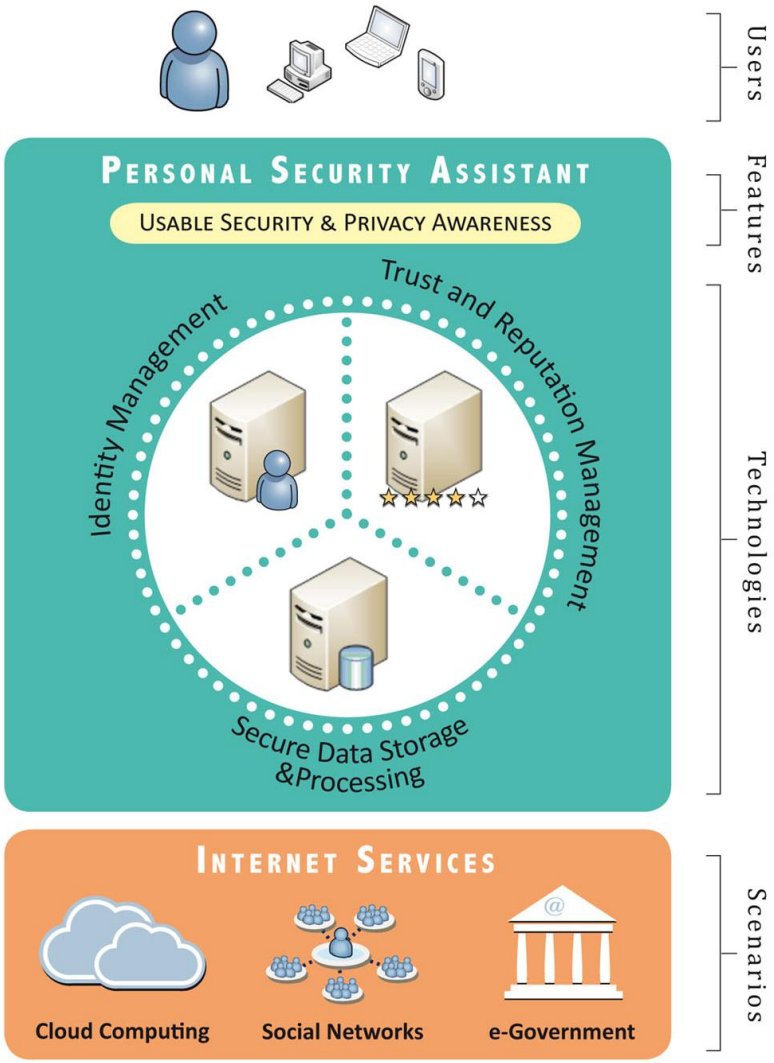

Figure 1. Overall illustration of SPHERICS

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 extract the requirements from 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 a 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 Connect one, in a secure and reliable way.	**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 three options to protect her data.	**Secure data storage and processing**
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 and pictures to be available to all of his contacts.	**Privacy-awareness**
There exist several social network providers, but Bob has no previous experience with them. In short, he is unaware of their reputation and expected behaviour.	**Trust and reputation management**
He wants his profile to be confidentially linked with his identities and associated profiles in other internet services.	**Identity management**
Once Bob has made a decision, aided by the **SPHERICS** assistant, he would like the provider storing his data not to have access to the content. However, he would expect the provider still to be able to process the data, for example, performing 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**

Use case: e-Government

John lives in a country where its government provides user-centric services to its citizens. More than engaging users during service design and development, the government provides a Service Oriented Architecture platform (i.e. Enterprise Service Bus) where governmental services and public and Citizen's private information are also available for consumption. On top of such platform a set of web portals are available for service consumption and service provisioning and exposition. Moreover the e-Government platform trusts registered third party identity providers for citizens' authentication when accessing e-Government services. John is not only a citizen but also a freelancer developer. He is developing a new service that composes e-Government and Web 2.0 media services. The service requests its users to authenticate, once it needs private e-Government related information to work correctly.	**User-centricity and usability**

When fully developed, the service will be made available (it will be part of the e-Government available service catalogue) to all citizens on the e-Government platform. Citizens can use the service, if they think it is interesting and developers can develop on top of the service by reusing its open functionalities.

Privacy-awareness

During the development John followed all the rules and best practices for service and e-Government widgets development, which means that all the interactions related with user consent and authorization is using **SPHERICS** technology.

When first using e-Government platform, Helen configures the privacy policies related with the service in a user-friendly way. Policies are stored within **SPHERICS** functions and reused latter during the services consumption. John's service is "just" one more service that will reuse the privacy policies Helen configured globally.

Trust and reputation management

Helen realized that a new service, in which she is interested, is available. She consults the service description and noted that John was the developer/owner of the service. She used John services in the past and it was as good experience. Nevertheless and once the service consumption includes access to her private information, she decided to use **SPHERICS** facilitator middleware to be sure that the service is safe to be used and will behave as expected.

Identity management

e-Government infrastructure provides open built-in Identity Management functions to be reused by all the services, which means citizens may use their e-Government IDs for authentication, authorization, etc. However Helen usually uses her Operator as her preferred Identity Provider. She configured the Operator's IdP to provide only the essential information for the requested Service Providers. Her identities are federated between both domains and disclose attributes pre-configured.

Secure data storage and processing

The service developed by John and being used by Helen requests access to Helen micro-blogging posts and permission to store locally such information for future processing. That information is private and Helen hesitates on permitting the service to store it. Nevertheless she knows that the e-Government platform guarantees information confidentiality and cryptographic data storage, guaranteeing that the information is not read by e-Government people and non-authorized services. She decides to give the needed authorization.

1.1.2 Objectives

Our goal:

This project aims to design and develop a simple, friendly user-centric security assistant to help service consumers in two of the most common interactions with different providers offering similar services: *i) selection of service providers based on their reputation;* *ii) secure interaction with the selected provider by means of secure data storage and processing mechanisms;*

Objective 1: Design and specification of a modular, extensible and user-centric middleware facilitator to help end-users securely select and interact with service providers in the Internet

This objective consists of specifying the overall architecture of the facilitator, as well as the usage scenarios (namely Cloud Computing, Social Networks and e-Government), derived from the collected user and service requirements. Usability and experience will be evaluated by performing end-user validation through application mock-ups. A set of open APIs will be developed using standard technologies suitable for a range of different devices (including mobile devices).

Relevant WPs: WP2, WP6

Key deliverables: D2.1, D2.2, D2.3, D2.4, D2.5, D6.1, D6.2, D6.3, D6.4

Related Milestones: MS3**,** MS5. The final architecture of **SPHERICS** will be realized in MS3 and MS5 will give as a result the final outcomes of **SPHERICS**.

Measures of success: Specification of the architecture that integrates the three enablers available as a basis for the implementation and integration. Evaluation results of the architecture including the application mock-ups.

Objective 2: Enabler "Advanced user-centric identity management" allowing users to maintain control over their personal data in the Internet

Today, users access services in the Internet through a range of devices from PCs to laptops or mobile devices (such as smartphones, tablets, etc). Moreover, their personal profiles and data are usually spread across and even duplicated in multiple third party locations/data storages, leading to a loss of control over their private and sensitive data. This project will focus on investigating advanced user-centric IdM techniques to foster Single Sign-On solutions while providing users with the ability to securely control and monitor the usage of their personal profiles and data in the Internet.

Relevant WPs: WP3

Key deliverables: D3.1, D3.2, D3.3

Related Milestones: MS1, MS2, MS3, MS4. MS1 will provide with the state of the art on identity management plus the requirements for the scenarios from this point of view. This will set up the basis for a preliminary architecture of the Identity Management component (MS2) that is going to be integrated into the final

architecture of **SPHERICS** (MS3). The component and the architecture will be tested later on (MS4).

Measures of success: Contributions beyond the state of the art in user-centric identity management. Integration of user-centric identity management in the overall architecture. Evaluation of the components and validation within the usage scenarios.

Objective 3: Enabler "Advanced trust and reputation management mechanisms" helping users to make informed choices between service providers

*With the continually growing number of service providers in the Internet, and the rapid evolution and adaptation of attackers, new risks are appearing all the time, and it is not always easy, or even feasible, to cope with all of them. Hence, we cannot expect a user to know every service provider and its likely behaviour beforehand. The **SPHERICS** middleware facilitator aims to provide advanced trust and reputation management mechanisms to inform end users and assist them in making smarter decisions on whom to interact with. Such selection would be based on the reputation of the service provider from the perspective of the service consumers.*

Relevant WPs: WP4

Key deliverables: D4.1, D4.2, D4.3

Related Milestones: MS1, MS2, MS3, MS4. MS1 will provide with the state of the art on trust and reputation management plus the requirements for the scenarios in this area. This will set up the basis for a preliminary architecture of the reputation-based trust management component (MS2) that is going to be integrated into the final architecture of **SPHERICS** (MS3). The component and the architecture will be tested later on (MS4).

Measures of success: Contributions beyond the state of the art in trust and reputation management. Integration of trust and reputation management in the overall architecture. Evaluation of the components and validation within the usage scenarios.

Objective 4: Enabler "Secure data storage and processing mechanisms" to allow users to take control of the security of their data

*The amount of personal and sensitive users' data stored at different service providers in the Internet is steadily increasing, and with them, the perception of the new risks and threats to privacy that arise from the outsourcing of such data. In **SPHERICS**, secure data storage and processing by means of advanced cryptography techniques will be a key research area. The focus will be on techniques that users can apply to protect their own data and not have to rely on service providers for this where possible, while still allowing the service providers to store and process this data on the users' behalf. Where this is not possible, we will analyse, select and develop techniques that allow users to enhance control of their data, and hence allow for the level of trust in service providers to be significantly reduced from the current situation. In addition, we will analyse, select and develop techniques that enable the seamless and secure portability of end users' data between different service providers.*

Relevant WPs: WP5

Key deliverables: D5.1, D5.2, D5.3

Related Milestones: MS1, MS2, MS3, MS4. MS1 will provide with the state of the art on secure data and storage plus the requirements for the use cases from the perspective of secure storage and processing. This will set up the basis for a preliminary architecture of the secure data and storage component (MS2) that is going to be integrated into the final architecture of **SPHERICS** (MS3). The component and the architecture will be tested later on (MS4).

Measures of success: Contributions beyond the state of the art in secure data storage and processing. Integration of secure storage and processing in the overall architecture. Evaluation of the components and validation within the usage scenarios.

Objective 5: Integrated proof-of-concept prototype

As a way of validating our ideas we will integrate the enablers developed in WP3, WP4 and WP5 to form a proof-of-concept prototype. The prototype will be built on top of the three technology enablers and it will feature three selected usage scenarios (Cloud Computing, Social Networks and e-Government) by implementing the final versions of the proof-of-concept applications. To this end, input from the evaluation of application mock-ups and of the early Proof-of-Concept applications will be taken into consideration.

Relevant WPs: WP2, WP6

Key deliverables: D2.1, D2.2, D2.3, D2.4, D2.5, D6.1, D6.2, D6.3, D6.4

Related Milestones: MS5. The enablers developed during the project will be integrated into a single architecture, following well-defined interfaces. This will give as a result an assistant (**SPHERICS**) to be used for the realization of the proposed scenarios.

Measures of success: Prototypes of the security assistant implemented. Realisation of the usage scenarios with the security assistant. Validation results for the prototype and the usage scenarios.

Objective 6: Dissemination, Standardization and Exploitation of the achieved results.

Solutions developed by the project will be more effective if the interfaces, specifications and protocols developed are widely supported by most of the service providers in the Internet today. To promote the successful acceptance and deployment of our solutions, the project will disseminate the developed and successfully validated technologies through standardization activities. A detailed exploitation plan will describe how the achieved results can be brought to a broad audience by means of enhancements of existing products and even development of new ones.

Relevant WPs: WP7

Key deliverables: D7.1, D7.2, D7.3.1, D7.3.2, D7.3.3, D7.4.1, D7.4.2, D7.5.1, D7.5.2

Related Milestones: MS1, MS2, MS3, MS4, MS5. All the results achieved at all the milestones of the project have to be disseminated through the usual channels of communication (publications, website, workshops, etc.).

Measures of success: Refereed scientific publications in conference proceedings and journals, contributions to standards organisations, exploitation plans of the consortium.

1.2 Progress beyond the state-of-the-art

In **SPHERICS** the main focus is to significantly increase the users' security and privacy in the Internet by offering an intermediate element, called assistant, which empowers the users to control their data. While application development is "state-of-the-art", the discussion on plug-in security, security managers and security measures in heterogeneous systems is an open issue.

The current focus on provider-oriented security has the ultimate goal of "*preventing the company from unacceptable losses"* due to e.g. hazardous products, leakage of confidential customer information or bad publicity. Storing all customer locations is an example of a corporate approach demonstrating that *"Apple does what is best for Apple"*, but not what is best for the customer.

In **SPHERICS** we focus on an approach that will help customers to be in control of their data. The business of such an approach is not yet proven, even though some indications postulate that "*customers will pay for the secure handling of their information"*. This is the starting point for our advances in the areas of Identity Management, Trust and Reputation, and Secure Data Storage/Processing. This section will provide a brief overview over the state of the art (SoTa) in the selected topics, and identify the progress achieved through **SPHERICS**.

1.2.1 Identity Management

Table 1 provides the progress related to Identity Management.

Table 1: Progress beyond the state of the art in Identity Management (WP3)

State of the art	Progress by SPHERICS
Current IdM systems for both web and corporate users adopt usually a centric (provider and user) access control approach, where every request to any service provider is bundled with the user identity and all the entitlement information. The identity is tied to a domain, but is portable. It usually supports pseudonyms and multiple identities to protect user privacy. Usually an IdM solution designed for a given environment like cloud computing or social networking does not work well across different domains. The federated identity management (FIM) [2] is a process whereby a user's identification is conducted on the Web with the process called Single-Sign-on (SSO). SAML [3] defines an XML based framework for exchanging security information for enabling SSO. It is broadly adopted in many of the identity management implementations. But SAML alone is not enough to enable access control. It is also	In the InterCloud paradigm different clouds of different nature cooperate with others with the aim of expanding both their computing and storage capabilities [6]. In order to perform the authentication and authorization among heterogeneous environments it is required to establish a federation level of interoperability between different security technologies (authentication and IdM). Trusted third parties can be in charge of storing the access credentials and securing them. To this end, the identity mechanisms to be designed in **SPHERICS** (T3.2, T3.3) will interoperate with different identity schemes and the information will be converted to different formats, so that the approach can be scalable and targets different public and hybrid clouds (T6.2). In what concerns social networking (T6.3), several challenges to IdM will be considered as part of this project. As users take a more active role in different social networks, their IdM tasks tend to become

needed the capability to adapt to the customer privileges and manage access to the resources. Standards like the eXtensible Access Control Markup Language (XACML) [4] can be used by a provider to do this. An important aspect in any IdM is the lifecycle management of user identities. The identity provisioning in distributed environments as those targeted in this project requires just-in-time (JIT) or on-demand provisioning and de-provisioning of identity information without sharing prior data. Service Provisioning Markup Language (SPML) [5] provides XML based structures for representing provisioning or de-provisioning requests intended for identity lifecycle management. SPML can make use of Security Assertion Markup Language (SAML) assertions and facilitate a complete trust model between senders and receivers.	chaotic [7]. If they have a different account in each site, with a specific set of credentials and information, a lot of personal and maybe professional information starts to be scattered in different sites and protected with many different access and protection policies. In **SPHERICS** enhancing security will be a compromise between usability and mobility (T3.1, T3.2). Another important aspect to be considered in this project will be to focus on maintaining the identity management as a simple task for end-users. Hence, **SPHERICS** will be using open standards (T3.1, T7.2) to define user profiles and represent their associated information (e.g., attributes, policies and preferences). Restrictions to "open data" describing the user will be exploited. These restrictions might be achieved through a semantic attribute-based access control to the user profile or other data describing the user [8]. **SPHERICS** will also address fine-grained access restrictions to parts of the profile, opening for "context-aware" profiles and preferences.

1.2.2 Trust and Reputation Management

Table 2 provides the progress related to Trust and Reputation Management.

Table 2: Progress beyond the state of the art in Trust and Reputation Management (WP4)

State of the art	Progress by SPHERICS
Trust management has been a very important tool for the decision-making process. The knowledge available about other entities is an essential key for establishing a secure exchange of information. Trust management systems try to provide this kind of knowledge by enabling the establishment of a common framework that comprises credentials and security rules and policies. In the last years, due to the growth of electronic communications and transactions, having a trust management system becomes very helpful for assisting the trust decision process. Trust can be reached from different mechanisms or technologies, including the reputation level, being this concept much more objective than trust [9]. Reputation systems have	The facilitator we aim to build needs a trust mechanism capable of determining which providers are trustworthy giving both a quantitative and a qualitative measure of it (T4.2, T4.3). This mechanism would not only indicate which providers are more trusted for interacting with, but also would give information about their expected behaviour, taking for example past experiences as a basis. Furthermore, the information provided by the facilitator might be personalized according to the users' preferences or their context. Another aspect that will be investigated in **SPHERICS** is the synergy between Identity, Trust and Privacy (T4.1) [13]. The concept of trust-based security is

been developed to aid trust management systems, collecting information related to the behaviour of the entities, even when direct trust relationships are difficult to be established. Thus, in order to build trust on entities knowing their behaviour becomes a key source of information. However, reputation is highly dependent on the context and its semantic is most of the times ambiguous. A trust management system [10], [11], [12], is usually composed of a symbolic language for representing trust and a way of measuring it (trust metrics). When we are dealing with transitive trust, the corresponding metric defines how trust propagates among entities.	well known since 2001 [14], while trust-based privacy was introduced around 2006 [15]. The concepts have always been connected in the digital world. Trust evidences are tied to a digital identity and when digital identities change previous trust evidences are no longer valid. In an identity federation scenario, the different identities of each party are linked by the federation. We could take advantage of those links to reuse reputation information within the cloud environment (T6.2), the social networks scenario (T6.3) and the e-Government one (T6.4). Since the Identity Management System within **SPHERICS** will enable the establishment of complex relationships between the entities of the digital ecosystem, the Trust and Reputation system must, in consequence, understand such relationships in order to provide consistent metrics of trust [16]. The proposed Trust and Reputation system should also be transparent to its users, enabling end users and providers to preserve their trust and reputation levels even when they change their identities (or more exactly, their identifiers). This way, the Trust and Reputation system will contribute to preserve the connections between entities, identities and trust.

1.2.3 Secure data Storage and Processing

Table 3 provides the progress related to Secure data Storage and Processing.

Table 3: Progress beyond the state of the art in Secure Data Storage and Processing (WP5)

State of the art	Progress by SPHERICS
The main remote storage providers today, such as Amazon, Dropbox or Microsoft, either do not encrypt their stored data or apply server-side encryption, where the key is under the control of the storage provider. Encryption under the control of the user can be implemented on top of the existing services and is offered e.g. by Spideroak [17] and GoldKey [18]. Many cryptographic schemes for operating on encrypted data exist. Searchable encryption [19]	**SPHERICS** will realise a secure storage architecture with different security levels and assumptions (T5.2, T5.3). Methods will be chosen that allow further processing of the data on remote servers e.g. in the cloud (T6.2). The user's security assistant will keep track of the data stored in various locations and will offer support for key management to ensure that the user remains in control of the data.

allows the creation of encrypted databases where single entries can be queried based on search patterns. Private Information retrieval [20] is stricter in hiding additionally the access pattern. More flexible approaches of operating on encrypted data are possible using homomorphic encryption [21] and secret sharing [22]. However, current homomorphic encryption schemes introduce a significant overhead [23], which has prevented their adoption in practice so far. A more general concept than homomorphic encryption is Secure multi-party computation (MPC) [24], which is a technique for securely processing data with the help of several parties. Parties that hold different sets of secret data collaborate and process all their data together in such a way that no party learns anything about any other party's secret data except for whatever is revealed by the output of the analysis. Initially solutions used garbled Boolean circuits. Since operating on bits can be inefficient, solutions working with larger primitive values were proposed, using secret sharing and arithmetic circuits [25]. Recent breakthroughs in fully homomorphic encryption (FHE) [26] may lead to secure arithmetic circuits without the need for secret sharing and several parties. However, current FHE implementations are several orders of magnitude slower compared to secret sharing [27]. Some systems for secure multi-party computation exist. Currently the most advanced ones are VIFF [28], JSMC [29], TASTY [30], SEPIA [31] and Sharemind [32].	The following techniques will be applied and further developed: separation of data and keys, homomorphic encryption, searchable encryption and secret sharing. Another key feature of **SPHERICS** is the integration of the developed secure storage mechanisms with the trust and reputation management system [16] to support the user in choosing the right storage system for their needs. Furthermore, **SPHERICS** will work on enhancing secure storage with multi party computation. By this method the user can be involved as one party in resolving queries on the data securely stored on remote servers. On the other hand, it allows very flexible data analysis compared to secure storage solutions in the state of the art (T5.1).

1.2.4 Related EU projects

In this section we provide a list of on-going and finished European projects that are somehow related with the main technical fields of **SPHERICS**. These projects have objectives and outcomes that are in line with some ideas of our proposal, and consequently, we will analyse their results during the execution of **SPHERICS**. In addition, we also provide a visual representation of these projects in Figure 2, arranged in a conceptual map according to their main areas of impact for **SPHERICS**. As it can be observed, **SPHERICS** fills the gap where no other EU project is working, i.e., the intersection between identity management, trust and reputation management and secure data storage and processing.

