prisma cloud

Privacy and Security Maintaining Services in the Cloud

Contract Number: 644962

Call: H2020-ICT-2014-1

Deliverable D2.1

LEGAL, SOCIAL AND HCI REQUIREMENTS

Deliverable due date: 01.11.2015

Document Information	
Title	Legal, Social and HCI Requirements
Editors	Alaa Alaqra, Simone Fischer-Hübner, John Sören Pettersson
Deliverable no.	D2.1
Work Package No.	WP 2
Nature	Report
Dissemination Level	Public
Date	04. May 2016
Reviewers	Thomas Länger (UNIL), Daniel Slamanig (TU GRAZ), Marco Decandia Brocca (LISPA), Peter Wolf (MPL)

Authors List

Organization	Name	E-mail
UKARL	Alaa Alaqra	Alaa.alaqra@kau.se
UKARL	Simone Fischer-Hübner	Simone.Fischer-Hübner@kau.se
UKARL	John Sören Pettersson	john_soren.pettersson@kau.se
UKARL	Frank van Gelllerken	frank.vangeelkerken@kau.se
UKARL	Erik Wästlund	erik.wastlund@kau.se
UKARL	Melanie Volkamer	Melanie.volkamer@kau.se
UNIL	Thomas Länger	thomas.laenger@unil.ch
UNI PASSAU	Henrich C. Pöhls	hp@sec.uni-passau.de

Further Contributors

The following persons/organisations contributed to the organisation of the focus groups, surveys and interviews:

Thomas Lorünser (AIT), Christian Wagner (AIT), Daniel Slamanig (TU Graz), Thomas Gross (Uni Newcastle), Helmut Aschbacher (Xitrust), Marco Decandia Brocca (LISPA), Santiago Cáceres Elvira (ETRA).

List of Contents

List of Tables

List of Figures

1. Executive Summary

This Deliverable presents legal, social, and HCI (Human Computer Interaction) requirements for the PRISMACLOUD project, which were elicited within the first nine months of the project for clarifying the legal status of novel signature schemes to be used in the project and for following a human-centred design approach.

Legal requirements for malleable and functional signatures, which will be used in PRISMACLOUD for enhancing privacy and verifiability of cloud computing, were derived through an analysis of the EU Regulation on Electronic Identification and Trust Services (EU 910/2014). The analysis concludes that the legal status of both malleable and functional signatures can, depending on the cryptographic properties of the signature scheme, be regarded as similar to that of a qualified electronic signature that has the same legal effect as a handwritten signature.

Literature studies helped us to elicit on social factors determining end user trust and technology acceptance that may be of importance for PRISMACLOUD, such as: comprehensibility of the extent to which they can act under pseudonyms and the properties, underlying assumptions and remaining risks of pseudonyms; trust that one can manage in a life-long way the information associated with different identities; awareness of trustworthy assessments of trustworthiness; perception of external control; perceived security and privacy; and actual privacy/security guarantees.

For eliciting more in depth end user and HCI-related requirements, we conducted semi-structured interviews, surveys and focus groups with end users and key stakeholders that have a good understanding of the end user needs and expectations. The results of these elicitation activities are in particular confirming the need of usable guidelines, suitable metaphors and policies for the handling of personal data, clarifying the roles, rights and restrictions of actors for the use of malleable and functional signatures and other PRISMACLOUD crypto functions as well as templates for enforcing such restrictions.

Branding, standardization and certification schemes as well as a restriction to private and/or European-based cloud will also play an important role for establishing end user trust in PRISMACLOUD solutions.

Finally, in the end, this deliverable provides a table summarising all elicited requirements, which are further classified into the topologies system requirements, user/human factor, usability and/or general requirements. These topologies specify the nature of the requirements to indicate by which type of developers the requirements should be addressed.

2. Abbreviations and acronyms

ABC	Attribute Based Credentials
AS	Advanced electronic signature
BS	Basic electronic signature
DMA	Direct Marketing Association
dMS	Derived malleable signature
DoS	Denial of Service
ECC-net	European Consumer Centres Network
eIDAS	Regulation on Electronic Identification and Trust Services (EU 910/2014)
ESD	Electronic Signature Directive
EU	European Union
FS	Functional signature
GPS	Geographic Positioning System
HCI	Human Computer Interaction
ICT	Information and Communication Technology
FPE	Format preserving encryption
FPT	Format preserving tokenisation
MS	Malleable signature
NFC	Near Field Communication
OPE	Order preserving encryption
OPT	Order preserving tokenisation
PKI	Public Key Infrastructure
PMT	Protection Motivation Theory
QC	Qualified certificate
QD	Qualified electronic signature creation device
QS	Qualified electronic signature
TAM	Technology Acceptance Model
TTAT	Technology Threat Avoidance Theory
UI	User Interface

3. Introduction

3.1. Aims and Scope

The PRISMACLOUD project develops a portfolio of novel security and privacy enabled cloud services, ensuring security and privacy for sensitive data in the cloud. User privacy issues are addressed by data minimization and anonymization technologies based on privacy-preserving cryptographic techniques. As feasibility proofs, three use cases in the area of SmartCity, e-Government and e-Health will be implemented and evaluated by the project.

PRISMACLOUD technical solutions will however only be successfully deployed if they are at least legally compliant and acknowledged, trusted and perceived as valuable by end users and if they are usable. Therefore, important legal, social and HCI (Human Computer Interaction) requirements should be considered right from the start of the PRISMACLOUD project and included in the whole design and development cycles of all PRISMACLOUD solutions, following a human-centred design[1] approach. Such requirements were elicited by PRISMACLOUD task 2.1 "Requirement Elicitation" during the first 9 months of the project, mostly in close cooperation with key stakeholders and end users.

This project deliverable D2.1 reports about these legal and social trust requirements, as well as end user requirements, in regard to the PRISMACLOUD use cases and HCI requirements that were elicited by PRISMACLOUD task 2.1 and that should provide input and guidance for the development of PRISMACLOUD use cases, technical solutions and user interfaces (UIs).

3.2. Research Questions

For the elicitation of legal, social trust, end user as well as HCI requirements, we addressed the following research questions:

- What is the legal status of novel cryptographic signature primitives, such as malleable and functional signatures, that PRISMACLOUD is proposing? Under which conditions can they be legally regarded as advanced or qualified signatures?
- What social factors are important for users putting trust into the security and privacy of their data in the Cloud?
- What factors may influence user acceptance and adoption of (future) cloud services?
- What are requirements by end users in regard to the PRISMACLOUD use cases?
- What human factors need to be addressed for meeting such end user requirements?

3.3. Methodology

For the requirement elicitation, we have used different research methods:

- We performed an analysis of the European legal framework for electronic signatures consisting of the Electronic Signature Directive 1999/93/EC [1] and the new Regulation on electronic

[11] Human-centred design is defined by ISO 9241-210, 2010 as an approach to interactive systems development that aims to make systems usable and useful by focusing on the users, their needs and requirements, and by applying human factors/ergonomics, and usability knowledge and techniques (ISO 9241-210:2010(en), [56]).

identification and trust services (eIDAS) [2] in order to elicit legal requirements that malleable and functional signatures have to fulfil for being legally acknowledged as advanced and/or qualified signatures.

- Social Trust requirements were elicited with reviews of literature related to social trust factors of privacy and cloud-related technologies. This literature review is partly based upon and extending a literature review that we conducted earlier for the A4Cloud[2] project [3]. Another literature review for eliciting requirements in regard to user acceptance was conducted, related to technology acceptance models in general and security/privacy technology acceptance models in particular.
- Furthermore, we have elicited end user and HCI requirements in close interaction with end users, stakeholders and experts that understand end user needs and problems. For this, we have used the methods of semi-structured interviews, expert focus groups and surveys.
    - Semi-structured interviews are interviews where not all questions are designed or planned before the interview, allowing the interview to follow and explore new directions as they come up in the interview process [4]. Semi-structured interviews with key stakeholders and end users were considered a right method for capturing the challenges regarding the use of PRISMACLOUD technical solutions in different use case scenarios.
    - Surveys were conducted right after the semi-structured interviews for receiving more information about their attitudes and views. Besides, a survey was conducted with cloud business users and providers to analyse their perceived value and challenges of crypto privacy solutions for the Cloud.
    - Focus groups are appropriate for bringing together a cross-section of users so that they can collaboratively share and unveil their opinions and needs regarding particular challenges foreseen in the design of a system, where the moderator can stimulate participants to discuss these opinions with the group by using different approaches, e.g. by asking direct questions to participants, encouraging brainstorming, etc. Four focus groups with expert users allowed us to receive input on the expert users' perceived opportunities and risks of PRISMACLOUD technical functions in the envisioned use cases, and to discuss requirements that need to be fulfilled for addressing such risks.

3.4. Relation to other Tasks and Deliverables in PRISMACLOUD

The end user-related requirements that we elicited in Task 2.1 and that are reported in this Deliverable D2.1 will guide the design and development user interface prototypes and the HCI research done by PRISMACLOUD Task 3.2 on "HCI concepts and guidance". In addition to guiding the user interface design, our requirements should also more generally provide input to the design and implementation of PRISMACLOUD solutions and use cases. Table 5 in Section 8.1 specifies the nature of the requirements to indicate for which type of developers the requirements should be addressed.

Further functional and security requirements of more technical nature will in addition be elicited by the other task of PRISMACLOUD work package 2.

[2] EU FP7 project A4Cloud (Accountability for the Cloud), http://www.a4cloud.eu/

While this deliverable focusses on providing an early set of legal, social and HCI requirements after the first nine project months for the PRISMACLOUD project, future deliverables such as D3.2 (HCI Guidelines) and D3.3 (HCI Research Report) will report about the mapping of the HCI and end user requirements to User Interface solutions that we will develop within the remaining project lifetime. Nonetheless, for illustrating some of HCI and end user requirements, we are in Appendix VI providing examples of high level User Interface solutions that we suggest as adequate for addressing these requirements.

3.5. Related work

PRISMACLOUD researches innovative approaches for applying rather novel privacy cryptographic primitives for enhancing security and privacy in the Cloud. Due to the novelty of the PRISMACLOUD approach, there is no direct work on legal, social and HCI requirements for PRISMACLOUD technologies for the Cloud. However, a related set of HCI and social trust requirements [3] as well as legal requirements [5] for transparency and accountability in the Cloud context were elicited by the A4Cloud EU FP7 project, which are however focussed on transparency and accountability tools for the Cloud that the A4Cloud project has developed, and thus they only partly overlap with the scope of PRISMACLOUD. In this deliverable, especially in chapter 6, we will refer to this earlier work.

3.6. Outline

The remainder of this deliverable is structured as follows:

- Chapter 4 provides an overview to the PRISMACLOUD cryptographic primitives and the first version of the PRISMACLOUD envisioned use case scenarios that are deploying most of those primitives in a Cloud application context;
- Chapter 5 discusses the legal status and requirements for legal acknowledgements of novel signature schemes that will be used by PRISMACLOUD for the authentication and data minimisation of stored and processed data in the Cloud;
- Chapter 6 presents a literature review for relevant social trust requirements and Security Technology Acceptance Models;
- Chapter 7 presents the user and HCI requirements that we elicited by interviews, focus groups and surveys;
- Chapter 8 finally provides a complete list of all elicited requirements and to what type of developers these requirements address, and will summarise the main conclusions from this deliverable.

Annex I –IV presents the interview guide, consent form and survey forms that were used for conducting our semi-structured interviews and surveys. Annex V lists the agenda for our focus groups. Finally, Annex VI, as mentioned, presents suggestions for high-level UI solutions for illustrating how some of the elicited HCI requirements could be implemented.

4. Background

This chapter provides an overview of the cryptographic primitives that are used in PRISMACLOUD for enhancing privacy and security for the cloud (section 4.1) and of the first version of use case scenarios that we used for our interviews and focus groups for eliciting requirements (section 4.2).

4.1. PRISMACLOUD cryptographic primitives

The PRISMACLOUD project proposes a set of several **cryptographic primitives** for countering some of the most pressing threats currently present in cloud computing. Cryptographic primitives are basic cryptographic functions (or algorithms) which can be used in cryptographic protocols in security relevant information and communication technology (ICT) applications. A **cryptographic protocol** can be defined as an exact description of how a specific cryptographic functionality is carried out: It describes the exact steps of application of the cryptographic algorithms, as well as the structure of the data on which the algorithms operate. Without exception, the PRISMACLOUD cryptographic primitives are either extensions of existing cryptographic primitives (where they add functionality and/or cryptographic strength), or security enhancements of functions that were not equipped with security functionalities before.

In this chapter we will present a compact **ontology of the PRISMACLOUD cryptographic primitives** for subsequent use in the elicitation of the legal, social, and HCI requirements. We will define the names of the cryptographic primitives, and list - and to some extent analyse - their generic properties, and especially their security properties. We will relate them to the primitives they were derived from, and to other functions (cryptographic or not) which will be used together with them. This ontology shall facilitate a consistent presentation of the legal, social, and HCI requirements, and enable the understanding of their technical and especially cryptographic background for the legal experts, sociologists, and non-cryptographic-technicians involved in the requirements elicitation.

The PRISMACLOUD cryptographic primitives are from **three specific fields** in which security and privacy issues are pending in current cloud applications and services. These are the fields of **data storage in the cloud**, of **authentication of stored and processed data**, and of **protection of user privacy** by minimisation of data which is unnecessarily exposed in cloud applications and services. The individual cryptographic primitives are regarded from a high level perspective, focusing on properties, particularities, and implications of their application. Application detail is only presented where it is deemed to be necessary for the understanding of properties, particularities and implications.

4.1.1. Data storage in the cloud

Secure cloud storage using a cryptographic storage network

Current solutions: currently, most available cloud storage services store the data either unencrypted or apply encryption which remains under complete control of the cloud service provider; some cloud users locally encrypt their data before they store it in the cloud.
Implications:

1. In the first case the cloud provider has to be trusted to provide effective protection of the data with respect to regard confidentiality and integrity. This includes all copies and replications of the data which are created for availability purposes in all layers of a storage

architecture. Users also have to consider, that the cloud provider is capable of reading all the data in plain and has to be trusted not to exploit that knowledge[3].

2. Also with respect to availability of data and of cloud services, the user is dependent on the provider. There are cases known where bankruptcy of a cloud provider led to sudden loss of access to customer data.
3. Deletion of data in clouds is also a big issue and it is not sufficiently solved how a physical deletion of data in all replications and backups could be substantiated.
4. When cloud users use end-to-end encryption to mitigate some of the mentioned problems and threats (i.e. when they encrypt the data before passing it to the cloud) they are required to implement and maintain a cryptographic key management system and an access control mechanism, with all its known complexities and implications.

Proposed solution: PRISMACLOUD proposes a cryptographic storage network with increased practical usability for the secure, distributed storage of data [6] [7]. Through the use of an information-dispersal algorithm, i.e. secret sharing [8], the information is split into a number of shares, of which any subset of a fixed number smaller than the number of shares allows the reconstruction of the original data. The numbers have to be selected at the time of storing the data and typically remain fixed throughout its lifetime. An example would be a threshold of a "3 out of 5 system", where the data can be reconstructed using any three shares of the produced five shares. The five shares are distributed over encrypted channels to different cloud providers.

Implications:

1. The cryptographic storage network provides sort of a 'keyless' cryptographic solution, under the assumption, that not a number of cloud storage providers greater or equal the threshold of the storage network do maliciously cooperate (non-collusion assumption). The secret sharing algorithm itself is considerably stronger than commonly used cryptographic systems and capable of long-term security [9] and therefore applicable in scenarios with highest confidentiality requirements, like in eHealth or eGovernment.
2. The cryptographic storage network enables the collaboration of several users on the data, but it requires an explicit access control system;
3. The secret sharing also solves the availability problem at the user level, without the need of explicit backups. Also single shares can be taken out of the system and be replaced by newly generated ones. This prevents vendor lock-in and, when shares are continuously replaced, enables long-term data security (as it minimises the chance of an attacker to get a sufficient number of shares for reconstructing the information by attacking one cloud provider after the other);
4. Leakage of metadata, which occurs during storage and retrieval of the single shares, and by synchronisation activity between the single storage providers during share renewal, may present a privacy problem and needs to be investigated.

[3] We do here discuss solely applications and services beyond the 'free of monetary charge' cloud offerings, for which users pay by granting to the cloud provider extensive exploitation rights on the data.

Data security for database applications:

Current solutions: Many businesses and administrations rely on legacy database applications which store data unencrypted, either out of compatibility and interoperability issues, or because they have a valid certification in compliance with some mandatory regulation.

