ABC4Trust

- Project description -

Table of Contents

1. CONCEPT AND OBJECTIVES, PROGRESS BEYOND STATE-OF-THE-ART, S/T METHODOLOGY AND WORK PLAN

1.1 Concept and project objective(s)

Key Takeaways

- ✓ The goal of this project is to address the federation and "interchangeability" of technologies that support trustworthy yet privacy-preserving Attribute-based Credentials (ABC).
- ✓ The aim of this project is to deepen the understanding in ABC technologies, enable their efficient/effective deployment in practice, and their federation in different domains.
- ✓ These results will enable stakeholders to better understand privacy-preserving ABC technologies, compare the relative merits of different technologies in different scenarios. To ensure this, the project will conduct two trials.
- ✓ With IBM and Microsoft, the two leading ICT companies in this area will provide input to development and standardization in this domain under impartial leadership.
- ✓ ABC4Trust relates to Objective ICT-2009.1.4 "Trustworthy ICT" in Challenge 1 "Pervasive and Trustworthy Network and Service Architectures" especially by contributing to trustworthy European infrastructures via trustworthy identity management.

The goal of ABC4Trust is to address the federation and interchangeability of technologies that support trustworthy yet privacy-preserving Attribute-based Credentials (ABC). Classical trustworthy credentials normally do not respect privacy. They invariably reveal the identity of the holder even though the application at hand often needs much less information, for instance only confirmation that the holder is a teenager or is eligible for social benefits. In contrast to that, Attribute-based Credentials allow a holder to reveal just the minimal information required by the application, without giving away a full identity. These credentials thus facilitate the implementation of a trustworthy and at the same time privacy-protecting digital society.

The objective of this project, ABC4Trust, is (1) to define a common, unified architecture for ABC systems to allow comparing their respective features and combining them on common platforms, and (2) to deliver open reference implementations of selected ABC systems and deploy them in actual production pilots allowing provably accredited members of restricted communities to provide anonymous feedback on their community or its members.

1.1.1 Concept: Enabling Multilateral Trust into Attribute-based Credentials

Almost all applications and services based on computer systems require some authentication of participants to establish trust relations, either for only one endpoint of communication or for both. One widely used mechanism for this is password-based authentication. Given the weaknesses of such a simple authentication method, multiple alternate techniques have been developed to provide a higher degree of security. Cryptographic certificates are one known example of this. Although such certificates can offer sufficient security for many purposes, they do not typically cater to privacy because they are bound to the identity of a real person. Any usage of such a certificate exposes the identity of the holder to the party requesting authentication. There are many scenarios where the use of such certificates unnecessarily reveals the identity of their holder, for instance scenarios where a service platform only needs to verify the age of a user but not his/her actual identity. Revealing more information than necessary not only harms the privacy of the users but also increases the risk of abuse of information such as identify theft when information revealed falls in the wrong hands.

Over the past 25 years, a number of technologies have been developed to build ABC systems in a way that they can be trusted, like normal cryptographic certificates, while at the same time protecting the

privacy of their holder (e.g., hiding the real holder's identity). Such Attribute-based credentials (ABCs) are issued just like ordinary cryptographic credentials (e.g., X.509 credentials) using a digital (secret) signature key. However, ABCs allow their holder to transform them into a new credential that contains only a subset of the attributes contained in the original credential. Still, these transformed credentials can be verified just like ordinary cryptographic credentials (using the public verification key of the issuer) and offer the same strong security (Figure 1).

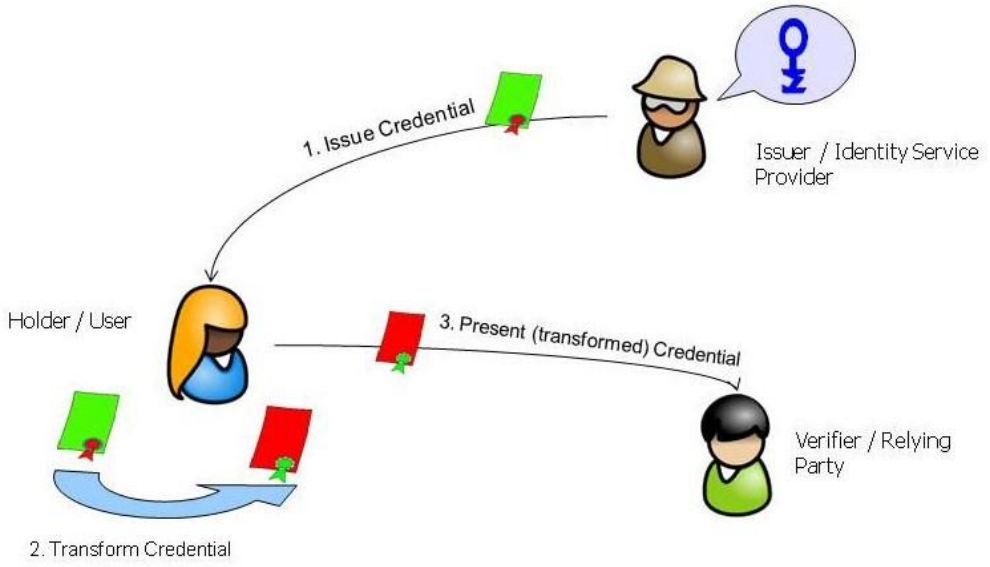

Figure 1: Basic functionality of an ABC system

There are a handful of proposals of how to realize an ABC system in the literature [Cha85, Brands00, CamLys01, CamLys04]. Notable is especially the appearance of two technologies, IBM's Identity Mixer and Microsoft's U-Prove. As these are supported by two of the leading ICT companies, they are among the best candidates to provide input to standardization in this domain. However, the complexity of ABC technologies and the client-server interactions they entail have so far overwhelmed potential users and consequently hindered their effective large scale deployment. Overcoming these hurdles requires an in-depth comparative study of the functionalities of the different ABC technologies and an analysis of their security and efficiency properties to provide a common understanding of their applicability to diverse application fields and scenarios.

With a comparative understanding of these technologies, it will be easier for different user communities to decide which technology best serves them in which application scenario. It will also be easier to migrate to newer ABC technologies that will undoubtedly appear over time. In addition the same users may want to access applications requiring different ABC technologies, and the same applications may want to cater to user communities preferring different ABC technologies. Hence, it is also necessary that different ABC technologies be able to coexist or be interchanged across scenarios involving the same users and application platforms. It may also be sometimes desirable to convert ABCs from one technology into another so as to federate them across different domains, as is done today between different authentication domains using standards such as SAML, Kerberos, or OpenID. There are no commonly agreed sets of functions, features, formats, protocols, and metrics to gauge and compare ABC technologies, so it is hard to judge their respective pros and cons. There is also currently no established practice or standard to allow for the interchangeability and federation of ABC technologies.

A number of countries have already introduced or are about to introduce electronic identity cards (eID) and drivers licenses. Electronic ticketing and toll systems are also widely used all over the world. As such electronic devices become widespread for identification, authentication, and payment

(which links them to people through credit card systems) in a broad range of scenarios, the users' privacy and traceability will be increasingly threatened in the future internet society. If and when eIDs are rolled out, society and countries are well advised to build privacy protection techniques into them.

The aim of this project is to deepen the understanding in ABC technologies, enable their efficient/effective deployment in practice, and their federation in different domains. To this end, the project will

1. Produce an architectural framework for ABC technologies that allows different realizations of these technologies to coexist, be interchanged, and federated
    a. Identify and describe the different functional components of ABC technologies, e.g. for request and issue of credentials (Figure 2) and for claims proof (Figure 3);
    b. Produce a specification of data formats, interfaces, and protocols formats for this framework;
2. Define criteria to compare the properties of realizations of these components in different technologies; and
3. Provide reference implementations of each of these components.