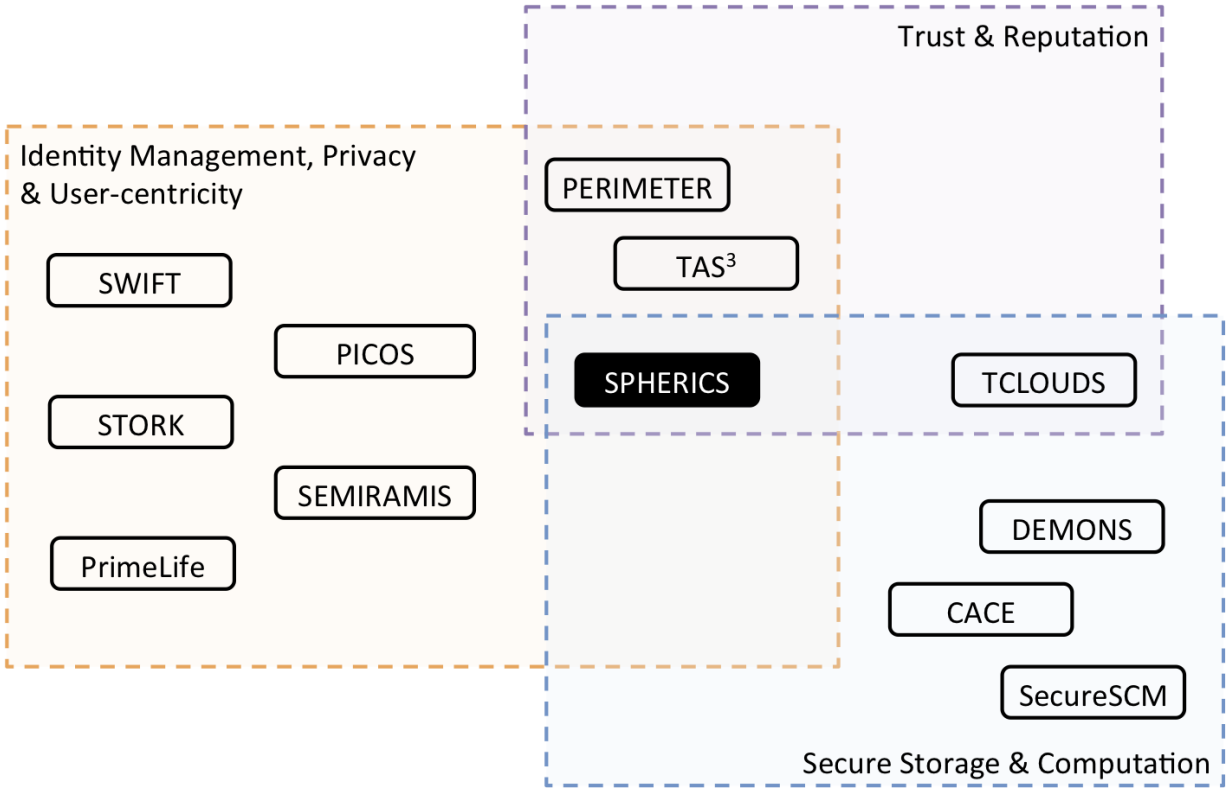

Figure 2: Conceptual map of European projects

- **PERIMETER [33]:** The main goal of this project is to enhance user-centric seamless mobility in the Future Internet scenario. This project has some results in the field of trust and reputation that should be studied during the analysis of the state of the art.

- **TAS3 (Trusted Architecture for Securely Shared Services) [34]:** This project aims to safely manage personal life-event information over long periods. This objective is partially related with our social network use case.

- **TCLOUDS [35]:** This project is centred in enhancing trustworthiness in cloud computing, by protecting privacy and ensuring resilience against failures and attacks. The results of this project could be useful for the analysis of the cloud computing use case of **SPHERICS**. This project also has some results related to trust and secure computation in cloud computing.

- **SWIFT (Secure Widespread Identities for Federated Telecommunications) [36]:** Its goal is to extend identity functions and federation into telecommunication networks, using a vertical approach. Its results can be useful to identify the main challenges of the identity management module to be designed as part of **SPHERICS**.

- **PICOS (Privacy and Identity Management for Community Services) [37]:** This project developed a platform for providing the privacy and identity management aspects of social community services and applications on the Internet and in mobile communication networks. The outcomes of this project will be useful for the analysis of the social networks use case within **SPHERICS**.

- **STORK (Secure Identity Across Borders Linked) [38]:** The main goal of STORK is to enhance the interoperability of electronic identity between countries. Although the scopes of STORK and **SPHERICS** are not directly related, some of the outcomes of STORK regarding interoperability of identity management systems could be of use for our project.

- **SEMIRAMIS (Secure Management of Information across Multiple Stakeholders) [39]**: This project is considering identity management and privacy issues when dealing with attribute recovery and secure transactions across different domains. The output of this project will be directly considered as part of the identity management component of the **SPHERICS** project and how portability can be approached in this particular side of the solution.

- **PrimeLife [40]:** The main objective of this project was to bring sustainable privacy and identity management to future networks and services. **SPHERICS** will go beyond this approach integrating identity and trust & reputation management as well as secure data storage in a user driven personal security and privacy assistant.

- **DEMONS (Decentralized, Cooperative, and Privacy-Preserving Monitoring For Trustworthiness) [41]**: The goal of DEMONS is to produce a highly distributed approach for network monitoring, where key monitoring elements share their information with other elements in its own network and even beyond, breaking domain borders and allowing a full-scope monitoring activity, bringing it to a new level. Some of the concepts related with privacy preserving management of information will be analysed as part of the state of the art tasks in **SPHERICS** for the secure data storage component.

- **CACE (Computer Aided Cryptography Engineering) [42]:** This project aimed to develop a set of cryptographic tools for producing high-performance applications. In relation with **SPHERICS**, this project produced some results in the field of secure multiparty computation.

- **SecureSCM [43]:** The scope of this project is focused in the application of cryptographic techniques to the processes of a supply chain, and more specifically, secure multiparty computation protocols. Then, it will be also considered for the analysis and design tasks of the secure data storage and computation component of the **SPHERICS** project.

1.2.5 User interface design of identity and reputation management tools

Several approaches in user interface design in recent years build the rich source of **SPHERICS** design study. In the course of the envisioned project, pros and cons will be analysed in detail before deciding the most promising design principles for our own prototypes. One source – for example – is a proposal called *Privacy Dashboard* developed by PrimeLife [40], an EU-funded integrated project (2008-2011). This dashboard is integrated into the Mozilla browser in order to specifically analyse and manage the privacy level when visiting websites (Figure 3a). Second, there is the well-known CardSpace [44] approach by Microsoft. Microsoft spent more than six years in the development of *CardSpace* (Figure 3b) and its corresponding Identity Metasystem before they stopped all activities in early 2011. Last but not least, there is a recent approach proposed by Kantara's User Managed Access (UMA) working group [45] called *CopMonkey* (Figure 3c). CopMonkey is a user-centric interface managing authorisations and policies.

a) PrimeLife Privacy Dashboard b) Microsoft CardSpace c) Kantara/UMA "CopMonkey"

Figure 3: Approaches in Identity & Reputation Management

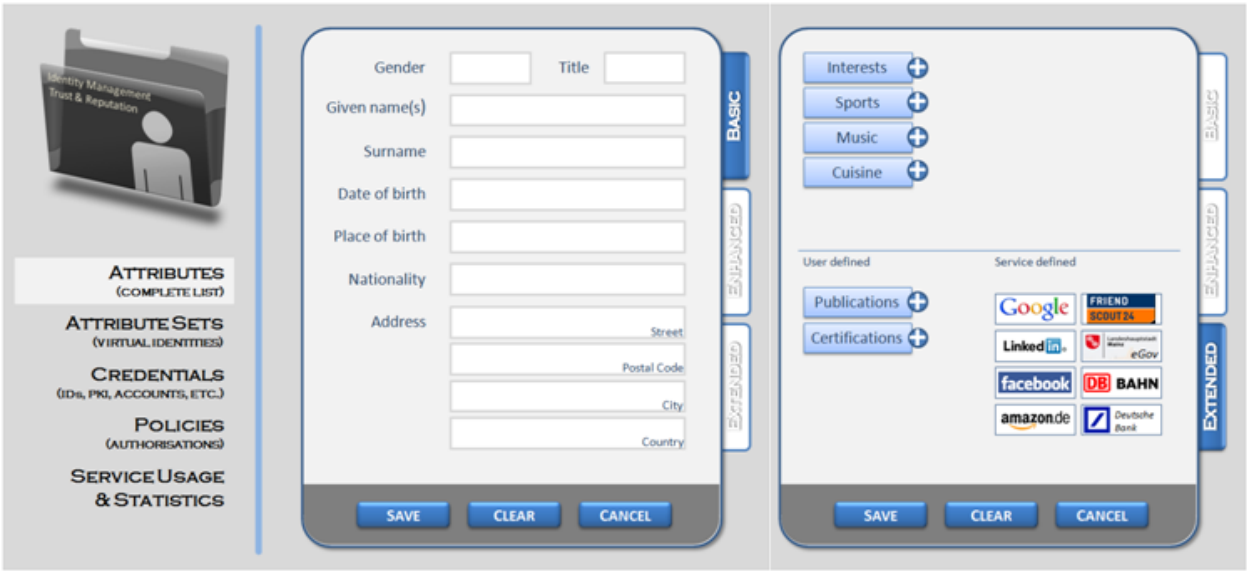

Figure 4: SPHERICS Personal Security Assistant - Design Study

The approach of **SPHERICS** is the integration of the different aforementioned aspects in a user-centric, browser and platform independent way. The goal is empowering users to manage, maintain and control secure storage of, and authorised access to, personal information. This will facilitate the concise and unified management of (virtual) identities, trust relationships and reputation of both the users and service providers.

A design study of **SPHERICS** approach of a Personal Security Assistant is shown in Figure 4. Here, basic personal information such as gender, name, and address is administered in a unified user-friendly way comprising user defined as well as service defined attributes. Further aspects such as management of virtual/partial identities and claims, management of credentials and policies and – last but not least – a comprehensive overview about service usage, history, and statistics will enable **SPHERICS**' Personal Security Assistant to be an everyday security & privacy facilitator in the digital world.

1.3 S/T methodology and associated work plan

1.3.1 Overall strategy and general description

The overall strategy and work plan have been directly derived from the project objectives. Besides project management, work is structured into six packages, which jointly address the six project objectives as shown in section 1.1.2.

The **SPHERICS** R&D activities will be conducted in Work Packages 2-7, for which the main interdependencies are shown in Figure 5. In greater detail:

- Work package 2 will extract the formal requirements of the security assistant; it will define the overall architecture and will validate the **SPHERICS** facilitator against certain security threats.
- Work packages 3, 4 and 5, will develop the enables described in objectives 2, 3 and 4, respectively.
- Work package 6 will integrate the developed enablers to build the security assistant and will validate it within the aforementioned selected usage scenarios, namely cloud computing, social networks and e-Government.
- Work package 7 will be responsible for the dissemination, standardisation and exploitation of the achieved results from **SPHERICS**.

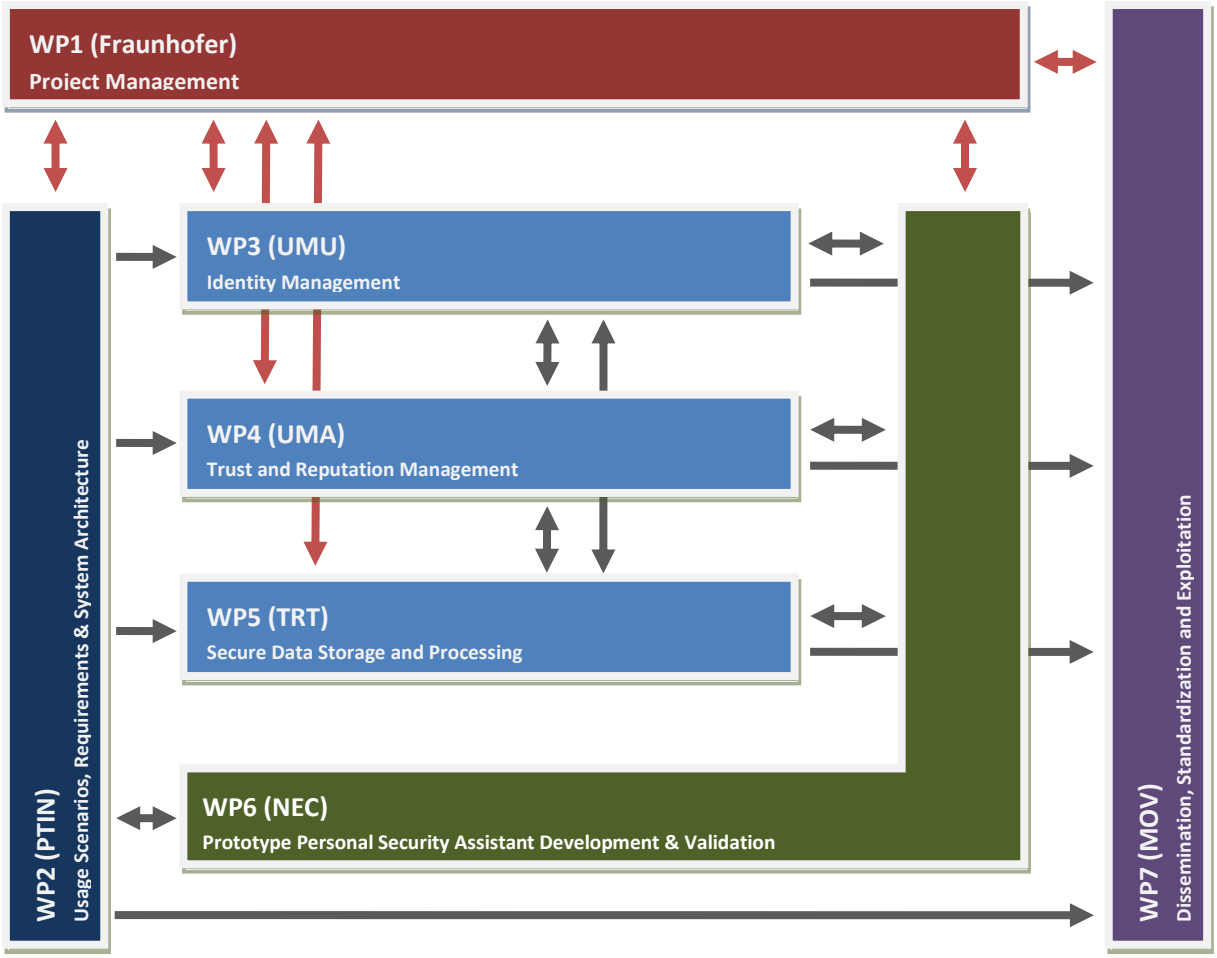

Figure 5. SPHERICS project structure

1.3.2 Work package interdependencies and timing

Figure 6 shows the interdependencies amongst the tasks considered within work packages 2-6, while Figure 7 shows the Gantt diagram depicting the scheduling of each work package, task, deliverable, synchronization point, milestone and development cycle of **SPHERICS**.

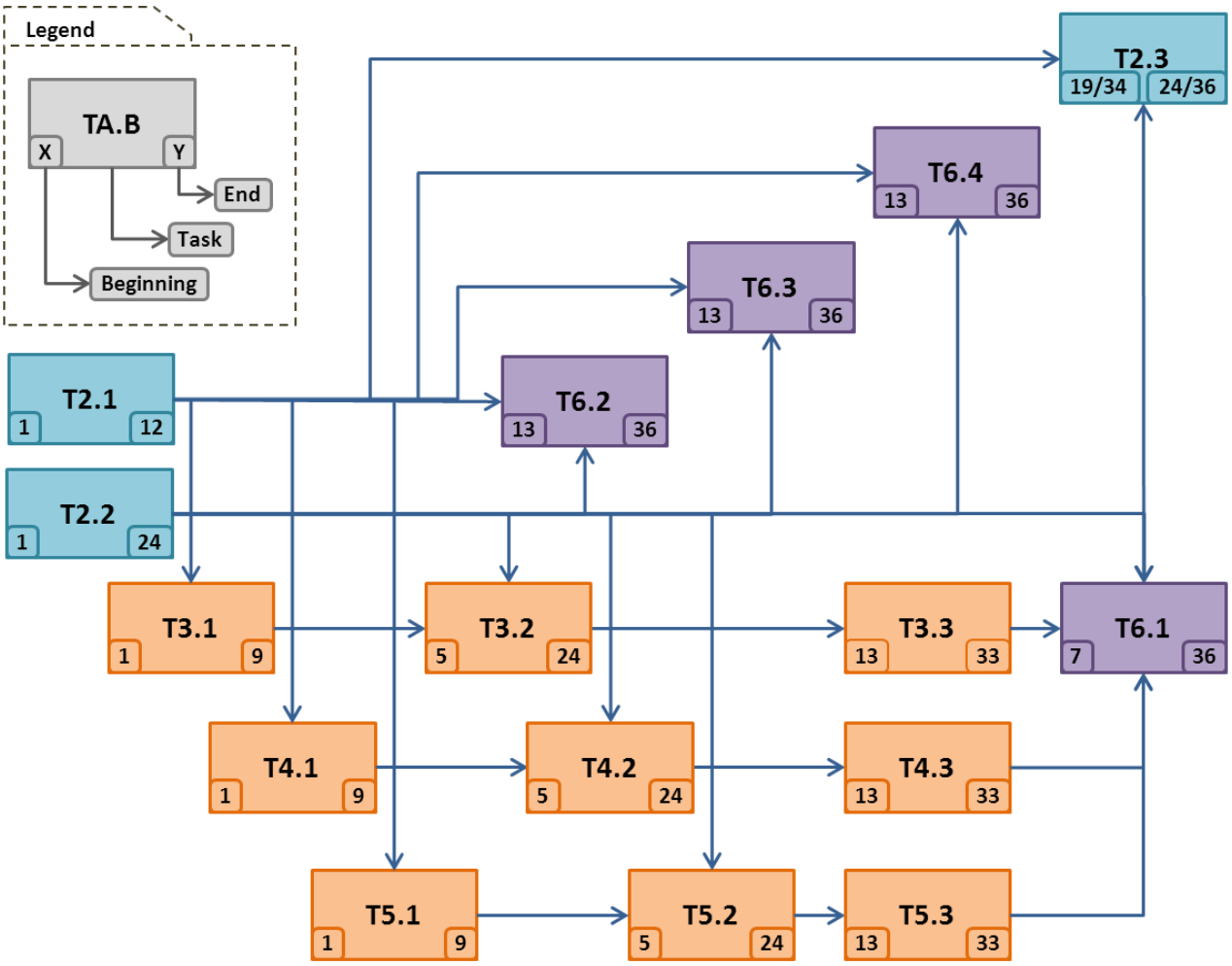

Figure 6. SPHERICS tasks interdependencies and timing

As it can be observed, T2.1 and T2.2 will be the tasks with the highest influence in the other ones since they will define both the usage scenarios requirements and the overall system architecture, respectively.

Each one of the technical work packages (WP3, WP4, WP5) are, in turn, structured in three tasks dealing with analysis of the state-of-the-art, the design of the corresponding enabler and its final implementation and testing.

Work package 6, however, consists of four tasks. The first of them, T6.1, will be responsible for the integration of all the enablers developed in WP3, WP4 and WP5, in order to build the final security assistant for **SPHERICS**, which will be additionally validated against the selected usage scenarios: cloud computing (T6.2), social networks (T6.3) and e-Government (T6.4).

Finally, work package 7 will consider the dissemination of the achieved results through several channels (web site, publications, workshops, etc), the standardisation of such achievements and the exploitation plans in order to bring them to real end users.

