First Contribution to Open Source

Heartbeat: H 3.3.1

Editors:	Patrik Bichsel (IBM), Jan Camenisch (IBM)
Reviewers:	Claudio Ardagna (UNIMI), Sandra Steinbrecher (TUD)
Identifier:	H3.3.1
Type:	Heartbeat
Class:	Internal
Date:	20 August 2009

Abstract

This document provides an overview of the activites that have been carried out in the Open Source space. A main contribution being the release of Identity Mixer, an anonymous credential system developed within PRIME and extended in the PrimeLife project. Further, the heartbeat summarizes the plans for future contributions to Open Source of all workpackages.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 216483.

Members of the PrimeLife Consortium

1.	IBM Research GmbH	IBM	Switzerland
2.	Unabhängiges Landeszentrum für Datenschutz	ULD	Germany
3.	Technische Universität Dresden	TUD	Germany
4.	Karlstads Universitet	KAU	Sweden
5.	Università degli Studi di Milano	UNIMI	Italy
6.	Johann Wolfgang Goethe - Universität Frankfurt am Main	GUF	Germany
7.	Stichting Katholieke Universiteit Brabant	TILT	Netherlands
8.	GEIE ERCIM	W3C	France
9.	Katholieke Universiteit Leuven	K.U.Leuven	Belgium
10.	Università degli Studi di Bergamo	UNIBG	Italy
11.	Giesecke & Devrient GmbH	GD	Germany
12.	Center for Usability Research & Engineering	CURE	Austria
13.	Europäisches Microsoft Innovations Center GmbH	EMIC	Germany
14.	SAP AG	SAP	Germany
15.	Brown University	UBR	USA

List of Contributors

Contributions from several PrimeLife partners are contained in this document. The following list presents the contributors for the chapters of this deliverable.

Chapter	**Author(s)**
Introduction	Jan Camenisch (IBM)
Contributions	Jan Camenisch (IBM), Immanuel Scholz (TUD)
Potential Contributions	Patrik Bichsel (IBM), Jan Camenisch (IBM), Sabrina De Capitani di Vimercati (UNIMI), Benjamin Kellermann (TUD), Stefano Paraboschi (UNIBG), Immanuel Scholz (TUD)
Conclusion	Jan Camenisch (IBM)

This deliverable was rendered from HTML pages using Prince XML from YesLogic Pty Ltd. YesLogic has donated a license of Prince XML to W3C.

Table Of Contents

Chapter 1

Introduction

The objective of the PrimeLife project is to bring sustainable privacy to future network and services. One of the core means to achieve this is making privacy-enabling technologies widely available to the public so that they can be used to build privacy-enabled application and services. Therefore the goal of the Open Source work package is to

- monitor the existing open source initiatives in this space (e.g., [SunXACML], [OAuth], [Shibboleth], [TOR]);
- to work with the other PrimeLife workpackages to identify the components that are mature enough and are suitable for contribution to the Open Source community; and then
- to make these components available either as contribution to existing initiatives or individually.

For the latter, it will be important that sufficient documentation and example applications are provided, so that the concepts underlying the mechanisms can be understood, used, and we achieve the best possible impact. However, we will distinguish between very mature components where the code is of high quality and components that are rather research prototypes. We will invest time in the documentation and in example applications of the former. We plan to release the research prototypes on an "as-is" basis to the community.

In particular, the workpackage has two tasks:

Task 3.3.1
Monitoring Open Source projects, and identify technologies and mechanisms developed by the project (and by the predecessor project PRIME) which is suitable to be contributed to Open Source initiatives or can be made Open Source otherwise.

Task 3.3.2
Making available developed components as Open Source and working with the Open Source community towards adoption of these components.

This heartbeat reports on the progress and plans with respect to the latter task.