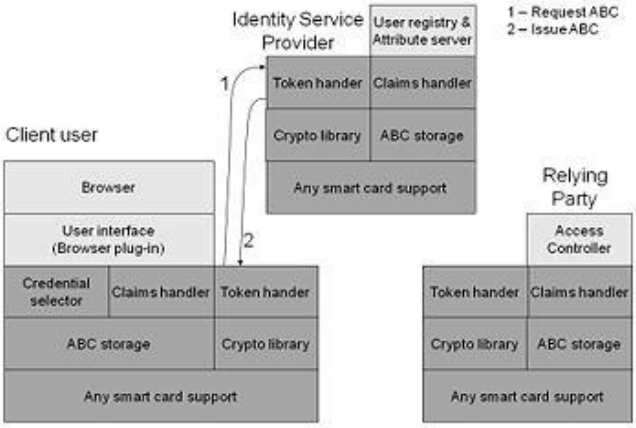

Figure 2: Request and Issue Credential

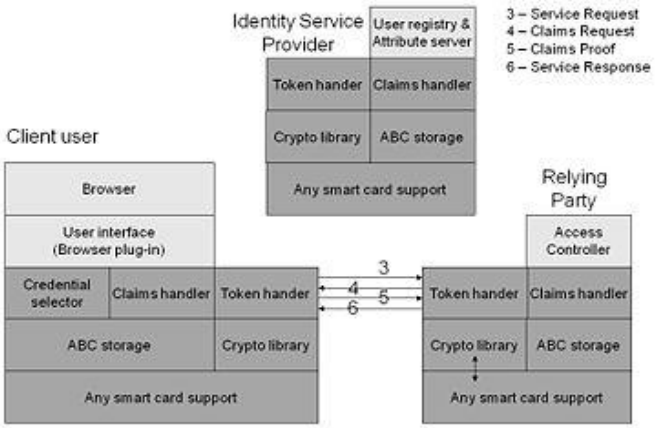

Figure 3: Claims Proof

In line with the paradigm of Multilateral Security [Rannen00] these three results will enable stakeholders to better understand privacy-preserving ABC technologies, compare the relative merits of different technologies in different scenarios, fully exploit their privacy-enhancing features, and thereby effectively deploy these technologies with the confidence that there is a roadmap to evolve or replace them over time. To ensure this, the project will conduct two trials as part of work packages WP6 and WP7, both of them addressing possible tensions between accountability and privacy in application fields.

We note that employing ABC technologies of course requires a number of surrounding infrastructure components as they need to be integrated into authorization and access control systems. In this respect policy languages play a particularly important role. While this project will build this surrounding infrastructure for the pilot applications it does not focus on these parts. Instead we will draw on the results of the EU-funded projects that concentrate on these surrounding components including PrimeLife, TAS3, and MASTER as well as applicable international standards.

1.1.2 Project Objectives

The proposed project will target six objectives:

1. Propose a framework of technology-independent architectural interfaces, formats, and protocols, for operating ABC technologies so that different ones can coexist to cater to different application requirements and be interchanged and federated as the technologies evolve.
2. Analyze and compare emerging ABC technologies with regard to their features, information flows, related security, performance, and other advantages and disadvantages in various application scenarios.
3. Develop reference implementations of these technologies that can be ported to different platforms or combination of platforms (e.g., PC, mobile phone, SIM, or NFC cards).
4. Identify application and business requirements to prepare pilot trials of some of the technologies.
5. Deploy pilot trials to validate the above architectural proposal, investigate ABC technologies in practice, and evaluate their usability in actual application and business scenarios.
6. Leverage the influence of the leading companies involved in ABC4Trust to target standardization and widely disseminate project outcomes, including organizing a summit event at the end of the project and publishing a book that makes knowledge of ABC technology and ABC4Trust pilots accessible to the general public.

The following project milestones will mark progress along the way to the project objectives. The selected milestones are both time-wise and content-wise defined in a manner that crucial decisions about the further roadmap can be made early enough to keep the objectives achievable.

Milestone 1 is the definition of first version of the architecture and of the pilot scenarios. This includes the architectural framework and the complete identification of the pilots' settings. All participants and their interactions must be defined so that the implementation of the pilots can begin. This milestone refers especially to Objectives 1, 2, 4, and 5.

Milestone 2 marks the point in time where the initial reference implementation and pilot software and the pilot software are ready for rollout. This very crucial milestone is the essential precondition for beginning the pilot trials. It refers especially to Objectives 3 and 5.

Milestone 3 is completing the pilot trials successfully. This milestone refers especially to Objectives 3, 4, and 5, but also to Objectives 1 and 2.

Milestone 4 is arranging a project summit event where all outcomes of ABC4Trust research and development are summarized and presented to a broader public. Besides presenting the results of each work package, there will be a more generalized summary of ABC4Trust as a whole. This milestone refers to all objectives, but especially to Objective 6.

Milestone 5 is the publication of the ABC4Trust Summit Book which shall bring all project outcomes and lessons learned to the general public. This milestone refers to all objectives, but especially to Objective 6.

The project will utilize two specific pilots to address possible tensions between accountability and privacy in two different application fields. Therefore Milestone 3 will actually include two pilot trials:

1. The first pilot application at a Swedish school will involve pseudonymous community access and social networking for school students (pupils). This pilot addresses the specific challenges posed by the fact that Internet users get ever younger and often are minors. Swedish schools today are mainly using the Internet for communication between teachers, pupils and parents. They are using different portals and private communities to make this communication possible. A big threat to the privacy of the pupils is unauthorized access to sensitive personal information such as individual plans, presence reports, grades, exam results and other information and functions available through the school portal. Several applications, such as social networking or privacy preserving student counselling or medical advice will benefit from the ABC4Trust project as it allows combining strong authentication and privacy protection into one solution. The proposed community will protect the pupils' identity against theft while protecting their privacy. On one hand, pupils will be able to identify themselves to access restricted chat rooms and restricted information. On the other hand they will be able to remain unnamed when asking private and sensitive questions from school personnel, while assuring the school personnel that it communicates with authorized pupils of the respective school or class. The pilot will help to gather information on the usability of the proposed ABC system under especially challenging usability conditions posed by children users.
2. The second pilot application at a Greek university will involve polling, especially anonymously collection of feedback from authorized students about the courses they took and the teachers who taught them. This pilot addresses the special challenge that for important and influential results of a poll to be correct and credible, the privacy of the people expressing their opinion must be preserved. Course evaluations have become standard practice in most universities in the industrial world. However they are typically conducted outside computers to protect the students' privacy. If they are conducted through computers, the computers are operated by a neutral trusted organization independent from the school doing the evaluation; otherwise the students need to put a lot of trust in the fairness and privacy practices of their school. ABC technologies will allow each university to issue its own students identity cards or badges, including lists of courses each student took. Thereafter the university will be able to run its own computerized feedback system without having to be trusted by the students, because the ABC technologies on the identity cards will sever all possible links between incoming electronic feedback and the identity of the student who submitted it while guaranteeing that feedback comes from duly accredited students. The pilot will help to gather information on the reactions of a typically critical group of users.

1.2 Progress beyond the state of the art

Key Takeaways

- ✓ A first contribution of this project to the state of the art will be the definition of a common unified architecture for federating and interchanging different ABC systems.
- ✓ A second contribution will be the elaboration of a metrics framework for comparing different ABC systems.
- ✓ The project will provide reference implementations for the components defining an ABC system.
- ✓ The project consortium will run the first ever pilots of ABC deployments in production environments.