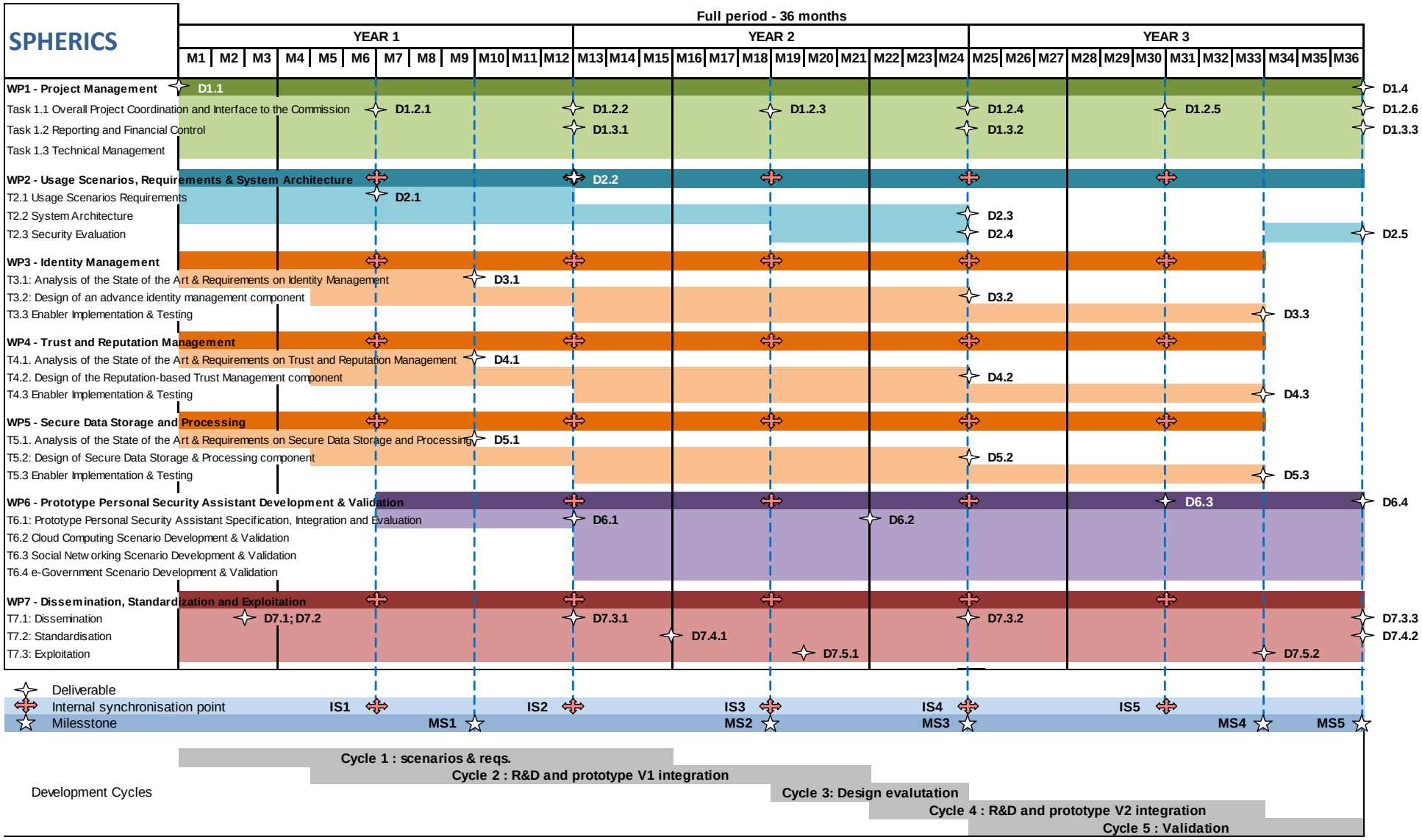

Figure 7. Gantt Chart for SPHERICS

1.3.3 Detailed work package description

Table 4: Work packages list

WP	Work package title	Type of activity	Lead particip. no.	Lead particip. name	Person months	Start	End
WP1	Project Management	MGT	1	**Fraunhofer**	24	M1	M36
WP2	Usage Scenarios, Requirements & System Architecture	RTD	6	**PTIN**	74	M1	M36
WP3	Identity Management	RTD	3	**UMU**	78	M1	M33
WP4	Trust and Reputation Management	RTD	4	**UMA**	79	M1	M33
WP5	Secure Data Storage and Processing	RTD	5	**TRT**	65	M1	M33
WP6	Prototype Personal Security Assistant Development & Validation	RTD	2	**NEC**	83	M6	M36
WP7	Dissemination, Standardization and Exploitation	RTD	7	**MOV**	36	M1	M36
Total					**439**		

Table 5: List of deliverables

ID	Deliverable name	WP	Leading partner	Nature	Dissemination level	Delivery date
D1.1	Consortium Agreement	WP1	Fraunhofer	R	CO	M0
D1.2.n	Periodic 6-monthly Progress Report	WP1	Fraunhofer	R	CO	M6...
D1.3.n	Yearly Financial Report	WP1	Fraunhofer	R	CO	M12...
D1.4	Final Project Report	WP1	Fraunhofer	R	PU	M36
D2.1	Scenarios description	WP2	PTIN	R	PU	M6
D2.2	Report on requirements analysis	WP2	PTIN	R	PU	M12
D2.3	Architecture definition	WP2	TRT	R	PU	M24

ID	Deliverable name	WP	Leading partner	Nature	Dissemination level	Delivery date
D2.4	System security evaluation, basic	WP2	Fraunhofer	R	PU	M24
D2.5	System security evaluation, enhanced	WP2	Fraunhofer	R	PU	M36
D3.1	Challenges in identity management applied to eServices	WP3	PTIN	R	PU	M9
D3.2	Design of the advanced identity management component	WP3	UMU	R	PU	M24
D3.3	Implementation of the IdM module	WP3	Fraunhofer	R/P	CO*	M33
D4.1	Report on the State of the art and Requirements on Trust and Reputation Management Systems	WP4	UMU	R	PU	M9
D4.2	Final Architecture of the Reputation-based Trust Management system	WP4	UMA	R	PU	M24
D4.3	Reputation-based Trust component implementation	WP4	MOV	R/P	CO*	M33
D5.1	State of the Art and Requirement Specification – Secure Data Storage and Processing	WP5	UMA	R	PU	M9
D5.2	Design of the Secure Data Storage and Processing Enabler	WP5	TRT	R	PU	M24
D5.3	Secure Data Storage and Processing Enabler Implementation and Testing	WP5	NEC	R/P	CO*	M33
D6.1	Interfaces for the Security Assistant	WP6	NEC	R	PU	M12
D6.2	System Integration Report	WP6	Fraunhofer	R	PU	M21
D6.3	Realization of Prototypes	WP6	NEC	R/P	CO*	M30
D6.4	Final architecture, system realization and evaluation	WP6	NEC	R	PU	M36
D7.1	Web site of the project	WP7	Fraunhofer	O	PU	M2
D7.2	Collaborative platform for research and dissemination	WP7	MOV	O	RE	M2
D7.3.1	Identification of key players for the SPHERICS ecosystem and periodic dissemination activity report for year 1	WP7	MOV	O	PU	M12
D7.3.2	Dissemination Report for year 2	WP7	MOV	O	PU	M24

ID	Deliverable name	WP	Leading partner	Nature	Dissemination level	Delivery date
D7.3.3	Final Dissemination Activity report for year 3	WP7	MOV	O	PU	M36
D7.4.1	Standardization plan	WP7	Fraunhofer	R	RE	M15
D7.4.2	Standardization report	WP7	Fraunhofer	O	PU	M36
D7.5.1	Notes and presentation material from business exploitation workshop	WP7	PTIN	O	PU	M19
D7.5.2	Exploitation plan and business opportunities	WP7	PTIN	R	RE	M33

* These deliverables will include a public report and a public demonstrable prototype. When required, a confidential annex to the public report will be maintained within the Consortium. The dissemination level of the source code is subject to the IPR regime and it might therefore be kept unpublished/confidential.

Dissemination level:

PU = Public,

RE = Restricted to a group specified by the Consortium,

PP = Restricted to other program participants (including Commission Services),

CO= Confidential, only for members of the Consortium (including the Commission Services)

Nature of Deliverable:

P= Prototype,

R= Report,

S= Specification,

T= Tool,

O = Other, including Web.

Table 6: List of milestones

Milestone number	Milestone name	WP(s) involved	Expected date	Means of verification
MS1	User requirements identified and State of the art analysis finished	WP2, WP3, WP4, WP5	M9	D2.1, D2.2, D3.1, D4.1, D5.1
MS2	Preliminary version of the SPHERICS	WP2, WP3,	M18	Once MS1 has been achieved T3.2, T4.2 and T5.2 will work in parallel in order to build

	components	WP4, WP5, WP6, WP7		the **SPHERICS** components. A preliminary architecture should be realised before the final components are available.
MS3	Final Architecture of the **SPHERICS** Assistant	WP2, WP3, WP4, WP5, WP6, WP7	M24	The final architecture of the components (D3.2, D4.2 and D5.2) will be the basis for the final architecture of **SPHERICS** together with the definition of the interfaces (D6.1) and the guidelines for the integration (D6.2).
MS4	Testing of the **SPHERICS** components and realization of prototypes	WP3, WP4, WP5, WP6, WP7	M33	The components will be tested (D3.3, D4.3 and D5.3) and prototypes for the scenarios will be realised according to the final architecture (D6.3).
MS5	Integrated version of the **SPHERICS** Assistant	WP6, WP7	M36	This will be the final result of **SPHERICS**

Table 7: Work package 1 description

WP number	**WP1**	Start month	**M01**	Activity type	**MNG**
WP title	**Project Management**				

Participant ID	**P01**	P02	P03	P04	P05	P06	P07
Participant short name	**Fraunhofer**	NEC	UMU	UMA	TRT	PTIN	MOV
Person months	**12**	7	1	1	1	1	1

Objectives

This work-package is responsible for the overall coordination of the project and to deal with management issues.

The primary objectives of this work package are:

- Close monitoring of all work packages and technical contributions from the beneficiaries
- Coordination/management of project contents and contributions
- Validation and review of project results, project controlling
- Ensuring the correct reporting and work plan execution
- Preparation of strategic project decisions
- Communication to project participants, the board and the EU

The work package will further manage liaisons and external co-operations, as well as external events and the content for overall external presentation.

Description of work

Following activities belong to the responsibilities of the project management:

- The overall legal, contractual, ethical, and administrative management of the project
- Financial management and collection of financial reports
- Cost calculations for: Personnel (contracts, time-sheets, etc.), travel, meetings, and equipment (amortisation, monitoring of resources)…
- Overseeing the promotion of gender equality in the project
- Preparing, updating, and managing the consortium agreement between the participants
- Decisions on documentation standards
- Project manual for the consortium
- Obtaining audit certificates (as and when required) by each of the contractors

Preparation and coordination of project documents such as progress and final reports: Form C, Management reports, Technical reports, socioeconomic report and publishable summary.

T1.1 Overall Project Coordination and Interface to the Commission

Leader	*Fraunhofer*	***Participants***	

- Report to the Commission and represent the project in all official matters, including an overview of all project matters
- Deal with legal issues related to the EU contract, consortium agreement and IPR policy
- Ensure the communication flow within the project and across Work Packages
- Provide conflict resolution between beneficiaries if these cannot be resolved at WP level

T1.2 Reporting and Financial Control

Leader	*Fraunhofer*	***Participants***	

- Retrieve and aggregate individual beneficiary reports
- Map and monitor current expenditure with the project work plan
- Perform internal (3 month period) and external reporting (6 month period)

T1.3 Technical Management

Leader	*NEC*	***Participants***	*ALL*

- Manage deliverable approval and other internal technical work flows
- Prepare strategic decisions on the project direction and technical adaptations of Annex I, including actions needed in case of technical risk factors, such as disruptive technologies

Deliverables

ID	Month	Name and brief description
D1.1	**M0**	***Consortium Agreement***
D1.2.n	**M6, M12, M18, M24, M30, M36**	***Periodic 6-monthly Progress Report*** This report will provide detailed information on project progress (including problems encountered and remedial actions taken); it will also include specific feedback from major activities being performed in the period as well as results of on-going dissemination and exploitation planning.
D1.3.n	**M12, M24, M36**	***Yearly Financial Report*** This report will provide full details on incurred efforts and costs and set the basis for the interim-payment process until the final period will be reached when a consolidated financial report will have to be issued.
D1.4	**M36**	***Final project report*** This report will represent a clear, concise and explicative explanation of **SPHERICS** project deployment, from its initial objectives (as set forth in this document) to its achievements, their validation and potential exploitation. The document is intended to be a publicly available concise version of the relevant information held in the various period progress reports that will be issued during the project life.

Role of partners
Fraunhofer will conduct overall coordination of the project. It is responsible for orchestrating the work done in the work packages and establishing appropriate communication channels between the partners and between the project and the Commission. **NEC** will act as technical coordinator of the project and will therefore lead task T1.3. **UMU** will contribute to the technical management of the project as WP3 leader. **UMA** will contribute to T1.3 as leader of WP4. **TRT** will contribute to the technical management of the project as leader of WP5. **PTIN** will contribute with technical advice and orientation to strategic decisions and deliverables to be revised. The financial and control management respecting to PTIN will be always done according to the plan. **MOV** will contribute with the knowledge of collaborative R&I and the semantic MediaWiki.

Table 8: Work package 2 description

WP number	**WP2**	Start month	**M01**	Activity type	**RTD**
WP title	**Usage Scenarios, Requirements & System Architecture**				

Participant ID	P01	P02	P03	P04	P05	**P06**	P07
Participant short name	Fraunhofer	NEC	UMU	UMA	TRT	**PTIN**	MOV
Person months	16	12	10	9	11	**16**	0

Objectives

The objectives of this work package are the:

- Definition and description of the usage scenarios for **SPHERICS**.
- Identification of the requirements on the system, concerning Identity Management, Trust and Reputation, and Secure data storage, derived from the usage scenarios.
- Definition of the system architecture, which integrates the aforementioned requirements.

Description of work

The tasks included in this WP will firstly be responsible for the identification of potential application scenarios and their requirements derivation. The requirements will concern Identity Management, Trust and Reputation, and Secure data storage and processing as basic enablers, as well as the other main technical challenges of the project: user-centricity and usability, privacy-awareness, and seamless data portability.

The work will be done for the three main scenarios that have been identified as part of the project, i.e., cloud computing, social networking and e-Government. If any other scenario is being considered as of interest for the project objectives during its lifetime, this work package will analyse it and derive its main requirements.

The resultant requirements will then be used to define the system architecture in task 2.2, and as inputs to WP3, WP4, WP5 and WP6. In task 2.1 we propose the possible usage scenarios and capture their requirements, and in task 2.2 the requirements will be used to develop the system's architecture, meeting the objectives of modular design, user-centric identity management, trust and reputation, and secure data storage as well as portability and a seamless middleware system.

T2.1 Usage scenarios requirements

Leader	*PTIN*	***Participants***	*Fraunhofer, NEC, UMU, UMA, TRT*

This task identifies, describes and finally selects scenarios relevant for **SPHERICS** (namely, Cloud Computing, Social Networks and e-Government). The scenarios identification will be based on the interesting cases identified for **SPHERICS** and already described in the Concept and Objectives section. The description of each scenario will follow a "storybook" and use a formal description method like SDL/UML. Each of them will be documented in technical, application, and business terms. This task includes the development of relevant use cases and processes for **SPHERICS**. These will then be used as the basis for carrying out the requirements analysis and definition.

T2.2 System Architecture			
Leader	*TRT*	***Participants***	*Fraunhofer, NEC, UMU, UMA, PTIN*
In this task the requirements will be mapped into a proposed architecture for the system that meets the objectives of the project and includes the Identity Management, Trust and Reputation Management, and Secure Data storage and processing components. This architecture will integrate the components of each of these areas of interest.			
T2.3 Security Evaluation			
Leader	*Fraunhofer*	***Participants***	*NEC, UMU, PTIN*
As a central component for trust and identity management it is necessary to define and evaluate underlying security concepts for the overall facilitator. This task gathers necessary security criteria based on commonly accepted standards. In addition this task also includes a subsequent validation of the prototype against those defined security concepts.			

Deliverables		
ID	**Month**	**Name and brief description**
D2.1	**M6**	***Scenarios description*** This deliverable will include the Scenarios identification and description, using a formal description method.
D2.2	**M12**	***Report on requirements analysis*** This deliverable will present the analysis performed for each scenario in order to derive the requirements that should be met by the system's architecture
D2.3	**M24**	***Architecture definition*** This deliverable will present the proposed system architecture with the different components that the system should include.
D2.4	**M24**	***System security evaluation, basic*** This deliverable will present the underlying basic security concept for the overall facilitator and evaluates "prototype V1" (cycle 2) according to the security requirements.
D2.5	**M36**	***System security evaluation, enhanced*** This deliverable will present the underlying enhanced security concepts for the overall facilitator and evaluates "prototype V2" (cycle 4) according to the security requirements.

Role of partners
Fraunhofer will be providing its expertise in identity management and privacy protection during the requirements analysis and systems design. As leader of an implementation task (T3.3) Fraunhofer will have a focus on the implementability of the systems design. As leader of the Security Evaluation (T2.3) Fraunhofer will bring in its expertise from its conceptual work in the field of IT-security and penetration testing as well as from practical security tests. **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. **UMU** will be participating in this WP by providing its expertise in gathering security and privacy requirements from real scenarios, paying special attention to the cloud computing scenario. UMU will be also contributing to the design of the architecture of the personal assistant, as well as providing the insights for the seamless data portability requirements. **UMA** will contribute to the description of some scenarios and the requirements derived from them, with a special care for those regarding security and trust and the social networks scenario. They will also participate in the definition of the testing and validation plan for the scenarios they contribute in. **TRT** will contribute to the definition and requirements analysis of the e-government scenario, as well as to the system architecture definition. **PTIN** will lead WP2 and provide its knowledge and expertise in the scenario description and identification, offering real world experience and problems related to the domains **SPHERICS** is addressing. Moreover PTIN will participate in the requirements analysis and system's architecture definition.

Table 9: Work package 3 description

WP number	**WP3**	Start month	**M01**	Activity type	**RTD**
WP title	**Identity Management**				

Participant ID	P01	P02	**P03**	P04	P05	P06	P07
Participant short name	Fraunhofer	NEC	**UMU**	UMA	TRT	PTIN	MOV
Person months	18	6	**20**	10	0	17	7

Objectives

The objectives of this work package are:

- To analyse the current state of the art on identity management systems according to the requirements derived from WP2 and the three scenarios proposed as part of the project.
- To design an identity management solution characterised for being user centric and context based and able to provide users with an integrated and easy-to-use identity life-cycle management process.
- To implement the resulting design so it is integrated with other enablers as part of the general **SPHERICS** architecture.

The design and later implementation of this enabler will be driven by the following principles: the user, as main actor for this component, is able to define, create, modify and delete one or several identities as requested and/or needed; she is having an easy-to-use and intuitive interface to manage all of her identities; she is able to create private identifiers on demand to get access to certain services; she is able to define the policies driving the use of the personal information and data associated to her identity (e.g., her age, bank account information, mobile phone number, etc.); she can monitor how, where, when and by which service provider or another identity manager her information has been used; she is able to interact seamlessly with different identity providers (e.g., major search engines, cloud providers, social networking platforms, eGov providers, etc.) and technologies (e.g., SAML, OpenID, etc.); and she is able to make use of a service providing portability from one identity management provider to another.

Description of work

The first task in this work package (T3.1) will be identifying the main missing components that should be addressed with regard to identity management systems in order to cover the requirements derived from WP2. These requirements include the ones derived from the identified scenarios and the particular requirements defined for the personal security assistant. Then, a design task T3.2 will start by covering all the requirements and gaps identified before and providing a complete design of the identity management and its interfaces. A final task, T3.3, will address the implementation of this component in such a way that it can be released as an output to WP6 and being integrated with the other two enablers in the scenarios defined in the project and later validated as part of them.

T3.1: Analysis of the State of the Art & Requirements on Identity Management

Leader	*PTIN*	***Participants***	*Fraunhofer, NEC, UMU, UMA*

This task is intended to review the state of the art in the identity management field following the principles indicated as part of the main objective of this WP and the design requirements derived from WP2 analysis of the proposed project scenarios. The result of this task will help to better identify the main aspects to be considered as part of the design and implementation work to be accomplished during the project.			
T3.2: Design of an advance identity management component			
Leader	*UMU*	***Participants***	*Fraunhofer, NEC, UMA, PTIN, MOV*
This task is intended to provide the definition and design of the main modules and the interacting interface that the identity management component should have in order to meet all the requirements identified in previous tasks.			
T3.3: Enabler Implementation & Testing			
Leader	*Fraunhofer*	***Participants***	*NEC, UMU, PTIN, MOV*
This task is intended to provide a first implementation of the IdM component to be considered as part of the structure of the facilitator. This task will also accomplish a first testing of the prototype in order to verify that the requirements identified and the design provided are well reflected in the final software module.			

Deliverables		
ID	**Month**	**Name and brief description**
D3.1	**M9**	***Challenges in identity management applied to eServices*** Presents the main open issues and limitations that need to be addressed by an identity management system characterised for being user-centric, policy- and privacy-aware, easy-to-use, integrating a whole life-cycle for the identities, providing interoperability and portability of information, and easing the task of monitoring the use of a given identity and its associated data.
D3.2	**M24**	***Design of the advanced identity management component*** This document provides a final definition of the architecture and design of the identity management component provided as part of this project.
D3.3	**M33**	***Implementation of the IdM module*** This deliverable will be directly associated with the prototype being released as final result of this work package in the form of an IdM solution covering all the requirements derived from the analysis provided in WP2 and T3.1.

Role of partners
Fraunhofer will support the state of the art analysis and the module design with its expertise in identity management as well as lead the implementation of the IdM module. **NEC** will contribute to identity management for cloud applications. A particular focus will be on identity

management needs for seamless data portability.

UMU will be coordinating this work package, as well as having an active role in the definition of the IdM-related requirements of the personal security assistant, the design of the overall IdM solution and its interfaces, and the implementation of the IdM module.

UMA will participate in the analysis of the state of the art and in the identification of requirements. They will also contribute to the design of the IdM component.

