1 Publishable summary

Project Objectives and Expected Outcome

The use and disclosure of personal information for private and business life is a major trend in information society. Advantages like enhancing social contacts and personalising services and products compromise with notable privacy risks arising from the user's loss of control over their personal data and digital footprints. Large amounts of scattered personal data lead to information overload, disorientation and loss of efficiency, while users share their information without control on social networks, neglecting security issues and privacy implications.

The *di.me project* aims at integrating personal data in a personal information sphere by a single, user-controlled point of access: the di.me userware. This user-controlled personal service provides intelligent personal information management and is targeted on integrating social web systems and communities. The research prototype realises decentral communication allowing for private data storage and avoiding undesired disclosure.

The di.me userware prototype is planned to act as a personal information repository and broker for personal or collective use, where information is organized semantically, protected, and its distribution can be controlled with high granularity by its owner. Users are enabled to define multiple profiles and connect to their existing social network profiles. This way they are able to update their information and content from one single place that will be reflected to other users and external social networks.

A distinctive characteristic shall be the capability of providing intelligent advisory about what to share and to whom. Research activities of the project aim at developing a semantic core with personal data mining and reasoning to support an intelligent management of personal data including recommendations. Metrics for trust of communication partners and privacy of documents will guide the user to avoid risky behaviour, e.g. when sharing data.

www.dime-project.eu

Main achievements made in the first period from Nov. 2010 to Oct. 2011 are the following:

User Requirements and Validations

- The application partners have specified requirements and added-value from the three envisioned major application fields: Private Users in all Life Spheres, Business Conferences and Smart Events, Enterprise Customer Relationship Management. A consolidated version of user requirements in the form of use cases and personas have been described, the central concepts for the di.me userware were defined.
- The general evaluation approach and methodology was developed, including a framework of user experience, standardized subjective measures and a concept for the di.me "self-evaluation"-methodology to be used for quantitative evaluation.
- A first lab study investigating usability, acceptance, and usefulness of of the di.me userware tested an early user interface mockup. 21 users from the three di.me user groups (professional users on business events, private end-users, users in customer-relationship-management) were tested at 4 test locations in Germany and Spain. The overall evaluation of acceptance, user experience, and utility yielded positive results for the general di.me approach and yielded many valuable results are used for the user interface and tool

development. Most attractive features were control of personal data, privacy warnings, and self-organised networking on events.

Semantic Modelling

- A di.me Ontology Framework enables the semantic modelling and representation of the user's extended personal information sphere. An integration of adopted, extended and newly-engineered ontologies supports the modelling of personal information in an ubiquitous setting, including the modelling of emerging information elements, device context, user presence, privacy, trust and access rights, user interaction and situation history.

Multi-Dimensional Trust Metrics

- A trust metric considering multiple dimensions (e.g. privacy of information, current context, history) has been developed. A first implementation is provided by the Trust Engine which is raises privacy warnings based on direct trust evaluation and dynamically adapts privacy and trust based on user interaction.

Anonymity and Security on the Network Level

- A Multi-Process anonymity component for supporting Tor hidden services at-runtime is was implemented. This component is the key for solving a discovered privacy/linkability risk with respect to an essential communication scheme concerning various di.me scenarios. Furthermore, the possibility to build a di.me own Tor network for better performance is described and tested.

Security at Application Level for digital.me Userware

- Essential mechanisms for securing internal and external communications and data exchange were integrated. The implemented two-layer design of the access control allows for flexible decoupling of the ontology access control from environmental security attributes responsible for securing communications, Role Based Access Control based authentication, authorisation, and secure business logic access. A persistent access control repository helps by managing these attributes at-runtime in a secure manner.

Identity Management System Prototype for Dynamic and Semi-automatic Trust Evaluation

- The introduced authentication based on Role Based Access Control supports various provider with the help of an abstraction authentication layer. Latter will allow for including potential Identity Management Solutions such as Idemix or WebID by just providing the respective Spring Security Framework conform Authentication Provider. The Role Based Access Control part responsible for assigning authorisation attributes, namely, permissions/authorities supports any di.me accepted provider.

User Interface

- A user interface concept including all basic structures, as well as patterns advanced intelligent system behaviour like situation change, privacy- and trust-level visualisation, has been developed. With an early mockup, the design has been tested in a lab study and optimisations have been worked in. Based on that, a technical user interface model and application programming interface was defined and a implementation of the user interface as proof of concept was realised.

System Architecture and Integration

- The system architecture has been first sketched and later specified in detail as a result of the efforts collaboratively carried out within Task 6.1 on System Architecture. The resulting architectural specification has provided a well-known and robust framework for the integration of the different subsystems within the system proof of concept.
- A fully functional system prototype providing the core functionalities targeted in the use-cases and requirements has been integrated and deployed as the system proof of concept.

Service Gateways and Web-Service-Integration

- A flexible service gateway framework has been established allowing flexibility to add additional services with relatively low effort and the ability to account for differing security, authentication, authorization, and protocol requirements on a specific service level.

Software Engineering

- The adapted software engineering methodology for managing the development lifecycle has been specified as a combination of an agile approach on use-cases engineering and modelling and a more traditional approach on architecture description.
- The development methodology has been implemented through bi-weekly development cycles as defined by the agile principle providing modelling, development and testing activities in an iterative fashion.
- Best practices for software quality and risk mitigation, such as Test-Driven development and continuous integration, have been adopted and implemented by all the technical partners

Context Recognition

- A di.me Mobile Context Crawler component for Android-devices which assesses context sensors WiFi, Position, Cell-Id and communicates with the di.me personal server.

Recommender Engine

- A di.me component has been established to support social recommendation of interesting items based on algorithms that take network-based voting as input.

Dissemination and Exploitation

- Dissemination materials (including website, newsletters, leaflet) have been prepared and published.
- Several scientific publications were submitted to international conferences and workshop and published.
- The project was disseminated within several national and international events and press
- Based on a general dissemination and exploitation plan, a concrete exploitation strategy has been developed, containing concrete exploitation steps which are linked to project milestones.