PrimeLife – Privacy and Identity Management in Europe for Life

Privacy on Mobile equipment

An adequate infrastructure for privacy and identity management in a mobile environment needs to incorporate the server-side, the mobile devices and an adequate business model to make the approach interesting to customers and end users.

PrimeLife contributed to all of these three aspects. Here we introduce the solution for mobile devices and the server side.

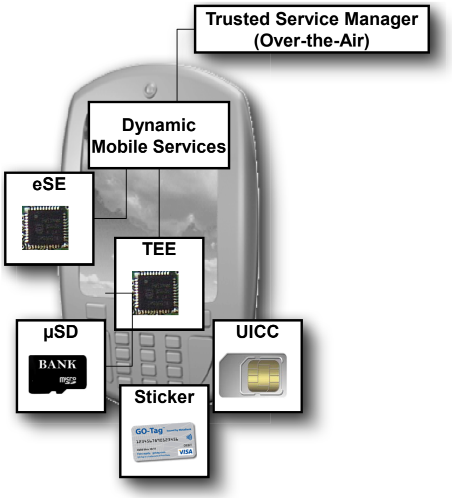
Privacy on Mobile Devices

In PrimeLife, the consortia partners, under the lead of G&D, SAP and EMIC have developed a demonstrator for the privacy-enhanced, trustworthy interaction between web-based services and mobile devices. The concept shown in the demonstrator allows the end consumer to use highly secure and privacy-protecting applications in a trusted execution environment of an Android Nexus mobile telephone. Herein, a Secure Micro SD card serves as privacy- and identity-providing Secure Element. Interactions are secured by a "Privacy-PIN".

Based on Secure Element technologies (in the form of a G&D Secure Micro SD Card), the demonstrator provides an example of how individual mobile phone end users can interact with complex processes of cloud-based services through a PIN-protected and encrypted "Private World" application. Private world applications root in secure elements in the mobile phone and enable the user to flexibly access and use secure services, without jeopardizing privacy.

In the future, this new solution can be used for secure mobile banking and payment, travel applications, loyalty programs, social networking, government solutions, health & insurance services, privacy protection, job-hunting, sales force interaction with company servers and secure business communication (e.g. encryption).

The solution presented by G&D, EMIC and SAP for the PrimeLife consortium is the first to offer identity provisioning, trusted execution and privacy protection in a highly flexible manner. For example, an end user can post a full personal profile online. Whenever a service provider requires information (e.g. age verification, social security number etc.) for particular services, the mobile phone application is triggered and assists the end user in controlling which data shall be released to the service provider and which policies are applicable for these data. This interaction is enabled in a PIN-protected "Private World" application, through which secure and private communication between the parties is assured.


Trusted Service Manager (Over-the-Air)

Dynamic Mobile Services

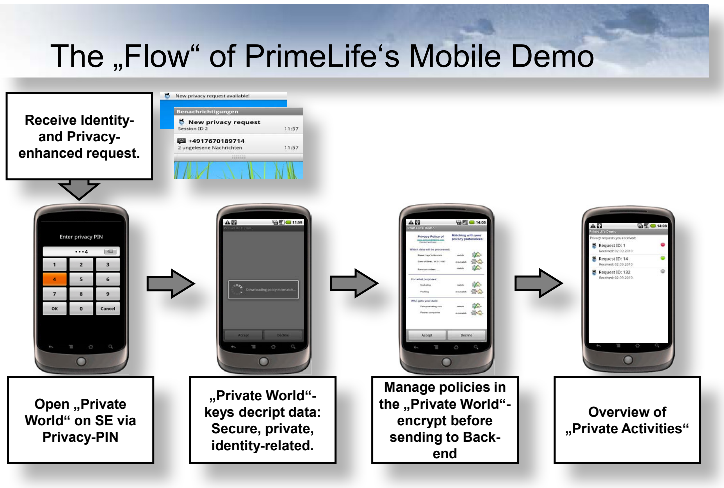
eSE

TEE

µSD

UICC

Sticker


The „Flow" of PrimeLife's Mobile Demo

Receive Identity- and Privacy-enhanced request.

New privacy request available!

Benachrichtigungen

New privacy request Session ID 2 11:57

+4917670189714 2 ungelesene Nachrichten 11:57

Open „Private World" on SE via Privacy-PIN

„Private World"-keys decript data: Secure, private, identity-related.

Manage policies in the „Private World"-encrypt before sending to Back-end

Overview of „Private Activities"

Personal and confidential data such as private data, usernames, passwords, location, and banking data are stored and processed within a separate trusted environment – the "Private World". In the future, this technology can equally be embedded into a plethora of Mobile Devices – from Mobile Phones to Tablet PCs or even the navigation and entertainment systems of cars.

Privacy in Server-side processes

In PrimeLife, we've used the secure mobile device in a Service-Oriented Architecture (SOA) application to enhance end user's control over already disclosed data. The application implements a privacy approach where personal data travels alongside with privacy policies. Those "sticky policies" are attached to the data and describe if and how this specific data may be processed by the data controller. The SOA application utilizes a policy matching engine that is able to determine if the sticky policy complies with an intended use of the respective data.

In case of a mismatch, i.e. the sticky policy does not allow using the data for the intended purpose, the data controller may communicate with the user to obtain consent. This enables the user to override her own sticky policy allowing the data controller the data usage for this specific purpose.

The trusted mobile device provides a convenient, yet secure and privacy compliant way to contact the user. It delivers a new quality of user-driven data control by letting the user influence the processing of data even after disclosure. All that is needed is an expressive policy language such as the PrimeLife Policy Language, sticky policies attached to the data, and a secure and trustworthy mobile device.

PrimeLife at a glance

Project reference:

216483

PrimeLife's objective:

Bring sustainable privacy and identity management to the web and develop tools for privacy-friendly identity management

Project duration:

March 2008 - June 2011

Partners:

15 partners from industry, academia, research centres and data protection authorities

Total cost:

About € 15.5 Million

Total EC funding:

€ 10.2 Million

Funding:

The PrimeLife project receives research funding from the European Union's 7th Framework Programme.

Contact:

Marit Hansen

t:+49-431-988-1214
f:+49-431-988-1223
primelife@datenschutzzentrum.de

Date of publication of this Primer:

May 2011

Want more info?

Various deliverables are available online:
http://www.primelife.eu/

PrimeLife