1.1 Summary of work in first project half

Deliverable D3.3.1 “Overview and Analysis of Open Source Initiatives” is delivered. In the open source space, the deliverable analyses the landscape of ongoing initiatives and will be used as a tool for selecting open source initiatives to which we will make contributions of results. Main goals for the selection of the target initiatives are take-up potential of our results in practice and best-possible leverage of our resources by the multiplier effects of the open source community. As well, an experience-based assessment of the individual communities may play a role in the decisions. The assessment of the open source space will be a continuous effort and D3.3.1 is only a first baseline of work in this area.

First implementation, code polishing, simplification and documentation work on our open source code from PRIME is mostly done and results are ideally made available to the public already during the second project year. In addition, the Identity Mixer implementation has undergone major restructuring and is now available to the public. No major new PrimeLife components has been ready in the first half of the project for being open sourced. Activity 1 already produced a number of prototypes whereof a majority can be open sourced.

An important issue that has to be considered is the presence of industrial partners with significant responsibility on the design and implementation of various implementations. For at least some of these partners, it is uncertain what level of investment and support they can dedicate to a software system that is going to become open source. In each case we need to realise a precise assessment within the partners to identify if the effort planned can be directly transferred to the work in WP3.3. There is the risk of having to adapt code, and possibly rewrite some code or omit some modules and functionality.

1.2 Summary of plans

We plan to release future demonstrators and prototypes arising from Activity 1 to the open source community on an “as is” basis. An implementation of a privacy friendly event scheduler is in the process of being released to the public. In addition, the implementation of a *trusted wallet* that allows a user to centrally and intuitively manage her credentials, a privacy enhancement to existing social networks and a mechanism to index encrypted data. They will possibly be extended with documentation and examples before being released. The user interfaces will be made available with the core components that they are built for. Also, Activity 5 plans to make an implementation of the policy language or selected relevant aspects thereof open source for a wide adoption of the technology and aligns its development closely with a widespread standard to foster potential adoption.

Chapter 2

Contributions

The contributions we could make during the first half of the project lifetime consist of Identity Mixer and several PRIME components. We release Identity Mixer in a re-implemented version and under a dedicated open source license. We could largely improve the PRIME components, which we release to the community.

2.1 Identity Mixer

Let us first provide a broad overview over the anonymous credential system technology before we analyse the future plans of the cryptographic library.

2.1.1 Technology Overview

The IBM identity mixer system developed at IBM's Zurich Research Laboratory is an implementation of the Camenisch-Lysyanskaya anonymous credential system [Credential Systems]. A credential system consists of users and organisations. Organisations know the users only by pseudonyms. Different pseudonyms of the same user cannot be linked. Yet, an organisation can issue a credential to a pseudonym and the corresponding user can prove possession of this credential to another organisation (who knows this user by a different pseudonym) without revealing anything more than the fact that such a credential is in the user's possession. Credentials can be set for unlimited use (these are called multiple-show credentials) and for one-time use (these are called one-show credentials). Possession of a multiple-show credential can be demonstrated an arbitrary number of times; these demonstrations cannot be linked to each other. Additionally, Identity Mixer supports relational proofs. A numeric value in a credential can be proven to be greater or smaller than a given number without revealing the actual value in the credential.

Apart from the pure cryptographic operations of the Camenisch-Lysyanskaya credential system, Identity Mixer also implements the high-level protocols and policies to deal with credentials (issue and presentation) as well as user interfaces to select credentials upon a request for information. The first version of the Identity Mixer software was developed by IBM Research about 6 years ago and has been subject to continuous improvement ever since, in particular in the context of the PRIME project. All parts of Identity Mixer except for the

cryptographic operations have been made available as open source within the framework of the Higgins project [Higgins]. The cryptographic parts are expected to be available shortly.

Anonymous credentials are a core element to enable privacy enhancing identity management. The Identity Mixer system will be maintained and extended through the PrimeLife project. While contributing Identity Mixer to the open source community is an ongoing effort, not many aspects of it (nor anonymous credential in general) have been standardised. Relevant aspects include token formats, wire formats, cryptographic algorithms, claim languages, or an API for a credential system. Both, open source and standardisation lead to better industry adoption of a new technology.