Implications:

> Such applications cannot easily be transferred to the cloud, where the confidentiality of the information is at stake.

Proposed solution: Add a layer of cryptography directly into the data fields of the database applications: Format preserving encryption (FPE) and Format preserving tokenisation (FPT) apply encryption in a manner such that the ciphertext has the same format as the plaintext (e.g. a social security number is mapped into a cryptogram with the format of a social security number). The encrypted data items can thus be stored in the same fields/tables as the plaintext. The encryption is done when the data leaves the security perimeter, i.e. before it is stored into the cloud. Order preserving encryption and tokenisation (OPE and OPT) work in a similar way as FPE and FPT, but provide the additional property, that the order relation of the plaintext is preserved on the ciphertexts.

Implications:

1. Enables integration of encrypted data into existing legacy applications;
2. Application functionality can be preserved (e.g. validity checks will pass).

4.1.2. Authentication of stored and processed data

Malleable signatures

Current solution: One practical advantage of cloud systems (besides their often cited flexibility and elasticity) is that collaborative applications may easily be implemented. In order to control the authenticity of data, current solutions use electronic signatures.

Implications:

1. In collaborative applications, several parties usually also need to modify common data;
2. Common electronic signatures are static: one single modification in the authenticated data invalidates the signature and removes the authenticity property from the data.

Proposed solution: employ the technology of malleable signatures (cf. [10]) which allow controlled modification (or redaction) of certain parts of the signed data without the signature losing its validity. The allowed modifications are being formally described and the malleable signature for a specific data item is created. At a later time the authenticity of the modified data can be verified, and thus, the verifying entity can gain cryptographic assurance that only allowed modifications were made.

Implications:

1. Only controlled modification is allowed on the data;
2. Allowed modifications do not need the secret signing key;

3. Modification may be allowed for everyone, or for specific parties in possession of a specific cryptographic key;
4. Correct modification preserves the validity of the signature;
5. Modification beyond what is allowed, renders the signature invalid. The authenticity property for the entire signed data item is destroyed;
6. Allowed modifications may be described on a document level (which parts may be edited) or allow the application of specific arithmetic functions;
7. Currently, only linear functions (counting, summation…) and polynomial functions (variance, covariance…) are feasible;
8. Arbitrary functions are possible in theory, but currently not practically feasible.

Verifiable computation

Current solution: Today, several approaches for the implementation of verifiable computing are proposed but are not yet developed for practical application.

Implications:

The delegation of computing cannot be verified without a dedicated application serving all involved parties (outsourcer, cloud provider, verifier)

Proposed solution: Verifiable computing involves the use of malleable or functional signatures for privately and publicly verifiable computation [11] [12]. A client hands signed data plus a secondary signing key, which is connected to a cloud service which applies a function on the data. When the client gets the data back, he or she can verify that only the allowed function was applied.

Implications:

1. Verifiable computing allows new types of collaborative applications
2. Efficient solutions are only available for simple calculations (linear functions, e.g. sums)
3. The privacy of the outsourced data is typically not regarded

Certification of virtualised infrastructures

Current solution: In order to provide assurance for cloud customers, cloud service providers have their services certified according to security standards. Technically, there exist measures for the attestation of the security of physical and virtual machines. Trusted components monitor the systems on all levels and layers.

Implications:

1. The customer still has to trust, that the cloud service is correctly and securely configured,
2. That the audit and verification of the virtualised infrastructures has been carried out correctly.
3. The service provider and the auditor need to be trusted.

Proposed solution: Using recently developed methods for representing virtualised infrastructure in graph structures [13], extend current audit procedures with a means for proving the correct configuration of virtualised infrastructures.

Implications:

1. A (human) auditor verifies an actual infrastructure and represents it in a graph, which he signs with a graph signature. With the help of this graph signature, the verification of the auditor is bound to the actual infrastructure as it was configured at the time when the audit was carried out.
2. The graph signature algorithm lets the customer prove topology properties of the virtualised infrastructure (like connectivity isolation) without revealing actual details of the topology to the customer.

4.1.3. User privacy protection

Anonymous credentials

Current solution: User authentication and authorisation is often provided with the use of signed identity certificates having all sorts of information about the bearer stored in them. In most cloud services users are uniquely identified (by name, social security number, credit card number, etc.) and can be tracked in their activities by cloud service providers.

Implications:

1. In currents systems, users often reveal much more data than necessary for performing or delegating a specific task. Such data is prone to being accumulated and data mined by the cloud provider and by other parties eventually getting in possession of the data. This represents a severe privacy threat for the user. For example, if a user presents a signed identity certificate, he or she usually exposes all the personal information contained in that certificate, even if it is of no relevance for the authorisation which shall be granted.
2. Often users have to expose their identities when just the simple property 'of being authorised or eligible' needs to be proven. This makes events linkable and generates metadata on peoples' behaviour and whereabouts, completely irrelevant for the application. The exploitation of such metadata by specialised companies and authorities, and other parties, poses a severe threat against user privacy.

Proposed solution: Use the technology of 'anonymous credentials' [14] to enable the implementation of privacy protecting and data minimising authentication and authorisation systems for cloud applications and services.

Implications:

1. Users may prove the authorisation for a service without revealing their identity;
2. Anonymous credentials allow the encoding of attributes in credentials such, that statements about the encoded attributes can be proven to a verifier without revealing the values of the attributes;
3. Anonymous credentials are effective tools for data minimisation—the amount of data which is revealed during transactions is effectively reduced;
4. If events need to be linkable, anonymous credentials allow to anonymously prove the possession of a pseudonym

Big data anonymisation

Current solution: Efficient and practical solutions for anonymisation of very big data sets do not exist. K-anonymisation of data [15], which means, that in a set of data, for each entry, there are at least (k-1) other entries, from which it cannot be distinguished, is a NP hard problem [16].

Proposed solution: New, more efficient approaches to anonymising big sets of data have improved in efficiency and are now capable of anonymising very large data sets.

4.2. Use case scenarios

For eliciting requirements for the project, use case scenarios are needed to provide context for the cryptographic functions and methods at hand as well as to facilitate discussions for the empirical methods used (Interviews and focus group workshop, Chapter 7). However, due to the fact that this work has been carried out in the earlier stages of the project and in parallel to the process of use cases specifications, only a preliminary version of the scenarios was used; there might be alterations in comparison to the use cases specification deliverable D2.3.

The three main theme areas in PRISMACLOUD which were used for the use cases scenarios are based on (I) E-health, (II) E-government, and (III) Smart city, provided by PRISMACLOUD partners (AIT, ETRA, ATOS, LISPA). The use case scenarios were for E-health: (a) blood test and (b) smart phone monitor application, for E-government: (c) disaster files recovery and (d) incident reports, and for smart city: (e) handicap parking authorization. Descriptions of each of the scenarios are presented below and in the interview guide in Annex I.

(a) E-health: blood test

Consider a case where a patient goes to the doctor for a routine check-up and takes an extensive blood test. The blood test is taken by the doctor's nurse and the results are uploaded to a Cloud portal and are digitally signed by the nurse. The doctor has access to the complete blood test results. Later, the patient visits a dietitian who requires few specific fields of the blood test. The patient doesn't want to reveal all fields from the extensive blood test. So the patient selects the mandatory fields from the extensive blood test for the dietitian to see and "blacks-out" the other fields.

Alternative case:
Consider a case where the patient goes to the doctor for a routine check-up and takes an extensive blood test. The blood test results and diagnosis report are uploaded to a Cloud portal and are digitally signed by the doctor. The doctor has access to the complete blood test results. However, the patient wants a second opinion from another doctor regarding her results. The patient doesn't want to reveal the diagnosis fields from the report. So the patient selects the blood test results for the second doctor while "blacking-out" the diagnosis field.

(b) E-health: smart phone monitor application

Consider a case where a patient has a smart phone training application that uses the sensors on the phone/wearable device to monitor and collect personal data of the patient. The patient would like to share only activity progress information of the data collected by the application to her trainer without revealing private data.

(c) E-government: disaster files recovery

For disaster recovery and backup purposes, IT providers of governmental institutions split their databases into multiple parts (shares) that are stored at independent cloud providers. Consider a case where a disaster occurs and a potential data loss is at risk. To reconstruct data, only a predefined subset of shares stored at different cloud providers would be required, e.g., 4 shares out of 7.

(d) E-government: incidents report

Consider a case where a forest fire occurs. Later the government has produced a report that includes personal information, e.g. about victims or rescue workers, and potentially other classified information (all signed) regarding the cause and the incident response procedure. The conclusions are signed by relevant experts. Based on this, the intention is to release a report to the public where one wants to anonymize all personal information and classified information, but keep the electronic signed conclusions.

(e) Smart city: handicap parking

Consider a case where handicaps are required to use either their regular phones or smart phones to validate themselves in order for them to park at the handicap parking spot. When using a regular phone, a control station by the parking will be used to authorize the parking using an SMS. When using a smart phone, the parking app would use the NFC badge (digital identification) and GPS location for authorization.

5. The legal status of electronic signatures and legal requirements

In this chapter, we discuss the legal status of malleable and functional signatures and derive legal requirements for them. The chapter focusses on the legal aspects of these signature schemes to be used in PRISMACLOUD, as due to their novelty, their legal status has hardly been discussed yet. More general legal privacy requirements in relation to Cloud Computing pursuant to the EU Data Protection Directive 95/46/EC [17] and the upcoming EU General Data Protection Regulation [18] have been discussed by other projects earlier, such as the EU project A4Cloud and the Cloud Legal projects. For a discussion and list of such general legal privacy requirements we therefore refer to publications by these projects (see [5], [19] and [20]).

To determine the legal status at a European Union level of more recently emerged forms of electronic signatures such as malleable- and functional signatures, first in section 5.1 the (legal) definition and -status of different categories of electronic signatures will be elaborated on. Thereafter, we go over some technical details of existing and legally accepted technical mechanisms in section 5.1.2. In section 5.1.3, respectively malleable- and functional signatures schemes will be elaborated on, to conclude with an overview of the key-differences between on the one hand the different kinds of electronic signatures already (explicitly) regulated and on the other hand malleable- and functional signatures. Based on these key-differences, in section 5.1.4, the legal status of malleable- and functional signatures in light of effectual regulation at a European Union level will be determined and a list of high level requirements will be provided. This section will not go into too many cryptographic details, for the more technical aspects of signatures, see PRISMACLOUD deliverable D4.4 [10] and for an in-depth analysis of the legal evidentiary value of malleable signatures [21].

5.1. Specifically regulated categories of electronic signatures in the EU

The legal status of different forms of electronic signatures was, from 19 January 2000 until 16 September 2014, regulated through Directive 1999/93/EC[4] (hereafter ESD). From 17 September 2014 Regulation EU 910/2014[5] (hereafter eIDAS) partially[6] repeals the ESD and as of 1 July 2016 the ESD is fully repealed. Both the ESD and the eIDAS define the different categories of existing electronic signatures, these definitions are, however, at times slightly dissimilar. As such both the definitions provided in the ESD as well as those provided in the eIDAS will be elaborated on if this difference in definition is relevant. Before it is possible to properly define the different forms of electronic signatures and assess their legal status, it is important to first elaborate on three related terms. Based on respectively article 3 section 9, section 13, and section 22 eIDAS:

- Signatory means a natural person who creates an electronic signature;
- Electronic signature-creation data means unique data which is used by the signatory to create an electronic signature; and

[4] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (*OJ* 2000, L 013/12-20). Hereafter referred to as ESD.
[5] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Hereafter referred to as eIDAS or the Regulation.
[6] The Regulation entered into force on 17 September 2014 ex article 52 section 1 eIDAS, and will apply as of 1 July 2016 except for the articles mentioned in article 52 section 2 sub a, b, and c eIDAS.

- Electronic signature-creation device means configured software or hardware used to create an electronic signature.

It is possible to distinguish between three different categories of electronic signature (hereafter referred to as an ***ES***):

1. A basic electronic signature (hereafter referred to as a ***BS***);
2. An advanced electronic signature (hereafter referred to as an ***AS***); and
3. A qualified electronic signatures (hereafter to as a ***QS***)

(Basic) electronic signature (*BS*)

What a basic electronic signature is defined in article 3 section 10 eIDAS as follows;

> *Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.*[7]

As such for data to be considered an electronic signature the data has to fulfil the following requirements:

1. The data needs to be in electronic form;
2. The data needs to be attached to, or logically associated with, other electronic data; and
3. That other electronic data needs to be used by the signatory to sign.

This form of electronic signatures is, however, not very often used in practice except for maybe scanned (written) signatures because a ***BS*** does not provide for more or a better legal protection. These requirements are, however, crucial as they make clear that *any* kind of electronic signature, be it an advanced-, qualified, malleable-, or functional signature, in its essence is nothing more than a piece of data which is in connection to two different other pieces of data, the electronic document that is getting signed, and the electronic data that is used by a natural person to generate the signature (the electronic signature creation data).

Advanced electronic signature (*AS*)

Advanced electronic signatures – which in difference to the afore elaborated on basic signatures *are* used more often in practice – are defined in article 3 section 11 j°. 26 eIDAS. The most notable difference to a ***BS*** is that additional requirements are put on the linking and the data used to create the signature.

When combining the different requirements of these articles, in combination with the aforementioned definitions, the following definition can be constructed:

> *An advanced electronic signature is an electronic signature which is created using unique electronic signature-creation data that the natural person who created the signature can, with a high level of confidence, use under his sole control and which is both uniquely linked to and capable of identifying that natural person, as well as is linked to the data signed therewith in such a way*

[7] The ESD [1] used a slightly different phrasing;
Data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.
but this difference is of no consequence for the underlying research.

that any subsequent change in the data is detectable.

Therefore, in its barest essence, an advanced electronic signature is a (basic) electronic signature that additionally fulfils the following requirements:

1. The ***BS*** is uniquely linked to the natural person who created the signature;
2. The ***BS*** is capable of identifying the natural person who created the signature;
3. The ***BS*** is created using unique data (termed electronic signature creation data[8]) that the natural person who created the signature can, with a high level of confidence, use under his sole control; and
4. The ***BS*** is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Qualified electronic signature (*QS*)

The third category of electronic signatures, a qualified electronic signature, is defined in article 3 section 12 eIDAS. Based on this article in conjunction with article 3 sections 10 and 11 eIDAS and article 26 eIDAS, the following definition of a qualified electronic signature can be constructed:

A qualified electronic signature is an advanced electronic signature which is created using unique electronic signature-creation data that the natural person who created the signature can, with a high level of confidence, use under his sole control and which is both uniquely linked to and capable of identifying that natural person, as well as is linked to the data signed therewith in such a way that any subsequent change in the data is detectable that is created by a qualified electronic signature creation device, and the electronic signature-creation data is based on a qualified certificate for electronic signatures.

Therefore, in its barest essence, a qualified electronic signature is an electronic signature that is:

1. uniquely linked to the signatory;
2. capable of identifying the signatory;
3. created using means the signatory can maintain under his sole control;
4. linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;
5. created by a qualified electronic signature creation device (hereafter ***QD***); and
6. created using electronic signature-creation data based on a qualified certificate for electronic signatures (hereafter ***QC***).

The requirements for a qualified certificate for electronic signatures and qualified electronic signature creation device are defined in respectively Annex I and Annex II of the eIDAS. The qualified certificate is of less relevance to the underlying technical research. For the certificate issuing indeed the only technical aspect is to have a public signature verification key, then it remains to define a common exchange format for the cryptographic keys. As apart from those two, this will not be elaborated on at this point. Regarding the QD, the technical research is to identify if the algorithms that compute the signature and thus need the secret electronic signature creation data can be run on hardware security modules (HSM), most commonly known also under the term SmartCard. It is important to note though that based on article 25 section 1 eIDAS, *all* electronics signatures à priori

[8] Electronic signature creation data is the legal notion, in cryptography you would call this the secret signature generation key or in short secret key often abbreviated as ***sk***.

have legal effect and are admissible in legal proceedings, and that a qualified electronic signature has the same legal effect as a handwritten signature. The eIDAS, as well as ESD, make no further statement – other than the equality to handwritten signatures – about the evidentiary value of a document signed with either a basic-, advanced-, or qualified electronic signature. The evidentiary value of a document signed with an electronic signature is left to the national legislation of the individual EU Member State. More over eIDAS and ESD have been worded to be technologically neutral.[9]

5.2. Legally well accepted technical mechanisms to create qualified electronic signatures

Neither the ESD nor eIDAS are targeted at a certain technical mechanisms to generate qualified electronic signatures.[10] It will probably take some time for additional court rulings until it is clear[11] what eIDAS' flexibility[12] will additionally allow. In most Member States the implementation of the ESD led to the development of technical standards, released by the standardization bodies of those individual Member States, to describe in more technical detail which cryptographic strength and which technical mechanisms were suitable.

