1. Publishable Summary

1.1 Project objectives and context

Identity management (IdM) has emerged as a promising technology to distribute identity information across security domains. In e-business scenarios, federated identity management is increasingly used to connect enterprises along the value chain and enables them to reduce transaction costs significantly. On the web it offers the promise of single sign-on for different domains and service providers, offering a common authentication and authorization infrastructure that eliminates the necessity of managing individual accounts and passwords. On the other hand several EU member states (e.g. Finland, Belgium, Estonia, Austria, Sweden, Italy, Spain, Portugal and Germany) have issued electronic identity cards (eID) to their citizens.

While the strategy to build a trustworthy, comprehensive, user-centric and privacy aware identity management system for Europe based on existing eID and trust infrastructures seems to be compelling and straightforward, there are many unsolved problems, which prevent the interoperable, secure, ubiquitous, easy and privacy-friendly use of strong authentication mechanisms across Europe. First, there is no standard conform eID client yet, which would be capable of supporting all the identity cards issued across Europe. In consequence it is very cumbersome for typical services providers to integrate a variety of different authentication devices and services. In addition to the cumbersome technical integration of the different authentication services, the lack of a coherent European infrastructure for trust management imposes additional obstacles, which prevent the easy, reliable and accountable deployment of electronic identity technology. Also, todays solutions often have obvious privacy concerns such as the unprotected transmission of sensitive information including the real name and other unique identifiers. Furthermore, non-technical problems like poor usability, low perceived usefulness, low awareness and the lack of applications also have seem to hindered the success of eIDs.

Therefore, the goal of the FutureID project is to build a comprehensive, flexible, privacy-aware and ubiquitously usable identity management infrastructure for Europe, which integrates existing eID technology and trust infrastructures, emerging federated identity management services and modern credential technologies to provide a user-centric system for the trustworthy and accountable management of identity claims. The FutureID infrastructure will provide great benefits to all stakeholders involved in the eID value chain. Users will benefit from the availability of a ubiquitously usable open source eID client that is capable of running on arbitrary desktop PCs, tablets and modern smart phones.

FutureID will allow application and service providers to easily integrate their existing services with the FutureID infrastructure, providing them with the benefits from the strong security offered by eIDs without requiring them to make substantial investments. This will enable service providers to offer this technology to users as an alternative to

username/password based systems, providing them with a choice for a more trustworthy, usable and innovative technology. For existing and emerging trust service providers and card issuers FutureID will provide an integrative framework, which eases using their authentication and signature related products across Europe and beyond. To demonstrate the applicability of the developed technologies and the feasibility of the overall approach FutureID will develop two pilot applications and is open for additional application services who want to use the innovative FutureID technology.

FutureID runs for three years and is partially funded under the EC's Seventh Framework Programme (FP7) as a large scale integrating project with a total budget of 14,517,219 €. The consortium is composed of 19 partners from 11 European countries, and combines the multi-disciplinary and complementary competence of large industry, small and medium enterprises, top research organizations and universities, a data protection agency, and a non-profit association.

1.2 Progress of work and achievements in Period P1

The work on this project officially started at November 1 2012. From November 14 to November 16 the Kickoff-meeting took place, hosted by the project coordinator Fraunhofer IAO (FHG) in Stuttgart, Germany. Newsletters where sent out and a press-release was published to raise the awareness of the project. A public website (www.futureid.eu) was set up, to promote the project and to inform the public of important news. There, partners also have access to important collaboration tools, including a project management web application, a document management system and a Wiki. These are being used actively by all partners in order to coordinate their work, distribute documents and inform the consortium about their progress. Besides this, a mailing list was set up.