- ✓ ABC4Trust will keep the ecosphere of application developers as well as technology providers informed and aware of progress in making ABC system usable.
- ✓ The integration of legal experts into the technical work packages in form of a horizontal activity will ensure that legal requirements will be known to the researchers at an early stage and enable short ways for interdisciplinary interchange.

1.2.1 State of the Art

The amount of daily transactions that we perform electronically is rising very fast. Many of us use the Internet on a daily basis for a number of purposes ranging from accessing information to electronic commerce and e-banking to interactions with government bodies. Securing these transactions requires the use of strong authentication. Electronic authentication tokens and mechanisms that provide this become common not only for the use with the Internet but elsewhere. Indeed, electronic identity cards, authentication by mobile phone, RFID tokens are spreading fast. These authentication mechanisms unfortunately have the shortcoming that they use unique identifiers that present the risk that transactions by the same user can be linked, thus seriously threatening the user's privacy.

In several application areas, unique identification is inappropriate and privacy-preserving attribute-based authentication is therefore desirable. Indeed, a position paper issued in February 2009 by ENISA on "Privacy Features of European eID Card Specifications" [ENISA09] underlines the need for "privacy-respecting use of unique identifiers" (personal number that uniquely identify a user) in emerging European eID cards, and explicitly refers to the emerging attribute-based credentials (ABC) technologies ("privacy-enhanced PKI tokens" in their terminology), as having significant potential in this arena. Also the EU-funded project FIDIS (www.fidis.net) has identified several scenarios, in which identification depends from appropriate privacy protection to be multilaterally trustworthy [RaRoDe09].

ABC technologies, often called anonymous credential systems in the literature [Cha85, Brands00; CamLys01, CamLys04], allow an identity service provider to issue a credential (or certificate) to a user. This credential contains attributes of the user such as address or date of birth but also the user's rights or roles as attributes. Using the credential, the user can prove to a third party that she possesses a credential containing a given attribute or role without revealing any other information stored in the credential. For instance, the user could use a government-issued anonymous ID credential to prove that she is of proper age, i.e., that she possesses a credential that contains a date of birth which is further in the past than 18 years. Thus, anonymous credentials promise to be an important cornerstone in protecting users' privacy in an electronic environment. Research has put forth a number of different proposals how to realise anonymous credentials [Cha85, Brands00; CamLys01, CamLys04] which are based on different number-theoretic problems and also differ somewhat in the functionality that they offer.

The EU-funded projects PRIME (www.prime-project.eu) and PrimeLife (www.primelife.eu) have actually shown that the state-of-the art research prototypes of ABC systems can indeed confront to this challenge. The PRIME project has designed architecture for privacy-enhancing identity management that combines anonymous credentials with attribute-based access control, and anonymous communication. That project has further demonstrated the practical feasibility with a prototypical implementation of that architecture and demonstrators for application areas such as e-learning and location-based services. PRIME has, however, also uncovered that in order for these concepts to be applicable in practice further research is needed in the areas of user interfaces, policy languages, and infrastructures. The PrimeLife project has set out in 2008 to take up these challenges and already has made very promising steps towards solutions in these areas. For instance, it has shown that ABC systems can be employed on Smart Cards and thus address the requirements of privacy-protecting eID cards [BCGS09]. Also, in the last decade, a large number of research papers have been published solve probably all roadblocks to employ ABC technologies in practice. This include means to revoke certificates [BrDeDe07, CamLys02, CaKoSo09], protection of credentials from malware [Cameni06], protection against credential abuse [CHKLM06, CaHoLy06], proving properties about certified attributes [CamGro08, CaChSh08], and means to revoke anonymity in case of misuse [CamSho03].

Despite all of this, the effort of understanding ABC technologies so-far was rather theoretical and limited to individual research prototypes. In fact, there is still no knowledge of how to apply ABC technology in concrete cross-domain federation scenarios. So far Prime and PrimeLife only showed that ABC technologies provide privacy-protection in principle. There exist a few ABC technologies, most prominently Microsoft's U-Prove [Brands00, U-Prove] and IBM's Identity Mixer [CamHer02], however these have different properties. There are no commonly agreed set of functions, features, formats, protocols, and metrics to gauge and compare these ABC technologies, and it is hard to judge the pros and cons of the different technologies to understand which ones are best suited to which scenarios. Thus, there is still a gap between the technical cryptography and protocol sides of these technologies and the reality of deploying them in production environments. A related problem with these emerging technologies is the lack of standards to deploy them. As a result the ENISA paper mentioned above observes that ABC "technologies have been available for a long time, [but] there has not been much adoption in mainstream applications and eID card applications" even though countries such as Austria and Germany have taken some important steps in this sense.

1.2.2 Progress beyond State of the Art in detail

ABC4Trust would provide progress beyond the state of the art in at least seven areas. They are listed below starting from more scientific to more generally strategic aspects:

1. A Framework for ABC Federation and Interchangeability (cf. 1.2.2.1)
2. Thorough Metrics for Comparison of existing ABC systems (cf. 1.2.2.2)
3. A Reference implementation for selected ABC systems (cf. 1.2.2.3)
4. Experience from Production of the Pilots (cf. 1.2.2.4)
5. Input for the European Electronic Identity Management Infrastructure (cf. 1.2.2.5)
6. Dissemination towards Leaders in Application and Technology (cf. 1.2.2.6)
7. Addressing Legal Questions in a horizontal activity (cf. 1.2.2.7)

1.2.2.1 A Framework for ABC Federation and Interchangeability

A number of standards and architectures exist to allow federation and interchangeability of identification schemes and mechanisms, e.g. Liberty Alliance, OpenID, OASIS Information Cards, etc. However such unified standards and architectures do not exist for federating and interchanging ABC systems.

A first contribution of this project to the state of the art will be the definition of such a common unified architecture for federating and interchanging different ABC systems in a way that

1. users will be able to obtain credentials for many ABC technologies and use them indifferently on the same hardware and software platforms,
2. service providers will be able to adopt whatever ABC technology best suits their needs, and
3. identity service providers will be able to accept credentials under one ABC technology and issue corresponding ones under another ABC technology, again using the same hardware and software platforms.

1.2.2.2 Thorough Metrics for Comparison of existing ABC systems

Identity-based credentials have been around for many years and there exist many examples and implementations of such technologies [X509, EMV, DANID, ESTID]. Attribute-based credentials (ABCs) that allow people to prove properties or attributes about themselves without necessarily revealing their exact identity are a more recent concept [Cha85, Brands00; CamLys01, CamLys04]. Only a few designs mentioned earlier – IBM's Identity Mixer [CamHer02] and Microsoft's recently released U-Prove [Brands00, U-Prove] technologies – have been proposed so far.

There is hardly any experience with implementing these, much less with deploying and using them in practice. In fact these technologies are at different stages of maturity and offer different potentials for

extensions and generalizations. For instance Identity Mixer is really a family of protocols of which there exists one proof of concept implementation while U-Prove [U-Prove] is a specification offering the core functionality of a much broader set of protocols [Brands00]. There is however no systematic way to analyze and compare these technologies. The project will provide a framework for doing so rigorously.

The project will contribute to the state of the art [Savo07, Savo08] by elaborating a metrics framework for comparing different ABC systems, component by component, along four dimensions: functional coverage, security properties, performance, and necessary as well as potential hardware support for performance or security reasons, specifically:

- A systematic functional overview and comparison of properties of different ABC systems – only ad-hoc overviews exist which do not provide any solid foundation for comparing functional properties.
- A systematic security analysis of available ABC protocols and systems – for some of them, the literature provides only heuristic security proofs.
- A systematic comparison of the relative performance one can expect from different ABC systems.
- A systematic analysis of what sort of hardware support each ABC system needs or can support for both enhanced security or enhanced performance purposes.
- Metrics for evaluating ABC systems along the above functional, security, performance and hardware support dimensions.