This resulted in specific cryptographic algorithms, key sizes and technical systems for secure electronic signature creation devices, which were considered legally accepted in light of the ESD or eIDAS. Without elaborating too much on the details of each of these algorithms, let us – as an example of EU Member State regulation – briefly walk through the catalogue of allowed algorithms referenced by [13]the German signature legislation. The following are listed: RSA, DSA, EC-DSA, EC-KCDSA, and EC-GDSA.[14] Moreover, details on their parameters, including but not limited to key length, are prescribed.

All the above schemes are technically based on asymmetric cryptography. This means that the cryptographic operations are considering a key pair, instead of a single key. This key pair contains

[9] See recital 27 of eIDAS stating:
This Regulation should be technology-neutral. The legal effects it grants should be achievable by any technical means provided that the requirements of this Regulation are met.

[10] Laborde notes that by "establishing requirements that, so far, can only be fulfilled by using digital signatures'' it is not completely technology neutral, see C.M. Laborde. Electronic Signatures in International Contracts, volume 4982. Peter Lang, 2010.

[11] See: Alexander Roßnagel. Neue Regeln für sichere elektronische Transaktionen, Neue juristische Wochenzeitung (NJW), volume 51, page 3686. Beck Juristischer Verlag, 2014. (German only)

[12] See: Vojtech Kment. European regulation eIDA: The impuls to unify the electronic signature and identification in the EU, Jurisprudence, Season XXIII(6):25–35, 2014.

[13]BNetzA, Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), Dec. 2014, <https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2015Algorithmenkatalog.pdf>.

[14] For details on each algorithm:
- RSA: ISO, ISO/IEC 14888-2:2008 Information technology – Security techniques – Digital signatures with appendix – Part 2: Integer factorization based mechanisms, 2008
- DSA: NIST, FIPS Publication 186-4: Digital Signature Standard (DSS), Juli 2013
- EC-DSA: ANSI, ANSI X9.62:2005 Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (EC-DSA), 2005
- EC-DGSA: ANSI, ANSI X9.62:2005 Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (EC-DSA), 2005

two keys: the secret signature creation key (***sk***) and a public signature verification key (***pk***). There is the following mathematical relationship between these two keys used in digital signatures: (1) the secret key cannot be derived from the public key and (2) it is possible to verify with the public key that the secret key was used in an operation.

This relationship is used to implement two key functionalities: Signature creation (in short often referred to as Sign) and signature verification (in short Verify). The resulting workflow is depicted in Figure 1. Simplified, the sign algorithm takes the secret signing key and the document and generates a signature value. The verify algorithm takes the signature value, the document and the public verification key to obtain the result. If the result is positive this means that the signature is valid. In turn this yields two things: First, the document has not been altered according to an integrity policy and second, the signature value has been created involving the secret key corresponding to public key used for verification.

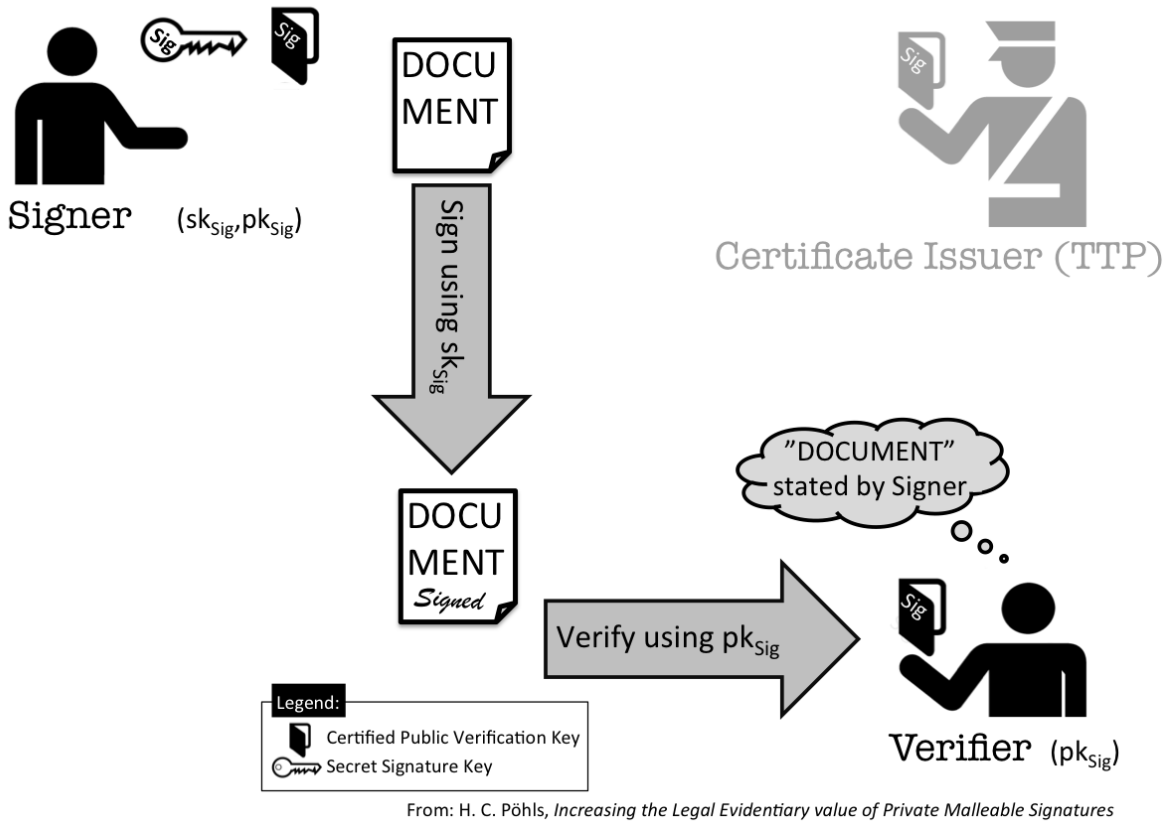

Figure 1: Workflow of the signature generation and verification using asymmetric key pair consisting of the signer's secret signature generation key (sk_{Sig}) and a related public verification key cryptographically related to (think "linked only to") that signer's secret key (pk_{Sig}) [21]

The terms document and message are used interchangeably in the remainder of this chapter.

All above listed legally accepted signature schemes cryptographically enforce that a valid signature under a public key on a message can only be produced knowing the corresponding secret signing key. Hence, the opposite – generating a signature on a message that verifies without knowledge of the

secret key – must be computationally infeasible. [15] This property in cryptography is called unforgeability. A cryptographic model for unforgeability that is considered sufficient for practical applications is UNF-CMA also referred to as EUF-CMA.[16] In this model – and for the remainder of this deliverable – existential unforgeability under adaptive chosen message attack (EUF-CMA), or unforgeability in short, means the following: The attacker does not know the secret signature generation key. But the attacker is given the ability to ask the signer to generate a signature for an attacker provided message using that key. Then the attacker can see the resulting valid signature and can ask for another signature on another message of the attacker's choice. Hence, the name adaptive chosen message attack. To generate a forgery, the attacker must create a valid signature for a message – and that can be also a random message, i.e., it does not require to conform to a specific given document structure – that the attacker has never before asked the signer to sign. In other words, the message must just exist – not make sense – and the valid signature must have been created not with the help of the signer, but only by the attacker.

All the legally accepted schemes offer this strength of unforgeability. Further, for efficiency a lot of the legally accepted schemes involve a step called secure cryptographic hash-function. From a cryptographic perspective this is done for efficiency reasons. Sometimes high level discussions and also legal discussions on the subject describe this hash as if it is the only way to generate the dependence of the signature to the message that is prescribed by the legal framework.

In the end the digital signature schemes need to fulfil this fourth requirement for an ***AS*** or ***QS*** – linked to the data to which it relates in such a manner that any subsequent change of data is detectable . A cryptographically secure hash gives this due its properties, for example one property ensures that a single change of the document will result in a different hash[17]. To summarize our short detour to hashing: technically it is the hash function that establishes the link between the message and the signature. It is there for efficiency of the cryptographic algorithms. As defined by law, the signature "is linked to the data signed therewith in such a way that any subsequent change in the data is detectable". The technical mechanisms listed as suitable for secure hashing under German law are: SHA-256, SHA-512/256, SHA-384, and SHA-512.1.[18]

To elaborate briefly on the other properties, the first requirement, linking the ***ES*** to the signatory is done through the relation between the public and the secret keys and can be fulfilled when the signature achieves unforgeability. Regarding the second requirement; basically a third party – often called trusted third party and abbreviated as TTP – holds a list of IDs of signatories and their public keys. As such, when using the public key that corresponds to the ID of a signatory it is possible to determine whether the related secret key was used. And because only the signatory has (or at least should have) access to the secret key, the third requirement – created using means the signatory can maintain under his sole control – is also fulfilled. Of course the secure operation of this TTP, also

[15] Computationally infeasible means that it *is* possible, but that doing so would require a very long time and very powerful resources, for example the factorisation of very large integers, as is the underlying problem of the RSA algorithm. Because of this computationally infeasibility the use of cryptography is acceptable as a basis for evidence cf. the adage of "a degree of probability bordering on certainty".

[16] See S. Goldwasser, S. Micali, and R. L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. In SIAM Journal on Computing, volume 17, 1988.

[17] This is why the hash is sometimes figuratively described as "the fingerprint" of a document in the sense that it is unique to the document.

[18] NIST: FIPS Publication 180-4: Secure Hash Standard (SHS), March 2012

known as certification authority (CA), and the processes associated to it, e.g. the checking of the actual natural person's attributes that get associated to the public signature verification key, need to follow organisational rules again that are codified in eIDAS respectively member state legal texts and subsidiary technical standards issued by national or international standardisation bodies.

Based on this background information on what is legally required and what is usually accepted, let us look at signatures which are different and whether they can be constructed in such a way that they are close, or equal in their behaviour, to the legally accepted categories elaborated on before.

5.3. Not yet legally well accepted technical mechanisms to create qualified electronic signatures

To determine the legal status of more recently emerged – and not yet specifically regulated – forms of electronic signatures at a European Union level, in the following two sub-sections respectively malleable- and functional signatures schemes will be elaborated on and assessed in light of existing regulated forms of electronic signatures.

Malleable electronic signature scheme (MS)

In short, a malleable signature-scheme can be defined as:

> *A digital signature scheme with an additional function whereby, on input of a message (**m**) and a signature (**σ**)* by a signer*, it is possible to efficiently compute a derived signature (**σ'**) on an altered message (**m'**) for a transformation (**T**) that has been allowed with respect to the message (**m**) and the signature (**σ**), i.e. **m' = T(m),** so that the derived signature **σ'** on **T(m)** can be still verified with the signer's public key .*[19]

As such, when a malleable signature (hereafter referred to as an ***MS***) is used by the Signer[20] to sign a message, this message can be altered by a third party (hereafter referred to as Sanitizer[21]) – within a scope predefined by the Signer – without invalidating the original electronic signature. This makes it possible to, for instance, redact a text as illustrated in Figure 2.

[19] Derived from; Chase M., Kohlweiss M., Lysyanskaya A., and Meiklejohn S., *Malleable Signatures: Complex Unary Transformations and Delegatable Anonymous Credentials*, Cryptology ePrint Archive, report 2013/179, 2013, p. 1. <https://eprint.iacr.org/2013/179.pdf> [51]

[20] Hereafter the term Signer is used to refer to the initial signatory mandating a Sanitizer to sign on its behalf.

[21] We use the term "Sanitizer" in that spelling, as this is the term found in cryptographic literature, in other cryptographic works call it "Redacter"

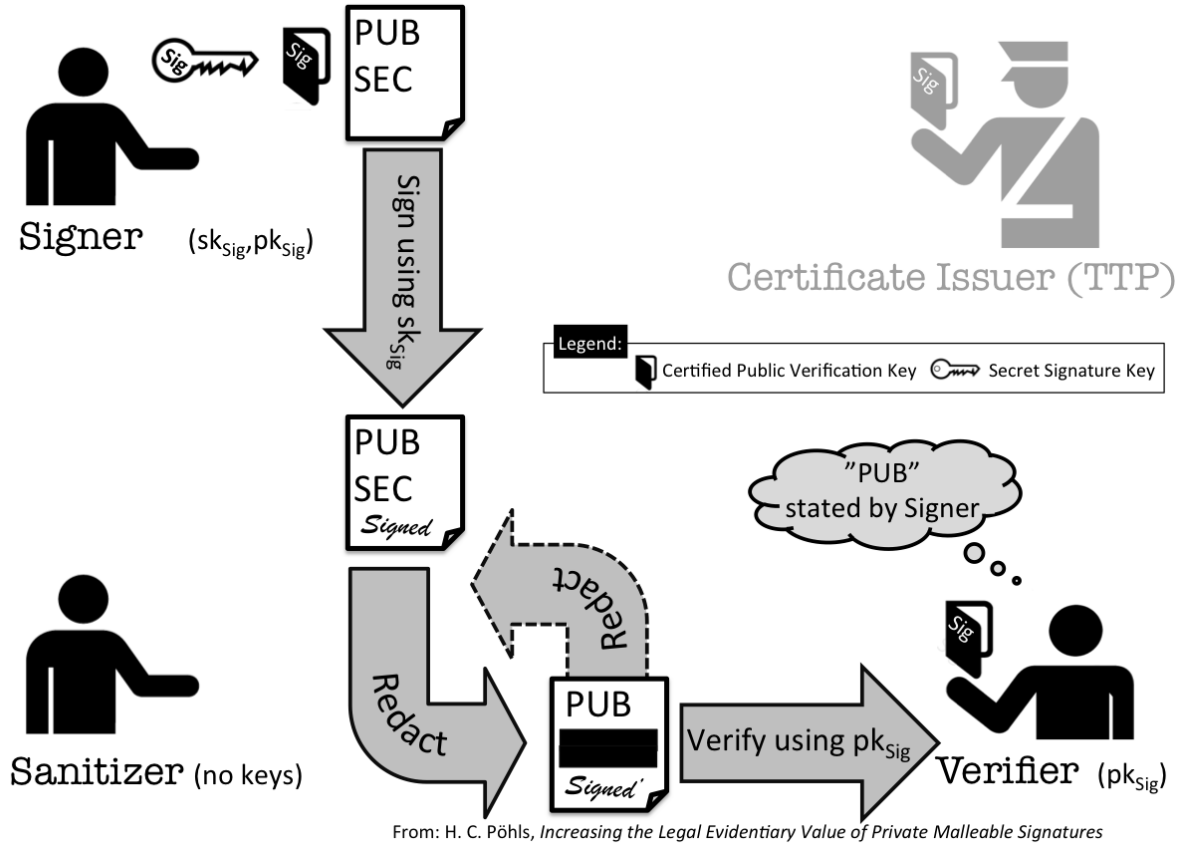

Figure 2: Workflow showing that an ***MS*** can allow a Sanitizer to redact text and, if authorised by the Signer, to compute/create a derived signature which corresponds to the redacted text and which still verifies under the Signer's public signature verification key without the need of additional keys. [21]

As an ***MS*** is in electronic form, it is attached to, or logically associated with, other electronic data (the document to sign), and electronic data (the Signer's key) is used by the signatory to sign, no elaboration is necessary to conclude that a malleable signature is an electronic signature (i.e. a ***BS***) ex article 3 section 10 eIDAS. Hereafter, the characteristics of ***MS***s will be analysed to assess whether they (can) fulfil the requirements of – and thus can be qualified as – an ***AS*** or ***QS***.

Notational we will use the following shorthands: The Signer produces a signature σ over a message m using his secret signature key sk_{sig} (his secret signature creation data), which is denoted as $Sign(m,sk_{sig})= \sigma$. The verification process will be denoted as $Verify(m, \sigma, pk_{sig})$. It returns ***Valid*** if the message was not altered in an unauthorised way. Note, both notations are just simplifications to explain the cryptographic algorithms and highlight the process of signing and verifying. Additionally, the characteristics of ***MS***s contain the term derived signature (hereafter referred to as ***ds***). While the term Signer is used to refer to the party which produced the initial signature over a message m using his secret signature key sk_{sig} (his secret signature creation data), the derived signature is also an electronic signature. In fact, any signature derivation using the allowed transform T on a signed message, generates a transformed message m' and a valid electronic signature for that message. This newly generated signature, for which the secret signature generation key of the signer is not necessary, is called derived signature (denoted as ***ds*** or σ' in cryptographic literature). The following analysis uses the term signatory when referring to the legal meaning. Further to the role of a Signer, we refer to the party that created a subsequent derived signature by the term Sanitizer.