PTIN will contribute with know-how on the Identity management area. PTIN will lead task 3.1 and analyse the state of the art in what is concerned with the technologies and techniques that could be applied to this project. This study will help the consortium to find the requirements of IdM for the project and improve the results.

MOV will contribute to the advanced IdM, based on experiences from our cloud solution.

Table 10: Work package 4 description

WP number	**WP4**	Start month	**M01**	Activity type	**RTD**
WP title	**Trust and Reputation Management**				

Participant ID	P01	P02	P03	**P04**	P05	P06	P07
Participant short name	Fraunhofer	NEC	UMU	**UMA**	TRT	PTIN	MOV
Person months	11	19	18	**21**	0	0	10

Objectives

The objectives of this work package are

- To design a reputation-based trust management component that offers quantitative and qualitative trust indicators about service providers, using reputation values and end-users' personal preferences as inputs
- To investigate the relationships of trust and reputation with identity aspects
- To implement a reputation-based trust component complying with the general architecture of **SPHERICS**

Description of work

The main goal of WP4 is to define an advanced trust and reputation management component, which will be one of the essential sub-systems of the **SPHERICS** system. This component will provide users with trust and reputation indicators about service providers and will assist them during their interactions. This information might be also important for end users before starting a seamless data portability process from one service provider to another. To this end, this work package will firstly perform a review on the state of the art. As a consequence of this study, the findings derived from the analysis of both the state of the art and the requirements of the scenarios of the project (WP2) will aid to determine which relevant evidences could be used to feed the reputation-based trust management system. First, we will design a reputation module that will take into account the quantitative and objective feedback from the users. On top of this basic module, the trust module will capture more complex aspects, such as the qualitative and subjective feedback from the users. The two of them will be combined and presented in such a way that aids users on the decision making process.

The reputation-based trust management component will be scalable and flexible enough to work with an increasing number of service providers and in multiple scenarios. An important part of this task will be to determine how to use identity information about both users and service providers to enhance trust indicators. Finally, this task will produce a formal definition of the architecture of the trust management component, which must be interoperable with the main system of **SPHERICS**.

T4.1. Analysis of the State of the Art and Requirements on Trust and Reputation Management

Leader	*UMU*	***Participants***	*Fraunhofer, NEC, UMA*

This task will provide a review of the state of the art on Trust and Reputation Management in order to analyze possible solutions as well as to identify the research gaps that may be solved by the project. Based on this analysis, this task will also produce a set of requirements and recommendations that will guide the subsequent tasks for improving over the current research landscape.

T4.2. Design of the Reputation-based Trust Management component

Leader	*UMA*	***Participants***	*Fraunhofer, NEC, UMU, MOV*

The goal of this task is to design the Reputation-based Trust Management component of **SPHERICS**, which must be scalable for supporting a large and increasing number of service providers, and flexible for working properly in multiple scenarios. This component will provide trust indicators using suitable metrics that enable both qualitative and quantitative evaluations of the entities' trustworthiness. Thus, we should pay special attention to the relationships between identity and trust in order to use it as a relevant factor for this evaluation. This task will include the context as a measure of "trusted environments", indicating what kind of information might be revealed in a given context. The outcome of this task should be formally captured in an architecture that will be part of the general architecture of **SPHERICS** in WP2 (T2.2).

T4.3 Enabler implementation and testing

Leader	*MOV*	***Participants***	*Fraunhofer, NEC, UMU, UMA*

Following the general architecture of **SPHERICS** defined in T2.2 and the specific architecture of the component derived from T4.2, we will implement the reputation-based trust management component, including a context measure of the environment. The code produced during this task will be continually tested in order to assure its correctness, following a test-driven approach. Interoperability and open standards are our design goals, allowing for a testing in the *development version* of the InnoBors [46] in addition to platforms being identified in the first phase of the project.

Deliverables

ID	Month	Name and brief description
D4.1	**M9**	***Report on the State of the art and Requirements on Trust and Reputation Management Systems*** This report consolidates existing research and state of the art in Trust and Reputation Systems, with an emphasis on the techniques that could be of use for the application scenarios of the project. This report will also include a set of requirements for **SPHERICS** that are specific to Trust and Reputation Management, as well as a set of recommendations to guide the developments in further stages of the project.
D4.2	**M24**	***Final Architecture of the Reputation-based Trust Management system*** This deliverable will embody the final architecture of the Reputation-based Trust Management component. This final architecture will be refined from the results of the validation processes carried out in WP6.

D4.3	**M33**	***Reputation-based Trust component implementation*** This deliverable will contain the artefacts derived from the implementation and testing of the component.

Role of partners
Fraunhofer will support the progress in this work package with their experiences in several federated identity and trust protocols. One focus will be the investigation of the relationship between identity and trust and their impacts on each other. **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. **UMU** will lead T4.1 thus helping actively to identify the missing parts of current trust and reputation solutions when applied to a system as the one proposed in this project. UMU will be also working on the design of this module and how it can be integrated with the identity management solution described in WP3 and with the portability requirements identified as part of the project. **UMA** will lead WP4 and T4.2, which will be devoted to the design of the reputation-based trust component for **SPHERICS**. They will contribute to the other tasks as well. **MOV** will lead the implementation of the Trust and Reputation Management (T4.3), and link the reputation to social network activities and professional relations.

Table 11: Work package 5 description

WP number	**WP5**	Start month	**M01**	Activity type	**RTD**
WP title	**Secure Data Storage and Processing**				

Participant ID	P01	P02	P03	P04	**P05**	P06	P07
Participant short name	Fraunhofer	NEC	UMU	UMA	**TRT**	PTIN	MOV
Person months	6	18	6	17	**18**	0	0

Objectives

The objectives of this work package are to:

- Analyse state of the art techniques for secure data storage and processing
- Develop secure data storage and processing mechanisms that protect the user's security and privacy when data is outsourced to service providers that are untrusted
- Develop secure data storage and processing mechanisms to protect the security and privacy of user's outsourced data from partially trusted service providers

The overall aim of this work package is to develop a security enabler that provides secure data storage and processing. This enabler will allow users to control the security and privacy of their data when it is outsourced to service providers.

Description of work

This work package will firstly review state of the art techniques for secure data storage and processing. The results of the review will be used to select mechanisms and identify gaps in the state of the art that should be addressed in the secure data storage and processing to meet the requirements derived in WP2. Secondly, T5.2 will design the secure data storage and processing enabler to meet the requirements and address gaps in the state of the art. Finally, T3.3 will implement and test a prototype of the enabler and selected secure data storage and processing mechanisms.

T5.1. Analysis of the State of the Art and Requirements on Secure Data Storage and Processing

Leader	*UMA*	***Participants***	*Fraunhofer, NEC, UMU, TRT*

This task will analyse state of the art mechanisms for secure data storage and data processing. The goal is to determine their suitability for enabling users to securely store and retrieve data and to outsource data processing to a partially trusted or completely untrusted service provider. This task will recommend the work items to the subsequent tasks of the work package that will advance the state of the art. Appropriate technologies will then be selected and any gaps in the state of the art will be identified. This task will also capture additional functional and security requirements for the secure data storage and processing enabler, which build on those identified in WP2, paying special attention to the seamless data portability.

T5.2: Design of Secure Data Storage and Processing component

Leader	*TRT*	***Participants***	*Fraunhofer, NEC, UMU, UMA*

This task will design mechanisms to fill the gaps identified in T5.1, focusing on techniques that can be employed by users to protect their own data. It will also develop an architecture that pulls together the secure data storage and processing techniques identified and developed in T5.1 and T5.2 to show how they could work both in the user's personal security facilitator and on the service providers in general.

T5.3: Enabler Implementation and Testing			
Leader	*NEC*	***Participants***	*Fraunhofer, UMA, TRT*

This task will implement a prototype of the secure data storage and processing enabler, including selected mechanisms designed in T5.2. It will also perform initial testing of the prototype against the requirements identified in WP2 and T5.1.

Deliverables

ID	Month	Name and brief description
D5.1	**M9**	***State of the Art and Requirement Specification – Secure Data Storage and Processing*** This deliverable will describe the state of the art mechanisms for secure data storage and processing. It will describe the selection of mechanisms and the identification of gaps in the state of the art. This deliverable will also specify the functional and security requirements of the secure data storage and processing enabler.
D5.2	**M24**	***Design of the Secure Data Storage and Processing Enabler*** This deliverable will describe the mechanisms for secure data storage and processing that have been developed and define the architecture of the secure data storage and processing security enabler.
D5.3	**M33**	***Secure Data Storage and Processing Enabler Implementation and Testing*** This deliverable will describe the prototype implementation and initial testing of the secure data storage and processing enabler.

Role of partners

Fraunhofer will act as a reviewer of the all the deliverables of this work package and evaluate those against the background of their experiences in the field of secure cloud storage and data processing.

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.

UMU will collaborate in T5.1 with the analysis of the SoTa of Secure Data Storage and Processing.

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 the corresponding component (T5.2).

TRT will lead the 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.

Table 12: Work package 6 description

WP number	**WP6**	Start month	**M07**	Activity type	**RTD**
WP title	**Prototype Personal Security Assistant Development & Validation**				

Participant ID	P01	**P02**	P03	P04	P05	P06	P07
Participant short name	Fraunhofer	**NEC**	UMU	UMA	TRT	PTIN	MOV
Person months	16	**16**	14	9	10	10	8

Objectives

The objectives of this work package are as follows:

- Complete and realise the security assistant specification
- Integrate the enablers developed in WP3, WP4 and WP5 into the security assistant
- Develop technical scenarios based on those defined in WP2 and implement and evaluate prototypes for these scenarios against the requirements derived in WP2

This work package is responsible for developing the personal security assistant and takes care of the integration of the results of WP3, WP4 and WP5 into this personal security assistant. WP6 will build on the architecture of the security assistant defined in WP2 and develop a detailed specification. In addition, it will integrate each of the security enablers developed in these work packages in order to build the final user-centric security assistant. Moreover, building on the usage scenarios defined in WP2, this work package will develop detailed prototype scenarios, which will be used to perform the end-user validation.

Description of work

The tasks included in this WP will responsible for the realisation of the security assistant and demonstration and validation of the assistant in three scenarios. The requirements and initial descriptions of both, the security assistant and the scenarios will be provided by WP2. The technical WPs, WP3, WP4 and WP5, will provide the components according to the requirements. Task 6.1 will integrate the components suitable for Tasks 6.2, 6.3, and 6.4 to demonstrate and validate the security assistant in different scenarios.

T6.1: Prototype Personal Security Assistant Specification, Integration and Evaluation

Leader	*NEC*	***Participants***	*Fraunhofer, UMU, UMA, TRT, PTIN*

This task will use the system requirements and architecture from WP2 to develop a technical specification capable of integrating the results from WP3, WP4 and WP5. This task will also define the necessary technical interfaces between the technical WPs as well as the graphical user interface and integrate the implementation of the enablers from WP3-WP5 to build the security assistant.

T6.2 Cloud Computing Scenario Development & Validation

Leader	*Fraunhofer*	***Participants***	*NEC, UMU, TRT, MOV*

This task develops the cloud computing scenario. It will demonstrate how to use the personal security assistant in combination with the security enablers to realize this scenario.

The task starts with defining a detailed cloud computing scenario, building on the one specified in WP2. The prototype of the security assistant developed in T6.1 and the security enablers will then be adapted for this example scenario, and will be validated against the requirements derived in WP2. The prototype will focus on several different aspects from the developed technologies around reputation, user-centric identity management and cryptographic solutions for storage and computation.

T6.3 Social Networking Scenario Development & Validation			
Leader	*MOV*	***Participants***	*Fraunhofer, NEC, UMA, TRT*

This task is responsible for a social networking scenario that involves the personal security assistant in combination with the security enablers and context measures.

The basis for this scenario is the description developed in WP2. This task will develop functions specific to this scenario and integrate the security assistant.

The scenario development will be validated against the requirements derived in WP2 and in a trial with end users. The prototype will focus on several different aspects from the developed technologies around reputation, user-centric identity management and cryptographic solutions for storage and computation.

T6.4 e-Government Scenario Development & Validation			
Leader	*TRT*	***Participants***	*Fraunhofer, PTIN*

The objective of this task is to show how the personal assistant can help on a real situation with e-government platforms.

The first part of the task is to define and build a detailed scenario in line with the requirements identified in WP2. After that, follows the task of adapting the prototype developed in T6.1 and integrate it to fit this scenario.

The last part of this task is the validation of the scenario against the requirements and the **SPHERICS** concepts of user-centricity, usability, privacy, trust and reputation management, Identity management and secure storage.

Deliverables		
ID	**Month**	**Name and brief description**
D6.1	**M12**	***Interfaces for the Security Assistant*** Defines the interfaces of the security assistant. This builds the foundation for the implementation in WP3 – 5 and resolves dependencies between the technical work packages. The deliverable will also present the initial mock-ups of the user interface.
D6.2	**M21**	***System Integration Report*** Presents updates on the architecture as well as progress on the security assistant development and integration of the first modules from the technical WPs (WP3, WP4 and WP5).

D6.3	**M30**	***Realization of Prototypes*** Presents the design, implementation issues and results of selected prototypes. These prototypes illustrate the use of the security assistant in selected scenarios.
D6.4	**M36**	***Final Architecture, system realization and evaluation*** Presents the final version of the system architecture and realization of the security assistant as well as updates of the prototypes based on the user validation.

Role of partners
Fraunhofer will be responsible for the task T6.2, the Development & Validation of the cloud computing scenario and contribute to the other tasks with their experience in e-Government and validation related projects. **NEC** will be responsible for the coordination of the integration work, and contribute to the creation of a prototype for the "Cloud Computing" scenario. **UMU** will be integrating the outcomes from WP3 into the general architecture, as well as creating the prototype for the scenario "Cloud Computing". UMU will be also helping in the validation of the proposed solution in the "Cloud Computing" scenario, in particular when considering data portability from one cloud provider to another. **UMA** will contribute to the integration of the outcomes from WP4 into the general architecture. They will also participate on the development of the prototype for the scenario "Social Networks" **PTIN** will validate the implementation of the system requirements identified in the WP2, for each scenario defined, and creating the prototype scenario "e-Government". PTIN will contribute with Knowledge on IdM and trust management to find the final architecture to the assistant. **TRT** will integrate of the results of WP5 into the general architecture and coordinate the e-Government scenario validation. **MOV** will be responsible for task T6.3, where concepts of the social networking solution of **SPHERICS** will be implemented and evaluated against the real-world requirements from Movation's *InnoBors* solution [46]. This includes involvement of players in the eco-systems, including business angles, entrepreneurs and society members.

Table 13: Work package 7 description

WP number	**WP7**	Start month	**M01**	Activity type	**RTD**
WP title	**Dissemination, Standardization and Exploitation**				

Participant ID	P01	P02	P03	P04	P05	P06	**P07**
Participant short name	Fraunhofer	NEC	UMU	UMA	TRT	PTIN	**MOV**
Person months	5	6	6	6	2	5	**6**

Objectives

The objectives of this work package are the following ones:

- Achieve a high visibility of both the project itself and its related results within the scientific community in the field of security in ICT.
- Identify key players for targeted industrial dissemination in order to create the ecosystem for industrial take-up of **SPHERICS**.
- Participation in standardization groups and relevant industry such as ITU-T, IETF, OASIS, CSA, Kantara, ETSI and W3C.
- Establish business workshops to encourage exploitation of results.

Description of work

The purpose of this work package is twofold. On the one hand, to disseminate the outcomes obtained from the project by means of publications in high-quality international conferences and journals, as well as the development of a website for the activities related to the project, included targeted and dedicated workshops. A specific focus is towards creating business ecosystems, which will create accelerated innovation for the expected outcomes of **SPHERICS**.

On the other hand, it is intended to participate in standardization activities, which is seen by the EC and the industry as a new issue of strategic importance for the creation of markets. While the funding situation in Europe does not support big initiatives like Google or Facebook, the advantage of Europe is in the collaborative market opportunities using these global infrastructures. Thus a focus in the standardization activities of **SPHERICS** is in the support of open frameworks, with cross-domain tools and technology for a wide range of application sectors.

Knowledge management and intellectual property, has an economical value that can be directly exploited, in terms both of patents, business development and opportunities for creating spin-offs. Academia and research institutes will exploit knowledge, in terms of both internal exploitation (training of personnel or students) and external exploitation (promotion of partners' visibility in the research community). All partners will work towards dissemination by publications in international, refereed journals and at targeted conferences, and will also actively support individual promotions.

T7.1: Dissemination

Leader	*MOV*	***Participants***	*ALL*

A first level of dissemination is non-public dissemination of project findings and results in the project

consortium, and subsequently on in the partner level. This internal information transfer will be conducted in the consortium using an internal section of the collaborative project web, a newsletter and the regularly scheduled project meetings.

The project will use several dissemination channels to spread awareness of the project contents and achievements to as many people and organizations as possible. **SPHERICS** considers four different levels of dissemination to respond to all the potential target groups:

- Scientific dissemination for uptake and state-of-the-art research.
- Industrial dissemination for widespread acceptance.
- Targeted dissemination for building the business ecosystem.
- Large audience dissemination for public attention.

The purpose of this task is to provide measuring criteria for evaluating the socio-economic impact related to the project and the exploitation of the project results. To reach the target audiences (SMEs and Society) methods based on modern marketing, advertising strategies, mass-media, conferences, workshops will be defined and planned, a business case for the process will be developed and companies who could use the process will be targeted.

The task will further deal with the proactive dissemination of information about the project and project results to a broad public audience. Scientific results are to be published in high-visibility conferences and journals. To target a broader audience, suitable material such as a website, leaflets, press releases, etc. will be prepared as appropriate.

Task 7.2: Standardisation

Leader	*Fraunhofer*	***Participants***	*NEC, UMU, UMA, PTIN*

In order for the security assistant to be widely accepted and deployed, it will rely on current existing standards for many of the aspects considered in each of the composite enablers.

Moreover, the participation in several standardization bodies, such as OASIS Cloud TC, amongst others, is an expected activity within the frame of **SPHERICS**. Such standardisation efforts are seen by the EC and the industry as a new issue of strategic importance for the creation of markets. Thus a focus in the standardization activities of **SPHERICS** is in the support of open frameworks, with cross-domain tools and technology for a wide range of application sectors.

Task 7.3: Exploitation

Leader	*PTIN*	***Participants***	*NEC, UMU, TRT, MOV*

This task will promote detailed exploitation, based on the individual exploitation plans and workshops with representatives from business angles networks (eBAN, NorBAN,…). While “RTD-partners” typically are excellent in their research domain, they often lack the competence of bringing ideas and products to the market. Here comes the novel approach of **SPHERICS**, where the results of the “R&D and prototype integration” are taken into a dedicated workshop with selected business angles in order to focus on innovation and products. Bringing external experts into the picture will promote the “impact-based” approach of **SPHERICS**. The successful external exploitation of **SPHERICS** is very important to the continuity of the project results. Based on these business workshops a dedicated exploitation plan of each partner will be discussed an analysed through the standardized Scorecard process of Movation, providing indications for business, branding, team, partnering and technology, amongst others.

Deliverables		
ID	**Month**	**Name and brief description**
D7.1	**M2**	***Web site of the project*** Creates the Web page for the project with focus on interoperability and services.
D7.2	**M2**	***Collaborative platform for research and dissemination*** The envisaged collaboration will be supported by means of an on-line platform for research and dissemination. Several alternatives such as MediaWiki and BSCW will be analysed to study their specific suitability to **SPHERICS**.
D7.3.1	**M12**	***Identification of key players for the SPHERICS ecosystem and periodic dissemination activity report for year 1*** This deliverable describes the **SPHERICS** ecosystem and the necessary players to enable market acceptance. Key players in a regional, national and international level will be identified. The deliverable contains also the section on scientific dissemination, tutorials and trainings.
D7.3.2	**M24**	***Dissemination Report for year 2*** This deliverable describes the dissemination activities in year 2, and adds feedback from targeted dissemination, the "lessons learned" when discussing with business people. It will also contain a section on trends in research relevant for **SPHERICS**.
D7.3.3	**M36**	***Final Dissemination Activity report for year 3*** This deliverable describes the dissemination activities in the final year, and adds feedback from targeted dissemination. It will also contain a comparison of our approaches with the state of the art in research in the field.
D7.4.1	**M15**	***Standardization plan*** Though we have already identified areas for standardisation in the proposal, this deliverable will provide a structured review of the bodies and the planned contributions, together with a time-line.
D7.4.2	**M36**	***Standardization report*** This deliverable will provide details on where **SPHERICS** has contributed to standards, list the patent applications related to the work and outline open issues for standardisation.
D7.5.1	**M19**	***Notes and presentation material from business exploitation workshop*** Presentation material, comments and conclusions of the business exploitation workshop will be made available through the collaborative platform in form of presentations, videos, and web pages. We envisage using social media such as LinkedIn for the distribution and attraction of workshops.

D7.5.2	**M33**	***Exploitation plan and business opportunities*** The exploitation plan will focus on exploitation into the ecosystem, focussing on which contributions are necessary to let the **SPHERICS** prototypes become products. The report will also summarise the outcomes of discussions with business angles, organisations and companies.