2.1.2 Status and Plans

A version of the identity mixer system is available for download at Technische Universität Dresden [Identity Mixer] under an irrevocable license allowing for free and unrestricted use.

Also, a new version of the library with the following additional features will be released:

- Signed Messages: inclusion of message values in Fiat-Shamir hash challenge
- Support for pseudonyms and domain-pseudonyms
- Support for Pedersen commitments [Pedersen Commitments]
- Support for epoch-based certificate validity (can be used for certificate expiration) and re-generation
- Multi-certificate support [Identity Mixer Spec].

2.2 PRIME core components

The code of the project PRIME has been inherited to PrimeLife. Figure 1 shows an architecture overview of the PRIME core components. Arrows point from the component that uses towards the component beeing used. Only the webservices are accessible from outside. The Debug-Webservice has been omited, as it would contain an arrow to almost any component shown but is not meant to be part of the release architecture.

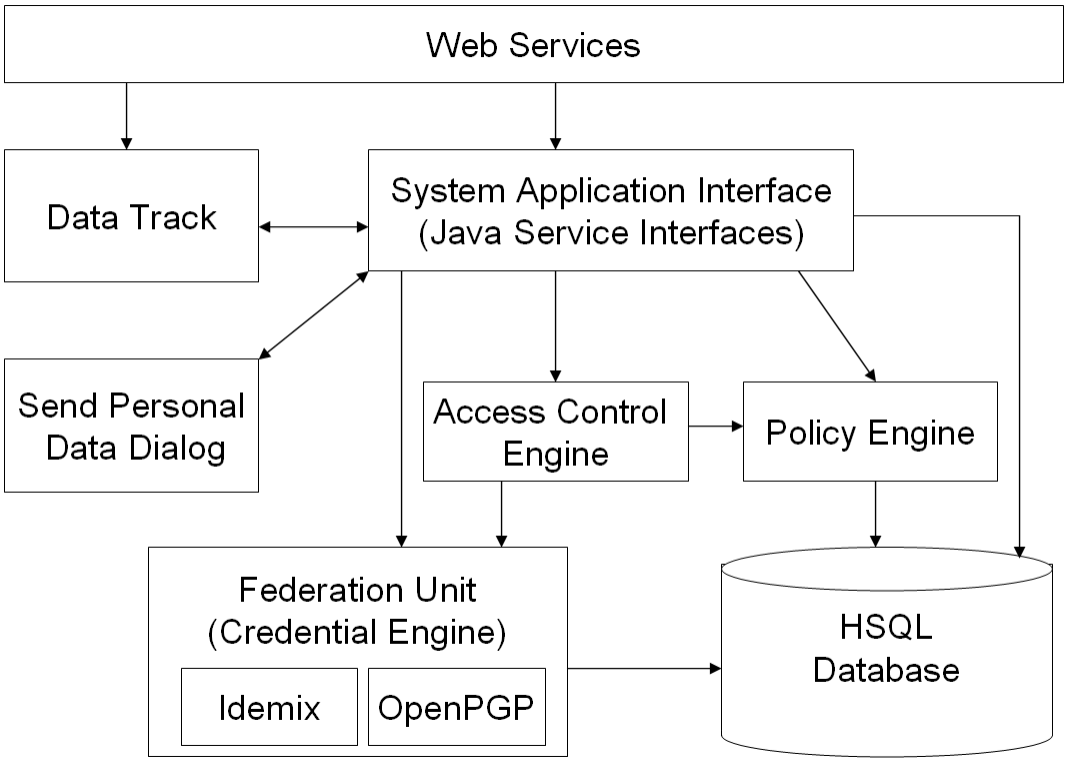

Figure 1: Architecture of the components in PRIME, where Idemix is short for Identity Mixer.

2.2.1 Modularisation of the Authentication System

The PRIME authentication system was designed to be replaceable from the beginning. However, the interfaces to the authentication subsystem were not clearly specified and the linkage to the submodules were static, so that they could not be combined seamlessly with other open source libraries. License difficulties for libraries like Identity Mixer made it impossible to release the source code under an open source license.