1.2.2.3 A Reference implementation for selected ABC systems

The project will provide reference implementations for the components defining an ABC system as defined by the architecture mentioned earlier, where for some of the components more cryptographic algorithms will be implemented. This will show the extent to which the different proposals for ABC systems are interoperable and is crucial to achieve the project's aim.

Implementations of ABC systems already exist for both Microsoft's U-Prove and IBM's Identity Mixer systems. However, these implementations follow different architectures; there are no commonly agreed sets of functions, features, formats, and protocols that would allow for federation or interoperability, let alone cooperation within some common scenario. A reference implementation conforming to the federated architecture framework will provide such improvements over the state of the art. It should even allow storing and managing credentials for either system in a common repository, possibly on smart cards. The reference implementation of ABC4Trust will be delivered embedded into example applications showing how to integrate the reference components to a user interface on a client and a server platform, such as Apache and Tomcat.

1.2.2.4 Experience from Piloting

The project consortium will run the first ever implementation of ABC systems in production environments. Thus this will be the first time that research on operation, interoperability, user acceptance, and so forth can be conducted in a real life environment. ABC4Trust will gather this experience in two specific environments. Having these two specific pilots will give us the opportunity to test credentials use and performance with two user groups of differing skills and needs. One user group will be children at a school environment in Sweden, whereas the other will be students at a Greek university. The use cases we are aiming for are quite different in order to cover a broad variety of requirements and thus as well credentials.

Furthermore the direction of information exchange differs with respect to whose privacy is protected (provider of information in Greece and requester of information or advice in Sweden) and the structure of information exchange differs (form-based in Greece vs. free-form chatting in Sweden). In this sense, the two trials are complementary and will provide feedback of distinct value to the developers of the reference implementation and therefore are needed as the project's real life research environment.

In ABC4Trust following use cases will be considered:

- Protecting the privacy of children in a school environment located in Sweden. This trial deals with online communication and exchange of sensitive personal concerns and advice between pupils and the school personnel. Pupils will be able to seek advice from doctors, nurses, psychologists and other coaches on intimate questions related to their physical, psychological, social, financial, or other situation without necessarily revealing their true identity.
- Remote course evaluation within universities. In this trial the students of a Greek university will be issued credentials that certify a number of facts about them (e.g. year of study, major, percentage of attendance of a course, etc.), allowing students with proper credentials to anonymously provide feedback on courses and teachers they had during a semester or school year. To be eligible to participate, the students' credentials should prove some facts about them, i.e. whether they have taken the course, the year of their first registration to the university department, and their course attendance ratio. The sufficiency of attendance will not be proven by revealing the exact attendance percentage (as this might be used to identify students), but by showing that it is above the predefined attendance threshold that allows the student to enter the evaluation process.

By taking into account the collection of criteria and the design / implementation of the necessary infrastructure (identity service provider, infrastructure to issue credentials [e.g. based on smart cards], attribute databases, etc.), the evaluation of these pilots will provide a clear proof of concept of both the unified anonymous credentials idea (harmonization of various ABC protocols) as well as the reference architecture, providing at the same time feedback for enhancements.

1.2.2.5 Input for the European Electronic Identity Management Infrastructure

Europe aims for an electronic identity management infrastructure as a basis for trustworthy services in e-government and e-commerce to overcome fragmentation, closed solutions and lack of user control and transparency [CEC09]. At the same time the position paper issued by ENISA on "Privacy Features of European eID Card Specifications" [ENISA09] underlines the need for "privacy-respecting use of unique identifiers" in emerging European eID cards, and explicitly refers to ABC technologies as having significant potential in this space.

ABC4Trust can deliver important input for the design of the upcoming electronic identity management infrastructure, and e.g. the related European Large Scale Action (ELSA) by e.g.:

- A protocol-independent understanding of ABC technology closing the gap between the architectural framework level and the crypto level, that slows down the adoption of ABC systems.
- Information on the federation of ABC systems to avoid dependence from just one ABC technology, which could result in a monopoly situation that would not be acceptable for an infrastructure.

ABC4Trust will keep this strategic dimension in mind when producing its reports and the related guidance documents and will also strive for an excellent relation to the stakeholders of the new infrastructures. Several stakeholders including member state infrastructure organisations responsible for electronic identity management as well as the EU co-funded project STORK (Secure idenTity acrOss boRders linKed) have showed interest in the project and in collaboration.

1.2.2.6 Dissemination towards Leaders in Application and Technology

ABC4Trust will keep the ecosphere of application developers as well as technology providers informed and aware of progress in making ABC system usable.

ABC4Trust will work with selected standardization bodies dealing with attribute-based credentials and will also approach domain-specific interoperability working groups, among others on e-government, to encourage them to integrate adequate concepts of attribute-based credentials.

The project's results will be disseminated to stakeholders. The Outreach Strategy will take into account different target groups and their specific interests. It will comprise ways to communicate the project's results as well as a plan for handling external collaboration and cooperation. The project will provide PR material for specific audiences so that they become aware of the potential of attribute-based credentials, understand better how they work and how they can be part of today's and upcoming applications. An important means to get input from stakeholders is the Reference Group which will be established by ABC4Trust. Its members will be asked for feedback on concepts and implementations done within the project.

The project's results will be summarized in the ABC4Trust book, which will mainly address ICT application developers ICT providers, researchers, and policy makers.

1.2.2.7 Addressing Legal Questions in a horizontal activity

Among legal practitioners and particularly company lawyers collecting relevant information to raise a civil lawsuit or to enable criminal prosecution is a necessary and common practice. Deploying Identity Management tools, let alone ABC technologies, is hindered by such legal practices. Collecting and identifying such obstacles across legal domains in EC law and some selected national laws is a necessary prerequisite to successfully deploy ABC technologies. Deriving necessary legal requirements for ABC technologies and the evaluation how ABC technologies can solve these factual and legal problems will bring legal research beyond the state of the art, e.g. by enabling anonymous transactions in online relations while providing a method to raise claims in civil actions. Whether this necessarily includes a fast, trusted and reliable way to revoke anonymity as could be provided by Attribute-based Credentials and if so under which conditions anonymity may be revoked to pursue civil claims are legal questions that ABC4Trust will address. Offered solutions may also comprise specifying recommendations for EC or national legislators regarding the incorporation of Attribute-based Credentials in a European eID scheme, defining the evidentiary value of credentials within civil lawsuits or on regulations deciding which court or body is competent to decide upon the conditions for the revocation of anonymity, when the domicile is unknown. Results of the research may be communicated to the relevant stakeholders such as the Art. 29 Working Party.

The integration of the legal experts into the technical work packages in form of a horizontal activity will ensure that legal requirements will be known to the researchers at an early stage and enable short ways for interdisciplinary interchange. This will be continued by a legal evaluation of the pilots. This way legal conformity with relevant directives on data protection is ensured.

1.3 S/T Methodology and associated work plan

1.3.1 Overall strategy and general description

The project is arranged into 6 technical work packages as well as one management work package, one dissemination work package, and one horizontal activity (cf. Figure 4).