Role of partners
Fraunhofer will lead Task 7.2 Standardisation in order to ensure visibility in and impact to the most important standardisation bodies. Besides national bodies Fraunhofer will focus on corresponding international working groups in ITU-T, IETF, OASIS, CSA, and Kantara. **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 forthcoming business unit projects. **UMU** will be contributing actively with the dissemination of the project results in the form of academic papers to be published in relevant international conferences and journals. Moreover, UMU will be actively promoting the project results for the academia and the research community by participating in relevant conferences and exhibitions. **UMA** will contribute to the dissemination activities in terms of research publications in international conferences and journals and the production of MSc theses. They will also contribute to the organization of events or presenting the results of the project in adequate forums. **TRT** will contribute to the dissemination activities of the project through the production of publicity material and academic papers. TRT 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. **PTIN** will lead the task T7.3 of this WP and will participate in the dissemination tasks with some promotion initiatives internal to the company's group. PTIN will lead the exploitation task revising the participant's individual plans and promoting the tools and techniques developed in **SPHERICS** scope, to the PT group companies and to other PT partners outside the consortium. **MOV** will lead WP7 and 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.

Table 14: Summary of staff effort (WP leader in bold)

Partner no.	Partner short name	Work package							Total
		WP1	WP2	WP3	WP4	WP5	WP6	WP7	
P01	**Fraunhofer**	**12**	16	18	11	6	16	5	**84**
P02	**NEC**	7	12	6	19	18	**16**	6	**84**
P03	**UMU**	1	10	**20**	18	6	14	6	**75**
P04	**UMA**	1	9	10	**21**	17	9	6	**73**
P05	**TRT**	1	11	0	0	**18**	10	2	**42**
P06	**PTIN**	1	**16**	17	0	0	10	5	**49**
P07	**MOV**	1	0	7	10	0	8	**6**	**32**
Total		**24**	**74**	**78**	**79**	**65**	**83**	**36**	**439**

Resource allocation to each **SPHERICS** partner (see Figure 8) will be distributed as to avoid unnecessary overlap while limiting the overall budget to a reasonable value. The effort allocation of each Work Package has been carefully elaborated in order to spend the budget purposefully and efficiently.

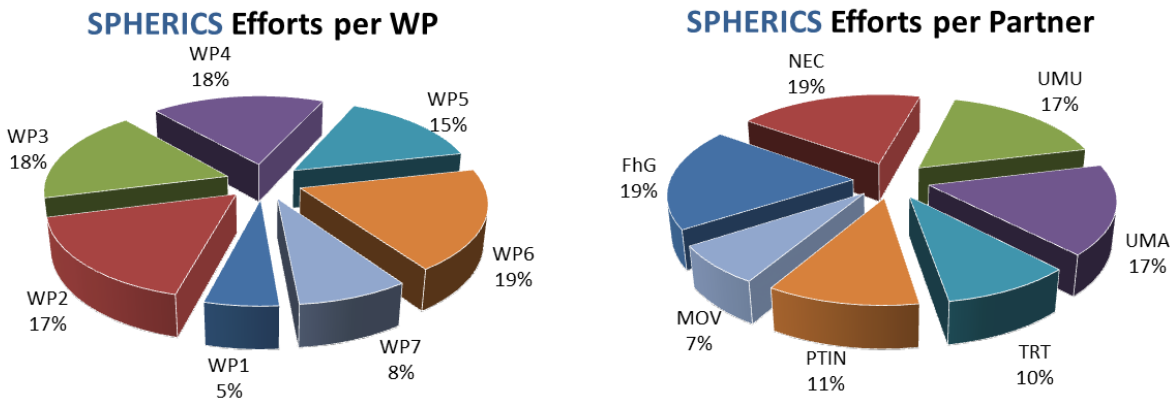

Figure 8: Percentage effort per work package (left) and per partner (right)

Each partner is committed to take over one WP leadership (see Table 14 and Table 15). The **SPHERICS** project plans a total effort contribution of 439 person months over 36 months. This constitutes a yearly average of 11.5 FTE in RTD, and 0.67 FTE in Project Management on the **SPHERICS** project.

Table 15: Detailed breakdown of person month contribution per partner

			FhG	NEC	UMU	UMA	TRT	PTIN	MOV	
		Leader	1	2	3	4	5	6	7	Totals:
WP1		FhG	12	7	1	1	1	1	1	24
Task 1.1	MGT	FhG	3	0	0	0	0	0	0	3
Task 1.2	MGT	FhG	7	0	0	0	0	0	0	7
Task 1.3	MGT	NEC	2	7	1	1	1	1	1	14
Totals WP1:	MGT		12	7	1	1	1	1	1	24
	RTD		0	0	0	0	0	0	0	0
	DEM		0	0	0	0	0	0	0	0
WP2		PTIN	16	12	10	9	11	16	0	74
Task 2.1	RTD	PTIN	3	5	4	4	3	8	0	27
Task 2.2	RTD	TRT	6	6	4	5	8	6	0	35
Task 2.3	RTD	FhG	7	1	2	0	0	2	0	12
Totals WP2:	MGT		0	0	0	0	0	0	0	0
	RTD		16	12	10	9	11	16	0	74
	DEM		0	0	0	0	0	0	0	0
WP3		UMU	18	6	20	10	0	17	7	78
Task 3.1	RTD	PTIN	3	1	4	4	0	4	0	16
Task 3.2	RTD	UMU	6	3	9	6	0	7	3	34
Task 3.3	RTD	FhG	9	2	7	0	0	6	4	28
Totals WP3:	MGT		0	0	0	0	0	0	0	0
	RTD		18	6	20	10	0	17	7	78
	DEM		0	0	0	0	0	0	0	0
WP4		UMA	11	19	18	21	0	0	10	79
Task 4.1	RTD	UMU	2	2	8	6	0	0	0	18
Task 4.2	RTD	UMA	3	9	8	11	0	0	4	35
Task 4.3	RTD	MOV	6	8	2	4	0	0	6	26
Totals WP4:	MGT		0	0	0	0	0	0	0	0
	RTD		11	19	18	21	0	0	10	79
	DEM		0	0	0	0	0	0	0	0
WP5		TRT	6	18	6	17	18	0	0	65
Task 5.1	RTD	UMA	2	2	4	7	4	0	0	19
Task 5.2	RTD	TRT	2	8	2	6	6	0	0	24
Task 5.3	RTD	NEC	2	8	0	4	8	0	0	22
Totals WP5:	MGT		0	0	0	0	0	0	0	0
	RTD		6	18	6	17	18	0	0	65
	DEM		0	0	0	0	0	0	0	0
WP6		NEC	16	16	14	9	10	10	8	83
Task 6.1	RTD	NEC	4	10	7	3	4	4	0	32
Task 6.2	RTD	FhG	7	5	7	0	1	0	1	21
Task 6.3	RTD	MOV	1	1	0	6	1	0	7	16
Task 6.4	RTD	TRT	4	0	0	0	4	6	0	14
Totals WP6:	MGT		0	0	0	0	0	0	0	0
	RTD		16	16	14	9	10	10	8	83
	DEM		0	0	0	0	0	0	0	0
WP7		MOV	5	6	6	6	2	5	6	36
Task 7.1	RTD	MOV	2.5	2	3	4	1	1	4	17.5
Task 7.2	RTD	FhG	2.5	2	1	2	0	1	0	8.5
Task 7.3	RTD	PTIN	0	2	2	0	1	3	2	10
Totals WP7:	MGT		0	0	0	0	0	0	0	0
	RTD		5	6	6	6	2	5	6	36
	DEM		0	0	0	0	0	0	0	0
Final totals:	MGT		12	7	1	1	1	1	1	24
	RTD		72	77	74	72	41	48	31	415
	DEM		0	0	0	0	0	0	0	0
		TOTAL	84	84	75	73	42	49	32	439

1.3.4 Risks and contingency plans

In a project involving different organisations it is likely that problems will occur from time to time. For this reason, it is extremely important that the Consortium is prepared beforehand to handle these threats, by identifying and analysing potential risks and defining the necessary corrective actions.

The Risk Management process consists of four main steps:

1. Identification of the potential risk for the project
2. Assessment of the probability of occurrence and possible impact on the project
3. Definition of contingency plans in order to avoid the risk or, at least, reduce its impact.
4. Monitoring of the current state of the project, with the objective of identifying new risks and supervising the corrective actions taken to mitigate occurring risks.

Risk Management should be considered as a continuous process that takes place during the whole duration of the project. Consequently, the project management board will be constantly carrying out a Risk Management process in order to assess the risks and take corrective actions as needed.

Risk identification and contingency plans

As an initial contribution to the Risk Management process, the **SPHERICS** Consortium has identified a set of risks, which has been divided into categories depending of their nature. For each identified risk, the Consortium has also assessed its probability of occurrence and the magnitude of its impact on the project. Finally, a contingency plan is presented, in order to avoid such risk, or at least minimize its possible effect in the project.

Managerial risks

Table 16: Risk assessment and contingency plan relating to SPHERICS Managerial activities

Risk description	Likelihood	Impact	Preventive measures / Contingency actions
Lack of commitment or underperformance of one of the partners.	Low	High	In the event of detecting a recurrent lack of fulfilment of a partner's obligations, the project coordinator will issue a warning to the partner and will require corrective actions by a specific date. If the problem remains unresolved after this date, the partner's workload and budget will be redistributed between partners. In the event that the partner's activities cannot be re-distributed, a new partner will be invited into the consortium to take on the work.

Technical risks

Table 17: Risk assessment and contingency plan relating to SPHERICS Technical activities

Risk description	Likelihood	Impact	Preventive measures / Contingency actions
Delay in the delivery of key elements of the project.	Low	High	The project partners involved in that key elements will be requested for a first version with at least a set of interfaces that the rest of the project components can follow to interact with that particular component. In the meantime, the missing component should be developed possibly adding some additional effort to this tasks and work package.
The results derived from the validation process are not as expected.	Low	Medium	The feedback and lessons learnt would be reported as intermediate results of the project and new measures will be taken to re-adapt current designs and implementations to the scenario requirements.
The requirements extraction and validation phases do not have access to the right end-users.	Low	High	New stakeholders would be considered and certain additional promotion activities would be performed by project partners.
Project developments may conflict with Data Protection laws.	Medium	High	**SPHERICS** will take the necessary precautions to handle personal data in an appropriate way, for example, by using data anonymization techniques. However, one of the main contributions of the project is the development of privacy-preserving mechanisms for the storage and processing of information.

Dissemination and exploitation risks

Table 18: Risk assessment and contingency plan relating to SPHERICS Dissemination and Exploitation activities

Risk description	Likelihood	Impact	Preventive measures / Contingency actions
The dissemination activities receive a negative response from the potential target audience.	Low	High	Dissemination activities are scheduled throughout the whole project so that feedback from relevant stakeholders can be taken into consideration during the project.
Standardization activities do not achieve the contribution of project outcomes into standards.	Low	High	Partners of the consortium currently participate in standardisation activities and bodies. However, if the project outcomes were not accepted by the standardisation bodies, a reactive measure would be taken to promote the ideas in other relevant bodies or to explore new designs of the project components with the aim of promoting project results in the standardisation community.

Section 2: Implementation

2.1 Management structure and procedures

This section describes how the **SPHERICS** project will be managed, the decision-making structures to be applied, the communication flows within the consortium and the quality assurance measures that will be implemented. This section also identifies possible points of failure in the project and suggests ways and correcting actions to implement in order to put the project back on track.

2.1.1 Management Structure

High priority and attention will be given to the crucial area of project management. The project partners are fully committed and agree to work together with the utmost cooperation for the timely fulfilment of their responsibilities. The **Project Coordination** will implement clear management processes and promote a qualitative and dynamic management of all aspects of the project.

The ***Project Coordinator***, Mr. Mario Hoffmann from Fraunhofer, has more than twelve years R&D experience at Fraunhofer coordinating national and international research projects. He will be responsible for the overall project strategy, ensuring that all parties within the Consortium know exactly what is expected from them, as described in the individual work packages. Mr. Hoffmann will take care of the management of the project and will ensure the execution of the contract. He will be responsible for ensuring that all objectives are met and that all costs and milestones are in-line with the budgets and the provided Gantt Chart. Any deviation will be immediately communicated to the Consortium members and the EC Project Officer.

The Project Coordinator will appoint a ***Technical Manager***. The Technical Manager will be responsible for the technical coordination and supervision of the work packages, planning and control of activities and preparation of deliverables, as well as collecting contributions from other partners participating in the task.

Two committees, the ***Steering Committee*** and the ***Technical Committee***, will be the main elements of the project management structure. The management will be organised in a two-tier fashion as depicted in the diagram shown in Figure 9.

The remainder of this sub-section describes the roles of the individual management structures, namely the roles of: Project Coordinator, Technical Manager, Steering Committee, Technical Committee, and Work Package Leaders.

The Project Coordinator

As the Coordinator, Mr. Hoffmann is the single point of contact between the European Commission and the Consortium. In this function the Coordinator shall:

- Sign the Contract with the European Commission
- Ensure accession to the contract by the other contractors
- Ensure the communication between the Consortium and Commission
- Receive and distribute the EC contribution
- Collect from all Contractors the cost and other statements for submission to the European Commission

- Prepare, with the support of the Technical Manager and the members of the Steering Committee, the reports and project documents required by the European Commission
- Ensure prompt delivery of all hardware, software, and data identified as deliverable items in the Contract or requested by the European Commission for reviews and audits, including the results of the financial audits prepared by independent auditors.

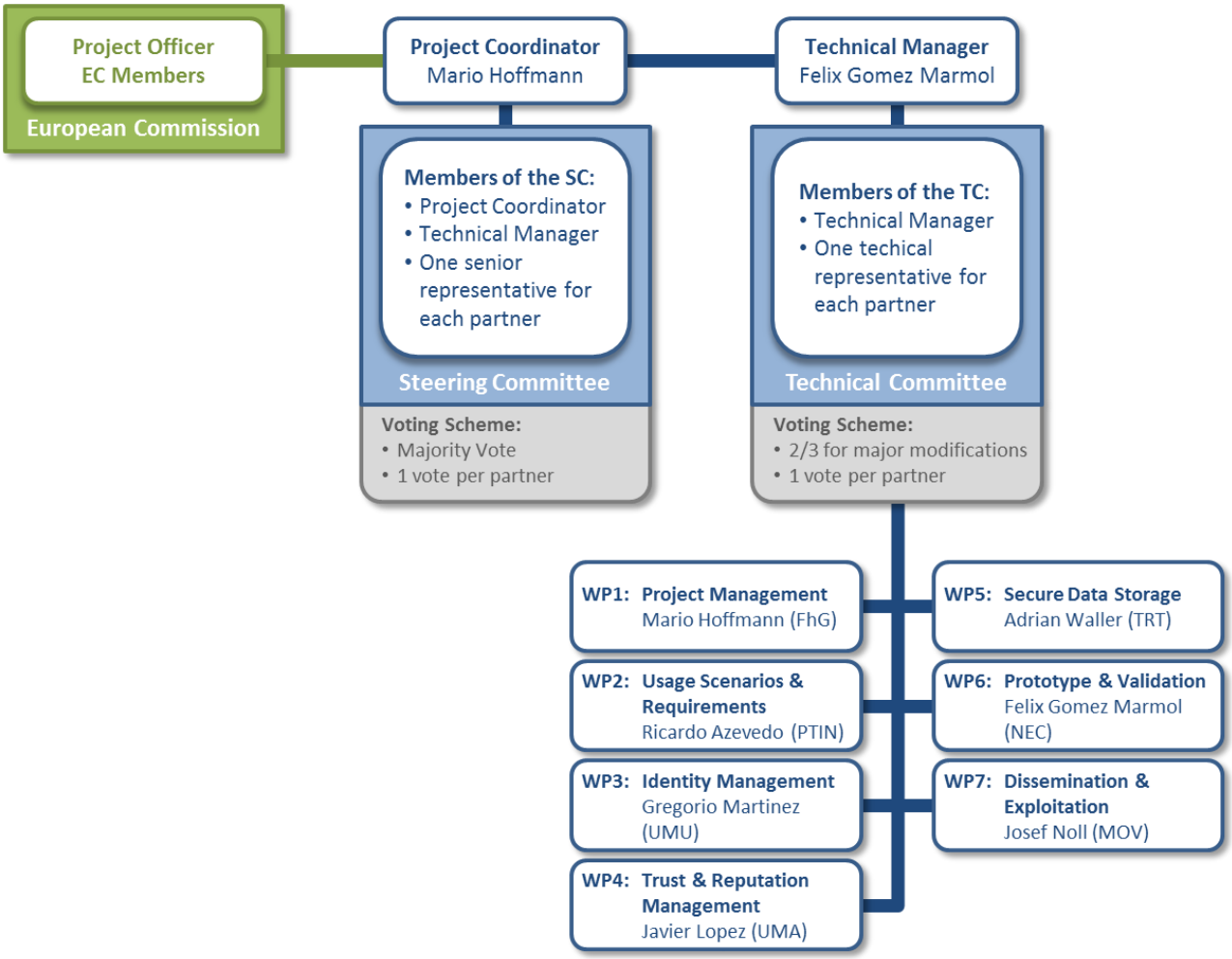

Figure 9: Management scheme for SPHERICS

Mr. Hoffmann will be authorised to execute the project management and will be accountable to the project Steering Committee. Mr. Hoffmann will also be responsible for the preparation of the meetings and decisions and the chairing of the Steering Committee. He approves all outputs and reports and is the prime external interface.

The Technical Manager

The Technical Manager will be appointed by the Coordinator. The designated Technical Manager is Dr. Felix Gomez Marmol from NEC. Dr. Gomez Marmol will chair a Technical Committee consisting of the key technical staff (normally work package leaders). The Technical Manager must be aware of on-going technical developments outside the project in order to include or adapt for example new standards in the project. The Technical Manager will also sit in the Steering Committee ex officio. Following activities belong to the responsibilities of the technical management:

- Supervision of project objectives and timeliness of the work plan

- Monitoring of important dates and deadlines, maintaining project calendar
- Day-to-day management activities, e.g. organisation of meetings, management of letters, reminders, transactions, monitoring and illustration of the Project status and data of the partners
- Implementation of decisions made by the Coordinator and the Steering Committee

2.1.2 Committees

The **SPHERICS** project has a clear structure and a well-defined management scheme (see Figure 9) with two committees, namely the Steering Committee and the Technical Committee.

The **Steering Committee (SC)** is the core organisational and decision-making body and has the obligation to ensure that the Consortium functions properly. It will be responsible for the successful completion of the project and the exploitation of its results. It will be chaired by the appointed Project Coordinator. Further core members of the SC will be the Technical Manager and one representative of each partner. Decisions regarding the project will be made by vote with each partner having a single vote. In cases of a tie, the Project Coordinator will have a casting vote. Non-voting members and external experts may be invited to the Committee by the Chair.

The Steering Committee will normally meet at six monthly intervals. In practical terms the Steering Committee represents the Consortium in all related affairs. The duties include, but are not limited to:

- All budget-related matters
- The structure and restructuring of the work packages
- The alteration of the Consortium Agreement
- The premature completion / termination of the project
- Preparation of all documents (financial, reporting, audit, etc.)
- Management of knowledge
- Communication between the Consortium and the Commission
- Communication between the Consortium and third parties
- Publicity
- Establishment and overview of intellectual property procedures
- Preparation of detailed work plan
- Steering of the Consortium

The Chair calls the Steering Committee to a meeting. The **voting scheme** for the Steering Committee is by majority vote with each partner having a single vote. A majority of voting members (at least half of the number of members of the Steering Committee) is required to conduct a meeting (quorum). A simple majority (at least half of the members present during the voting) is required to make formal decisions.

A **European Commission Representative** may participate as an observer at the meetings of the Steering Committee.

The **Technical Committee (TC)** is conceived as the technical central body of **SPHERICS**. It is chaired by the Technical Manager. It is formed by representatives of the partners involved in the **SPHERICS** Project, namely by one person appointed by each organisation, preferably by the responsible of each of the work packages. In this way, the TC joins expertise in the various technical fields relevant to the **SPHERICS** work packages, thus being, in practical terms, the technical guidance to guarantee successful advancement.

The duties of the Technical Committee include, but are not limited to:

- Coordinate activities covering more than one technical area

- Contribute to the overall technical affairs of the Consortium
- Be responsible for the integration of the individual developments stemming from the WPs.

The Technical Committee shapes based on the strategy approved by the European Commission for ICT Project description of goals and methods. The **voting scheme** for the technical committee is the following: It decides with a majority of 2/3 about the required modifications and changes due to unexpected findings or events during the course of the project implementation. The Technical Committee is planned to meet every three months. It is furthermore planned that TC will meet at least 6 times along the 36 months duration joined to Steering Committee meetings.

2.1.3 The Work Package Leaders

The **work package leaders** are senior members of the partners' and coordinator's staff. They will act like operating executives in a commercial company, and will be responsible for the completion of their work package and successful production of deliverables. They direct all aspects of activity in the work package and report to the Technical Committee in co-ordination with the Technical Coordinator. In more details, the work package leader is appointed by each work package and is responsible for:

- The performance and progress of the work package with regard to the project plan
- The horizontal information flow to other work package leaders
- Identification and reporting of problems

Each task in a WP is led by a partner. The **Task Leader** reports to the WP Leader, co-ordinates technical work for his/her activity according to the project and WP objectives, assists in the preparation of reports. Each of the partners has at least one task responsibility, and is co-ordinating the work done in this task.