Can an MS be qualified as an AS?

To be able to conclude that an ***MS*** can be qualified as an ***AS***, an ***MS*** has to fulfil all the requirements the eIDAS prescribes for an ***AS***. As elaborated on previously, a ***BS*** has to fulfil four requirements to be qualified an *advanced* electronic signature.

Note however, that the requirements set forth by the eIDAS are not very technical,[22] which means that in order to transpose them into the mathematical space of cryptography they need to be closely interpreted. For example, neither the eIDAS nor the ESD define technical terminology like integrity but rather describe the desired impact, e.g. "any subsequent change of data is detectable". This means that the definition of the terms "change" and "detectable" will need to be based on technical definitions. Pöhls, for instance, defines a change of data as:

> *[…] any alteration of data (including the creation, or insertion or deletion of data) that results in observable consequences during further processing (including, but not limited to, an observable different output) when comparing it with the processing or output of unchanged data [21].*

Our analysis does not elaborate further into the details of technically mapping these legal requirements.[23] In light of the constraints of this research, we will keep the analysis as high level as possible. To maintain this level, for the sake of readability, we needed to abstract from the cryptographic solutions that implement ***MS*** and thus present the concept of ***MS*** very general, maybe even too general from a cryptographic point of view. Note, that the detailed properties of an ***MS*** are defined cryptographically,[24] and it's those cryptographic properties which allow them to adequately meet legal requirements. So an instantiation of an ***MS***-scheme[25] that is cryptographically carefully constructed and provably achieves exactly those properties allows meeting specific legal requirements, while the concept of an ***MS*** in general might not.

The first three requirements for a ***BS*** to be qualified as an ***AS*** are that it is

1. uniquely linked to the signatory;
2. capable of identifying the signatory; and
3. created using means the signatory can maintain under his sole control.

These requirements can be fulfilled with the aid of asymmetric cryptography. The third requirement because the signature generation key can be kept secret and under sole control as only the verification key needs to be known to others. In general, a ***MS*** is built on asymmetric cryptography. To achieve the requirements regarding linkage and identification there are already trust infrastructures that can provide the link between the public verification key and the signatory; best

[22] Indeed, recital 27 of eIDAS points out that "The legal effects it grants should be achievable by any technical means provided that the requirements of this Regulation are met."
[23] However we draw on work that has done this rigorously on the lower cryptographic levels [17], [52] or [56].
[24] A good overview of all the properties of signature schemes for the cloud was done as PRISMACLOUD Deliverable D4.4 [10] [56].
[25] An "instantiation" in the cryptographic literature means the actual implementable algorithm; a "***MS***-scheme" is the cryptographic term for a special algorithm achieving at least the general properties of a malleable signature (***MS***).

known is the public key infrastructures (PKI) currently in place in the Internet[26]. If the ***MS*** can be constructed such that the Signer's signature is generated by a signature algorithm that is legally established and for which the keys are deployed in the existing trust infrastructure, then the MS can achieve the first and second requirement by facilitating existing trust infrastructures[27].

An ***MS*** based on a cryptographic signature algorithm which is legally accepted fulfils the requirement of the Signer's initial signature being created using unique signature creation data. Next to that, the signatory can keep these unique signature creation data under his sole control,[28] and thus the signature created by the ***MS*** is both uniquely linked to- and capable of identifying the signatory. It can therefore be concluded that an MS complies with the first three of the four requirements laid down in article 3 section 11 jo. 26 eIDAS.

Compliance with the fourth and last requirement – the electronic signature is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable – might, however, appear to pose a problem seeing as an ***MS***-scheme is specifically used to make it possible for a Sanitizer – who, from the viewpoint of the verifier who only knows and trusts the Signer, is a third party – to alter the message after it has been signed.

Here, the definition of "detectable" – after the definition of what constitutes a "change" (of data) – is the second link between technical cryptographic definitions and legal definitions which is of paramount importance. In general, the fact that in an ***MS***-scheme the source message can be altered does, however, not mean that such a change would not be detectable, for verification yields:

$$\textbf{Verify } (m, \sigma, \mathbf{pk}) = \textbf{Valid} \text{ and } \textbf{Verify } (m'_{[scope]}, \sigma', \mathbf{pk}) = \textbf{Valid}$$

Meaning that the verification only yields true in two situations:

1. The message (m), the signature (σ), and the private key ($\mathbf{pk}$) remain unaltered; or
2. The message has been altered within the scope predefined by the principal ($m'_{[scope]}$), and a derived signature ($\sigma'_{[scope]}$) has been generated.

If the original message (m) is altered by a party beyond the scope predefined by the principal (resulting in $m'_{[non\text{-}scope]}$) the verification will yield:

$$\textbf{Verify } (m'_{[non\text{-}scope]}, \sigma, \mathbf{pk}) = \textbf{False}$$

Note, that the MS also prohibits producing a valid derived signature if the change was out of the scope[29]. Therefore, in the generality that ***MS*** was discussed so far it does not detect the subsequent authorised change. In order for an ***MS*** to fulfil the aforementioned fourth criterion of "being linked

[26] Currently Certificate Authorities (CA) issue so-called public key certificates; they are also known by the name of the technical format as X.509 certificates.

[27] For example there are schemes designed with this in mind, see [56]

[28] Or at least use with a high level of confidence that these data can be used under his sole control.

[29] The verify algorithm will issue ***False*** instead of ***Valid*** also in the situation where the signature is altered, but the unaltered message is provided, or for the situation where both the signature and the message are altered but the alterations are outside the scope authorised by the Signer, i.e.

$$\textit{Verify } (\mathrm{m}, \sigma'_{[non\text{-}scope]}, pk) = \textit{False} \textit{ and } \textit{Verify } (\mathrm{m}'_{[non\text{-}scope]}, \sigma'_{[non\text{-}scope]}, pk) = \textit{False}$$

to the data to which it relates in such a manner that any subsequent change of the data is detectable." The authorised – within scope – subsequent change needs to become distinguishable. This level of detection can be described as follows:

> *The verifier detects that at least one change to an integrity protected message has occurred. The exact number of occurred changes or where they happened remains invisible to the verifier. [21]*

This detectability must hold true regardless of the change being authorised or unauthorised, as the eIDAS clearly states "any subsequent change".[30] Hence, we need to be able to verify an ***MS*** and get the following three results:

1. Valid and unchanged (signature created by the Signer)
2. Valid and subsequently modified within the authorised scope (derived signature computed by Sanitizer)
3. Invalidly modified (MS does not verify, indicating malicious or erroneous modification / corruption[31]

In order to allow this form of detectability – mimicking closely the functionality of existing legally accepted digital signature schemes – the ***MS*** needs to offer a cryptographic property especially designed for this task called *non-interactive public accountability*.[32]

An ***MS*** satisfies non-interactive public accountability, if and only if, given a valid message and a signature over the message, a third party can correctly decide whether the message-signature pair originates from the Signer or from the Sanitizer without interacting with the Signer or Sanitizer, i.e. just from using public knowledge of the message, the signature and the Signer's (or the Sanitizer's) public signature verification key.[33]

It is important to note that the derived signature (***dS)*** still verifies under the Signer's public key if the subsequent changes were within the authorised scope which allows the Signer to still be identified (technically) as the signatory for any derived message/document. This of course might, or might not, be beneficial in light of different applications, however, that is how the verify operation works in ***MS***.

That said, this means that a malleable signature that additionally is non-interactive public accountable fulfils all four criteria of article 3 section 11 j°. 26 eIDAS, and it can therefore be concluded that in light of the eIDAS an ***MS*** is an ***AS***, and that there is no difference between the legal position of an ***MS*** and that of an ***AS***.

To summarise: the use of an ***MS*** with the additional cryptographic property of public non-interactive accountability fulfils the aforementioned fourth requirement of "being linked to the data to which it relates in such a manner that any subsequent change of the data is detectable". This means that a

[30] There are differences in the level of detectability in technical algorithms, as well as in technical definitions of the protection goal of Integrity, for more see [17]
[31] In computer science (data) corruption refers to errors in data that can occur during the reading, writing, storing, transmission, or processing, of this data. These errors create unintended changes to the original data.
[32] Cryptographically first defined in [17] for the legal purpose of making an MS scheme which behaves very closely to existing legally accepted schemes
[33] Slightly adopted from the original definition to increase readability

malleable signature fulfils all criteria of article 3 section 11 j°. 26 eIDAS, and that can be concluded that in light of the eIDAS an ***MS*** is an ***AS***, and that there is no difference between the legal position of an ***MS*** and that of an ***AS***. Note however, that the signatory still is the Signer, which comes with all the legal implications, especially regarding the signatories external relationship with the verifier. Finally note that a ***keyedMS*** – discussed in more detail a little later – can help to settle disputes between Sanitizers and the signatory in their internal relationship such as allowing claiming for compensation due to damages.

Can an MS be qualified as a QS?

To answer the question what the legal position is of an ***MS*** and whether an ***MS*** can be qualified as a ***QS***, it is necessary to evaluate whether an ***MS*** complies with the six requirements a ***QS*** has to comply with. Seeing as an ***MS*** can be qualified as an ***AS*** an ***MS*** complies with the first four requirements, which means it is necessary to assess whether it is possible to create an ***MS*** based on a qualified certificate for electronic signatures (***QC***) using a qualified electronic signature creation device (***QD***).[34]

As follows from Annex I to the eIDAS a ***QC*** has to comply with ten requirements, and none of these requirements specifically pose more of a problem in the case of malleable signatures when compared to other forms of electronic signatures. It is therefore safe to conclude that it is just as possible to create an ***MS*** based on a ***QC*** as it is to create any other ***ES*** based on a ***QC***.

The requirements of the ***QD*** are described in four articles in Annex II of the eIDAS. Article 1 Annex II eIDAS contains (technical) requirements a ***QD*** has to comply with, and these should, similar to the (technical) requirements a ***QC*** has to comply with, not specifically pose more of a problem in the case of malleable signatures when compared to other form of electronic signatures. In fact, Pöhls et al. [22] showed that several cryptographically secure MS-schemes, even those that do work with standard signatures, can be tweaked to work on off-the-shelf QD – known as smartcards or hardware security modules (HSM) – such that the secret signature-creation data never leaves the QD. As such requirements of Article 1 Annex II eIDAS are not a problem for ***MS*** and will not be elaborated on further. Article 3 Annex II eIDAS states that only a qualified trust service provider (ex. article 3 section 20 eIDAS) may generate or manage electronic signature creation data. Because this provision is irrelevant for answering the question whether an ***MS*** can be qualified as a ***QS*** this provision will not be elaborated on. Article 4 Annex II eIDAS states that qualified trust service providers may only duplicate the electronic signature creation data (as defined in article 3 section 13 eIDAS) for back-up purposes under specific conditions. Because this provision, like article 3 Annex II eIDAS, is irrelevant for answering whether an ***MS*** can be qualified as a ***QS,*** hence this provision will not be elaborated on. However, article 2 might become problematic for ***MS***.

Article 2 Annex II eIDAS is highly relevant in light of the question whether an ***MS*** can be qualified as a ***QS,*** and thus what the legal position is of an ***MS***, as it reads:

> *[**QDs**] shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.*

In essence article 2 Annex II eIDAS creates two requirements a ***QD*** has to fulfil:

---

[34] Considering the constraints of this research, only the requirement(s) which are of direct relevance for the aforementioned question will be elaborated on.

1. A ***QD*** shall not alter the contents of the data to be signed prior to signing;[35] and
2. A ***QD*** shall not make it impossible to show the data to the signatory prior to signing.[36]

According to an article by Höhne et al.[37] the problem of not knowing (and thus not showing) all possible derivations of a document signed by a ***MS*** would prevent an ***MS*** from being qualified as a ***QS***[38] because:

> *When using an MS, the future modifications are not known to the signatory at the time of signature creation and therefore cannot be presented. […] Barely because of this incapability to present the entire data to-be-signed to the signatory before the signature is created, malleable signatures are not a QS in the sense of the German signature law.*[39,40]

After consulting with all the authors of the original work it became clear that the above cited text is based on a very strict interpretation of German legislative texts that requires electronic signatures to be functionally equivalent to handwritten ones and lists those functions.[41] Höhne et al. concluded that under a strict grammatical interpretation the ***MS*** could on the one hand not fulfil the conclusory function (in German 'Abschlussfunktion') and on the other hand not fulfil the archiving or integrity function (in German 'Perpetuierungs- oder Integritätsfunktion'). The argument for the above cited conclusion was that the ***MS*** during signature generation will not be able to present to the signatory all the different versions it might have after subsequent authorised changes. Hence, the argument was more related to the general problem in ***MS*** of how to show all the different versions that the Signer signs, rather than being a problem of the ***QD*** specifically making that impossible.

However, in (as of yet not published[42]) follow up work of the author the reasoning is less strict. Under the following assumptions the ***MS*** can be treated as a blanket statement.[43] Treating the ***MS*** as an underspecified statement and cryptographically (or by technical means) allowing the verifier to detect that it was underspecified and to be able to prove to a third party like a judge that the signatory consented to it, adds confidence. It can be assumed that a signature created with an ***MS*** is

---

35 A qualified electronic signature creation device can in that sense be likened to an automated postage meter or franking machine, the application of postage or franking to an envelope does not alter the contents of the envelope.

36 As such, based on the previously used analogy, the signatory can verify that the contents of the envelope were not altered by the application of postage or franking.

37 Höhne, Pöhls, and Samelin, 'Rechtsfolgen editierbarer Signaturen' [52] in German.

38 Höhne et. al.'s article based their conclusion on (the now repealed) art. 2 Annex III ESD. This article is very similar to art. 2 Annex II eIDAS though as it reads;

> *Secure signature-creation devices must not alter the data to be signed* ***or prevent such data from being presented to the signatory prior to the signature process****.*

39 *Infra* 15, p. 487-488.

40 Translation from German by the author; Original in German: Bei Benutzung einer editierbaren Signatur sind Modifikationen […] dem Unterzeichner nicht zum Zeitpunkt der Signaturerstellung bekannt und daher nicht darstellbar. […] Nur wegen der fehlenden Anzeigemöglichkeiten stellen editierte Signaturen keine qualifizierten Signaturen im Rechtssinne dar. [52]

41 Deutscher Bundestag. Drucksache 14/4987. dip21.bundestag.de/dip21/btd/ 14/049/1404987.pdf, Dec. 2000.

42 Henrich C. Pöhls actually argues for a less strict interpretation in his PhD. thesis [17].

43 Blanket statements are underspecified statements, similar to blank cheques. Legally, you are allowed to leave certain fields underspecified or empty, allowing them to be filled with information later. If done in a consented way, any specific information filled in later is attributed to the original signatory of a blanket statement.

technically distinguishable from a standard signature scheme, for example verification with a standard scheme's verification algorithm will not work.

Hence, even though the signatory was not presented with all possible modifications that could be derived from the document signed with an ***MS,*** the signatory was well aware that he created a blanket statement using the ***MS*** and marking specific areas as modifiable by a specific third-party group later.

In other words, the reduction of the integrity protection, which is offered by an ***MS,*** is assumed to both be known-to and consented-to by the signatory. The scope of protection, in other words all the possible subsequent changes, is made clearly visible towards the Signer, but might also need to be visible to the verifier.[44] The latter is not true for ***MS*** in general, but must (again) be achieved by cryptographically designing the ***MS*** algorithms such that this can be deduced.[45]

In PRISMACLOUD we do share this opinion: The Signer consents to the subsequent authorised changes because the Signer signs the message, i.e. creates a valid signature for it, and at that time also defines the scope within which a (specific) third party is authorised to modify the contents of that (signed) message.