For this reason TUD has modularised the authentication system and extracted the Identity Mixer in a separate linked library, so that the remaining source code can be released under an open source license (some parts of the Identity Mixer library are currently not released under a compatible license to PRIME).

2.2.2 Integrating OpenPGP into PRIME

TUD integrated BouncyCastle [BC], an implementation of the OpenPGP [OpenPGP] interface as an alternative to the identity mixer interface. OpenPGP is an authentication system mainly used in email traffic today with a user-based web of trust [WoT]. Although it is a well established protocol and open source for a long time now, it lacks several security features such as anonymous credentials, one-time-credentials or the ability to select partial attributes from an signed credential (Partial Credentials). Still, it is of use to migrate existing credentials and adopt the usage of PRIME components to existing trust networks. Following a list of different features and their support in the PRIME framework.

Comparison between Identity Mixer and OpenPGP.

	Identity Mixer	OpenPGP
Unlinkable Pseudonyms	yes	no
Partial Credentials	yes	no
Relational Proofs	yes	no
One-Show Credentials	not supported in PRIME	no
Create Credentials	yes	yes
Present Credentials	yes	yes
Key Management	not supported in PRIME	use of existing keys

Current features of OpenPGP PRIME

The OpenPGP component acts as possible full replacement for the Identity Mixer credential system. It will be activated as default when the Identity Mixer library is missing, or by explicitly specifying OpenPGP as proof method. Supported are signing and verification of signatures. Unlike Identity Mixer credentials, OpenPGP signatures are linkable, which are always shown as full credentials and relations cannot be proved.

Unimplemented features of OpenPGP PRIME

Key Management of OpenPGP keys is not done in PRIME. Instead, already existing keys are used. There exist numerous key management tools for PGP keys, for example, Windows Privacy Tray [WinPT].

When verifying signatures, keys are not immediately checked for revocations. However, if a key in the users keyring is marked as invalid, the verification will fail as expected. Separate tools that check for revoked keys and mark them accordingly are recommended, for example, Gnu Privacy Assistant [GPA].

2.2.3 Data Track

The *data track* logs at the user side all transactions where personal data are disclosed. Hence, it allows the users to keep track of their personal data disclosures. This includes the user's partial identities (data, credentials), but also meta-information like the purposes and the negotiated privacy policy. User-friendly search functions allowing users to easily locate transaction records of interest are currently implemented. Besides, the data track will include functions, which enable users to exercise their rights to access data, request correction or deletion online. Although the PRIME data track is meant to satisfy most application needs, some community applications may have to provide an own version of the data track, as their peers (individuals) might not provide the same data handling policy information (if they provide such information at all).

2.2.4 Trust evaluation

The trust evaluation can be based on information like privacy and trust seals certified by data protection commissions or independent certifiers. In addition, blacklists of a sites maintained by consumer organisations, security and privacy alert lists and anti-phishing alert lists can provide useful information. Another trust parameter that we have chosen measures the site’s benevolence to implement privacy-enhancing PrimeLife functions. For this, dynamic seals

can be used that can be generated in real-time by an “Assurance Evaluation component” at the service side. The usefulness of the trust evaluation function largely relies on the available trust information.

Chapter 3

Potential Contributions

In addition to the previously described contributions that have already been made Open Source there are components that have not yet been finished. We provide a list of possible additional contributions in the following sections where we structure the efforts by the activity that they will arise from.

3.1 Activity 1 - Privacy for Life

The components produced in the work packages of Activity 1 are meant to demonstrate the concepts and solutions developed. Such demonstrators are mostly used to illustrate a concept and do not have a large potential in getting a large community improving them. Consequently, we plan to make them available on an "as-is" basis. Currently, we have identified the following components:

- MediaWiki plug-in to enable MediaWiki with PRIME for authentication: Research code, example code for how to use the PRIME core
- Reputation components: research code, open source

3.1.1 Access Control MediaWiki plug-in

Activity 1 developed a plug-in for MediaWiki [Mediawiki] to enable access of PRIME functionality within the Wiki system. MediaWiki is one of the most common used Wiki software, especially for its use in Wikipedia [Wikipedia]. It is planned to make the plug-in available under the terms of EPL. With this plug-in, the user has the possibility to specify very fine-grained access control for wiki pages. To fulfil such a policy, it may be demanded that the user has to disclose some data or to prove some credentials with PRIME. A full description of the plug-in's features, its usage and a development manual is included in Heartbeat 1.2.4 and inside the source code. The plug-in is written in PHP, so it is technically not possible to release a binary-only version.