2.1.4 Management Procedure Tools

The Coordinator will establish the following management procedure tools:

1. **Project Handbook**: the Coordinator will set up an Implementation Strategy, including a draft of a Project Handbook for the purpose of managing information flow, timescales scheduling and finance planning as well as best project quality assurance and project documentation. This project handbook will be updated as appropriate throughout the duration of the project.

2. **Internal assessment**: the Coordinator will closely follow up and control the progress of the project and the work done by each partner. To reach this goal, the project Coordinator will regularly identify partners' risks using management tools and procedures. This identification will be screened according to four risk levels: very low, low, medium and high risk. Medium risk partners will be informed of the concerns and asked to take corrective actions. High-risk partners will be audited through internal audit carried out by the Coordinator and the concerned WP leader. The result of the audit will be then transmitted to the Steering Committee to take appropriate actions.

3. **The collaborative platform**: the collaborative platform is an internet-based secured collaborative workspace where all project partners can share and exchange information. This platform is intended to foster collaboration between all partners at all levels: Consortium, WP, Steering Committee, Coordinator, Project Officer etc. Its functions include technical, administrative, and financial information exchange and archiving.

4. **Project management Software**: the consortium will use a knowledge management software application, focused on managing FP7 funded projects. The software covers the key aspects of **Controlling:** Resource management, HRM, Travels, Equipment / consumables, Management costs and **Workflow:** Supervision, Comparison and Statistic.

2.1.5 Communication Flow

The establishment of a fast, reliable, and easily accessible communications infrastructure is vital to the proper operation of an European project. This can only be achieved through the intensive use of electronic communications (e.g., email, web based exchanges). A project website will also be used to enable fast and efficient exchanges of information. Thus, main communication channels are: Telephone calls and telephone conferences, email, web-based services such as internal discussion forums or chats, and personal meetings.

Internal communication includes physical meetings, starting with a 1-3 days kick-off meeting to guarantee in-depth knowledge exchange. Meetings are accompanied via fixed telephone conferences to discuss project progress and to take decisions. Also applied are the exchange of emails, letters etc. It will be decided at the kick-off meeting which solution will be used to share knowledge.

External communication includes the dissemination of all project results through publications, a project website, conferences, events, and the establishment of links to related projects and associations.

The experience in running research projects, the good relationships, and mutual knowledge of the partners, as well as the previous working together successfully for most of the partners, almost ensures the in-existence of problems regarding communication and information flow along the development of the **SPHERICS** Project.

2.1.6 Conflict Management

Conflict Resolution - Pragmatic negotiation will be the basis for the Consortium conflict resolution approach. Typical conflicts, which can arise in the project, can be due to a lack of productivity and/or quality, missed deadlines, different languages, and personality or cultural differences. It will be the responsibility of the Coordinator to identify these conflicts at an early stage and take steps to talk to the involved parties to quickly resolve the conflict. Negotiations and decisions taken by consensus will be the main tools to resolve conflicts.

Within each meeting, where unanimity is not possible, decisions will be made on the basis of a qualified majority of 2/3 of the authorised representatives of those partners present represented by proxy. If the conflict is upgraded to the Steering Committee level and the qualified majority of 2/3 is not reached, the decision will be based on simple majority.

The conflict resolution procedure will be described in more detail in the Consortium Agreement, which, along with the Contract, will constitute the basis upon which the project is managed.

2.1.7 Consortium Agreement

An agreement will be organised between all the consortium project partners, once the project has been accepted by the EC. The aim of this agreement is to determine the responsibilities fixed within the consortium and towards the EC. It will be presented to the EC for agreement.

2.2 Individual participants

2.2.1 Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer)

The Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. is the leading organisation for applied research in Europe and currently maintains 60 independent research institutes operating from different locations in 15 of the German states. A staff, of approximately 18 000 researchers, works with an annual research budget of about 1.7 billion Euro. The Fraunhofer-Institution for Applied and Integrated Security AISEC is the IT-Security expert within the Fraunhofer organisation and has experience in development and promotion of security technologies and in embedding of security technologies into already established applications to make them trustworthy. The working areas of about 80 employees range from basic applied research and development of prototypes to product testing as well as customising and implementing tailored security concepts and solutions.

The core competences of Fraunhofer AISEC comprise the security of cloud-and service-oriented computing, the identity management of people, things and services, product and intellectual property protection, network security, and the security of embedded systems. Fraunhofer AISEC maintains a cloud security lab for experimenting with and testing of new security solutions under realistic conditions.

In the project's scope Fraunhofer AISEC has much experience from preliminary work, e.g.: employees of Fraunhofer AISEC, the former Fraunhofer SIT-Munich, were leading the security work package in the EU-funded FP6 project HYDRA and have developed a virtualization layer for managing identities of users, devices, and value-added services as well as semantic security policies for context-aware application scenarios. Moreover, personnel of Fraunhofer AISEC were working on event modelling in the EU FP7 project MASSIF.

AISEC is the cloud security expert in the Fraunhofer group, working on different nationally funded cloud security research projects such as SealedCloud and ASMONIA. Besides research activities, AISEC is conducting security assessments of cloud and identity concepts & products for customers such as Nokia Siemens Networks, Fujitsu, RSA, Salesforce, and Germany's Federal Office for Information Security (BSI). AISEC is active member of Kantara Initiative (global umbrella for identity management), the Cloud Security Alliance, and many related national bodies.

Innovative role in the project

In **SPHERICS** Fraunhofer plays the role of bridging research concepts and industry interests. The R&D focus of Fraunhofer AISEC will be characterised by specifying and implementing protocols in order to ensure integration, interoperability and portability of user-centric approaches to identity management, trust and reputation taking advantage of modern Cloud services and secure data storage. The combination of those technologies is from Fraunhofer's point of view the key to secure and trustworthy innovative services in the Future Internet. In order to push an independent development far beyond **SPHERICS** Fraunhofer will play a key role in dissemination and standardisation activities.

Main tasks Fraunhofer is involved in

WP1: Fraunhofer will conduct overall coordination of the project. It is responsible for orchestrating the work done in the work packages and establishing appropriate communication channels between the partners and between the project and the Commission.

WP2: Fraunhofer will be providing its expertise in identity management and privacy protection during the requirements analysis and systems design. As leader of an implementation task (T3.3) Fraunhofer will have a focus on the implementation of the system design. As leader of the security evaluation (T2.3) Fraunhofer will bring in expertise in the field of IT-security and penetration testing as well as from practical security tests.

WP3: Fraunhofer will support the state of the art analysis and the module design with its expertise in identity management as well as lead the implementation of the IdM module.

WP4: Fraunhofer will support the progress in this work package with their experiences in several federated identity- and trust protocols. One focus will be the investigation of the relationship between identity and trust and their impacts on each other.

WP5: Fraunhofer will act as a reviewer of the all the deliverables of this work package and evaluate those against the background of their experiences in the field of secure cloud storage and data processing.

WP6: Fraunhofer will be responsible for the task T6.2, the Development & Validation of the cloud computing scenario and contribute to the other tasks with their experience in e-Government and validation related projects

WP7: Bridging research concepts and business interests Fraunhofer will lead Task 7.2 Standardisation in order to ensure visibility in and impact to the most important standardisation bodies. Besides national bodies Fraunhofer will focus on corresponding international working groups in ITU-T, IETF, OASIS, CSA, and Kantara.

Profile of key staff members

Mario D. Hoffmann (41) received his master degree in computer science from Darmstadt University of Technology, Darmstadt, Germany, in 1998. His master thesis he completed at Nanyang Technological University, Singapore.

In 1999 he joined the Fraunhofer-Gesellschaft zur Förderung der Angewandten Forschung e.V.; since 2009 he has been responsible for the research department “Secure Services & Quality Testing” at the Fraunhofer-Institution for Applied and Integrated Security (AISEC), Garching (near Munich); from 1999 to 2008 he was with the Fraunhofer-Institute for Secure Information Technology (SIT), Darmstadt, Germany. From May 2004 to Dec 2008 he was the head of the research department "Secure Mobile Systems".

Mario Hoffmann has been managing and coordinating projects for ten years now. One highlight was -from 2006 to 2010- the management of work package “Security & Trust” of EU’s FP6 Integrated Project HYDRA. In 2007/2008 he successfully coordinated two EU STREP proposals SWIFT and EVITA. In parallel to publicly funded projects he managed several projects funded by industry, incl. Nokia Siemens Networks and Vodafone. In research and development he personally focuses on multilateral secure identity management in context-aware ambient environments.

Mr. Hoffmann has been chair of the Working Group "Security&Trust" of the Wireless World Research Forum (WWRF) since 2005. Since 2009 he has been playing an active role in the Kantara Initiative. Moreover, he is a member of ACM, Cloud Security Alliance, GI (Germany) and CCC (Germany). He has been track chair and member of the programme committee of many conferences, e.g. IEEE CloudCom 2011.

Alam Nurul Mohammad was awarded his dual Master's degree in Information Technology by the Technical University of Poznan, Poland and Computer Science by the University of Applied Sciences Braunschweig, Germany in 2008. He had the distinction of securing his Bachelor Degree in Computer Engineering from the Voronezh State University, Russia in 2004.

He joined the Fraunhofer-Institution for Applied and Integrated Security (AISEC) in 2009 as a Scientific Researcher. He is focused on designing Identity & Access Management solutions, also has significant experience in cloud/SaaS-based solutions, Web/cloud security, and other IT management solutions.

Mr. Alam Mohammad is a voting member & contributor of the Kantara User-Managed Access (UMA) Work Group. He is also a speaker, presenter at independent industry events, conferences & shows.

Matthias Aumüller joined the Fraunhofer-Gesellschaft in 2009 after his graduation in business informatics (major field: information systems). Currently, he is a research fellow focussing on the topic identity management in the security group "secure services and quality testing" of the Fraunhofer AISEC as well as a doctoral candidate at the technical university of Munich. His research interests include identity management in heterogeneous environments and cloud computing, "identity as a service", ID cards and privacy technologies.

2.2.2 NEC Europe Ltd. (NEC)

NEC Corporation is a leader in the integration of IT and network technologies that benefit businesses and people around the world. By providing a combination of products and solutions that cross utilize the company's experience and global resources, NEC's advanced technologies meet the complex and ever-changing needs of its customers. NEC brings more than 100 years of expertise in technological innovation to empower people, businesses and society.

NEC Europe is a subsidiary of NEC Corporation based in the UK that builds upon its heritage and reputation for innovation and quality by providing its expertise, solutions and services to a broad range of customers, from telecom operators to enterprises and the public sector.

NEC Laboratories Europe is a laboratory established by NEC Europe Ltd. and is located in Heidelberg, Germany. NEC Labs Europe conducts leading research and development across IT and communications, including Future Internet and OpenFlow, next generation fixed and mobile networks, M2M, context-aware platforms and services, the Internet-of-Things, multimedia, security, energy-saving services and green technology. Special emphasis is placed on solutions that meet the needs of NEC's European customers and as well as collaboration with industrial and academic partners within the European R&D Framework Programme (FP7, etc.).

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), amongst others.

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

WP1: NEC will act as technical coordinator of the project and will therefore lead task T1.3.

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 forthcoming 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.

Joao Girao is the manager for the Security group at NEC Laboratories Europe. He received his diploma in Computer and Telematics from the University of Aveiro, Portugal, in 2003. In 2003 he joined the Ubiquitous Secure Computing group at NEC Laboratories Europe, in Heidelberg where he was responsible for the technical coordination of the Identity Management area. He has been involved in several European proposals and projects and up until recently was the work package leader responsible for the architecture in the EU Project SWIFT. As part of his duties in NEC, he has been responsible for several close to product projects and subsequent technology transfer. He has also been involved in several standards activities in Identity Management such as the ITU-T, ETSI, IETF and Liberty Alliance/Kantara. He has contributed NEC's IPR protection activities having secured several granted patents in the security area.

2.2.3 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 signalling, 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. UMU will be also working actively in the design of trust and reputation mechanisms and its integration with the IdM solution designed in the project. Additionally, UMU will be providing its expertise in the integration of security solutions as well as its high capacity to disseminate the results to the international research community.

Main tasks UMU is involved in

WP2: UMU will be contributing with the definition of requirements for the cloud computing scenario and how the seamless data portability can be accomplished in the project.

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.

WP5: UMU will contribute as part of the preparation of the state of the art of secure data storage and processing mechanism.

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

Dr. 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 centres 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.

Dr. 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 centres. He has published more than 40 papers in national and international conference proceedings, magazines and journals.

Dr. Diego Sevilla Ruiz received a M.S. and Ph.D. degrees in Computer Science at the University of Murcia in Spain. In 1998 he started as a teaching assistant in the Computer Engineering Department of the University of Murcia. His Ph.D. explored distributed component-based systems, fault tolerance systems and load balancing. Since 2006 he is an Associate Professor in that same Department. His main interests include distributed computing, modelling and meta-modelling, code generation, testing of distributed applications, testing of graphical applications, open-source development tools. He has worked in different national and European IST projects in these fields, and has also published several papers in these topics. He did several research visits, to the University of Indiana at Bloomington, and to the Vanderbilt University in Nashville, TN. Since 2006 he is in charge (jointly with Prof. Gregorio Martínez) of the "Catedra SAES-UMU", a joint effort of the company SAES and the University of Murcia to promote the usage of modelling technologies, modern development strategies, and the leverage of open-source tools to boost the quality and speed of software development.

2.2.4 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 the development of the component for Trust and Reputation Management. They will also provide their expertise in the development of Identity management solutions and secure data storage. UMA will contribute to the deployment of the social networking scenario.

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 management and cryptography. He is currently participating in the FP7 project PASSIVE, focusing in the area of identity management, authentication and authorization.

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.

2.2.6 Portugal Telecom Inovação, SA (PTIN)

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 centred 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 as 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 centre 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.

2.2.7 Movation (MOV)

Movation is the leading independent resource centre 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, amongst others 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 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 Telenor[2] 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 work package 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

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, amongst others, 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 of 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 start-up 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.

[2] Telenor and Google have announced a common App-Store

2.3 Consortium as a whole

SPHERICS aims to increase the users' security and privacy in the Internet, in order to foster the broad development and acceptance of Internet services solutions. To meet this objective, it will develop a secure personal assistant to provide user-centric security and privacy solutions that address three main security challenges:

- Identity management
- Trust and reputation management
- Secure data storage and processing

Tackling the research challenges in these three areas in an integrated manner requires a consortium with a breadth of expertise in security and privacy. With this in mind, the **SPHERICS** consortium consists of 7 partners with complementary competencies from 5 European countries: Germany, Norway, Portugal, Spain and the United Kingdom, as shown in Figure 10.

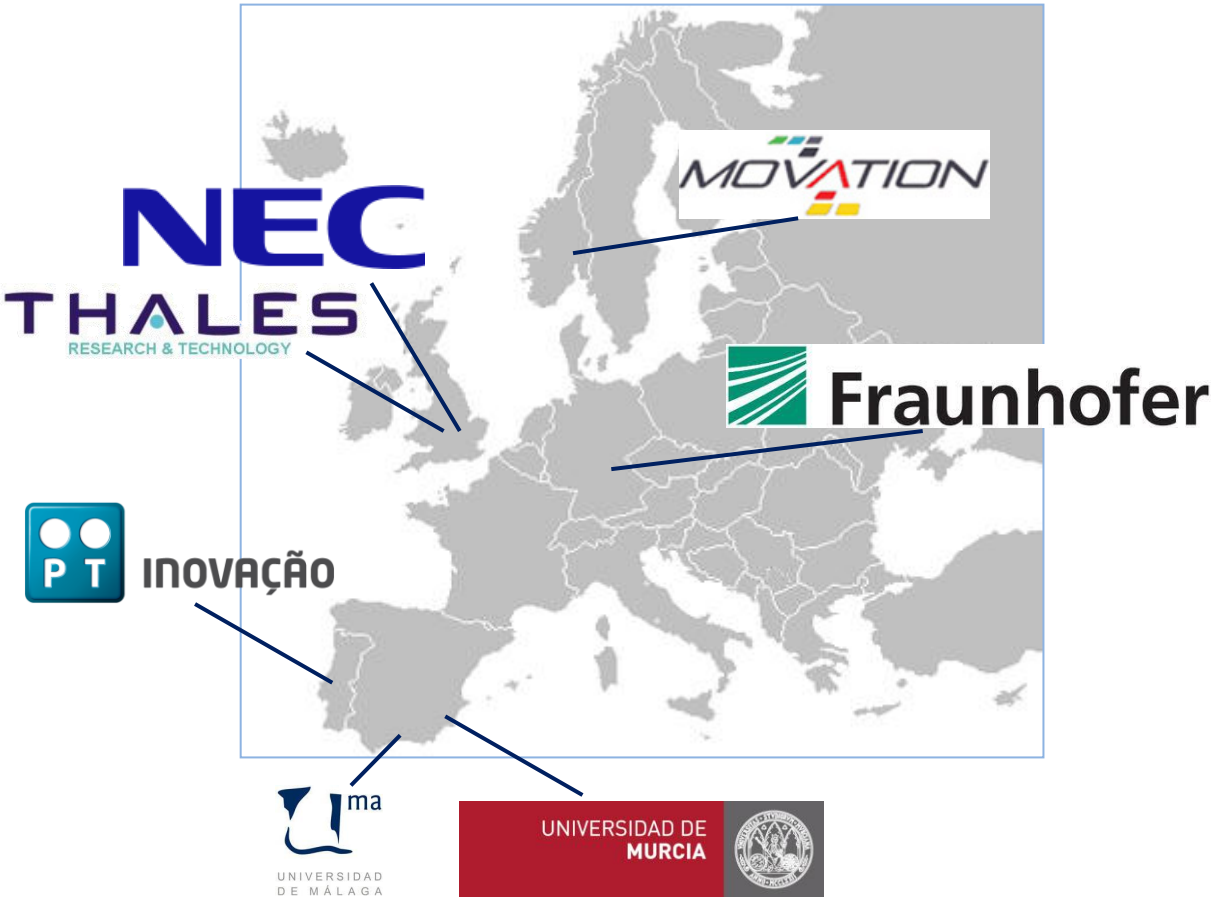

Figure 10: Consortium as a whole. Geographical distribution

The consortium consists of three industrial partners, complemented by an SME, a Research Institution and two universities. Thales is a global leader in mission-critical information systems for defence and security, aerospace and transportation. NEC is a world leader in IT and network solutions, and electronic devices. Portugal Telecom is a global telecommunications operator that has many solutions and research in other areas like security, cloud and identity management. Movation is an SME supported by corporates such as Telenor, Opera Software, Microsoft and Statoil to become the leading independent resource centre for open innovation in the Nordics. Fraunhofer is Europe's largest application-oriented research organization.

Both Universidad de Málaga and Universidad de Murcia have participated in a variety of national and European research projects in the area of security.

These consortium members are highly complementary in terms of business and user interests and the technical expertise necessary to perform the proposed research and development tasks. Figure 11 shows how the consortium partners have complementary skills in each of the three security challenges and achieve overall coverage of the **SPHERICS** scenarios.

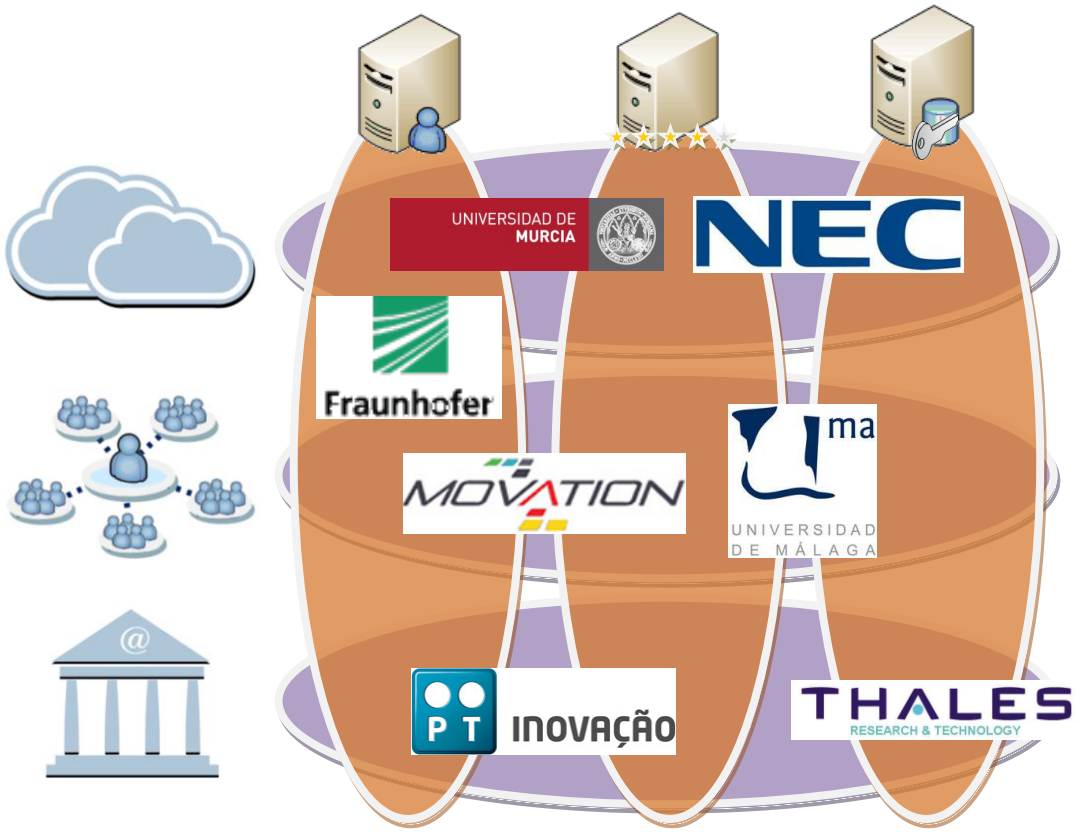

Figure 11: Consortium as a whole. Partners' expertise and contribution

Overall the consortium is coordinated and managed by Fraunhofer, which has experience in coordinating large multinational projects. It will also bring its knowledge on identity management and experience on both cloud computing and social networking. Technical Management is provided by NEC who has strong expertise in all three security challenges of the project and in cloud computing. Thales is contributing with their expertise in secure data storage and processing as well as with their industrial experience of e-government. In addition to their experience of working with e-government, Portugal Telecom will bring their expertise in both identity and reputation management. Universidad de Málaga will contribute with their expertise in trust and reputation management and their knowledge of social networking. In addition to their skills in managing identity, trust and reputation, Universidad de Murcia will contribute with their knowledge of cloud computing. Movation's experience in supporting start-ups and connect to established companies to create innovation will be used to identify business opportunities. Being the project leader of two Artemis security projects, Movation will also contribute to establishing the security value chain.

