1 Publishable summary

The use and disclosure of personal information for private and business life is a major trend in Information Society. Users publish information to network and stay in touch with friends, family, and business contacts, to exchange data for collaboration, or to use services from commercial providers in diverse sectors. These values for the users, like enhancing social contacts or personalising services and products, compromise with privacy risks arising from the user's loss of control over their personal data and digital footprints.

The di.me project researches technology that enables the user to use personal data in a controlled, trustworthy, and intelligent way.
. The project develops a di.me platform for end-user services like decentralized networking and identity-management. User-control is integrated deeply in design: A private service – the di.me userware – offers a central node in a decentralized network, connecting with distinct identities to other users or external services, e.g. social networking platforms. Intelligent features will guide users, in particular by giving advice on trust and privacy, e.g. when sharing sensitive information.

www.dime-project.eu

In the second year of the project, main achievements have been made:

System Modelling: Single-user and community-setup of the Userware

Analyses on potential exploitation options of the system indicated requirements for deployment of the system. These inputs taken from the initial market approach showed e.g. that the hosting costs related to the delivery of a di.me single-user-setup to every future end user could hinder the scalability of the exploitation approach. Therefore, it was decided, that the di.me userware shall enable two different technical setups*: 1. user-controlled single-user-setup,* and a *2. multi-user-deployment for trusted communities.* For both technical setups, main features of secure communication between users shall be identical.

- On this background, a relevant amount of the efforts within the period have been devoted to modelling activities. Technical requirements were gathered in order to specify a new version of the system providing the core functional features on private and secure information management from a multi-user deployment, the di.me community setup. Main concepts in this expansion of the system domain were defined from a consistent view with the already existing ones:
    - the *private service*, run by the di.me user
    - the *di.me single-user-setup* (achieved as MS-03)
    - the *di.me community-setup* (multi-user deployment)
    - the *di.me server*, managed by the *di.me community owner* for the *di.me community-setup* and by the *di.me user* in the already known *di.me single-user-setup*
- So, a new modelling iteration was performed in order to refactor the system architecture and provide support for the *di-me community*-setup. Technical decision was taken to explicitly avoid development forks and support both single and multi-tenant setups with no additional development required but just the setup of the deployment mode.

Issues such as handling of user identifiers, proper isolation of user data and support for multi-user notifications were addressed, and as a result an architectural refactoring was specified. The entire system architecture, including the clients and the proxy layer, is now intended to serve private service instances regardless the setup these are served from.

System Integration

Two major system integration cycles have been carried out:

- The *di.me single-user deployment:* First, the earlier proof-of-concept version (used as the basis for Y1 review) was evolved to the system release used for a user validation and system test: at an IT event organised by AMETIC, this system version was provided to the attendees, presented, and evaluated (milestone 03, M20). Previously missing functionalities on user and group management and content sharing were added until reaching a degree of maturity of a beta version. So, the release of the beta di.me single-user setup can be considered the first integration achievement in the year.
- The *di.me community-setup:* After that, and according to the outcomes of the modelling iteration described in the previous section, the system architecture has been upgraded in order to support the scalability and performance requirements related to the dime-community setup. A major refactoring of the internal component structure, targeting mainly the communications and controllers layer, is carried out until reaching a stable multi-user beta release as the basis for coming validations. The release of this *di.me community-setup* beta version is, then, the second major integration target.

The digital.me proxy layer has also been deployed within the reported period, providing the decentralized message routing facility that enables the interaction between private-service deployments. By design, this component provides a transparent operation both for *single-user* and *community* setups.

System Deployment

- An initial implementation of the deployment components was provided as part of the MS03 release. Issues such as the stabilization of the infrastructure, the simplified deployment and update of the virtual machine image containing the entire system were addressed and the unified management of all the deployed instances were covered.

Semantic Modelling

- Ontologies in the di.me Ontology Framework have been extended to cover additional knowledge representation requirements. In particular, the semantic models that represent user activity context and user and system histories were improved to better structure the knowledge persisted for these domains, and a new ontology modelled on top of them to enable the representation of context-driven rules.

Semantic Lifting

- Extension of existing crawlers to target additional personal information domains targeted by di.me, including the extraction of i) raw user activity context from various device and virtual sensors, ii) additional types of personal information from desktop devices and iii) personal information from additional social networks, private services and other personal devices.

- Development of a first prototype for an online profile matching service that aims to identify and link multiple profiles for the user or any of their contacts, as extracted from various sources device and online sources.