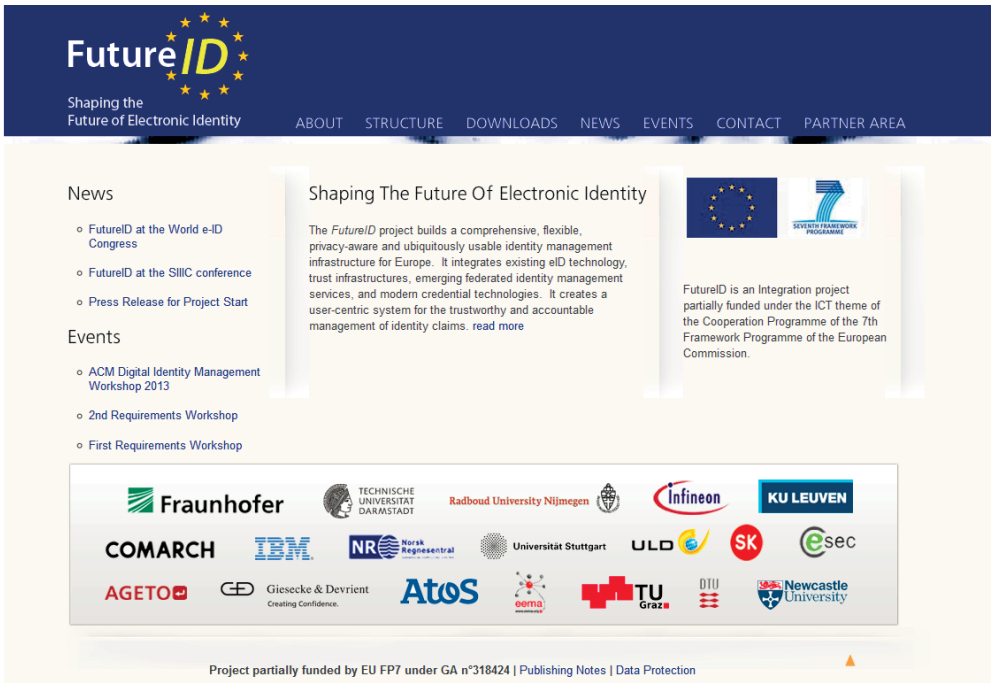

Figure 1: FutureID public website

For successful cooperation, several guidelines have been published to streamline the efforts among partners. Also the basis for a common terminology has been laid. A quality control manual describes all adopted procedures to guarantee the running of a quality assurance process all along the project. An advisory board has been set up, including experts from industry and research, representative of public administration, and potential users who will give constructive and critical advice throughout the duration of the project.

Lots of effort has been put into the survey and definition of technical, security, privacy, usability, socio-economic, legal and accessibility requirements. Also a test strategy has been conducted and the reference architecture has been finalized. Based on the results of these work packages, a test environment is set up and the FutureID client as well as the eID infrastructure is being developed. The implementation of the clients and the infrastructure has started in this period already.

In the last twelve months, several workshops and project meetings have been held, including general meetings in Madrid in April and Graz in October, where partners shared the progress on their work packages, efforts have been synchronized and important decisions have been made.

Furthermore, the FutureID project was present at several events and conferences, coming in touch with other relevant projects and informing potential users, beneficiaries and researchers about the FutureID project.

1.3 Final results and impact

As final results, the FutureID project will mainly provide a standardized, trustworthy and ubiquitously usable eID client, as well as a usable identity management infrastructure. For demonstration, the FutureID project will develop two pilot applications by integrating FutureID into the European eHealth Project epSOS[2] and into the Atos e-Learning Services for Enterprises. Besides this, FutureID will contribute to standardization efforts and will develop a new set of protocols for future eID solutions.

The results of the FutureID project will have an impact on eID stakeholders as well as the eID market.

Specific impacts on eID stakeholders

The FutureID infrastructure will provide benefits to all stakeholders involved in the eID value chain. This includes **users, application and service providers, e-government, businesses** and **identity service providers**.

Users will benefit from the user friendly open source eID client that is capable of running on arbitrary desktop PCs, tablets and modern smartphones. With the help of this client, users will be able to access different services that support the FutureID infrastructure. Therefore the project aims to provide application integration services that allow an easy integration of existing services into the FutureID infrastructure. This will in turn also provide benefits to application and service providers, enabling them to use trustworthy authentication services without the necessity of making large up-front investments in eID technologies or to meet legal obligations. Thereby also new consumer segments can be addressed easily. This will also allow governments to provide online services that so far could not have been offered by public administration due to security or legal constraints. Businesses will be able to use eID in their standard business activities and avoid high transaction costs in many cases. Last, Identity service providers will benefit from the increased pool of potential customers of their services.

Specific impacts on the eID market

With the help of FutureID the interoperability of eID systems will be improved and the fragmentation and complexity of the eID landscape will be overcome. This is achieved by providing a harmonized eID middleware implementation that allows an easy integration of services.

Also the relevant societal barriers will be addressed. The user-friendly and ubiquitous-usable user client will make it easier for citizens to benefit from eID services and will raise

[2] http://www.epsos.eu/

the awareness with the ability to rapidly include useful services and the development of convincing pilot applications.

The users' privacy concerns will be respected and the resulting challenge will be overcome by the design and development of privacy friendly authentication protocols, the development of guidelines for privacy friendly identifier systems and the design and implementation of minimal disclosure credentials.

By reducing large up-front investments and usage-costs, as well as increasing the number of potential customers for service providers, barriers on the economic side will be overcome.

Thereby the "chicken-egg" problem of the two-sided market for identity management is addressed.