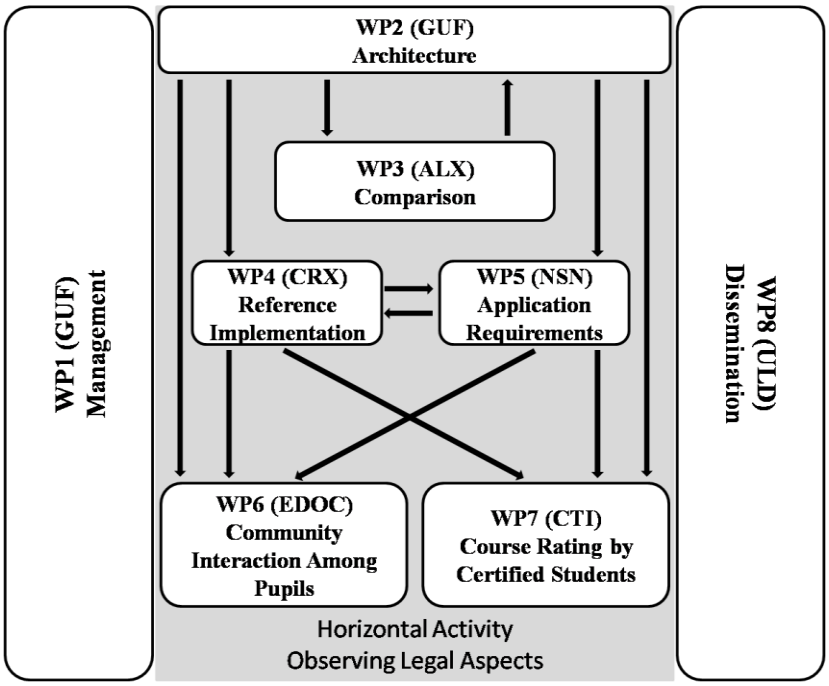

Figure 4: Work Package Structure

WP2 – Architecture – will develop a common architecture for federating ABC systems. This architecture will be the basis for the comparison of existing ABC systems in WP3, for their reference implementations in WP4, and for their deployment in the application pilots of WP6 and WP7. It will define

1. a modular decomposition of the mechanisms necessary for supporting ABC systems into functional modules,
2. common formats and APIs for interaction between these modules running on a common platform, and
3. formats and protocols for communication between peer modules running on different platforms involved in a common transaction across the network.

WP3 – Comparison – will compare different ABC systems, module by module, along four dimensions: functional coverage, security properties, performance, as well as potential hardware support for performance or security reasons. WP2 and WP3 are mutually dependent on one another in the sense that doing the component by component comparison in WP3 requires the modular decomposition defined in WP2 but the best way to define this decomposition will be influenced by the functional and architectural differences of already existing ABC implementations.

WP4 – Reference Implementation – will produce a reference implementation of the two major ABC systems (Identity Mixer and U-Prove) existing today in conformance with the WP2 architecture and wrap it in a toy application environment to illustrate and ease deployment of such a reference implementation in the WP6 and WP7 pilots or in future production environments.

WP5 – Application Requirements – will collect the requirements of the pilots that the project will run and evaluate them. It will further provide the basic infrastructure that is needed by those trials.

WP6 – Community Interaction Among Pupils – will realize a research trial environment where pupils (youngsters and teenagers of both sexes) in an anonymous and privacy preserving way can communicate with other pupils and with school health personnel (doctors, nurses, psychologists and other coaches). Pupils will be able to ask very private questions about their sexuality, weight and other physical and psychological health problems. Focus of the research of this WP is conducting the

investigation on how the pupils make use of privacy enabling functionalities of the employed ABC systems as well as the integration of the ABC systems into a newly developed real life application.

WP7 – Course Rating by Certified Students – will realize a second research trial environment where university students can anonymously rate courses they took while ensuring that 1) students have indeed taken the course and have had sufficient attendance (i.e. attribute based credentials will be employed to prove these facts) and 2) can only rate the course once, without keeping list of students who have already rated the courses, so as to protect student anonymity. Research focus of this WP is to investigate on how students make use of the privacy enabling functionalities of the employed ABC systems as well the implementation of the systems in an existing environment.

WP8 – Dissemination – will disseminate the project's results to a variety of stakeholders. It will organise the work on standardization and gather feedback on concepts and implementations from the project's Reference Group.

To ensure compliance with the data protection directive and other relevant regulations ULD will provide its legal expertise to the whole project thereby forming a **horizontal activity** across all R&D work packages. Inter alias legal requirements will be provided and discussed with the involved group of technical researchers. In particular the two work packages focusing on the research of ABC function implementation and usage (WP6, WP7) will be supported with specific legal advice, low-level requirements and an evaluation. This horizontal activity approach was specifically chosen to avoid mutual "isolation" of the work on legal issues and that on technical questions.

1.3.2 List of selected public deliverables and approximate publication dates

Deliverable name	**planned date**
Architecture for Attribute-based Credential Technologies – Version 1	Y2
Architecture for Attribute-based Credential Technologies – Final Version	Y4
Benchmarking criteria	Y4
Scientific comparison of ABC protocols	Y4
Description of the `common denominator' elements	Y2
Public website	Y1
Standardization Workshop	Y3-4
Architecture for Standardization V2 (Final)	Y4
Reference Implementation for Standardization V2	Y4
Final Event	end of project
ABC4Trust Book	end of project

Table 1: List of Deliverables

2. ABC4TRUST CONSORTIUM

Key Takeaways

- ✓ ABC4Trust consists of 12 well known partners from 5 EU Member States and Switzerland. All partners of the Consortium are well recognized players in their competence area.
- ✓ Industry partners are IBM, Microsoft, and Nokia-Siemens Networks.
- ✓ Universities of Frankfurt and Darmstadt as well as the non-profit research institutes R.A.CTI and The ALX Institute put together their research competences.
- ✓ CryptoExperts, Eurodocs, and Miracle A/S bring in the perspective of SMEs, Söderhamn Kommun and ULD that of Governmental Organizations.

2.1. Johann Wolfgang Goethe-Universität Frankfurt (GUF)

Johann Wolfgang Goethe-Universität, Frankfurt – Germany: The Chair for Mobile Business and Multilateral Security is part of the Institute of Business Informatics. Enjoying sponsorship by T-Mobile (the leading German mobile communications provider) the chair focuses its research on innovative mobile networks and their applications, as well as on related issues of security and privacy. Its mission is to find business models and technologies enabling the secure and privacy enabled use of mobile devices and mobile communication for applications and businesses. Typical research interests include:

- Mobile applications and Multilateral Security in e.g. M-Business, M-Commerce, M-Banking, and Location Based Services;
- Privacy and identity management, communication devices and infrastructures, such as personal security assistants and services;
- IT security evaluation and certification.

Based on numerous successful projects within the last years, like PRIME or FIDIS, the current research schedule contains projects such as PICOS, PrimeLife, ABC4Trust, GINI-SA, and PREMIUM-Services. The research activities in these projects are concerned with aspects of privacy and identity management in emerging internet applications and, especially in (mobile) community services (PICOS, PrimeLife, ABC4Trust, GINI-SA), as well as mobile marketing and context sensitive customer pricing aspects in mobile application scenarios (PREMIUM-Services). In addition, further research is conducted in close collaboration with T-Mobile / Deutsche Telekom as benefactor of the chair, with other major industry players and stakeholders in the civil society, and by active participation in ISO/IEC Standardisation activities (ISO/IEC JTC 1/SC 27/WG 5 “Identity Management and Privacy Technologies”).

2.2. Alexandra Institute AS (ALX)

The Alexandra Institute is a privately held non-profit SME with approximately 80 employees. ALX is located in Aarhus, Denmark, and is recognized by the Danish government as an advanced technology provider.

ALX focuses on applied research in computer science and has a proven track record in bridging the gap between research and industry. ALX has (among other areas) a focus on IT security with a particular focus on applied cryptography. ALX has strong competencies in moving theoretical computer science results into practical software. Focus has in particular been on implementing Secure Multiparty Computation (in the recent Danish "SIMAP" project as well as the ongoing FP7 project CACE).

2.3. Research Academic Computer Technology Institute (CTI)

The Research Academic Computer Technology Institute (R.A.CTI) is a non-profit institute for research and development in Information and Communications Technologies (ICT), supervised by the Greek Ministry of Education and operating under administrative and scientific independence. Its personnel consist of faculty members, researchers, scientific and administrative personnel as well as external fellow researchers. The Security Sector of R.A.CTI, involved in this project, is actively involved in information systems security conducting basic and applied research in this field.