The MediaWiki plug-in only accesses PRIME core functionality over a Web service, so its licensing terms can be chosen independently from those of PRIME. However, to benefit from the functionality, the user has to have a version of PRIME installed, so the free availability of

PRIME strongly influences the acceptance of the MediaWiki plugin within the Open Source community.

3.1.2 Reputation components

WP2.2 and WP1.1 developed a framework for distributed, anonymous Reputations. The implementation is done in Java and based on the Identity Mixer cryptographic library (see Section 2.1). The applets can be used as Add-Ons for the forum software phpBB. They allow the user of the forum to rate postings and receive reputation anonymously. Currently, the applets use a closed source version of Identity Mixer. For more information, see Heartbeat 2.2.4. Further, it is planned to extend the reputation component within Activity 1 to support MediaWiki. Similar to the phpBB applets, users can rate wiki entries and authors can receive reputation anonymously.

3.2 Activity 2 - Mechanisms

Activity 2 has the responsibility of investigating new privacy-aware techniques and mechanisms supporting the protection of privacy in the electronic society. The goal is the production of research results, with some effort dedicated to the implementation of prototypes demonstrating the applicability and validity of the research ideas. Each of the four work packages in which Activity 2 is organized plans to release two heartbeats (at M18 and M34) consisting of software prototypes. Most of these prototypes are expected to represent proofs of concept that will be mainly used to test the underlying concepts and principles upon which the solutions developed within the work packages will be built. A few selected prototypes developed within Activity 2 can become of interest for the work in WP3.3, dedicating effort to make them of interest to the open source community. We separately analyze the potential contributions deriving from each WP within Activity 2.

3.2.1 WP2.1 Cryptographic mechanism - "Wallets to safely store credentials"

The idea behind the so called "trusted wallet" or "secure wallet" is that a separation between the security and privacy relevant computations and general purpose computations. Many actions of a user can be carried out without having to release personal identifying information (PII). Those operations would not be changed through the presence of the wallet. However, when a user wants to carry out a transaction that includes the release of PII the wallet will facilitate the transfer. A requirement for this facilitation is that the wallet contains all PII which also simplifies the handling of this information for the user. The help in the transaction comes through the wallet handling requests from service providers and releasing the required information. We propose that the wallet makes use of anonymization techniques such as Identity Mixer to only release minimal data. The highly sensitive data handled by the wallet requires it to be trustworthy. This trustworthiness can be attained through techniques such as virtualization or the use of tamper resistant hardware. Where the use of tamper resistant hardware (e.g., a smart card) can even partially protect the data from being misused. For example, assuming the wallet manages exclusively Identity Mixer credentials, it would be impossible to use the credentials without breaking the authentication mechanism of the tamper resistant device or breaking the cryptographic assumptions the technology is based on. Given this protection mechanism the trust assumptions towards the host computation system can be minimised.

3.2.2 WP2.1 Cryptographic mechanisms - "Encryption overlay network for social networks"

Users in social network sites lack control over their data, e.g. their social network profile and their posts. Even if the social network supports audience segregation, i.e. it allows the user to configure who can see which data, the data is still potentially available to the social network provider, its business partners, and its employees. Enforcing access control by means of encryption is a mechanism to improve the user's control over his data.

Another approach for improving both availability and privacy of social networks is to distribute the social network over multiple nodes in a peer to peer fashion. In our work we do not directly consider this approach, and focus on the currently dominant social networking model with a central web-based social network site. However, by considering encryption independently as an overlay network for social content we achieve some independence of the underlying communication mechanism. We present a practical, SNS platform-independent "transparent" solution, for social network users to control their data.