Security at Application Level for digital.me Userware

- Further mechanisms for securing internal and external communications and data exchange were integrated. A dime proxy layer that also could act as an alternative anonymisation layer is fully specified and currently providing a dime DNS service (domain name system) as well as global registry for the dime virtual environment. This layer provides basic cryptographic means for avoiding various attacks and solves linkability problems that could arise. Furthermore, the design of the dime storage layer makes the overhead for hacking it in the case of single user reference implementation not suitable for potential attackers. A MasterKey solution keeps used encryption keys safe with the help of a trusted online service or mobile device(s) by allowing for ring signatures promise very high flexibility (when acquiring new devices) and tolerance (for device loss). Common security issues for mobile platforms and specific as well as cross-platform guidelines for developers as well as users are available or being compiled by considering the status of development and decisions in other work packages.

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

- The current Identity Management System Prototype was extended to support Login-Form based authentication and provides a Restful API for flexibly managing guest accounts as well controlling access to data via semantic model means. The dime-wide Identity Management System is provided in form of di.me Registry co-located in the current specification with the dime DNS service (domain name system) at the level of the proxy layer whereas each personal server manages its own guest accounts by means of local Access Control Repository. Intelligent support for avoiding linkability and unwanted information disclosure was builtin into the semantic model and eases the support of privacy recommendations for selected scenarios showing added value in dime.

User Interfaces and system clients

- A software interface (REST-API) for the communication between client user interfaces and the server-based private service of the di.me user interface was specified, implemented, and continuously further continuously reworked and detailed to reflect requirements on both server and client.
- The desktop user interface was further improved in several evolutional steps of development.
- A mobile user interface and client has been conceptualized, iteratively implemented and optimised based on validation results and changing functional requirements. In preparation of that an earlier wireframe-mockup was developed.

Service Gateways and Web-Service-Integration

- Based on the di.me service gateway, service adaptors for major required external services have been implemented, including services like LinkedIn, Facebook, Google+ and Twitter as well as smaller services operating in niche domains other than typical social networks, such as Fitbit. The di.me service gateway framework has been finalized. It allows adding

additional services to account for differing security, authentication, authorization, and protocol requirements on a specific service level.

Context Recognition

- The di.me component for mobile context crawleingassesses context sensors (e.g. Wi-Fi, Position, Cell-Id) and has been integrated with the di.me mobile client. Privacy settings to enable/disable context collection have been implemented. . Further di.me cloud-based services were designed and developed to enable location and proximity detection (the di.me Location Service and
- Proximity Service). For automatic situation recognition, a first prototype has been developed, that recognizes situations based on the aggregated user activity context knowledge, and a set of user-marked situations of interest.

Recommender Engine

- A first version of the Social Recommender Service has been implemented, offering software interfaces (REST APIs) to the di.me personal service. It includes different recommendation algorithms (Top N and Collaborative Filtering). This component was used during the project's user validations and system testing in Segovia (July 2012).

User Validations and System Testing

- A first validation for events was conducted at a Summer School "Las TIC en el nuevo entorno socio-económico", organized by AMETIC and Universidad Politécnica de Madrid. This course was used as a test bench. The test setup demonstrated the feasibility of the single-user userware deployment for a large set of systems which is a major outcome for the approach to have individual systems for each user. For the user validations, attendees were able to test the di.me tool and give their feedback to the consortium. This activity will also be useful for generating a future complete case-study.
- Usability, acceptance, and optimisations of the working clients and concepts of the di.me user interface was tested in a second usability lab study with a client on Android, as well as a prototype for the web user interface. The study yielded positive results on the general di.me approach, the usability of the clients, and on UI optimisations and requirements.
- Within the validation activities in Y2 and in preparation of the Y3 validations, the methods have been adapted and further developed (in particular the evaluation components that will be used in Y3).

Dissemination

Dissemination activities have been carried out through several dissemination channels:

- As major activities, the consortium has organized two dissemination events. The first one, coinciding with the first validation process of the project, took place in Segovia, Spain, in July. The second one was the mid-term dissemination event and was organized in Galway in the framework of the conference EKAW 2012 in October.
- Several scientific publications were submitted to international conferences and workshop and published.
- Dissemination to the general public and specific communities was done through press releases to national press media, and social media. A post on a technical blog has been published with an interesting impact on social networks like Google +

- Dissemination materials have been constantly updated, including the project's Web Site with improved layout and continuously updated content, the leaflet, and new dissemination materials like a poster and a roll-up.

Exploitation planning and Market research

- A first Market Report on digital.me applications was generated and then – in the modified format of a Market Scanning Table – continuously updated in order to periodically monitoring activities on relevant markets.
- An initial exploitation strategy of the digital.me project, making use of the market analysis was outlined taking into consideration the individual exploitation perspectives of the project partners.