The Sanitizer creates a derived signature (***σ'***) for that content,[46] hereafter referred to as ***ds***. Afterwards the modified contents of the signed message can be verified with that derived signature. As long as the modifications by the third party take place within the predefined authorised scope, verification will yield valid:

$$\textbf{Verify } (m'_{[scope]}, \sigma'_{[scope]}, \text{pk}) = \textbf{True}$$

Once the Signer has created a valid signature using an ***MS*** any authorised alteration or modification of the contents does not need the Signer's secret signature-creation data to generate the ***ds***, which means the (altered) data do not need to be shown to the signatory again. If the alteration or modification of the contents, however, exceeds the predefined authorised scope, verification will logically yield invalid:

$$\textbf{Verify } (m'_{[non\text{-}scope]}, \sigma'_{[scope]}, \text{pk}) = \textbf{False}$$

However, the Signer has created the signature and even a ***ds*** created by a Sanitizer – not the Signer – for a modified document containing only authorised alteration or modification of the contents verifies under his public verification key. Again, if the authorisation is verifiable by a third-party and was part of the signed document, the verifier can argue that the ***MS*** with this specific scope for subsequent authorised modifications was applied and was consented to by the Signer. This generates a blanket statement. In Germany this would mean the Signer remains the principal who initially signed and is the signatory of a blanket statement. In Germany the signatory is liable for the signed

[44] we do not go into the details on how this can be technically achieved here, but see for example again the construction in [56] or for a more detailed way of describing the allowed modifiaction.
[45] see again [56] as an example of a cryptographic way of achieving this. Also other schemes proposed by others allow achieving this.
[46] The signature affixed to a message by the third party authorised by the Signer to alter the message, hereafter referred to as ***ds***.

contents of any statement derived from the blanket statement to the extent that the signatories' liability depends on the specific legal circumstances.[47] To limit this liability and to further add accountability it is suggested that the Sanitizer (if it has created a valid ***ds***) can also be held accountable. Preferably by technically attributing this accountability with the aid of a legally recognized signature scheme. Hereafter identifiability of the Sanitizer will be referred to with the term ***keyedMS***.

Seeing as neither the requirements for a ***QC*** nor the requirements for a ***QD*** pose a problem in light of an ***MS***-scheme, it is possible to conclude that the legal position of an ***MS*** and a ***QS*** is the same as for the ***AS*** because an ***MS*** is:

1. uniquely linked to the signatory;
2. capable of identifying the signatory;
3. created using means the signatory can maintain under his sole control;
4. linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;
5. created by a qualified electronic signature creation device (***QD***); and
6. based on a qualified certificate for electronic signatures (***QC***).

So to summarize, an ***MS*** can be a ***QS*** if one is using an ***MS*** that is unforgeable and non-interactive public accountable and you are using a signature scheme (for at least the Signer) for which the secret signature-creation data can be based on qualified certificate (***QC***) securely stored and used inside the ***QD***. Both can be technically achieved.[48]

This raises the question, however, what the positive legal gain and impact of a ***keyedMS*** is, as it – like the general ***MS*** – can be qualified as an ***AS*** or ***QS***.

What are possible legal implications of a *keyedMS*?

It is possible for the Signer of an ***MS*** to select a specific set of Sanitizers, so that authorised modifications can only be done by a defined party. A general ***MS***-scheme allows the derivation function to be public, whereas a ***keyedMS*** achieves the exact opposite; there is one unique secret sanitisation key per Sanitizer which is required to derive a valid signature. The workflow for a ***keyedMS*** is depicted in Figure 3.

[47] § 172 Abs. 2 of the German civil code (BGB) can be applied [see Schramm § 172 BGB, Rn. 17, and also ruled by the German Federal Court of Justice (BGH) 11.7.1963 - VII ZR 120/62

[48] See several MS-schemes where the signature generations operate inside the smartcard and the secret signature generation data never leaves the confined perimeter of the smartcard in [18]

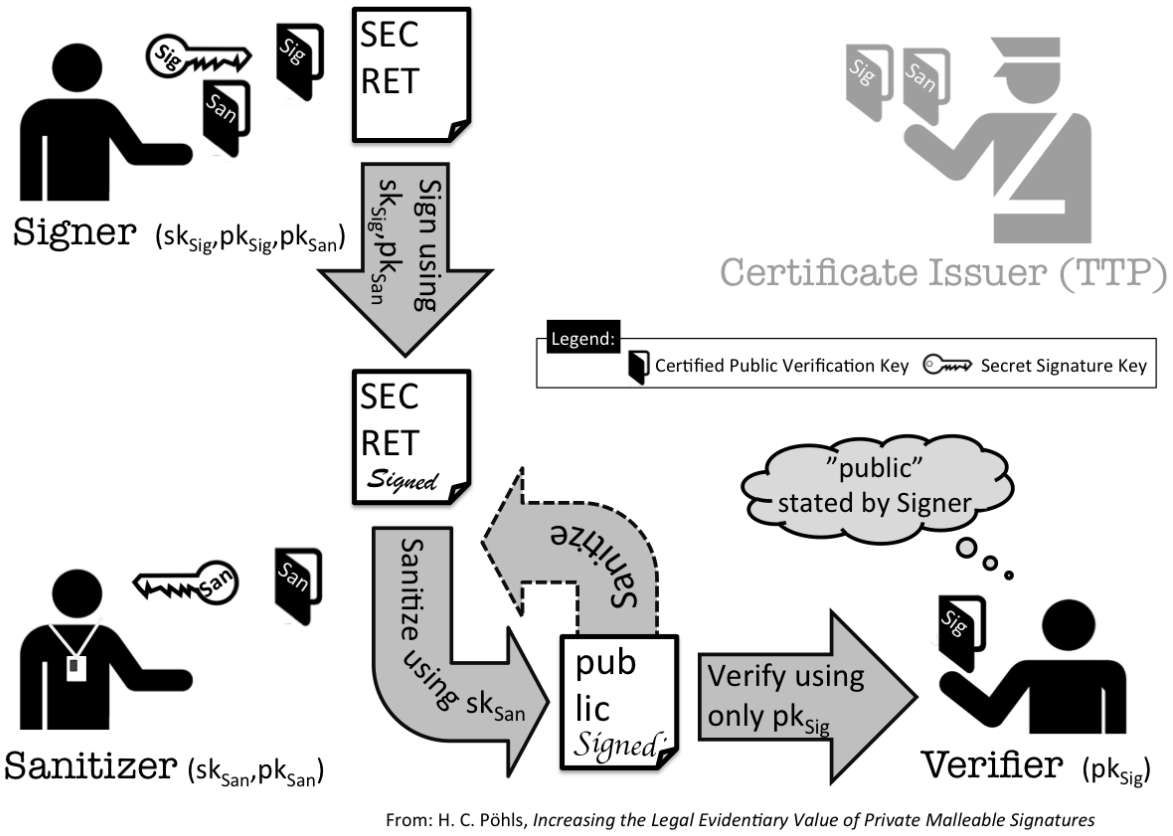

Figure 3: Workflow for a keyed malleable signature scheme, the Sanitizer needs a secret key to derive a signature; keys are distributed out-of-band beforehand; QC can be issued with the help of a trusted third party [21]

In general – and there are ***MS***-schemes that allow this – a ***keyedMS*** can use the same techniques for the Sanitizer's involvement of the secret sanitisation key as they use for generating a derived signature (***ds***). Hence, we argue that a public non-interactive accountable ***MS*** could allow linking the ***ds*** to the Sanitizer in such a way that it also identifies the Sanitizer. It will, however, still allow the identification of the Signer as this is required under the general functionality of an ***MS***. With a ***keyedMS*** we will assume we additionally gain the ability to link and identify the Sanitizer once it does an authorised subsequent change. Moreover, the Sanitizer's ***ds*** in a ***keyedMS*** is assumed to be linked to the changed message in such a way that any subsequent change can be detected. This additional linkage and identification of the Sanitizer does not negatively impact on the possibility of a ***keyedMS*** to be qualified as an ***AS*** or a ***QS***. A ***keyedMS***, if it is additionally non-interactive public accountable, fulfils the same requirements as those stipulated in respectively article 3 section 11 j°. 26 eIDAS and article 3 section 12 j°. article 3 section 10 j°. article 3 section 11 j°. article 26 eIDAS.

It is possible to distinguish between two different scenarios which are relevant for answering the question what the legal implication of a ***keyedMS*** is, and within each of these scenarios two different scenarios can in turn be distinguished.

1. The third party (Sanitizer) alters the message within the predefined scope (m'_{scope})
   A. The ***MS is keyed*** i.e. the third party *can* be identified through the ***ds***
   B. The ***MS*** is unkeyed i.e. the third party *cannot* be identified though the ***ds***
2. The third party (Sanitizer) alters the message beyond the predefined scope ($m'_{non\text{-}scope}$)
   C. The ***MS*** is keyed i.e. the third party *can* be identified through the ***ds***

D. The ***MS*** is unkeyed i.e. the third party *cannot* be identified through the ***ds***

In the first scenario (A) the legal status of the ***ds*** in relation to the Sanitizer is similar to, if not the same as, the legal position of a "normal" signature in an ***MS*** with respect to the Signer; it can be fulfil the requirement of both an ***AS*** and a ***QS***. Because the ***MS*** is keyed the third party that created the ***ds*** can be identified, which means a keyed ***MS*** complies with all of the six aforementioned requirements for a ***QS*** and the third party is the (mandated) signatory.

In the second scenario (B) the legal position of an ***MS*** is that of an ***AS*** or a ***QS***. Even when the verifier sees the ***ds*** in an unkeyed ***MS,*** the ***MS*** at its core still makes it possible to comply with the second requirement of an ***AS*** i.e. "the ***ES*** is capable of identifying the signatory". As such an unkeyed ***MS*** can in principle be qualified as an ***AS*** or a ***QS***. The Signer is the signatory and the Sanitizer can be attributed no status in light of the eIDAS. The fact that the Sanitizer has no formal status, can have (very) negative implications, for if it comes to a dispute between the Signer and Sanitizer, it is not possible to determine liability, let alone to assign remuneration for damages (third party) incurred. Next to that, it will be more difficult for the Verifier to assess the risk(s) in connection to the signed message.

The third scenario (C) might look similar to scenarios A and B, and as such the legal position of a keyed ***MS*** would appear to be the same. This is, however, not the case as in scenario C the signature verification fails, as – unlike the first scenario – it is not possible to determine the identity of the Signer nor of the Sanitizer. This same conclusion can be drawn in relation to scenario D, as an invalid signature does not provide any insights into whom – if anybody – modified the message which as a result invalidated the signature(s). In principle these modifications could have been performed by the Signer, the Sanitizer, the Verifier, or any other third party, next to just being the result of corrupted data as a result of errors during storage or transfer.

Functional electronic signature scheme (FS)

A functional electronic signature scheme, as the name suggests, relies on a functional electronic signature, hereafter referred to as an ***FS***. In short an ***FS***-scheme works based on a key pair consisting of a secret master key (**sk**) to sign messages with and a public key (**pk**) to verify these signed messages.

The **sk** can be used to sign any message with, and the signatory can derive a separate signing key for a specific task or function ($\mathbf{sk}_f$). This $\mathbf{sk}_f$ the signatory can hand over to any third party so that this party can perform a specific task or function on ***m*** on behalf of the principal. With the $\mathbf{sk}_f$ the third party can generate a valid signature after amending the original message based on the following equation:

$$\mathbf{Sign}\ (f(m), \mathbf{sk}_f) \rightarrow \sigma$$

Meaning that a valid signature is only created when $\mathbf{sk}_f$ is used to sign a message within the, by the principal predefined, functional scope. Therefore when σ on $f(m)$ is verified it yields:

$$\mathbf{Verify}\ (f(m), \sigma, \mathbf{pk}) = \mathbf{Valid}$$

Whereby it is important to note that the equation holds true if, and only if, the third party did not exceed the scope or range of the function it was authorised to sign by the principal. The use of a ***FS***-

scheme does not pose too many problems in light of the eIDAS as the term signatory is, as stated before, defined in article 3 section 9 eIDAS as:

> *A natural person who creates an electronic signature.*

In essence this definition states that a signatory is a person who can create any form of electronic signature, i.e. a ***BS***, ***AS***, ***QS***, ***MS***, or ***FS***, either on his own behalf or on behalf of a person or entity he represents.[49] And as an ***FS*** is in electronic form, it is attached to, or logically associated with, other electronic data, and is used by the signatory to sign, no elaboration is necessary to conclude that a functional signature is an electronic signature ex article 3 section 10 eIDAS.

Can an FS be qualified as either an AS or a QS?

To determine whether an ***FS*** can be qualified as either an AS or a QS, it is important to point out that an ***FS*** is, in principle, the same as any other electronic signature, except for the fact that:

- instead of using a **sk** the signatory (i.e. the third party) uses $\mathbf{sk}_f$ to create σ; and
- instead of being able to sign *any* m the third party is only authorised to sign a predefined function of m on behalf of the principal.

Because the four requirements an ***ES*** has to comply with to be qualified as an ***AS*** neither contain a requirement regarding the signature key, nor contain a requirement regarding the scope of the authorisation the signatory has to sign, it can be concluded that an ***FS*** can be qualified as an ***AS.***

Similarly, because the additional two requirements an ***ES*** has to comply with to be qualified as a ***QS*** (next to the first four which make it possible to qualify ***FS*** as an ***AS***) do not contain a requirement regarding either the signature key or the scope of the authorisation the signatory has to sign, it can be concluded that an ***FS*** can be qualified as a ***QS.***

Because the third party is always identifiable,[50] only the aforementioned scenarios A and B are possible in the case of an ***FS***-scheme, and the same conclusion(s) can be drawn. In both scenarios the third party to whom the principal provides the sk_f is identifiable which means the third party is the (mandated) signatory representing the principal.

In scenario A – the third party to whom the principal provides the $\mathbf{sk}_f$ does not exceed the scope or range of the function it was authorised to sign – the principal *is* bound by this signature and *is* liable for any damages it might incur because of the third party's signing, as follows from:

$$\textbf{Verify } (f(m'_{[scope]}), \sigma, \text{pk}) = \textbf{True}$$

[49] Despite the rephrasing of the definition in the eIDAS, similar to the (old) article 2 section 3 ESD, under the eIDAS a signatory can act either on his own behalf or on behalf of a person he represents.

[50] Seeing as the principal derives $\mathbf{sk}_f$ from **sk** for a specific task or function and for a specific party, this party is always identifiable. If the third party hands over the $\mathbf{sk}_f$ to another party who signs any message with it, the third party is considered the signatory and the third party will be liable for any damages which might arise from an alteration of the message beyond the predefined scope.

Whereas in scenario B – the third party to whom the principal provides the $\mathbf{sk}_f$ exceeds the scope or range of the function it was authorised to sign – the principal is *not* bound by this signature and is *not* liable for any damages it might incur because of the third party's signing, as follows from:

$$\textbf{Verify } (f(m'_{[non\text{-}scope]}), \sigma, \text{pk}) = \textbf{False}$$

Next to that if the third party exceeds the scope or range of the function it was authorised to sign, that party no longer represents the principal which means that the third party itself is bound by the signature as he or she is the signatory.[51]

5.4. Conclusions: Legal status and requirements for malleable- and functional signatures

Based on article 3 section 10 eIDAS, for data to be considered an ***ES*** the data needs to fulfil the following requirements:

1. The data needs to be in electronic form;
2. The data needs to be attached to, or logically associated with, other electronic data; and
3. The data needs to be used by the signatory to sign

Based on article 3 section 11 j°. article 26 eIDAS, for an ***ES*** to be considered an ***AS***, it needs to be:

1. **(RL1)** uniquely linked to the natural person who created the signature;
2. (**RL2**) capable of identifying the natural person who created the signature;
3. (**RL3**) created using electronic signature creation data that the natural person who created the signature (called signatory hereafter) can, with a high level of confidence, use under his sole control; and
4. (**RL4**) linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Based on article 3 section 12 j°. 3 section 11 j°. 26 eIDAS, for an ***ES*** to be considered a ***QS***, the ***ES*** needs to be:

1. (**RL1**) uniquely linked to the signatory;
2. (**RL2**) capable of identifying the signatory;
3. (**RL3**) created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control;
4. (**RL4**) linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;
5. (**RL5**) created by a qualified electronic signature creation device (***QD***); and
6. (**RL6**) based on a qualified certificate for electronic signatures (***QC***).

(For future references in the project, the legal requirements listed above are numbered with requirement reference numbers starting with the prefix RL.)

[51] In as far as it is possible to, first of all ascertain the identity of the third party, and second of all determine the message was modified deliberately outside of the predefined scope.

An ***MS*** – in its original form or in the form of a ***ds*** generated either with an additional key (***keyedMS***)[52] or without an additional key (unkeyed) – as well as an ***FS*** complies with the requirements of article 3 section 10 eIDAS, as such each of these is an ***ES*** in the sense of the eIDAS.