For the scenario in which the 'underlying communication protocol' is a centralized social network side that allows for web-based content posting and retrieval, we design and implement a client side application (a Firefox extension). The main idea is to create an encryption mechanism to enforce access control to a user's private information based on his privacy preferences. The mechanism used for the encryption of content data can be based on broadcast encryption or hierarchical encryption techniques. At the moment the mechanism is implemented using OpenPGP multiple recipients encryption [Multiple Recipient], but we consider improvements for key privacy and performance. An important performance factor is the size of the cipher text and the amount of key information needed when a user interacts in a complex and well-connected social network.

3.2.3 WP2.2 Mechanisms supporting privacy and trust - "Privacy-enhanced event scheduling"

Event schedulers, well-known from groupware and social software, typically share the problem that they disclose detailed availability patterns of their users. One of such a very popular Web 2.0 application is doodle [doodle]. To make it as simple as possible, everybody may not only create a poll, but also cast votes to existing polls, see results of other polls, and even change casted votes of an existing poll. When participating in a doodle poll, one has to share personal information with the server, the other participants, and even with the whole world. This information includes when exactly a particular user is available for the event. The so-called 'availability pattern' may contain sensitive information in at least two respects. First, direct inference from the availability at a particular date may reveal information about one's private life. ("Will my husband vote for the date of our wedding anniversary?") Second, indirect inference arises from the fact that availability patterns contain much entropy and thereby allow to (re-)identify individuals who would otherwise remain pseudonymous. ("The availability pattern of user *bunny23* looks suspiciously like the one of my employee John Doe!")

Goal of the "Privacy-enhanced event scheduling" is to design and implement such a Web 2.0 application with modified techniques known from e-voting to preserve the users privacy.

3.2.4 WP2.3 Privacy of data - "Indexing of encrypted data"

The goal of the WP is to propose mechanisms able to support the management of privacy requirements in scenarios with large collections of sensitive data. Several of the research lines active within this WP will be able to contribute software prototypes to H2.3.4 (M18) and H2.3.5 (M34). One tool that appears to offer a good potential for transfer to WP3.3 is a tool which is currently being developed to support the efficient design of database schemas with encrypted data. The work in WP3.3 on this tool is expected to occur after the tool will be released in H2.3.4, and most of the effort will then be spent in Y3 of the project. Specific attention will be paid to the integration with important open source systems able to exploit the services of the tool and to the production of documentation supporting the user in the configuration and deployment of the tool.

The tool supports the design of database schemas where some of the attributes are encrypted. The goal is to store sensitive data on honest-but-curious servers, supporting the efficient execution of queries. To protect the sensitive data contained in a table, the schema of the table is partitioned into different fragments. Each fragment contains some of the attributes in clear-text, and the remaining attributes in an encrypted format. The identification of the fragmentation starts from a formal definition of the confidentiality constraints on the data. Each confidentiality constraint is represented by a set of attributes: the interpretation is that the database must not expose together all the attributes appearing in the constraints. This model is able to capture the requirements of many real world scenarios, where the information that has to be protected is the association between values, rather than the presence in the database of specific values (e.g., it is the association between a person name and her salary that is sensitive, rather than the disclosure of their independent values). Constraints with a single attribute represent attributes whose values are in itself sensitive (e.g., the social security number in the US).

The tool starts from the specification of a relational database schema and a description of all the confidentiality constraints. It optionally can consider also a description of queries operating on the table. It then explores the potential fragmentations, identifying one characterized by a minimum number of fragments and lowest cost. The search problem is known to be NP-hard; for large schemas the program applies a heuristic search, which experimentally showed to be able to identify good solutions.

In WP2.3 we are also developing other tools supporting data storage on honest-but-curious servers, which may become interesting options for the open-source activity in WP3.3.