2.4. IBM Research GmbH (IBM)

IBM Zurich Research Laboratory (IBM Research GmbH) is the European branch of IBM's Research Division. The lab employs more than 200 researchers from over 20 countries, working on projects in computer science, communications, optoelectronics, and physics. In the area of information security, more than 20 researchers are focusing on privacy, cryptography, secure systems, and security management. The IBM Zurich Research Laboratory played a leading role in the development of IBM's Enterprise Privacy Architecture (EPA), and has several research projects related to privacy-friendly technologies, e.g., identity mixer (a privacy-enhanced pseudonym-based public key infrastructure), EPAL (a language and architecture for defining and enforcing enterprise privacy policies), and CDIM (a set of protocols for browser-based attribute exchange and federated identity management). The lab has participated regularly in projects funded by the European Union and other government sources. Much of this research has become or had a direct influence on IBM's products and services. Recent project engagements in EU-FP6 and FP7 include PrimeLife, PRIME, ECRYPT, FIDIS, and OpenTC. IBM ZRL was the technical leader in the EU FP6 funded project PRIME (www.prime-project.eu) and currently is leading the EU FP7 project PrimeLife (www.primelife.eu)

2.5. Miracle (MCL) A/S

Miracle (MCL) is a privately held SME with approximately 150 employees in Denmark with expertise in the areas of consultancy, project management, software development, integration and optimization of IT systems and business processes. Miracle is considered one of the leading companies in terms of expertise in database-centric platforms, and is renowned for its ability to rescue systems and databases, where others have had to give up.

Since 2005, Miracle has been responsible for delivering services in consulting, integration, technology innovation, system and software development for both private clients and the public sector. Security-wise, Miracle has for some years worked with the National IT and Telecom Agency on design and implementation of RASP (Reliable Asynchronous Secure Profile) and later also on development tasks within The PEPPOL EU Project (Pan-European Public Procurement Online). In September 2009 the electronic system for Property and Land Registration was launched in Denmark, to which Miracle has been a subcontractor in the areas of security and integration with existing systems.

2.6. Nokia-Siemens Networks (NSN)

Nokia Siemens Networks is a leading global enabler of telecommunications services. With its focus on innovation and sustainability, the company provides a complete portfolio of mobile, fixed and converged network technology, as well as professional services including consultancy and systems integration, deployment, maintenance and managed services. It is one of the largest telecommunications hardware, software and professional services companies in the world. Operating in 150 countries, its headquarters are in Espoo, Finland. The research group involved in this project has participated regularly in funded projects and transferred its results into the relevant business units. Recent involvements in European projects include SIMPLICITY, SPICE, or SERVERY.

2.7. Technische Universität Darmstadt (TUD)

TUD is Germany's premier Technical University and especially for Computer Science. Since its foundation in 1877, TUD has stood for internationalization and pioneering achievements. TUD is one

of the three best technical universities in Germany. It is an autonomous university which provides for self responsibility and flexibility, and leads to creative freedom and enthusiasm. TUD was elected as the Best-Practice University in Germany in 2002. According to many rankings, the CS department of the TUD is among Germany's best CS departments. TUD has developed to become one of the leading research centres for IT security and dependability in Europe. The Darmstadt Centre for IT Security was founded in 2002 as a central institution of TUD. The Centre bundles the activities of many TUD research groups, among them DEEDS. Currently 18 professors from the faculties of Business Administration, Economics and Law, Mathematics, Physics, Electrical Engineering and Information Technology, as well as Computer Science are associated with the Darmstadt Centre for IT Security. Within the CS department, the DEEDS (Dependable Systems and SW) Group specifically targets research for the development, assessment and validation of systems, services and protocols as an infrastructural basis for trustworthy systems and services. The group is internationally renowned for its dependability/security research and has garnered support from the European Commission, US NSF, US DARPA, Airbus, Audi, Saab, Volvo, Daimler, NASA, IBM, Boeing, Microsoft and Intel etc.

2.8. Unabhängiges Landeszentrum für Datenschutz (ULD)

Unabhängiges Landeszentrum für Datenschutz (ULD, Engl. Independent Centre for Privacy Protection) is the Data Protection Authority of Schleswig-Holstein, the northernmost Federal State of Germany. Its office with 40 employees is located in Kiel, Germany. The Privacy Commissioner of Schleswig-Holstein, Dr. Thilo Weichert, is head of ULD. ULD is responsible for both data protection and freedom of information in Schleswig-Holstein.

The basis for the work of ULD is laid down in the State Data Protection Act Schleswig-Holstein. This act is one of the most progressive ones worldwide and includes among others provisions on a seal of privacy for IT products and on privacy protection audits for public authorities. In addition to the privacy seal based on German national and regional law, ULD is coordinating the European Privacy Seal initiative EuroPriSe which grants privacy seals on the European level in case of a successful evaluation of compliance to European regulation.

Since 1998 ULD has been working on several national and international projects in the field of data security and privacy protection, among others, the EU-funded IST projects “FIDIS – Future of Identity in the Information Society”, “PRIME – Privacy and Identity Management for Europe” and PrimeLife.

2.9. Eurodocs AB (EDOC)

Eurodocs AB is a next generation IT Company that puts its efforts and power into developing smart, innovative and useful solutions focusing primarily on protecting the identity, anonymity and privacy of internet users. The company has in the last years brought forward new IT solutions that can be described as Web2.0S – where the ”S” stands for Security. The company was registered in 2000. Eurodocs vision is to make life easier for all users of online security identification. Our business concept is to combine security, user-friendly and cost-effective solutions together with powerful safety onto online personal integrity. Eurodocs does work for big and established companies and clients, such as TNS-Gallup, AstraZeneca, Fortum and Försäkringskassan (Swedish Regional Social Insurance Office). Eurodocs has received a lot of interest from the market. Recently, the CEO and founder Souheil ”Sosso” Bcheri has been rewarded by ALMI as Pioneer of The Year 2008 in Gävleborg (Sweden).

2.10. CryptoExperts (CRX)

CryptoExperts is a young start-up company founded by widely recognized industrial and academic researchers in IT security and cryptography. The company offers externalized R&D and consulting services in a wide variety of security areas, including advanced security evaluation of cryptographic software, products and services. The cryptographic expertise of the company includes: proof-based analysis of cryptographic systems and protocols, on-demand design of new cryptographic systems (access control, e-passports, secure storage, electronic commerce and e-cash systems, electronic voting, e-government applications, broadcast encryption and traitor tracing, digital signatures and

encryption with specific properties), practical applications of cryptography, security architectures, design and implementation of cryptographic libraries for embedded systems on specific hardware (crypto-processors, smart cards, USB tokens, HSM, etc), and security evaluation of cryptographic implementations (side-channel and fault-based analysis).

CryptoExperts has a research group of well-recognized experts in cryptography. Research areas include provable security for security infrastructures and application; the design and security evaluation of cryptographic functions, schemes and protocols; secure implementations and the physical security of embedded systems. Therefore the group's technical expertise simultaneously covers theoretical and very practical aspects of cryptographic systems.

User privacy and anonymity, and applications thereof (e.g. e-cash, e-vote) are long-lived research topics for the group members.

2.11. Microsoft Research And Development France (MS)

Microsoft Research and Development France dedicate itself to research activities related to software using Internet Search technologies and, more generally, to any type of applications and services for computers, Internet networks, telematics or networks online and mobile.

2.12. Söderhamn Kommun (SK)

Söderhamn is an active municipality in terms of ICT and school issues. Söderhamn has large commitment and are working hard to increase the number of ICT technology in teaching.