Because both an ***MS*** – the original signature or a *keyed* ***ds*** – as well as an ***FS*** is:

- created using unique data that the signatory can, with a high level of confidence, use under his sole control;
- is both uniquely linked to and capable of identifying the signatory; and
- linked to the data signed therewith in such a way that any subsequent change in the data is detectable

each of these is an ***AS*** in the sense of article 3 section 11 j°. article 26 eIDAS.

Depending on the implementation, it possible for both an ***MS*** as well as for an ***FS*** to be:

- created by a qualified electronic signature creation device; and
- based on a qualified certificate for electronic signatures

As such, an ***MS*** – in its original form or in the form of a derived signature (***ds***) generated either with an additional key (***keyedMS***) or without an additional key (unkeyed) – depending on the implementation of respectively the ***MS***-scheme can be a ***QS*** in the sense of article 3 section 12 jo. 3 section 11 jo. 26 eIDAS. Note, that a qualified certificate induces additional organisational security methods for the issuer of those certificates, known as the Certificate Authority or now identity provider (eIDAS).

Also, an ***FS***-scheme – depending on the implementation – can be a ***QS*** in the sense of article 3 section 12 j°. 3 section 11 j°. 26 eIDAS.

Finally note, that using a ***keyedMS*** allows identifying the Sanitizer as technically accountable for the modifications. To aid appointing liability it is advised to have a ***keyedMS*** implemented such that the Sanitizer's derived signature (***ds***) is also a ***QS***[53].

[52] Hereafter, we abbreviate the notion of derived signature (***ds***) generated with an additional key (***keyedMS***) as a *keyed* ***ds***

[53] This can be technically achieved, for example see Brzuska et al. [56] or De Meer et al. [56].

6. Social Trust Requirements

In this chapter we report of the results of literature studies that we conducted that helped us to elicit on social factors determining end trust and technology acceptance that may be of importance for PRISMACLOUD.

6.1. A4Cloud requirements survey summary and additional literature

The A4Cloud project (www.a4cloud.eu) made several surveys to gather requirements for their "Accountable Web" supporting tools (Fischer-Hübner et al. 2015) [23]. Among these was a literature review (A4Cloud deliverable D:C-7.1 [3], section 5.6) which will be summarised here with special emphasis on the trust issues and HCI requirements that were found (numbered from A-M). The distinction between individual end users (data subjects) and company cloud users will not be particularly emphasised below as the problems of misperceptions have implications for how end-to-end security is understood, and the requirements stated in A4Cloud should have close parallels in PRISMACLOUD. In addition, some more recent reports and papers will also be summarised here.

However, to start with, the A4Cloud requirements analysis derived from the literature surveyed resulted in this list of items that will be briefly explained and discussed below:

A. Users should be able to pursue experimentation and enquiring. Users should be guided beyond enquiring only friends and relatives.
B. Users should be clear about the difference between service performance and privacy performance.
C. Users should be able to balance their impressions gained from pricing with other relevant information about trustworthiness.
D. Users should not be frightened away from unattested sites if stakes are low (good prices are often worth the price of uncertainty). *
E. Users must develop robust models of trusted cloud computing services.
F. Business end users need to be correctly informed about cloud security, performance, and availability for individual cloud services they consider.
G. Internationalisation is more than just translation.
H. Clearly mark the possibility and ways of redress.*
I. Users should know when and where trustworthy transparency information is to be found.*
J. Users must be able to understand the extent to which they can act under pseudonyms and that such identification schemas can provide access to transparency information.
K. Users must trust that they can manage in a life-long way the information associated with different identities (implications for transparency and restitution controls).
L. Users must be able to put the right scope to their distrust.
M. As users do not check privacy statements etc., users must be made aware of trustworthy assessments of trustworthiness.

Several authors have stated or indicated that (A) well placed trust grows out of active enquiry ([24], [25], and Trustguide TG2 [26]). Users should be able to pursue experimentation and enquiring in safe environments which must not oversimplify the complex cloud service ecology. Tools should make it possible to enquire good sources so that users are guided beyond enquiring only friends and

relatives. This should also help users to (B) be aware of the difference between service performance and privacy performance – there is a general tendency to transfer trust: trust in the company itself is often transferred to trust in the security of their cloud services (inter alia DMA[54] and Marshall & Tang 2012 [27]). (C) There is likewise an unfounded belief among individual end users that cost implies higher trustworthiness [27]. This requires evaluation results concerning trustworthiness to be as prominent as cloud providers' cost schemes.

There are on the other hand also reasons not to alarm users. For individual end users must (D) situation-dependent risk-taking which includes a proportional risk assessment be preferred over exaggerated risk-avoidance ([28], Trustguide [26], p 20, [29]). Users should not be frightened away from unattested sites if stakes are low (good prices are often worth the price of uncertainty). An attitude that (E) "Internet is intrinsically insecure" ([27], [30], [31], [26]) must be met both in the user interface with direction to sources which sceptical users would normally rely on and also, as the Trustguide stresses [26], outside the user interface.

(F) "…perceived availability, access, security, and reliability would be key variables of cloud computing acceptance in public sectors since they were found to be influential in predicting the behavioural intention to use cloud technologies" Shin (2013 [32], p 200) Thus, correct information on these matters is required. This requirement holds for the private sector [33] as well as for the public sector. For the private sector this requirements also meets the problem of a "business first attitude" (where economic considerations far outweigh privacy concerns; Fischer-Hübner et al. 2015 [23], p. 101) if accountability measurements are included in the information so that such aspects can easily be included in the decision process.

Just as public and private sectors might sometimes differ, also (G) "Users from different countries may have different privacy expectations and understanding of privacy guarantees offered by the cloud storage system" [30] and this implies that simple translations are not enough but deeper understanding is required of different cultural traits.

Clear and actionable processes are helpful in trust building. (H) Restitution measures have positive trust effects and (I) transparency "brings increased confidence", according to the Trustguide [26]; and research by the Direct Marketing Association DMA showed similar results in the present decade.

There are also some problematic cases. One was identified already in the PRIME EU project[55]: (J) Unawareness of options for identity management, such as anonymity options, has negative effects on trust in privacy-enhancing technology [31]. Users must be able to understand the extent to which they can act under pseudonyms and that such identification schemas can provide access to transparency information. How could this be demonstrated within the user interface? Then there is also a problem that (K) users fear a lack of longevity of certain pseudonyms, such as email addresses. Work addresses might not work if they are changed. Thus, there is a user preference for long-lasting identifiers such as personal email addresses also when they should use professional identifiers [34]. Implications for end-to-end security in the cloud is that users must trust that they can manage in a life-long way the security "obstacles" that PRISMACLOUD security solutions provide.

[54] Direct Marketing Association (DMA) http://www.dma.org.uk
[55] EU FP6 project PRIME, www.prime-eu.com

Finally, the literature review conducted in A4Cloud showed two conflicting conclusions on the relation between trust and unsubstantiated claims. The Trustguide states that, (L) "trust is not built through unsubstantiated claims of security and protection. Being clear about the benefits and issues related to a service will engender far greater trust" [26]. "We have observed many instances where people have not engaged with a service simply because they did not like the terms and conditions because they did not inform them effectively in their risk assessment process." (ibid.). By contrast, in another study it was concluded that, (M) "A strong privacy statement, despite the presence of cues to lack of trustworthiness, increased participants' reported trust" (Joison et al. 2010 [35], p 16). The A4Cloud deliverable suggested an elaboration of the meaning of the term *unsubstantiated claims*: "For the future one might investigate the hypothesis that more specific claims (among the unsubstantiated claims) instils more trust than general bragging if we take "general bragging" to also include complex privacy statements, as people regard them as being deliberately complex to obfuscate the terms and conditions according to the Trustguide ([26], p 85); thus, they are not examples of specific claims because such claims need to be succinct enough for readers to grasp the specific claims being made."

To this review it can be worth adding a study by Lancelot Miltgen and Peyrat-Guilard published 2014 [36]. First, it elaborates a model for "antecedents and outcomes" of privacy concerns, based on Smith et al (2011) [37] and Li (2011) [38]. The model shall not be repeated here but it may be worth to consider adapting it for security concerns. Besides extensive literature discussions, the paper reports on a study on differences in privacy concerns between European countries and generations (with data collected in seven countries). They find a difference in the significance of responsibility versus trust, such that the more Internet savy French speak of responsibility of the individual while the less Internet familiar Greece would trust the company requesting personal data (p. 114). Interestingly, young people are "more confident of their ability to prevent possible data misuse […]. A reverse privacy paradox thus appears in our results: The lower [privacy concern] of young people combine with their higher protective behaviours to offer an explanatory framework for contradictory results in prior literature". (p. 119)

"Can I trust the trust mark?" asks the *Trust marks report 2013* from the European Consumer Centres Network (ECC-net) [39]. This report recognises that earlier research has found five major areas of concerns for e-commerce, namely security, privacy, unfamiliarity with services, lack of direct interaction, and the credibility of information. Security is pointed out as the key concern. Trust marks should give confidence, but an EU survey from 2012 showed that around half the respondents did not know what a trust mark is and even more did not know how to identify a trust mark. Moreover, the survey showed the many people do not know the criteria or if such criteria are evaluated. The report ends in recommendations on good criteria for trust marks including certifications, sanctions, and cooperation, and also on requirements of adherence to ADR/ORD schemas, that is, Alternative and Online Dispute Resolution. There is also a section on "The need for uniform practice" which is a requirement hard to follow for any individual project, such as PRISMACLOUD, but providing tools for guiding lay cloud users to using privacy-enhancing crypto solutions is part of the desired uniform practice.

We find the conclusion by Joinson and Piwek [40] pertinent: "In this paper we have argued that technology and tools can be used to extend, amplify and shape behaviours, and that in doing so they may have a transformative effect. As social scientists we usually assume that a behaviour is preceded by a decision or preference of some kind (e.g. theory of planned behaviour – Ajzen, 1991). However,

there is also evidence that behaviour creates a preference, rather than simply being the product of a preference (Ariely & Norton, 2007). So, if technology and tools are changing behaviour, they may, in turn, also be changing people's attitudes towards those same actions. We conclude therefore that it is critically important that we not only understand how new media technologies and tools are changing behaviour, but also how those processes can be harnessed in order to create a social good."

The Data protection Special Eurobarometer 2015 [41] factsheet[56] from June 2015 concludes that the Eurobarometer survey of March 2015 "confirms the need to finalise the data protection reform". Highlights include: "Only a minority (15%) feel they have complete control over the information they provide online; 31% think they have no control over it at all. • Two-thirds of respondents (67%) are concerned about not having complete control over the information they provide online. • A majority of respondents are concerned about the recording of their activities via payment cards and via mobile phones (55% in both cases)." These results definitively suggest mechanisms such as anonymous credentials and big data anonymization besides, of course, secure cloud storage using a cryptographic storage network. Furthermore, "two-thirds of respondents think it is important to be able to transfer personal information from an old service provider to a new one" and that 70% "are concerned about the information being used for a different purpose from the one it was collected for." This has implications along several of the PRISMACLOUD cryptographic primitives, such as the certification of virtualised infrastructures and data security for database applications.

Thus, there is ample evidence for the pertinence of the PRISMACLOUD ideas. In the same time, these newer works do not seem to add much detail to the previously collected requirements (A-M). However, some of these requirements reflect the purpose of the earlier project (D, H, and I).

Of the other requirements, the four last (i.e., J-M) would be particularly relevant for PRISMACLOUD.

The following section will take a special look at research on technology acceptance models which will generate high-level requirements very much like the more general ones above, while the next chapter will provide data on requirements gathered for the specific scenarios initially envisaged for the PRISMACLOUD project.

6.2. Technology Acceptance Models

The general goal of any security technology (which includes for the purpose of this section also privacy preserving technology) should be to provide an adequate level of security, to be usable, and to be actually used. The actual usage in application areas where people have a choice not to use the technology requires trust but also much more. Literature in the context of Technology Acceptance Models has researched on factors that influence acceptance and thus actual usage. Such factors are e.g. costs and benefits, while different factors influence each other.

Therefore, it is important to not only consider security/privacy, usability and trust but to consider all factors and how they influence each other. For this reason, we studied the literature in the area of Technology Acceptance Models in general and in particular those focussing on security aspects. This

[56] http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf

section first summarizes the factors that have been identified in the literature starting with general models and continuing with those specific for privacy and security.

6.2.1. General Models

There are actual two main paths. One is the actual Technology Acceptance Model (TAM); the other one is Unified theory of acceptance and use of technology (UTAUT) which was established in parallel.

The original TAM by Fred Davis [42] identified behavioural intention to use as precondition to actual usage. Furthermore, precondition to the behavioural intention are the users attitude towards using as well as perceived usefulness. In additional, both, perceived usefulness and attitude towards using are influenced by the perceived usefulness.

The focus of TAM2 [43] – the extension of TAM – is on external influencing factors. The identified factors are: subjective norms, experience, and image of the system, job relevance, the quality of the output and the demonstrability of the results.

TAM2 has been further studied and extended within TAM3 [44]. Additional external factors were identified. These are: Computer Self-efficacy, perception of external control, computer anxiety, computer play fullness, perceived enjoyment, and objective usability.

UTAUT [45] has a simpler core. The actual use of behaviour is mainly influenced by behavioural intention. The authors showed that demographics like gender and age influence behavioural intention. Additional factors that influence the behavioural intention: performance expectancy, effort expectancy, social influence, and facilitating conditions. The future work is UTAUT 2 [46]. While the authors identified more relationships between different factors they also identified three new factors namely hedonic motivation, price value, habit.

6.2.2. Security related Models

These foundations have been applied in several security and privacy critical contexts, i.e. based on the literature, a model for the precise system have been deduced and then evaluated in a user study or survey. Furthermore new factors have been evaluated and tested accordingly. For instance in [47], Lallmahamood studied the acceptance of E-Banking in Malaysia. Lallmahamood based the model mainly on the TAM model and added the factor perceived security and privacy and developed corresponding items for their survey to evaluate whether it has an influence. The author identified security/privacy issues as the most important determinants for non-intended usage.

Similarly the authors of [48] studied the adoption of E-Banking in Tunisia. The authors extended the TAM model by security and privacy, self-efficacy, social influence, and awareness of services and its benefits.

The authors of [49] studied the acceptance of email authentication services. They mainly base their model on TAM. Similar to the previous paper they identified and evaluated new security/privacy related factors, namely threat appraisal and privacy concerns.

The acceptance of anonymous credentials have been studied in [50]. The new factors in this paper are understandability of security technology and guarantees

While the previous papers study concrete application, Wang [51] studies the adoption of Information Security Technology. Again the author built the model on the TAM model. The new factors in this model are knowledge based on information available, awareness of the problem, and their past experience. Wang identified a strong correlation between knowledge and attitude and intention.

6.2.3. Summary

From this literature review a number of factors can be deduced that can influence acceptance and adoption. These are besides usability and perceived usefulness:

- Subjective norms*
- Experience*
- Image of the system / provider *
- Computer Self-efficacy*
- Perception of external control
- Demographics like gender and age *
- Social influence*
- Perceived security and privacy
- Awareness of the problem and abstract solutions
- Understandability / knowledge
- Privacy/security guarantees

Some of them can be influenced by the one who deploys a new security or privacy technology while some cannot be changed by external factors (labelled with *).

Note that these factors have the last one as a pre-condition, i.e., that adequate privacy and security guarantees are provided by the technology.

6.3. High-level requirements for trust and acceptance

From the two literature reviews presented in this chapter, it is possible to formulate the requirements that the following factors need to be considered (for future references in the project, they are numbered with requirement reference numbers starting with the prefix RS, where ‘S’ is for ‘Social’):

- (RS1) Users must understand the extent to which they can act under pseudonyms
- (RS2) Users should trust that one can manage in a life-long way the information associated with different identities
- (RS3) Users should be able to put the right scope to distrust
- (RS4) Users should be made aware of trustworthy assessments of trustworthiness
- (RS5) Users must believe that organizational and technical resources exist to support the use of the system (“external control”)
- (RS6) Perceived security and privacy should be high enough to motivate adoption
- (RS7) User should be aware of the problem and abstract solutions
- (RS8) Users should understand what technology implements abstract solutions
- (RS9) There should be privacy/security guarantees

Notably, some are better addressed in tutorials than in the user interface, and some must be addressed by certification/organisational means. The following chapter makes more specific suggestions for UI designs when commenting on requirements elicited within the PRISMACLOUD project.

7. End user and HCI-related requirements

7.1. Methodology

For following a human-centred approach, we in PRISMANCLOUD task 2.1 were in particular interested in understanding the needs and expectations of the end users. Hence, our objective has been to put a focus on the elicitation of requirements from stakeholders representing end users or understanding end user needs. Especially as PRISMACLOUD is focusing on cryptographic schemes presented in chapter 4 which may be counterintuitive to users, an important goal for the project is to elicit HCI requirements using empirical HCI methods in order to address usability aspects for the project.