3.2.5 WP2.4 Access control for the protection of user-generated data - "Data outsourcing"

The goal of the WP is the design of novel models and mechanisms for the definition and enforcement of access control restrictions in scenarios where user-generated data are stored on external servers and where therefore privacy constraints must be considered. One tool that will be released at M18 for H2.4.4 will demonstrate the techniques for the realization of access control policies with encryption. This line of research aims to achieve better protection for the resources (files, PII, and in general privacy-sensitive information) that users provide to external servers, for storage or dissemination to other selected users. The techniques apply encryption in a way that allows the server to store and distribute information and resources according to the access control policy specified by the user owning the information (data owner), without having access to the content. There is an interesting similarity with the work planned within WP1.2, where encryption is applied to a social networking scenario. This tool

can receive some attention within WP3.3 to produce a more robust and better documented release, able to be integrated within a current open source platform, facilitating its adoption by interested users. The plan is to work on the transfer to WP3.3 of the above-mentioned tool.

3.3 Activity 4 - Human Computer Interfaces

3.3.1 Data track

The data track functionality described earlier, clearly needs a user interface. The main issues of this component are the development of user-friendly search functions for tracking transaction records as well as user-friendly Online functions with which users can request access or access directly their data at service-sides. We develop the data track front-end for the user-side identity management system as open source.

3.3.2 Trust evaluation

We visualised a possible appearance of the trust evaluation function to the user. Its task is to let users evaluate the trustworthiness of their communication partners. As we previously mentioned, reliable information is the foundation of this functionality. Still, the appropriate presentation makes the trust assessment an intuitive and helpful feature. We specifically investigate what are suitable trust & assurance parameters (based on social trust factors) and how the evaluation of those parameters that may have different semantics and scopes can be best illustrated.

3.3.3 Privacy Preference Management

For a simplified privacy preference management, we are following the approach of allowing users to choose and adapt their privacy preferences "on the fly" (i.e., when a service is requesting data from them) rather than demanding from them to define their preferences beforehand. For this, we are offering predefined privacy preference profiles (so-called "PrivPrefs"), from which users can choose, including the most privacy-friendly ones of acting anonymous or releasing only the minimal amount of data needed for the purpose of the requested service. We are currently developing user interfaces for such a simplified privacy preference management and we plan to release them as open source.

3.3.4 Credential Selection

The design of well-understandable user interfaces for anonymous credential selection is a major challenge, as no real-world analogies for anonymous credentials exist, on which one can build upon. We have been exploring a series of design proposals based on the metaphor of a derived virtual card, which have however in our user tests not been completely understood by many test users. Further improvements addressing usability problems experienced in our user tests will be done. Besides, we will investigate also alternative metaphors that could be exploited.

3.4 Activity 5 - Policies

The general goal of Activity 5 is to design and implement novel privacy-aware policy systems. This activity is organized in three work packages focused on: the identification of

policy requirements (WP5.1); the design of novel policy languages able to provide users with the ability to effectively control access and use by others over their data (WP5.2); the production and implementation of novel policy languages (WP5.3).

In particular, work package WP5.3 aims to implement by M30, with a subsequent release at M36, a prototype supporting an extension of XACML for privacy requirements. WP5.3 also almost finished an implementation (due by M18) of an extension of the PRIME policy language that is able to incorporate XACML policies to investigate the integration between a privacy-centered architecture like PRIME with the current status of the XACML standard. The policy engine uses parts from the Sun XACML engine and from the PRIME policy engine. Analysis about the license under which the latter can be published as open source are currently carried out.

Work package WP5.2 could also produce small prototypes demonstrating advanced features of policy languages, but neither deliverables nor heartbeats are planned. For instance, SecPal will be studied in WP5.2 by partner EMIC, with expected benefits on the design of the XACML extension and on its implementation. Considering the transfer of tools and components developed in Activity 5 to WP3.3, the greatest potential certainly lies in the prototype implemented in WP5.3. The extension of XACML for privacy should also be proposed as an extension to the standard, with an effort by PrimeLife coordinated by WP3.4 on standardization. Significant support to this standardization initiative certainly derives from the availability of an open source implementation of the language.