As an education provider with responsibility for children up to the age of 20 (according to national legislation the municipalities have a responsibility for children/young people up to the age of 20) it is important for us that our students can feel safe in their ICT usage and therefore the ICT security and issues relating to student privacy is paramount.

3. IMPACT

Key Takeaways

- ✓ ABC4Trust promotes European privacy values in infrastructures and provides opportunities to advance European technological leadership in this field.
- ✓ ABC4Trust will support the future European Electronic Identity Management Infrastructure and e.g. the related European Large Scale Action (ELSA)
- ✓ ABC4Trust's pilots empower individuals and communities by increasing accountability, trustworthiness of information and allowing more elaborate access control, yet in a privacy preserving way.
- ✓ ABC4Trust's outcomes will help to increase productivity, stay ahead with non-EU competitors, and earn revenue with security and privacy-enhanced technologies.
- ✓ ABC4Trust will enable new types of services and will clearly lower the threshold for hesitating individuals to partake in online interactions.

ABC4Trust will have a major impact in line with the impacts expected in Objective ICT-2009.1.4: Trustworthy ICT:

- Demonstrable improvement of the trustworthiness of increasingly large scale heterogeneous networks and systems and in protecting against and handling of network threats and attacks and the reduction of security incidents.
- Significant contribution to the development of trustworthy European infrastructures and frameworks for network services; improved interoperability and support to standardisation. Demonstrable usability and societal acceptance of proposed handling of information and privacy.

- Improved European industrial competitiveness in markets of trustworthy ICT, by: facilitating economic conditions for wide take-up of results; offering clear business opportunities and consumer choice in usable innovative technologies; and increased awareness of the potential and relevance of trustworthy ICT.
- Adequate support to users to make informed decisions on the trustworthiness of ICT. Increased trust in the use of ICT by EU citizens and businesses. Increased societal acceptance of ICT through understanding of legal and societal consequences.

The impacts that can specifically be expected from ABC4Trust are described in the following subchapters.

3.1. Promoting European Privacy Values in Infrastructures

Europe has taken a specific direction with respect to privacy protection. The right to respect for private and family life, home and correspondence are deeply rooted in the European Convention on Human Rights and have since been the foundation for extensive regulation on privacy and data protection. Privacy protection in Europe is geared towards protection of a right to respect and personal dignity as well as to data minimisation and minimum disclosure as basic implementation principles on the infrastructural level. At the same time privacy is supported by an organisational infrastructure of e.g. Privacy Commissioners. This reflects the European care for dependable infrastructures.

ABC systems and protocols as well as the architectures enabled by them support privacy friendly approaches on the infrastructure level. ABC4Trust designs an architecture and interfaces that allow for the dependable deployment of ABC systems by e.g. avoiding the dependency from just one technology. Therefore ABC4Trust contributes to the promotion of European privacy values on the infrastructure level. This strong embedding of European privacy values into technology design developed by ABC4Trust provides opportunities to advance and show European technological leadership in this field.

3.2. Supporting the European Electronic Identity Management Infrastructure

Europe aims for an electronic identity management infrastructure as a basis for trustworthy services in e-government and e-commerce to overcome fragmentation, closed solutions and lack of user control and transparency [CEC09]. At the same time a position paper issued by ENISA on “Privacy Features of European eID Card Specifications” [ENISA09] underlines the need for “privacy-respecting use of unique identifiers” in emerging European eID cards, and explicitly refers to ABC technologies as having significant potential in this space.

ABC systems enable trustworthy identity management and trust relations between users and service providers while respecting privacy. Yet none of these technologies has been successfully deployed so far for lack of architectural guidance and practical experience. ABC4Trust develops and trials an ABC enabled architecture and related application pilots. This will result in important input for the design of the upcoming electronic identity management infrastructure, and e.g. the related European Large Scale Action (ELSA) by e.g.:

- A protocol-independent understanding of ABC technology closing the gap between the architectural framework level and the crypto level, that slows down the adoption of ABC systems
- Information on the federation of ABC systems to avoid dependence from just one ABC technology, which could result in a monopoly situation that would not be acceptable for an infrastructure.

3.3. Empowering Individuals and Communities

The ABC4Trust application trials will show how individuals and communities can overcome the limitations of nowadays Internet identity systems and Web 2.0 services. Today due to privacy reasons, many people hesitate to share their experience and opinions in today’s online platforms. At the same

time, people searching for reports on past experience with services or for health-related information is very careful about information found in today's Internet. A collaborative network that provides privacy while at the same time ensures that the given information is authentic would be a great step forward.

ABC enabled identity management will allow users to act pseudonymously in e.g. social networking systems, so that they can freely voice their opinion or provide their knowledge. At the same time ABC enabled identity management can support age verification to allow more secure access regulation for these social networks hindering unauthorised and unqualified parties from misuse. So individuals have more opportunities to express themselves in legitimate ways; while communities, e.g operators of social networks for pupils, can protect their clients from unwanted interactions.

3.4. Security and Privacy as Business Values for European Industry

ABC4Trust builds on and further develops technologies that are firmly rooted in European research. These technologies will be of growing importance in a world that will realise the importance of preserving citizen and customer privacy, e.g. in Web 2.0. European providers and European Industry will profit from the architectural and application pilot leadership ABC4Trust will show, and from the dependable infrastructure ABC4Trust will support.

3.5. Enabling new types of Services in Europe

ABC4Trust addresses emerging environments where privacy issues withhold potential users from participating, such as social networks, or refrain from voicing their opinion or providing their knowledge. An EU report [EU03] shows that "the impact of security concerns on people's willingness to shop or bank on-line is by far stronger in Europe than in the United States, although there are national specifications." This is a clear disadvantage for European online markets, and in consequence for the European industry. The potential impact of missing standards, security, and privacy mechanisms is explained in more detail by Gartner Research [WeBr06]. One of their key findings is that "standards (or lack of them), consumer privacy concerns, controlling or protecting content, and legacy IT present barriers to Web 2.0 implementation."

The results from ABC4Trust will enable European providers to build systems based on ABC technologies and offer privacy enhanced services as well as to make use of an ABC enhanced electronic identity management infrastructure. European providers will profit from the expertise ABC4Trust will communicate, especially the decision support and implementation guidance given by the project's reports, and the experiences from the ABC application pilots.

BIBLIOGRAPHY

[BCGS09] Patrik Bichsel, Jan Camenisch, Thomas Gross, Victor Shoup: Anonymous Credentials on a Standard Java Card. In ACM Computer and Communications Security 2009

[Brands00] Stefan Brands: Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy. First Edition, August 2000.

[BrDeDe07] Stefan Brands, Liesje Demuynck, Bart De Decker: A Practical System for Globally Revoking the Unlinkable Pseudonyms of Unknown Users. ACISP 2007: 400-415

[CaChSh08] Jan Camenisch, Rafik Chaabouni, Abhi Shelat: Efficient Protocols for Set Membership and Range Proofs. ASIACRYPT 2008: 234-252

[CaHoLy06] Jan Camenisch, Susan Hohenberger, Anna Lysyanskaya: Balancing Accountability and Privacy Using E-Cash (Extended Abstract). SCN 2006: 141-155

[CaKoSo09] Jan Camenisch, Markulf Kohlweiss, Claudio Soriente: An Accumulator Based on Bilinear Maps and Efficient Revocation for Anonymous Credentials. Public Key Cryptography 2009: 481-500

[Cameni06] Jan Camenisch: Protecting (Anonymous) Credentials with the Trusted Computing Group's TPM V1.2. SEC 2006: 135-147

[CamGro08] Jan Camenisch, Thomas Groß: Efficient attributes for anonymous credentials. ACM Conference on Computer and Communications Security 2008: 345-356

[CamHer02] Jan Camenisch, Els Van Herreweghen: Design and Implementation of the Idemix Anonymous Credential System. Research Report RZ 3419, IBM Research Division, June 2002. Also appeared in ACM Computer and Communication Security 2002

[CamLys01] Jan Camenisch, Anna Lysyanskaya. Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation. In Birgit Pfitzmann, editor, EUROCRYPT 2001, volume 2045 of LNCS, pages 93-118. Springer Verlag, 2001.