In this early stage of the project, the goal is to gain an understanding of stakeholders' current expectations and opinions; therefore mainly a qualitative approach was adopted.

The method of semi-structured interviews was chosen to capture qualitative data from different key-stakeholders, which are to a large extend representing or understanding the positions of users or user groups, in order to understand their status, needs, opinions, motivations for cryptographic solutions for the Cloud. The flexibility of semi-structured interviews allows exploration and open discussions of key points brought up throughout the interview. Our observations and elicited requirements from the interviews will be presented in section 7.1.1.

Furthermore, a workshop with four expert focus groups was conducted to gather qualitative data from group tasks and discussions of the proposed case scenarios for PRISMACLOUD in the areas of: (1)E-health, (2) E-government, (3) and smart city, which we had also used as a basis for the semi-structured interviews. Conclusions from these focus groups in the form of opportunities, concerns and elicited requirements are presented in section 7.1.4.

Additionally, surveys were conducted to provide some quantitative data on a wider scale.

7.1.1. Semi-structured interviews

In total, 19 interviews were conducted in different locations according to PRISMACLOUD partners: 1 pilot + 9 interviews by UKARL in Sweden, 5 interviews by XiTrust in Austria, 3 interviews by ETRA in Spain, and 1 interview by IRT in Italy. Participants interviewed in the areas of health, government, and smart cities were varying between top management, technical, and non-technical roles within their organizations; e.g., CEO, IT system management, nurses.

A basic structure was followed in order to unify interviews to a certain degree across partners conducting the interviews. A *guide* describing the structure was shared and included a consent form, Introduction, interview questions and scenarios, and post interviews questionnaires (see Appendices I and II). However due to the semi-structured nature of the interviews, questions were modified, skipped, and replaced by interviewers depending on the flow of each interview.

Interviews were scheduled for 60 minutes interview including a follow up questionnaire; however the duration of interviews varied between 50 and 190 minutes. There were 1-2 interviewers for each interview. Mainly notes were taken, and some interviewees consented for recording the sessions.

The basic structure of the interview consisted of three parts: (1) General inquiry, (2) Case scenarios, and (3) Requirements. In part (1), after briefing the interviewee and getting the consent form signed, inquiries about interviewees organization and their state of the art in regards to authenticating documents physically and digitally, as well as their experience in the Cloud. In part (2), one of the three target areas scenario (E-health, E-government, Smart city) was chosen corresponding to the interviewee. The case scenario was presented as a context, and a discussion aimed at understanding interviewees' expectations, opinions, experiences, and concerns in regards to the cryptographic schemes and functions proposed in the scenario. The final part (3) aimed at gathering requirements for a secure, private, trustworthy system in the cloud context.

Finally, a questionnaire was filled out by the interviewees in order to provide some quantitative data about their organization, Cloud services, and cryptographic solutions in regards to security, privacy, trust and usability (see Annex III).

Interview results: HCI requirements

Table 1below gives an overview of the interviews conducted. It represents information regarding the interviews: index number (i), PRISMACLOUD partner which conducted the interview, type of organization of the interviewee, area (government, health, smart city), and interviewees' role.

Table 1: Conducted Interviews by PRISMACLOUD partners

Interview number (i)	PRISMACLOUD Partner,location	Organization	Area	Role (U: non-technical user; IT: technical)
i1	UKARL, Sweden	County council	Government	(U) Development strategist
i2	UKARL, Sweden	E-ID board of Swedish government	Government	(IT) Lawyer/legal expert
i3	UKARL, Sweden	Public Healthcare organization	Health	(U) Nurse and a member of the nurse board association
i4	UKARL, Sweden	Public Healthcare organization	Health	(U) GP and CMO primary care
i5	UKARL, Sweden	Public Healthcare organization	Health	(U) Coordinator
i6	UKARL, Sweden	IT-city council	Government	(IT) IT architect
i7	UKARL, Sweden	County council	Government	(IT) Enterprise Architect
i8	UKARL, Sweden	Regional public health care	Health	(IT) Security top manager
i9	UKARL, Sweden	Public Healthcare organization	Health	(U) Nurse
i10	ETRA, Spain	ETRA Research and Development	Smart City	(IT) IT manager responsible for IT infrastructure deployment
i11	ETRA, Spain	Electronic Traffic	Smart City	(IT)IT security manager

i12	ETRA, Spain	Electronic Traffic	Smart City	IT system management
i13	IRT, Italy	Interoute Spa	Smart City	Sales Director
i14	XiTrust, Austria	Joanneum Research	Smart City	Head of Department
i15	XiTrust, Austria	XiTrust Secure Technologies	Health	CEO
i16	XiTrust, Austria	BBG (Federal Procurement Agency)	Government	Project Manager Information & Technology Management
i17	XiTrust, Austria	TU Graz - IAIK	Government	Senior Researcher
i18	XiTrust, Austria	Graz University	Health	CIO

The following sections summarise the results of the interviews per use case domain in the form of tables. The tables include a row for each relevant observation that we noted in the interviews, requirements (**RH** for health, **RG** for government, **RSC** for smart city) that can be derived from this observation and in some cases examples of implementations addressing these requirements. Throughout the table, there are some references to specific interviews, e.g., (**i5** refers to the fifth interview in the list of interviews), as well as a distinction between users with non-technical background (**U**) and those with technical expertise (**IT**).

Interviews and Requirements for E-Health

Table 2: Requirements for the eHealth

RH#	Observations	Derived Requirements (related to PRISMACLOUD technologies and technical concepts)
RH1 RH2	Basic security/usability issues with authentication via smartcards or password based login: - Health care personnel often do not remove their smart cards, so that others can easily use their accounts. They “trust their colleagues”. (Both U and IT opinions) - Card usability (forgetting the card at home, very difficult to do daily routines). (i3)	**RH1** Need for login and authentication when someone wants to sign a document and shall be made easy and unobtrusive. **RH2** Need for some “functional” benefits from logout/login for users’ incentives. (Relates to authentication, login/logout)

	- Concerns over the device itself. - Security requirements need to be more usable (too many rules hinder usability, e.g. work pc vs. personal computer). - Need more intelligent systems with eyes, biometrics for more security. (i4)	
RH3	Not everyone has his own computer (group log-in); not obvious who did what. (i4)	**RH3** Personal log-in is required for personal accountability. (Relates to login/logout)
RH4	Confidentiality means for many interviewees that the doctors do not talk to anybody else about medical data, but the data may be available technically to others. Even the fact that there is a psychiatric diagnosis is available to others, even though the content of the diagnosis is not. They usually trust that even researchers will not disclose confidential data that is not anonymized.	**RH4** Redacting ("blacking out") information and other pseudonymisation or anonymization functions shall happen by default (in the background of the system) as hospital personnel do not see the need for such measures directly, but they may anyhow appreciate them if these functions are there. (Relates to malleable signatures and other data minimisation/anonymisation techniques)
RH5	Attitude: "Privacy and security incentives are for banks and not in health care. Never needed in health sector. Risk of healthcare and safety issues." (i5)	**RH5** The UI shall remind the user of code of conduct. Incentives and risks in the health sector needs to be made clear. (Relates to general privacy awareness)

RH6	Trust in technicalities - (i3 trust in health organisation): Health Care personnel have full trust in "Landstinget" (county council in Sweden) as an organization, therefore also in its functions, operations, and system.	**RH6** Need to make use for the branding of systems that are important. (Relates to trust and certification)
RH7 RH8	There are concerns in regard to using the Cloud: Trust in regional council by end users (e.g., patients) may be impacted, if they cannot explain incidents in the clouds. (i8)	**RH7** Need for incidence reporting tools, which are able to respond to questions about incidents, giving feedback to end users. **RH8** IT incidents in the Cloud shall be detectable and accountable. (Relates to functional signatures & verifiable computation)
RH9	Trust in technical solutions by Swedish government – private cloud. (i2)	**RH9** Need for private Cloud run by the respective authority (e.g., Landstinget in Sweden). (Relates to security & trust in cloud computing in general)
RH10	Lack of understanding of Cloud benefits/services: No clear view of technical risks / constraints / benefits. (i3)	**RH10** General benefits, risks, limitations of Cloud Computing needs to be mediated to the users. (Relates to all PRISMACLOUD technologies)
RH11	Redaction of information by patients: The interviewees thought that patients have interest this. However, they had concerns over an unwarranted sense of security that patients might have. (i4)	**RH11** Need for clear responsibility differentiations; people need to be aware of the systems functions and limitations, and redaction roles. Responsibility should be clear: any issues stemming from the redactions are the patients' responsibility.

		Need for clear settings and rules. (Relates to malleable signatures)
RH12	Health manager have very little time to check access logs; increased monitoring can make staff less prone to peep. Increased monitoring of access to patient data when patients can access their medical record as well as logs listing health staff accessing this information. (i5)	**RH12** Need for means to prevent staff from peeping. (Relates to user privacy protection)
RH13	"Wearables" (Internet of medical Things): Health IT workers ("and politicians") are concerned that no sensitive data should leak or is misused. (i8)	**RH13** Need for an independent body to verify trustworthiness. (Relates to trust and verifiable computation)
RH14	Different formats of data can cause problems. For instance prescriptions from hospital to pharmacy where numbers are not coded in the same way. (i8)	**RH14** Need to standardize input, possibly via format preserving encryption. (The data requirement behind this is that medical records shall be searchable and different web services shall be able to speak to each other.) (Relates to format preserving encryption.)
RH15	Access to backup information within 10 minutes. (i8) (This work nowadays with a local IT center, but if in future cloud services are used and replaced regularly, the UI must be very consistent through such shifts so that users quickly understand how to retrieve backup information.)	**RH15** Backup services shall be readily available. This may put restrictions of secure cloud storage based on secret sharing protocols. (Relates to secure cloud storage using a cryptographic storage network.)

RH16	Apart from access to logs, not much control is given to patients when it comes to their data and records.	**RH16** Need to be open to patients and transparent, so that patients can have access to their own data. (Related to data storage in the cloud. May relate to verifiable computation.)
RH17	Concern over that access rights to patients' records are given to many people at the healthcare. Unauthorized access is hard to detect.(i5) Not much concern about data privacy, but acknowledge the possibility of a different target group. (i5)	**RH17** Access rights need to be reconfigured. Give more control to patients over the access to their records. An example is the digital card access in Taiwan, where doctors have access to patients' records through the card the patient is having. This can be combined with anonymous credentials for selective disclosures of data by patients. (Relates to anonymous credentials.)
RH18 RH19	Information stored indefinitely in the system, even if the patient has moved away (they had access to documents from the 60s of patient records and personal data). (i3)	**RH18** Available patient data shall be relevant for each user. **RH19** Need for blocking of data after expiration of retention period. Ex. If cloud storage is based on secret sharing, data can be practically deleted from the Cloud if shares are deleted. (May relate to secure cloud storage using a cryptographic storage network.)

The RH requirements thus reflect the health workers' including IT specialists' experience or idealisations of patients. They also reflect a rather cautious embrace of the cloud. Data protection laws as well as swift access in case ordinary systems break down are not preliminary UI design issues, but should not be neglected in the PRISMACLOUD demonstration prototypes which might mean definite indications in user interfaces. Suggestions are given in the RH requirements table.

Interviews and requirements for e-Government

Table 3: Requirements for e-Government

RG#	Observations	Derived Requirements

RG1	National or EU based cloud providers following EU/national privacy laws are more trusted.(i6) (i7) say Microsoft servers are located in Ireland, but PUL (Swedish Data Protection Act) requires specific contract to be signed with the data controller.	**RG1** Usable privacy policies for informing users about the location of cloud servers and jurisdictions that will apply. (Relates to privacy & trust in cloud computing in general)
RG2	Opinion on Cloud: leaks, not losses, are the issue. (i1)	**RG2** Logs and other accountability measures should be accessible in an understandable format for responsible public officers. Secure Cloud Storage can prevent this problem. (Relates to secure cloud storage and accountability measures)
RG3	User friendliness needed, today's electronic signatures solutions are difficult. (i2)	**RG3** Electronic signatures should be easy to use. (Relates to all types of electronic signatures)
RG4	e-ID: Business perspective is important, costs, and needs. Innovative solutions needed: users get to choose who to trust (if they don't want to use the bank, they can use something else). (i2)	**RG4** Citizens and officers can easily find and evaluate e-ID offers. (May relate to all types of electronic signatures based on eID)
RG5	Chain of different levels of operations -> consistency is needed. (i2)	**RG5** Consistency through chain of services. (Not directly related to the PRISMACLOUD technologies, but a dearly wanted feature of future solutions)
RG6 RG7	Public services need every identity as an alias as they might have to hide	**RG6** System input controls are sensitive to personal data and replaces such input in free format with aliases.

	citizen's name or social security number or relation to child. (i6)	**RG7** When sending a document, the user is asked to check what anonymity level is needed. (Relate to pseudonymisation – possibly via malleable signatures)
RG8	How can the public body ensure sorting out (=destroying data) afterward? (i6) Compare RH99. If a company delivers a service and has a lot of databases, then there is a risk that they combine info (illegally). (i7)	**RG8** Accountability tools should be available to check cloud services and automatically delete data after their retention periods, and make illegal operation detectable. Secret sharing can also help to enforce data destruction after the expiration of retention periods. (Relates to verifiable computation and certification of virtualised infrastructure, secure data storage.)
RG9	Organizational inertia: End users have the motivation and freedom to seek better solutions, but as an organization, they are happy with things the way they are. G-IT (i2)	**RG9** Benefits of new solutions should also include benefits for individual users, not only the organisations procuring the systems. (Compare RH2) (Relates to the entire Cloud concept.)
RG10	Government's supplier has the responsibility (cloud services have to live up to the requirements). -According to the agreement (procurement) they are supposed to test to see if they are living up to their requirements. (i2)	**RG10** Procurer must be able to verify cloud service performance (in various respects). (Relates to certification of virtualized infrastructures.)

Some dear old requirements show up in the observations pertaining to e-Government. e-ID has been regarded by many citizens as cumbersome, and this would need further refinement but probably the increased use of mobile-ID will make both citizens as well as solution providers used to the requirements of e-ID usage. Also the problem that different providers may have very different UI

solutions will provide a real problem for government staff as well as for citizens and organisations trying to use e-Gov services.

Interviews and Requirements for Smart City (RSC)

Table 4: Requirements for the Smart City use case

RSC#	Observations	Derived Requirements
RSC1 RSC2 RRSC2	Smart city, anonymous parking: "Very hard to prove I've been there. Parking companies have their routines and if there is a problem you cannot prove you been there and you get a fine." G-IT (i6)	**RSC1** There needs to be a backup solution in case that the anonymous reservation does not work. **RSC2** The user needs to get an electronic proof that he has successfully reserved a parking slot. (Relates to anonymous credentials, and possibly to group signatures)
RSC3 RSC4	Focus on audit to demonstrate to end user, from both qualitative and quantitative points of view, the security level of the tools he or she will use.	**RSC3** Solution design should focus also on the means to be evaluated. **RSC4** Performances should also be taken into account if the solution applies to large data set transfer (Relates to all PRISMACLOUD technologies)
RSC5	Increasing attention to hybrid cloud scenarios	**RSC5** PRISMACLOUD solution should be designed to be used by IaaS provider as a service to be offered to business user purchasing resources (something like Crypto-as-a-Service) (Relates to all PRISMACLOUD technologies)
RSC6	Wide range of possible deployment scenarios	**RSC6** PRISMACLOUD solution should be designed in a modular way, allowing to be deployed totally/partially in a large number of scenarios
RSC7	Interoperability	**RSC7** PRISMACLOUD solution should be designed as a software layer which can be deployed over actual cloud layers in a non-disruptive way
RSC8	Problems regarding signature verification –	**RSC8** All verification tools deliver the same result. Protocols need to be standardised.

	different verification tools deliver different results	
RSC9	Too much data is released (and stored infinitively).	**RSC9** Data should only be usable for a definite period of time (and –preferably deleted automatically after the retentions period expires). Secret sharing can enforce data destruction. (Relates to secure cloud storage.)
RSC10	Data are misused and analysed for example that movement patterns are received during the smart city case	**RSC10** Only necessary data are stored, the coordination points are unlinkable. (Relates to anonymous credentials.)