The second implementation involves an industrial partner, which might lead to adaptations that have to be made before the software can be released as open source. These adaptations are certainly easier if the design considers from the start the need to support the open source initiative. Before starting the design of the software architecture of the WP5.3 prototype, it is necessary to complete the assessment of the constraints on each partner. It is the responsibility of partners involved in both WP5.3 and WP3.3 to verify that the design in WP5.3 will carefully consider the need to eventually produce a contribution to WP3.3.

Chapter 4

Conclusion

In the first project year we have mainly dealt with the heritage from PRIME. Still, with the publication of the identity mixer code we have finally achieved what we failed to do in PRIME.

The plans for the second project year will be mainly to maintain and extend the published pieces. Also we will prepare ourselves as to make results from PrimeLife open source. One main contribution, the policy engine, shows how time consuming license discussions can be and we therefore expect most of the code to appear in the last project year.

References

[BC]
BouncyCastle, OpenSource Cryptographic Library including an OpenPGP implementation.
http://www.bouncycastle.org/

[Credential Systems]
Jan Camenisch and Anna Lysyanskaya, Efficient Non-transferable Anonymous Multi-show Credential System with Optional Anonymity Revocation, EUROCRYPT '01, Volume 2045 of LNCS (pages 93-118), Springer, 2001.
http://www.zurich.ibm.com/~jca/papers/eprint.pdf

[GPA]
GNU Privacy Assistant, Key Management Tool for OpenPGP including a key revocation check.
http://wald.intevation.org/projects/gpa/

[Higgins]
Higgins Open Source Identity Framework, accessed 17 August 2009.
http://www.eclipse.org/higgins/

[Identity Mixer]
Identity Mixer Library at TU Dresden, accessed 16 March 2009.
https://prime.inf.tu-dresden.de/idemix/

[Identity Mixer Spec]
IBM Research, Cryptographic Protocols of the Identity Mixer Library, v. 1.0, IBM Research Report, RZ3730, 2009.
http://domino.research.ibm.com/library/cyberdig.nsf/index.html

[Mediawiki]
Mediawiki, accessed 9 July 2009.
http://www.mediawiki.org/

[Multiple Recipient]
Adam Barth, Dan Boneh and Brent Waters, Privacy in Encrypted Content Distribution Using Private Broadcast Encryption, Financial Cryptography and Data Security, Volume 4106 of LNCS (pages 52-64), Springer, 2006.
http://www.springerlink.com/content/x587847626m06014/

[OAuth]
OAuth Implementation, accessed 17 August 2009.
http://oauth.net/

[OpenPGP]
OpenPGP Homepage, Standard for Email Encryption based on PGP, accessed 16 March 2009.
http://www.openpgp.org/

[Pedersen Commitments]
Torben P. Pedersen, Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing, CRYPTO '91, Volume 576 of LNCS (pages 129-140), Springer, 1991.
http://www.springerlink.com/content/pwqy90xna7thbxut/

[Shibboleth]
Internet2, Shibboleth - A project of the Internet2 Middleware Initiative, accessed 17 August 2009.
http://shibboleth.internet2.edu/

[SunXACML]
Sun Microsystems, Implementation of the XACML standard, accessed 17 August 2009.
http://sunxacml.sourceforge.net/

[TOR]
The Onion Router, accessed 17 August 2009.
http://www.torproject.org/

[Wikipedia]
Wikipedia, The Free Encyclopedia, accessed 9 July 2009.
http://www.wikipedia.org/

[WinPT]
Windows Privacy Tray, Key Management Tool for OpenPGP keys under Microsoft Windows.
http://wald.intevation.org/projects/winpt/

[WoT]
Web of Trust, Trust Model for a Public Key Infrastructure, accessed 16 March 2009.
http://en.wikipedia.org/wiki/Web_of_trust/

[doodle]
Michael Näf, Doodle Homepage, accessed 12 January 2009.
http://www.doodle.com/