[CamLys02] Jan Camenisch, Anna Lysyanskaya: Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials. CRYPTO 2002: 61-76

[CamSho03] Jan Camenisch, Victor Shoup: Practical Verifiable Encryption and Decryption of Discrete Logarithms. CRYPTO 2003: 126-144

[CamLys04] Jan Camenisch, Anna Lysyanskaya: Signature Schemes and Anonymous Credentials from Bilinear Maps. CRYPTO 2004: 56-72

[CEC09] Communication from the Commission of the European Communities: A Strategy for ICT R&D and Innovation in Europe: Raising the Game; COM(2009) 116 final; 2009-03-13; ISBN 978-92-79-11158-7; http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=4698

[Cha85] David Chaum, Security without identification: Transaction systems to make big brother obsolete. Communications of the ACM, 28(10):1030-1044, October 1985.

[CHKLM06] Jan Camenisch, Susan Hohenberger, Markulf Kohlweiss, Anna Lysyanskaya, Mira Meyerovich: How to win the clonewars: efficient periodic n-times anonymous authentication. ACM Conference on Computer and Communications Security 2006: 201-210

[DANID] DanID, https://danid.dk/

[EMV] EMV Specifications, www.emvco.com/specifications.aspx

[ENISA09] European Network and Information Security Agency: “Privacy Features of European eID Card Specifications”, February 2009, www.enisa.europa.eu/act/it/eid/eid-cards-en

[ESTID] ID, www.id.ee/?lang=en

[FiWäZw09] Fischer-Hübner, S., Wästlund, E., Zwingelberg, H. (Eds.), UI prototypes: Policy administration and presentation version 1, PrimeLife deliverable D4.3.1, published 2009, www.primelife.eu/images/stories/deliverables/d4.3.1-ui_prototypes-policy_administration_and_presentation_v1.pdf.

[HRSZ09] Hansen, M., Raguse, M., Storf, K., Zwingelberg, H. , Privacy from Womb to Tomb – Delegation from a European Perspective, in Proceedings of the fifth IFIP WG9.2,9.6/11.4, 11.6, 11.7/PrimeLife International Summer School, Nice, France, September 7-11, 2009, published 2010.

[JoMu07] Andréas Johansson and Brendan Murphy, "Failure Analysis of Windows Device Drivers", Reliability Analysis of System Failure Data, Cambridge UK, 2007

[JoSaSu06] A. Johansson, C. Sârbu, N. Suri "When is the Right Time to Inject an Error?", a fast abstract in International Conference on Dependable Systems and Networks (DSN), Philadelphia, USA, June 25 - 27, 2006

[JoSu05] Andréas Johansson and Neeraj Suri, "Error Propagation Profiling of Operating Systems", Proceedings of International Conference on Dependable Systems and Networks (DSN), Yokohama, Japan, June 28 - July 1, 2005

[JoSuMu07] Andréas Johansson, Neeraj Suri and Brendan Murphy, "On the Impact of Injection Triggers for OS Robustness Evaluation", in Proceedings of the International Symposium on Software Reliability Engineering (ISSRE), 2007

[JSM07] Andréas Johansson, Neeraj Suri and Brendan Murphy, "On the Selection of Error Model(s) For OS Robustness Evaluation", Proceedings of International Conference on Dependable Systems and Networks (DSN), 2007

[Keri06] John E. Kerivan "Heuristic Security-Testing Methods", Journal of Digital Forensic Practice, Volume 1, Issue 1, March 2006 – ISSN 1556-7281, http://www.ngran.com/images/HSTM1v3.pdf

[MaKaWi07] P. K. Manadhata, D. K. Kaynar, J. M. Wing: A Formal Model for A System's Attack Surface, CMU Technical Report CMU-CS-07-144, July 2007.

[MeScRo07] Peter Mell, Karen Scarfone, Sasha Romanosky, A Complete Guide to the Common Vulnerability Scoring System (CVSS), version 2.0, June, 2007, www.first.org/cvss/cvss-guide.html

[RaRoDe09] Kai Rannenberg, Denis Royer, André Deuker: The Future of Identity in the Information Society – Challenges and Opportunities, 2009, Springer, Heidelberg et al., ISBN 978-3-540-88480-4

[Rannen00] Kai Rannenberg: Multilateral Security – A concept and examples for balanced security; Pp. 151-162 in: Proceedings of the 9th ACM New Security Paradigms Workshop 2000, September 19-21, 2000 Cork, Ireland; ACM Press; ISBN 1-58113-260-3

[SaJoSa05] C. Sârbu , A. Johansson and A. Sârbu "On Improving Robustness Testing of COTS OS Extensions" – a fast abstract in High Assurance Systems Engineering Conference (HASE 2005 - supplement), Heidelberg, Germany, October 13 - 14, 2005.

[SaJo06] C Sârbu , A. Johansson "Behavior-Driven Testing of Windows Device Drivers", a fast abstract in International Conference on Dependable Systems and Networks (DSN), Philadelphia, USA, June 25 - 27, 2006

[SaSu08] C. Sârbu, N. Suri "On Building (and Sojourning) the State-space of Windows Device Drivers", SSEAT'08, in Proc. of International Symposium on Software Testing and Analysis (ISSTA'08), Seattle

[Savo07] Reijo Savola: Towards a Security Metrics Taxonomy for the Information and Communication Technology Industry, International Conference on Software Engineering Advances (ICSEA), 2007.

[Savo08] Reijo Savola: A Novel Security Metrics Taxonomy for R&D Organisations, Proceedings of the Innovative Minds Conference (ISSA), 2008

[SJFS06] C. Sârbu, A. Johansson, F. Fraikin and N. Suri "Improving Robustness Testing of COTS OS Extensions", in Proc. of the 3rd International Service Availability Symposium (ISAS'06), Helsinki, in Springer LNCS 4328, pp. 120-139

[SJSN08] C. Sârbu, A. Johansson, N. Suri and N. Nagappan "Profiling the Operational Behavior of OS Device Drivers", in Proc. of 19th International Symposium on Software Reliability Engineering (ISSRE'08), Seattle / Redmond, pp. 127-136

[StHaRa09] Storf, K., Hansen, M., Raguse, M. (Eds.), Requirements and concepts for privacy-enhancing daily life, PrimeLife internal deliverable H1.3.5, http://www.primelife.eu/results/documents

[U-Prove] Microsoft Corporation. U-Prove Community Technology Preview. www.microsoft.com/u-prove

[WeBr06] Allen Weiner, James Brancheau. The Web 2.0 Challenge for Media Companies. Gartner Research, 5 May 2006.

[WNZD06] Chris Wysopal, Lucas Nelson, Dino Dai Zovi, and Elfriede Dustin "The Art Of Software Security Testing: Identifying Software Security Flaws" Addison-Wesley press, ISBN 0-321-30486-1, 2006

[WSJS09] S. Winter, C Sârbu, A. Johansson and N. Suri "Impact of Error Models on OS Robustness Evaluations", a fast abstract at the International Symposium on Software Reliability Engineering (ISSRE), Mysuru/Bangalore, India, Nov. 2009, www.issre2009.org/papers/issre2009_237.pdf

[X509] Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, www.itu.int/rec/T-REC-X.509/en