Table 19 identifies the work package and task leaders, who are all experts in their field. Additionally, the table shows the partners contributing to each WP (roles and explicit person month allocation can be found in sections 1.3 and 2.4). Thus, it can be observed that the consortium meets the needs of the **SPHERICS** project.

Table 19: Contributors, work packages leaders and tasks leaders

	WP1	**WP2**	**WP3**	**WP4**	**WP5**	**WP6**	**WP7**
Fraunhofer	**WPL**, TL1.1, TL1.2	TL2.3	TL3.3	X	X	TL6.2	TL7.2
NEC	TL1.3	X	X	X	TL5.3	**WPL**, TL6.1	X
UMU	X	X	**WPL**, TL3.2	TL4.1	X	X	X
UMA	X	X	X	**WPL**, TL4.2	TL5.1	X	X
TRT	X	TL2.2			**WPL**, TL5.2	TL6.4	X
PTIN	X	**WPL**, TL2.1	TL3.1			X	TL7.3
MOV	X		X	TL4.3		TL6.3	**WPL**, TL7.1

X: Contributor; **WPL**: Work Package Leader; **TL**: Task Leader

2.4 Resources to be committed

A detailed budget and funding breakdown per partner is given in Table 20. The overall cost over the 36 months of the **SPHERICS** project will be 4.466.018 M€ with a requested EC contribution of 2.919.209 M€. The **SPHERICS** partners are convinced that the budget will suffice to successfully run the project as proposed. It has been ensured that by far the most person-power is attributed to the RTD activities. The project management costs account for only 6% of the total budget. Each partner in the project is responsible for a certain well-defined part of the project work. While the budget of each participant relates to its role and workload, it has been assured that all partners provide substantial resources in order to be able to work efficiently within the project.

Table 20: Detailed budget breakdown per partner and activity (EUR)

RTD / Innovation	FhG	NEC	UMU	UMA	TRT	PTIN	MOV	TOTALS
Direct personnel costs	9,250	6,678	4,100	4,000	9,072	4,788	10,764	
Indirect personnel costs	0	3,780	2,460	2,400	8,145	3,420	2,153	
Direct personnel costs	666,000	514,206	303,400	288,000	371,952	229,824	333,684	2,707,066
Travel expenses	43,000	29,260	25,000	40,000	20,000	25,000	18,000	200,260
Equipment costs	10,000	0	0	0	10,000	0	0	20,000
Consumables costs	1,000	0	2,000	0	0	0	0	3,000
Other specific costs	15,000	0	1,000	0	0	0	0	16,000
Subcontracting	0	0	0	0	0	0	0	0
Total direct costs	**735,000**	**543,466**	**331,400**	**328,000**	**401,952**	**254,824**	**351,684**	**2,946,326**
Total indirect costs	**0**	**291,060**	**198,840**	**196,800**	**333,927**	**164,160**	**66,737**	**1,251,524**
TOTAL Costs	**735,000**	**834,526**	**530,240**	**524,800**	**735,879**	**418,984**	**418,421**	**4,197,850**
Distribution per partners	17.5%	19.9%	12.6%	12.5%	17.5%	10.0%	10.0%	
RTD Funding rate	75%	50%	75%	75%	50%	50%	75%	
TOTAL EC Contribution	**551,250**	**417,263**	**397,680**	**393,600**	**367,940**	**209,492**	**313,816**	**2,651,041**
Distribution per partners	20.8%	15.7%	15.0%	14.8%	13.9%	7.9%	11.8%	

Project Management	FhG	NEC	UMU	UMA	TRT	PTIN	MOV	TOTALS
Direct personnel costs	9,500	6,678	4,100	4,000	9,072	4,788	10,764	
Indirect personnel costs	0	3,780	2,460	2,400	8,145	3,420	2,153	
Direct personnel costs	114,000	46,746	4,100	4,000	9,072	4,788	10,764	193,470
Travel expenses	5,000	2,660	0	0	0	0	0	7,660
Other costs	0	0	4,000	0	0	0	0	4,000
Subcontracting	5,000	6,000	0	4,000	3,000	0	0	18,000
Total direct costs	**124,000**	**55,406**	**8,100**	**8,000**	**12,072**	**4,788**	**10,764**	**223,130**
Total indirect costs	**0**	**26,460**	**2,460**	**2,400**	**8,145**	**3,420**	**2,153**	**45,038**
TOTAL Costs	**124,000**	**81,866**	**10,560**	**10,400**	**20,217**	**8,208**	**12,917**	**268,168**
Distribution per partners	46.2%	30.5%	3.9%	3.9%	7.5%	3.1%	4.8%	
RTD Funding rate	100%	100%	100%	100%	100%	100%	100%	
TOTAL EC Contribution	**124,000**	**81,866**	**10,560**	**10,400**	**20,217**	**8,208**	**12,917**	**268,168**
Distribution per partners	46.2%	30.5%	3.9%	3.9%	7.5%	3.1%	4.8%	

Total Budget	FhG	NEC	UMU	UMA	TRT	PTIN	MOV	TOTALS
TOTAL COSTS	**859,000**	**916,392**	**540,800**	**535,200**	**756,096**	**427,192**	**431,338**	**4,466,018**
Distribution per partners	19.2%	20.5%	12.1%	12.0%	16.9%	9.6%	9.7%	
TOTAL EC Contribution	**675,250**	**499,129**	**408,240**	**404,000**	**388,157**	**217,700**	**326,733**	**2,919,209**
Distribution per partners	23.1%	17.1%	14.0%	13.8%	13.3%	7.5%	11.2%	

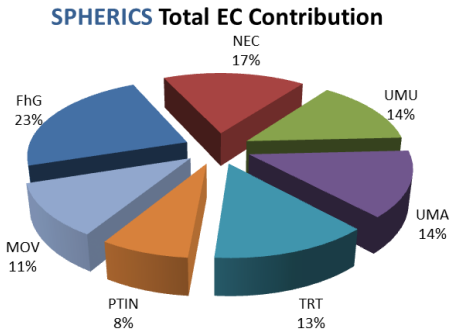

Figure 12: Total EC contribution per partner

Section 3: Impact

3.1 Expected impacts listed in the work programme

The three main technological pillars of **SPHERICS** are identity management to provide end-users with a tighter control of their personal and sensitive data in the Internet (WP3), trust and reputation management to help end-users selecting the most trustworthy services at each moment (WP4), and secure data storage and processing to enhance the security of the users' sensitive data handled in the Internet (WP5). Additionally, the three considered validating scenarios for the security personal assistant, namely Cloud Computing, Social Networks and e-Government, constitute an elegant benchmark covering some of the current hottest environments in the field of ICT (WP6). All together they address a comprehensive field of topics in line with the concept and objectives of **SPHERICS**, which in turn are aligned with the target outcomes of Objective ICT-2011.1.4 of the FP7-ICT Work Programme 2011-2012 (*Trustworthy ICT*) as listed in Table 21, and the expected impact, as shown in Table 22.

3.1.1 Target outcomes of Objective ICT-2011.1.4

Table 21: Target outcomes of Objective ICT-2011.1.4

Target Outcomes of Objective ICT-2011.1.4	Contributions by SPHERICS	Measures of success
a) Heterogeneous networked, service and computing environments: *"Enabling technologies, such as declarative languages, biometry, technology for certification and accreditation or cryptography for Trustworthy ICT"*	**From objectives 1 and 4:** In **SPHERICS**, secure data storage and processing by means of advanced cryptography techniques will be a key research area. These technologies will be available in the secure facilitator, thus helping users to take control of the security of their data in the three different scenarios considered as part of the project. This is a key aspect for users (European users and SMEs, for example) and it will make them less reluctant to use and interact with Internet-scale services and applications as their data will be protected while stored in the service providers.	The design and development of secure data storage and processing mechanisms to be later integrated as part of the user-centric security facilitator. In this sense, **SPHERICS** will be having, among others, the added value of designing and developing these mechanisms in order to protect the security and privacy of end users when their data is outsourced to service providers that can be partially trusted or untrusted. In certain scenarios, such as cloud computing, several different providers may appear as of interest for the users, although their trustworthiness may not be clear for the user.
b) Trust, eIdentity and Privacy	**From objectives 1 and 3:**	The design and development of advanced trust and reputation

management infrastructures. *"Development of trust architectures, protocols and models for trust assurance, including measures and rating models, and services and devices to enable trust assessment"*	The **SPHERICS** middleware facilitator aims to provide advanced trust and reputation management mechanisms to inform users and assist them in making smarter decisions on which service provider to interact with. Such selection would be based on the reputation of the service provider from the perspective of the service consumer. Thus, end users will be interacting with reputation mechanisms helping other users to take a better decision in the Internet service selection process in the future.	management mechanisms to be later integrated as part of the user-centric security facilitator. Such mechanisms will be also seamlessly integrated with the identity management solution and the secure data storage and processing mechanisms to be designed and developed as part of the project, thus providing also the added value of integrating three powerful protection mechanisms and making them available to end users in order to protect their personal data and information.
b) Trust, eIdentity and Privacy management infrastructures. *"Protocols for privacy infrastructures enabling multi-identity and tools to check privacy assurance and enable un-observability and un-linkability through search engines or social networks"*	**From objectives 1 and 2:** This project will focus on investigating advanced user-centric IdM techniques to foster Single Sign-On solutions while providing users with the ability to securely control and monitor the usage of their personal profiles and data in the Internet as part of a personal security facilitator. Moreover, this project will be providing a comprehensive solution for end-users as they will be able to manage the whole life-cycle of their identities, at the same time that the user will be also able to define the policies driving the use of the personal data.	The design and development of advanced user-centric identity management mechanisms to be later integrated as part of the user-centric security facilitator. This component will be having important added-values as being user-centric in their definition and design, considering for that purpose a wide range of aspects such as the seamless interaction with different technologies or its visual and easy-to-use aspect. This component will be also able to provide the end-users with the possibility to monitor how, where, when and by which service provider their private information has been used.
	From objective 5: This project will be considering three main scenarios to gather the requirements and validate the results. One of them will be social networks, which are currently having a big impact on end users and companies. For this particular	The development of a scenario integrating the user-centric security facilitator as part of some of the currently existing social networks. In fact, social networks are representing nowadays a big business as people and companies are uploading and sharing a lot of information (some of it of private

	scenario, real social network providers will be considered, so end users will be experiencing a more secure and privacy-aware way of accessing to this kind of services and interacting with them.	nature). Giving end users an easier and improved ways to interact in terms of security and privacy with these social networking platforms is an objective of this project.
b) Trust, eIdentity and Privacy management infrastructures. *"Interoperable or federated management of identity claims integrating flexible user-centric privacy, accountability, non-repudiation, traceability as well as the right to oblivion at the design level. Technologies and standardisation for use of multiple authentication devices, applicable to a diversity of services and ecosystems, and providing auditing, reporting and access control."*	**From objectives 1 and 2:** This project will focus on investigating advanced user-centric IdM techniques to foster Single Sign-On solutions while providing users with the ability to securely control and monitor the usage of their personal profiles and data in the Internet as part of a security facilitator. The integration of these two technologies, together with trust and reputation, is providing the end user with a set of powerful elements that will be seamlessly integrating and managing their identities while providing a privacy-aware and secure solution to the access of information in service providers.	The design and development of advanced user-centric identity management mechanisms to be later integrated as part of the user-centric security facilitator to be defined and implemented in this project. As indicated before, this component will be providing the end users with the possibility to manage the whole life cycle of their identities. Moreover, they will be able to monitor which particular service or identity provider has been accessing their information and when it has been done, thus establishing a central point where to observe the access to their personal data.
	From objective 6: To promote the successful acceptance and deployment of our solutions, the project will disseminate the developed and successfully validated technologies through standardization activities. To this end, the project will be considering the work that some partners are already performing in relevant standardisation bodies, while some others are interested to start new collaborations, so the project results can be evaluated and proposed as part of future standards.	The involvement of project partners in different standardization bodies with the intention of promoting the project results regarding the three main pillars of the project, i.e., identity management, trust and reputation management, and secure data storage and processing. The standardization bodies being considered in **SPHERICS** are: ETSI Industry Specification Group INS (Identity and Access Management for Networks and Services), OASIS Identity in the Cloud TC, or the Kantara User-Managed Access (UMA) Working Group, among others.

3.1.2 Expected impact of Objective ICT-2011.1.4

Table 22: Expected impact of Objective ICT-2011.1.4

Expected Impact of Objective ICT-2011.1.4	Contributions by SPHERICS
1) "Improved European industrial competitiveness in markets of trustworthy ICT, by: facilitating economic conditions for wide take-up of results; offering clear business opportunities and consumer choice in usable innovative technologies; and increased awareness of the potential and relevance of trustworthy ICT."	**From objectives 5 and 6:** The results of the project will be validated in three scenarios that are close to end users: social networks, cloud computing and e-government. Moreover, the validation of these three scenarios will be based on real service providers existing nowadays, so that European companies making use of the **SPHERICS** facilitator will have a security solution really close to the market. This solution directly targets the final users and it aims to bridge the gap between these users and the service providers in terms of security and privacy. Therefore, it will help to increase the use of certain services that users consider risky in terms of security, privacy, confidentiality and/or accountability. As indicated by Eve Maler, founder and chair of the User-Managed Access Work Group at the Kantara Initiative, after reading an extended abstract of the **SPHERICS** proposal: "*Individuals and small business owners seeking to aggregate and use a variety of cloud-based services want to ensure that they can treat the collection of services in a holistic, secure, compliant, trustable, and privacy-sensitive fashion. Today, they must connect services and share information between them in a point-to-point fashion. They would benefit from having a central coordination hub that ensures a 360-degree view of their data, their service usage, and the quality of their external aggregation partners*".
2) "Adequate support to users to make informed decisions on the trustworthiness of ICT. Increased confidence in the use of ICT by EU citizens and businesses. Increased usability and societal acceptance of ICT through understanding of legal and societal consequences."	**From objectives 1, 2, 3, 4:** The main objective of **SPHERICS** is to design and develop a simple, friendly user-centric security assistant to help service consumers in the most common interactions with different providers offering similar services. This help will be based on the integrated management of the different user identities, the provision to the user of the trust and reputation information of different services providers and the interaction with them by using secure storage and processing mechanisms. As indicated by Gunnar Nilsson, head of Investor Forum

	Norway, after reading an extended abstract of the **SPHERICS** proposal: "*Sharing of information between collaborating companies has proven to be a real success. Building a personal security assistant will pave the way to trust in global infrastructures, and thus promote our ideas of innovation through entrepreneurs*".
3) "Demonstrable improvement (i) of the trustworthiness of increasingly large scale heterogeneous networks and systems and (ii) in protecting against and handling of network threats and attacks and the reduction of security incidents."	**From objectives 1, 2, 3, 4:** This project is intended to provide a simple and friendly user-centric security assistant with the main purpose of improving the security perception of end users when selecting between different service providers. This will be achieved by using trust and reputation information to do such selection; interacting with these service providers and storing their data securely; and moving their data from one of these service providers to another, managing all their digital identities seamlessly. Finally, end users are also able to monitor which service provider has access to which particular data and take actions based on that. As indicated by Leif T. Aanensen, Deputy director general at The Data Inspectorate of Norway, after reading an extended abstract of the **SPHERICS** proposal: "*The approach of building a user-centric security and privacy assistant is very much appreciated. From our experiences with Internet providers, Facebook and Apple we know how hard it is to get privacy information revealed once it has been published*".
4) "Significant contribution to the development of trustworthy European infrastructures and frameworks for network services; improved interoperability and support to standardisation. Demonstrable usability and societal acceptance of proposed handling of information and privacy."	**From objectives 1 and 6:** Usability is one the key factors in the design of the security assistant and the enablers to be developed as part of **SPHERICS**. This helps to increase the adoption of different security mechanisms that are directly integrated in the facilitator, as they are in most cases transparent to the end users. The assistant will be based on different interfaces and security mechanisms, which are the basis for extensibility and interoperability of the proposed solution. These interfaces and security mechanisms also represent a key result of the project, thus being the main target for the dissemination and standardization tasks to be accomplished. Partners are already working (and some others will be)

	regarding the topics proposed in this project with major standardization bodies, including ITU-T, ETSI, W3C, OASIS, IETF or the Kantara initiative, among others. As indicated by Eve Maler, founder and chair of the User-Managed Access Work Group at the Kantara Initiative, after reading an extended abstract of the **SPHERICS** proposal: "*As founder and chair of the User-Managed Access Work Group at the Kantara Initiative and a specialist in emerging identity and privacy technologies, I am interested to learn the progress of the **SPHERICS** effort*".
5) Improved coordination and integration of research activities in Europe or internationally.	**From objective 6:** As part of the standardization and dissemination activities, project partners will be taking part in a number of forums to motivate the wider acceptance of the different enablers, mechanisms and interfaces proposed as part of **SPHERICS**. Project partners are also having a clear plan for the dissemination of the results in major conferences and journals. Moreover, particular workshops will be organised in major conferences worldwide and special issues will be also led by project partners in major journals and magazines.

Distributing the abstract of our proposal to relevant companies, authorities and business angles resulted in the support statements listed in this chapter. We see these statements as the first pre-dissemination, and we intend to use the support from the authors to invite key organisations for building the **SPHERICS** ecosystem. We believe that such an ecosystem will provide our solutions with visibility in the market, support from authorities and, last but not least, competent capital from business angles to exploit the **SPHERICS** results.

3.2 Dissemination and/or exploitation of project results, and management of intellectual property

WP7 "Dissemination, Standardization and Exploitation" will support the dissemination of **SPHERICS** results. As presented previously, the main tasks that will be carried in order to promote the methodology and research in this project are:

- Definition of the communication and dissemination plan.
- Initiate the process of standardization of the results (**SPHERICS** assistant) and register the intellectual property.
- Define the plan of exploitation of the results to maintain the **SPHERICS** sustainability.
- Promote dissemination activities, organizing workshops and press releases.

A detailed plan will be written for each one of the tasks with short and medium term actions to take. The dissemination, standardisation and exploitation tasks will be conducted during the entire project calendar. It is a continual work.

3.2.1 Dissemination

The aim of the dissemination tasks is above all, "to spread the word" and create an ecosystem for successful market uptake. Each one of the partners involved will carry out specific dissemination tasks. The scientific partners will disseminate the outcomes obtained from the project by means of publications in high-quality international conferences and journals. They will also drive the website for the activities related to the project. The industrial partners will focus more on targeted and dedicated workshops. A specific activity is towards creating business ecosystems, which will create accelerated innovation for the expected outcomes of **SPHERICS**.

Initiatives will be carried out in order to announce the project aims, motivation, results and challenges. The starting point of these tasks is the consortium participants, but a larger target population will be selected to contribute to the widespread of the results.

To promote the project some workshops will be organised to inform about how the objectives are being accomplished and one last workshop to disclose the results of the project and future challenges. All the activities carried out in this task will follow the built plan for dissemination.

To complete this task, all the other means to spread the information will be synchronised with that plan. The following dissemination activities will be taken:

- Conferences: Talks and presentations will be held at industrial and academic conferences and trade shows. Papers and scientific publications will be presented at these conferences.
- Publications: Technical and scientific articles will be published in magazines and academic journals. University partners will focus on the scientific publications and papers to be presented at academic conferences and in academic journals whereas the industrial partners will focus primarily on trade shows, commercial conferences and commercial and customer oriented literature.
- Promotion: Dissemination channels will include press releases, university lectures and a public web site.
- Teaching: The academic partners within the project will integrate the main issues of the project in their teaching and will offer special courses related to the outcomes of **SPHERICS**.

- Business dissemination: Evaluation of the socio-economic impact related to the project and the exploitation of the project results. To reach the target audiences (SMEs and Society) methods based on modern marketing, advertising strategies, mass-media, conferences, workshops will be defined and planned, a business case for the process will be developed and companies who could use the process will be targeted.

Public Dissemination

A public website will be built and maintained to provide information on the project activities. The website will be based on "open data[3] principles", allowing for living content with continuously updated with public documents and deliverables, publications and presentations. In addition, to promote the project at conferences, cluster meetings and concertation events, brochures and posters will be developed. Moreover the website will contain the **SPHERICS** calendar, project development stage and results.

Industrial partners will focus on dissemination in their business networks, both through sector specific workshops and through targeted dissemination as described earlier. A specific effort is given to business networks and trade shows, which are concerned with the target solutions.

Journal and Conference Publications

The results of the project will be exposed to the scientific community on relevant aspects. It will be a priority to target publications of high quality project results in International peer reviewed journals, magazines and book chapters. Project partners will proceed with the submission and publication of technological concepts and results achieved by the work to be carried on in selected internationally acknowledged journals and magazines as well as special issues related to identity management, privacy and trust research areas.

Relevant target conferences:

- IEEE ICC Communication and Information Systems Security (ICC-CISS) Symposium
- IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)
- International Conference on Applied Cryptography and Network Security (ACNS)
- International Conference on Network Security & Applications (CNSA)
- International Conference on New Technologies, Mobility and Security (NTMS)
- International ICST Conference on Security and Privacy in Mobile Information and Communication Systems (MobiSec)
- European Symposium on Research in Computer Security (ESORICS)
- International Conference on Trust, Privacy and security in Digital Business (TrustBus)

Relevant journals and magazines:

- Communications Magazine, IEEE
- Computers & Security, Elsevier
- Information Security, IET
- International Journal of Communication Systems, Wiley
- International Journal of Information Security, Springer
- Journal of Network and Systems Management, Springer

[3] Open data such as .rdf and tripplestores or Odata allow for exchange of information

- Security and Communication Networks, Wiley
- Security & Privacy, IEEE
- Transactions on Emerging Telecommunications Technologies, Wiley
- Transactions on Information and System Security, ACM

Due to the high impact of the possible results expected from the project, several PhD and MS students will be enrolled and it will be expected that the project research results will contribute them to obtain the PhD or Masters.

3.2.2 Standardisation

Dissemination towards standards will be one of the project objectives. Some partners are already involved in relevant standardisation bodies. Guidance and direction on this activity will be co-ordinated in WP7, in which a standardisation matrix will be developed at the start of the project and will be present in D7.3. Some of the proposed points where this project could engage standardisation activities are the following:

ETSI

Based in Sophia Antipolis (France), the European Telecommunications Standards Institute (ETSI) is officially responsible for standardisation of Information and Communication Technologies (ICT) within Europe.

A major focus will be on the ETSI Industry Specification Group INS (Identity and Access Management for Networks and Services) to advance standardisation in areas surrounding Identity Management, privacy and trust. Several partners are already involved in the group work.

ITU-T, SG17

Within ITU-T, Study Group 17 coordinates security-related work across all study groups. Cybersecurity remains high on SG 17's agenda and much work is being conducted on the exchange of cybersecurity information (CYBEX). Additionally, SG 17 is coordinating standardisation work covering e-health, cloud computing and SmartGrid security, open identity trust framework, Near Field Communication (NFC) security, and Child Online Protection. Here, **SPHERICS**' achievements and in particular the personal information assistant could be of specific interest.

OASIS

OASIS (Organization for the Advancement of Structured Information Standards) is a non-profit consortium that drives the definition and adoption of standards for the information society in several areas.

OASIS is having several technical committees where the results from **SPHERICS** can be considered. Of particular interest are those related with standards enabling the definition of identity management solutions, being the Identity in the Cloud TC one of the most suitable places where the results of this project can be considered.

Kantara Initiative

Kantara Initiative is a non-profit professional association focused on the advance of technical, legal and usability aspects of digital identity management. Some of the original founders of Kantara are the Liberty Alliance, the DataPortability Project, the Concordia Project, the Internet Society, the Information Card Foundation, OpenLiberty.org and XDI.org.

The Kantara User-Managed Access (UMA) Working Group is in charge of the design of the UMA protocol, which is intended to give a web user a unified control point for authorizing who and what can get access to their online personal data and services. Within the Kantara Initiative, the User-Managed Access Working Group conducts various liaison activities with other Kantara groups, such as the Privacy and Public Policy Work Group (P3WG), and also non-Kantara groups, such as the OAuth group in the IETF.

Fraunhofer AISEC has been a voting member of Kantara UMA since 2009. This will be of mutual benefit to SPHERICS. On the one hand **SPHERICS** could take advantage and consider the UMA protocol as one candidate for integration into the personal information assistant. On the other hand one of the goals of the Kantara UMA Working Group is to contribute the specifications of the UMA protocol to the IETF. Thus, any contribution from **SPHERICS** to the UMA protocol will form part of this standardisation proposal.

IETF

The Internet Engineering Task Force (IETF) develops and promotes Internet standards, cooperating closely with the W3C and ISO/IEC standards bodies and dealing in particular with standards of the TCP/IP and Internet protocol suite. It is an open standards organization, with no formal membership or membership requirements. Developments of **SPHERICS** could be introduced to Web Security working group in Applications Area and especially the OAuth working group of the Security Area.

W3C

The World Wide Web Consortium (W3C) is the main international standards organization for the World Wide Web. One of the most relevant standards for **SPHERICS** is P3P.

The Platform for Privacy Preferences Project, or P3P, is a protocol allowing websites to declare their intended use of information they collect about browsing users. P3P allows browsers to understand their privacy policies in a simplified and organized manner rather than searching throughout the entire website. By setting your own privacy settings on a certain level, P3P will automatically block any cookies that you might not want on your computer. Additionally, the W3C explains that P3P will allow browsers to transfer user data to services, ultimately promoting an online sharing community.

CSA

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders. Especially **SPHERICS**' cloud use cases will benefit from CSA "Security Guidelines" and "SecaaS Defined Categories of Service 2011". As a member of the German chapter particularly Fraunhofer AISEC can promote **SPHERICS** in the CSA.

3.2.3 Exploitation

In **SPHERICS**, the exploitation plan is very important to maintain the sustainability of the project. Many actions will be taken during the project to increase the exploitation potential.

The project offers partners and results adopters several routes for exploitation:

- Industrial exploitation

- Academic exploitation
- SME exploitation
- Business network exploitation

Each partner will be directly involved in the exploitation tasks. The individual exploitation plans will form the basis for a detailed analysis of the project's exploitation potential. The project exploitation task will co-ordinate all the project exploitation activities, and monitor and support the exploitation carried out by individual partners. The aim of the exploitation plan is to develop and support new products and services to the market through a close collaboration with industries. **SPHERICS** introduces a novel approach to make that happen, where the results of the "R&D and prototype integration" are taken into a dedicated workshop with selected business angles in order to focus on innovation and products. Bringing external experts into the picture will promote the "impact-based" approach of **SPHERICS**. Based on these business workshops the exploitation plans of each partner will be discussed an analysed through the standardized Scorecard process of Movation, providing indications for business, branding, team, partnering and technology, amongst others.

The exploitation strategy will thus be able to identify the exploitable results, their potential use and target users/companies. The exploitation will include a market analysis to help partners to determine the market opportunities for **SPHERICS**. The detailed analysis will include:

- Target market segment for **SPHERICS** results.
- Positioning of our products in to the market and relative position to its competitors.
- Competitive analysis providing detailed information about the implementation of SPHERICS results under real conditions. Maintain a market surveillance during all the project development.
- The exploitation plans from each partner will establish guidelines to commercial deployment of our products.

The envisaged **SPHERICS** results will address different market areas from cloud services providers to governmental entities. An earlier contact will be established to relevant actors in the area in order to be able to establish and ecosystem for **SPHERICS**. This might open for some real situations in the development of the security assistant testing it under real conditions.

Industrial exploitation plans

NEC focuses on solutions that meet the needs of NEC's European customers and is able to innovate its European products thanks to the R&D carried out at NEC Laboratories Europe. With the profile of a large multinational company the exploitation opportunities of NEC lie in the following areas:

- NEC's trustworthy ICT solution portfolio enhancement by performing several technology transfers to NEC Business Unit thanks to the concept of collaborative innovation in an European environment;
    - Core functionalities of the **SPHERICS** integrated identity management can improve NEC's identity and access management solutions, such as SECUREMASTER and the NC7000 series.
    - NEC aims to create and provide cloud solutions and services for Carrier, Enterprises and Social Infrastructures. **SPHERICS** is the right environment to create trustworthy cloud services and solutions that can be used to improve the user's acceptance of NEC's cloud technology.
    - The **SPHERICS** assistant can also improve NEC's mobile terminals, such as tablets and smart phones, to give the end user more control and privacy for his data and identities.

- Collaboration with top operators in the European market (PT) to trial innovative solutions and services in the area of Trustworthy ICT;
- Increase patent portfolio in the area of trustworthy ICT thanks to ideas derived from project investigations; enhance interoperability of its solutions by influencing international standards related to the development of new commercial solutions in the area of trustworthy ICT;
- Maintain the high level of scientific excellence of NEC's European R&D that was achieved over the past years through high-level publications and memberships at top conferences.

Portugal Telecom Inovação, SA – PTIN's role, as the R&D branch of the PT Group, is not only to support the group's Mobile and Fixed Operations in the search of innovative solutions and services, but also to provide training to PT technical staff. **SPHERICS** will provide PTIN the opportunity to exchange knowledge with other partners searching for innovative solutions in the area, which will be integrated into existing PTIN products/services and/or will promote the creation of new ones. Being, the PT Group, a global network operator, running several types of networks and providing a multitude of services, in different geographical regions of the world, the areas addressed in **SPHERICS**, in regards to identities management, privacy and trust, and on how these can be leveraged to support new services and business are of great importance for PTIN.

Thales Research & Technology (UK) Ltd is a provider of innovation and technology to the rest of the Thales group of companies. It is a centre of excellence for a variety of advanced technologies, which it develops for the use of the businesses and operating companies of the Group. The TRT exploitation strategy can be split into three main tracks:

- Continue to develop the **SPHERICS** security concepts through internally funded projects and in collaboration with other companies in the Thales Group.
- Promote the use of the **SPHERICS** components and technologies developed by TRT within the current product ranges of the companies in the Thales Group.
- Promote the use of the **SPHERICS** concepts and technologies to open up new areas of business for the companies in the Thales Group.

Academic exploitation plans

Universidad de Murcia will be doing an emphasis on the publication of project results in international conferences, journals and magazines. Moreover, the participation in this project will allow certain students to get involved in different Master Thesis and PhD doctorates directly related with the topics being addressed and researched as part of the project and supervised by the members of the team taking part in **SPHERICS**. Moreover, given the expertise of the UMU team, some Special Issues in international journals and particular workshops/symposiums in international conferences will be organised, thus helping the promotion of the knowledge being generated as part of the project and receiving new ideas from the research community.

As an academic institution, **Universidad de Málaga** exploitation plan is mainly related to **SPHERICS** as a vehicle to strengthen NICS Lab by the collaboration with other universities and private companies. At the same time, **SPHERICS** will contribute to increase the personnel of NICS Lab and, therefore strengthen it in order to establish further research projects while improving their quality. International publication is an important part of UMA research, and **SPHERICS** will be used as a vehicle for publication. Therefore, **SPHERICS** will exploit IPR through the normal routes of Academic Dissemination in journal articles, book chapters and conference presentations, and through using the technology developed and know-how

obtained as background for future research projects. Moreover, **SPHERICS** will also originate different PhD and/or MSc theses that will contribute to consolidate university research positions.

SME exploitation plan

Movation, being an SME itself, has analysed more than 150 SMEs through the last five years. While the initial request is "capital", the successful cases have shown that "competent capital" is more important. Finding the right expertise for the steering board, a network of partners to implement the prototype and a business ecosystem to develop the solution are essential for the success of a product. Movation currently has 15-20 ICT related companies on the stock exchange, some of them being market leader in their segment. The "implicit trust" in the Nordics has helped to establish the innovation ecosystem, but has limitations when it comes to the international market. Here is where the results of **SPHERICS** come into the game. Trust and reputation measures, applied for cloud services and social networks will help to create a trust network, such that entrepreneurs are "more safe" to find others helping him in exploiting the innovative ideas.

The **SPHERICS** results are essential for Movation as the provider of the Innovation Stock Exchange (InnoBors.eu), but also for the majority of SMEs promoting their ideas and developing innovative solutions.

Section 4: Ethical Issues

Ethical Issues		
	YES	**PAGE**
Informed Consent		
• Does the proposal involve children?		
• Does the proposal involve patients or persons not able to give consent?		
• Does the proposal involve adult healthy volunteers?		
• Does the proposal involve Human Genetic Material?		
• Does the proposal involve Human biological samples?		
• Does the proposal involve Human data collection?		
Research on Human embryo/foetus		
• Does the proposal involve Human Embryos?		
• Does the proposal involve Human Foetal Tissue / Cells?		
• Does the proposal involve Human Embryonic Stem Cells?		
Privacy		
• Does the proposal involve processing of genetic information or personal data (eg. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)		
• Does the proposal involve tracking the location or observation of people?		
Research on Animals		
• Does the proposal involve research on animals?		
• Are those animals transgenic small laboratory animals?		
• Are those animals transgenic farm animals?		
• Are those animals cloned farm animals?		
• Are those animals non-human primates?		
Research Involving Developing Countries		
• Use of local resources (genetic, animal, plant etc)		
• Benefit to local community (capacity building i.e. access to healthcare, education etc)		
Dual Use		
• Research having direct military application		
• Research having the potential for terrorist abuse		
ICT Implants		
• Does the proposal involve clinical trials of ICT implants?		
I CONFIRM THAT NONE OF THE ABOVE ISSUES APPLY TO MY PROPOSAL	**X**	

Annex: References

[1] E. Maler and D. Reed, "The venn of identity: Options and issues in federated identity management," *IEEE Security & Privacy*, pp. 16–23, 2008.

[2] Patricia Arias Cabarcos, Florina Almenárez Mendoza, Andres Marín Lopez and Daniel Díaz Sanchez. "Enabling SAML for Dynamic Identity Federation Management", *Wireless and Mobile Networking Conference*. Gdansk, Poland, 2009

[3] OASIS, Security Services (SAML) TC, 2012, http://www.oasis-open.org/committees/security/

[4] OASIS, eXtensible Access Control Markup Language (XACML) TC, 2012, http://www.oasis-open.org/committees/xacml/

[5] OASIS, Provisioning Services TC, 2012, http://www.oasis-open.org/committees/provision/

[6] R. Buyya, R. Ranjan and R. Calheiros, "Intercloud: Utility-oriented federation of cloud computing environments for scaling of application services" in *Algorithms and Architectures for Parallel Processing*, pp. 13-31, 2010

[7] H. Krasnova, O. Günther, S. Spiekermann and K. Koroleva, "Privacy concerns and identity in online social networks", in *Identity in the Information Society*, vol 2, pp. 39-63, 2009

[8] M. Pirretti, P. Traynor, P. McDaniel and B. Waters, "Secure attribute-based systems", in *Journal of Computer Security*, vol. 18, pp.799-837, 2010

[9] A. Jøsang and R. Ismail. "The Beta Reputation System", in *15th Bled Electronic Commerce Conference e-Reality: Constructing the e-Economy*, Bled, Slovenia, June 2002.

[10] I. Agudo, C. Fernandez-Gago, and J. Lopez, "A Model for Trust Metrics Analysis", in *5th International Conference on Trust, Privacy and Security in Digital Business (TrustBus'08)*, LNCS 5185, pp. 28-37, 2008.

[11] Félix Gómez Mármol, Gregorio Martínez Pérez, "Towards Pre-Standardization of Trust and Reputation Models for Distributed and Heterogeneous Systems", *Computer Standards & Interfaces, Special Issue on Information and Communications Security, Privacy and Trust: Standards and Regulations*, vol. 32, no. 4, pp. 185-196, 2010

[12] Félix Gómez Mármol, Gregorio Martínez Pérez, "Security Threats Scenarios in Trust and Reputation Models for Distributed Systems", *Elsevier Computers & Security*, vol. 28, no. 7, pp. 545-556, 2009

[13] Almenárez, F., Arias, P., Marín, A. and Díaz, D., "Towards dynamic trust establishment for identity federation", In *Proceedings of the 2009 Euro American Conference on Telematics and Information Systems* (Prague, Czech Republic, June 03 - 05, 2009). EATIS '09

[14] L. Kagal, T. Finin and A. Joshi, "Trust-based security in pervasive computing environments", in *Computer*, vol 34, pp. 154-157, 2001.

[15] Y. Lu, W. Wang, B. Bhargava and D.Xu, "Trust-based privacy preservation for peer-to-peer data sharing", in *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans,* vol 36, pp. 498-502, 2006.

[16] Félix Gómez Mármol, Joao Girao, Gregorio Martínez Pérez, "TRIMS, a Privacy-aware Trust and Reputation Model for Identity Management Systems", *Computer Networks, Special Issue on Managing Emerging Computing Environments*, vol. 54, no. 16, pp. 2899-2912, 2010

[17] Spideroak, https://spideroak.com/

[18] Goldkey, http://www.goldkey.com/

[19] R. Curtmola et al, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions", in *Proceedings of the 13th ACM conference on Computer and Communications Security*, Alexandria, Virginia, USA, pp. 79 – 88, 2006.

[20] R. Ostrovsky et al, "Survey of Single-database Private Information Retrieval: Techniques and Applications", in *Proceedings of the 10th International Conference on Practice and Theory in Public-key Cryptography*, *Lecture Notes In Computer Science* 4450, pp. 393-411, 2007.

[21] C. Fontaine et al, "A Survey of Homomorphic Encryption for Nonspecialists", in *EURASIP Journal on Information Security*, vol 2007, January 2007.

[22] A. Shamir, "How to share a secret", in *Communications of the ACM* 22, 11, pp. 612-613, November 1979.

[23] M. Naehrig, K. Lauter, and Vinod Vaikuntanathan, "Can homomorphic encryption be practical?", in Proceedings of the 3rd ACM workshop on Cloud computing security workshop (CCSW '11). ACM, 2011.

[24] A. C. Yao, "Protocols for Secure Computations", in *Proceedings of 23rd Annual Symposium on Foundations of Computer Science*, pp.160-164, 3-5 Nov. 1982.

[25] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness theorems for non-cryptographic fault-tolerant distributed computation", in Proceedings of the twentieth annual ACM symposium on Theory of computing (STOC '88), 1988.

[26] C. Gentry, "Fully homomorphic encryption using ideal lattices", in Proceedings of the 41st annual ACM symposium on Theory of computing (STOC '09), ACM, 2009.

[27] C. Gentry and S. Halevi, "Implementing Gentry's fully-homomorphic encryption scheme", in Proceedings of the 30th Annual international conference on Theory and applications of cryptographic techniques: advances in cryptology (EUROCRYPT'11), 2011.

[28] VIFF, the Virtual Ideal Functionality Framework, http://viff.dk/

[29] P. Bogetoft, I. Damgård, T. Jakobsen, K. Nielsen, J. Pagter, and T. Toft, "A practical implementation of secure auctions based on multiparty integer computation", in *Proceedings of Financial Cryptography '06*, vol 4107 of LNCS, pp. 142-147, Springer, 2006.

[30] W. Henecka, S. Kögl, A.-R. Sadeghi, T. Schneider and I. Wehrenberg, "TASTY: Tool for Automating Secure Two-party Computations", in *Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS '10)*, pp. 451-462. ACM, New York, USA, 2010.

[31] SEPIA, http://www.sepia.ee.ethz.ch

[32] D. Bogdanov, S. Laur, and J. Willemson, "Sharemind: A Framework for Fast Privacy-Preserving Computations", in *ESORICS*, pp. 192-206, 2008.

[33] EU Project PERIMETER, http://www.ict-perimeter.eu/

[34] EU Project TAS3 (Trusted Architecture for Securely Shared Services), http://www.tas3.eu/

[35] EU Project TCLOUDS, http://www.tclouds-project.eu/

[36] EU Project SWIFT (Secure Widespread Identities for Federated Telecommunications), http://www.ist-swift.org/

[37] EU Project PICOS (Privacy and Identity Management for Community Services), http://www.picos-project.eu/

[38] EU Project STORK (Secure Identity Across Borders Linked), https://www.eid-stork.eu/

[39] EU Project SEMIRAMIS (Secure Management of Information across Multiple Stakeholders), http://www.semiramis-cip.eu/

[40] EU Project PrimeLife, http://www.primelife.eu/

[41] EU Project DEMONS (Decentralized, Cooperative, and Privacy-Preserving Monitoring For Trustworthiness), http://fp7-demons.eu/

[42] EU Project CACE (Computer Aided Cryptography Engineering), http://www.cace-project.eu/

[43] EU Project SecureSCM, http://www.securescm.org/

[44] Microsoft CardSpace, http://msdn.microsoft.com/en-us/library/aa480189.aspx

[45] Kantara's User Managed Access (UMA) working group, http://kantarainitiative.org/wordpress/groups/user-managed-access-work-group

[46] InnoBors, http://innobors.eu