7.1.2. Post interview questionnaires

In order to investigate the interviewee's attitudes towards the usage of cloud services in general and towards the privacy and security aspects of cloud services in particular they were asked to fill out a short questionnaire after the interviews (see Annex III). The questionnaire consisted of Likert scales with statements and a five grade response scale ranging from 'strongly disagree' to 'strongly agree'. All in all a total of 14 participants (seven from the health- and government sector respectively) out of 18 filled out the questionnaire. Six of the participants described their role as IT professional and eight as Non-IT professionals. As this is a rather small sample we present the descriptive results of a subset of questions bellow.

First we asked the respondents if they were satisfied with the current state of cloud services (Figure 4). The results show that none of the participants were particularly happy with the current standard as the responses ranged from 'strongly disagree' to 'neutral' with an approximately even spread.

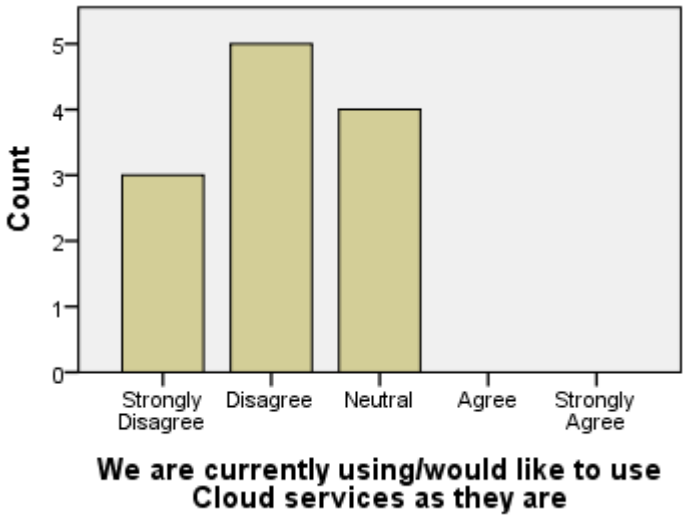

Figure 4: Using Cloud services as they are

We then turned our attention to the sources of concerns regarding the cloud services (Figure 5). The results showed that the participants were unhappy with current services in regards to privacy and security and that nearly all responses ranged from 'agree' to 'strongly agree'

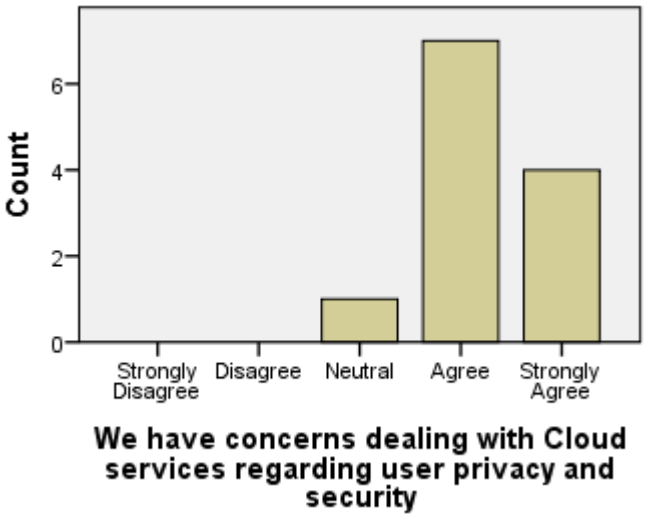

Figure 5: User privacy and security concerns in the Cloud

To further tease out the sources of discomfort we asked the participants if they saw a need for improvements regarding the security of data (Figure 6). Although most participants responded 'agree' there were also some that responded 'neutral' and even 'disagree' indication that at least some of the respondents thought that the current state of data security is acceptable as it is currently implemented.

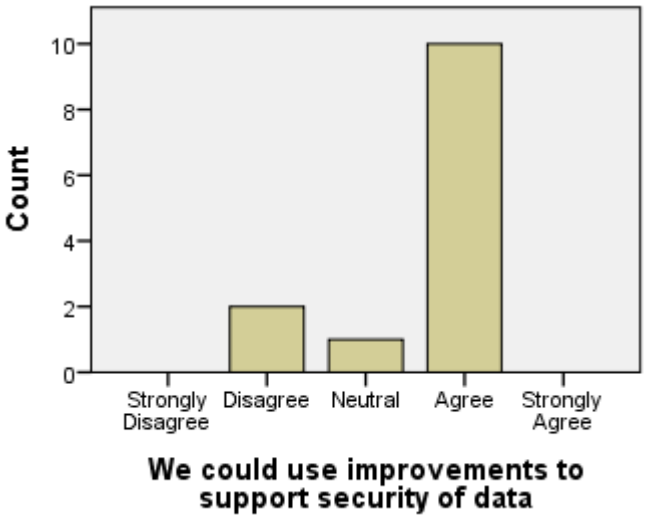

Figure 6: Need for data security improvements

In regards to privacy there were also some participants responding that they were happy with the current state of privacy. The majority, however, responded with 'agree' or 'strongly agree' indicating that improvements regarding privacy are much in demand and that it might be even of more concern than security (Figure 7).

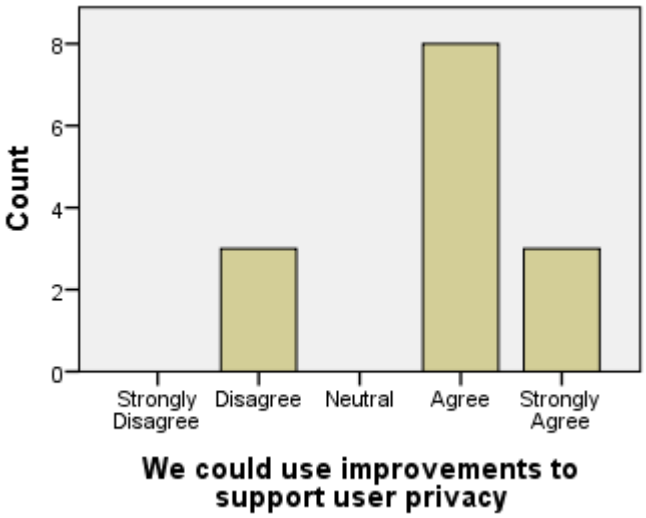

Figure 7: Need for user privacy improvements

To assess to what extent trust is an issue in regards to the usage of cloud services we asked the respondents to what extent improvements in data security and privacy would enhance their trust (Figure 8). The results show that trust is an imperative aspect as all responses were either 'agree' or 'strongly agree'.

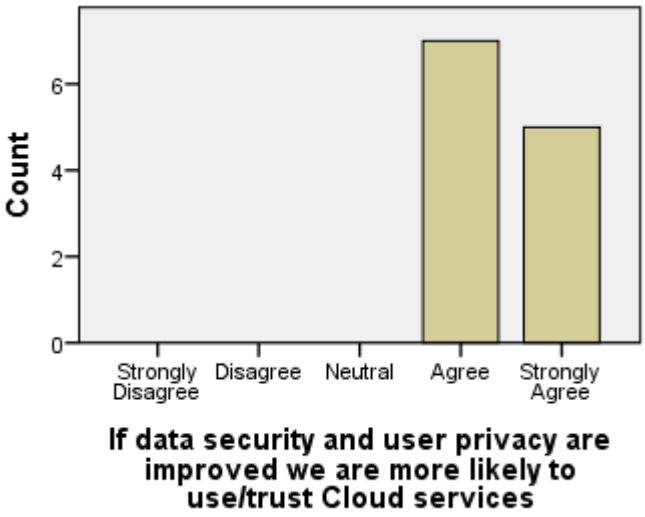

Figure 8: Using Cloud services after improvements

Finally we asked the respondents if the further implementations of cryptographic secure solution would increase the trust in cloud services (Figure 9). The majority of the respondents answer that this is the case with 'agree' or 'strongly agree' but there were also a few responding with 'neutral' and 'disagree' which indicates that there are also other factors, besides cryptographic solutions, that can be implemented to instill a higher level of trust in cloud services.

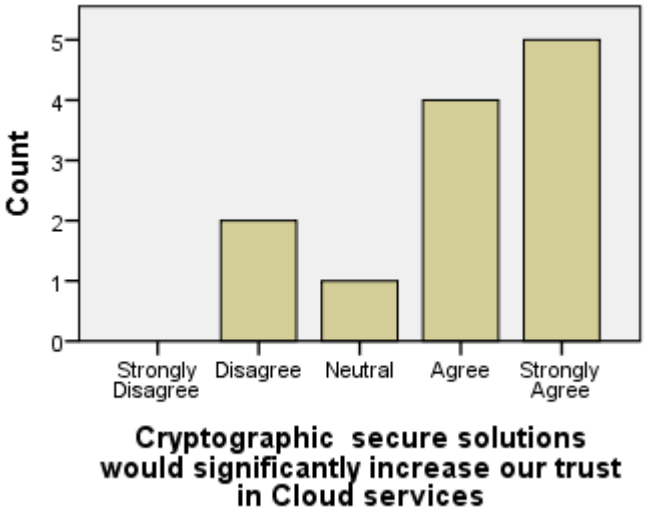

Figure 9: Trust increase of Cryptographic solutions of the Cloud

7.1.3. Requirements survey

In order to further investigate possible sources of trust in cloud service providers we distributed an expanded survey to participants of Secure Cloud seminars held in Austria (Future of the Cloud event) and Germany (CAST Workshop on Secure Cloud Services) in June 2015. This was done both in order to explore further sources of trust and in order to ensure that the results of the post-interview questioner were in fact a result of the interview session. All in all 57 participants completed the expanded survey. The participants were mainly from industry ≈ 80 % with the reaming ≈ 20 % being

from academia. Approximately 23 % reported being cloud service users, ≈ 18 % cloud service providers, and 12 % being both users and providers (the remaining participants entered 'none' or did not fill out the question).

The first part of the questionnaire consisted of five Likert scales with statements and a five grade response scale ranging from 'strongly disagree' to 'strongly agree' regarding the importance of certification of the service provider, the certification of the computing center, privacy policies, verifiable computing, and compliance with European privacy laws (see Annex IV, Question Q6). Statistic tests between the occupation of the participants (industry vs academia) and cloud service role (user, provider etc.) showed no statically significant differences. All in all the average of all the questions were approximately four showing that all trust factors were viewed as more or less equally important. This is apparent from the distribution of the responses where the majority of responses on all questions were 'agree' followed by 'strongly agree' (see Figure 10).

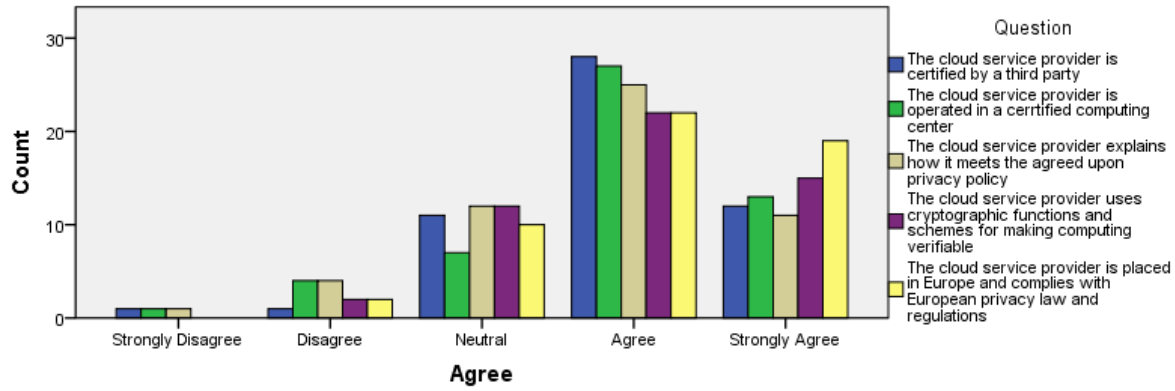

Figure 10: Requirements for trust in the Cloud

The second part of the questionnaire was designed to investigate which security aspects (integrity, usability, confidentiality, availability, anonymity/privacy, and accountability/verifiability) of cloud computing were viewed as more important (see Annex IV, Question Q9). This part was constructed as a ranking task and participants were instructed to rank the aspects in priority order from one as top priority to six as least priority. The results show that there is no single aspect that stands out as the most important (see Figure 11). The distributions of the priority ranks are pretty even when you add them up with the noteworthy exception of usability. The results indicate that there are two camps where one views privacy as a highly prioritized security aspect and another which views it as the least important security aspect.

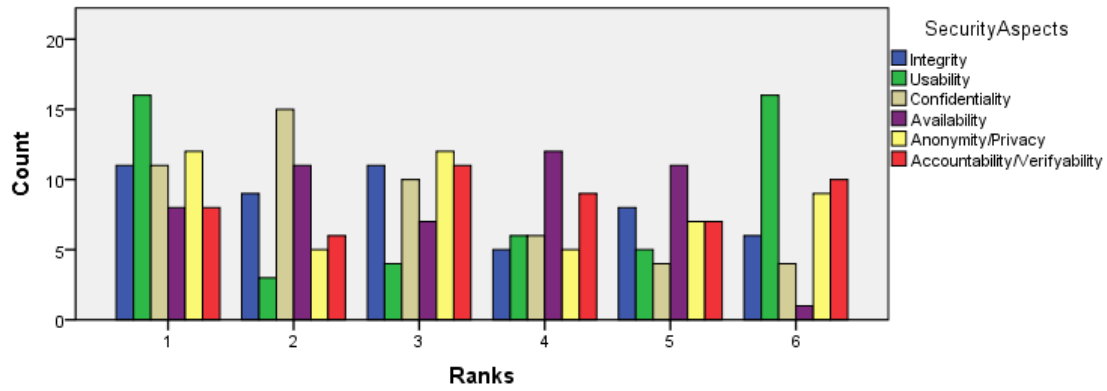

Figure 11: Ranks of Security aspects

In conclusion, the survey confirms that cryptography is a mediator of trust in cloud services but there exist other important trust factors such as certification schemes, data protection laws, legal protection, privacy policies. Hence, a high level requirement that can be derived is that PRISMACLOUD technologies should be complemented and supported by such other legal, technical and organisational means for establishing trust in Cloud technologies, i.e. the PRISMACLOUD project needs to take a holistic approach for protecting privacy and establishing trust.

7.1.4. Expert focus group workshops

A workshop in the form of expert focus group discussion was conducted consisting of experts in the field of privacy and security. Case scenarios in the areas of e-health, e-government, and smart cities developed in PRISMACLOUD, in order to give context of use for the cryptographic functions of the project, were used in the workshop. The aim of the focus group discussions was to explore HCI challenges of the case scenarios and further elicit requirements in regards to usability, trust, and privacy.

The workshop consisted of informative and interactive parts, which has taken place in IFIP summer school (Edinburgh, August 2015). In total 25 participants with different research level and background formed 5 interdisciplinary focus groups, coming mainly from Europe and Asia (and/or Middle East). The informative part consisted of a brief introduction to PRISMACLOUD, the three use-case scenarios, and a technical overview of signatures schemes covering malleable and functional signatures in preparations of the focus group tasks and discussions. Each group had a moderator who was guiding the group through tasks, brainstorming activities, discussions, and feedback throughout the interactive session.

The interactive session consisted of three parts: (a) an introduction to the workshops agenda (see Annex V), materials, group forming, and group members' introductions. (b) Discussions about case scenario selections and related cryptographic functions, and further the implications and features of those functions in regards to usability, privacy, and trust. (c) Requirements elicitation of cryptographic functions from part (b) to enhance usability, privacy, and trust in the Cloud.

Results from the focus group sessions were documented as summaries by the moderator of each group. The summaries below (Focus group No.1- 4) followed the basic structure of:

A. Brief summary of participants, number, background/experience

B. General description of the discussion in relation to the scenarios and functions (which scenarios, functions)
C. Highlights of features and issues discussed in relation to (2)
D. Elicited requirements

Focus Group No. 1:

(A) Brief summary of participants, number, background/experience

The workshop consisted of 4 Computer Science PhD students doing research in IT security & Privacy from Swedish, Dutch and British Universities plus a Swedish Computer Science professor and PRISMACLOUD project member, who acted as the workshop leader. The cultural background of the participants was diverse. Two participants came originally from European countries and 3 from the Middle East and/or Asia.

(B) General description of the discussion in relation to the scenarios and functions (which scenarios, functions)

As a scenario, the presented E-Health scenario on the redaction of blood test parameters in medical files stored in the Cloud via malleable signatures was chosen and not further modified. In this scenario, the fields of a blood test signed by a nurse (signer) can later be redacted ("blacked-out") by the patient (data subject and redactor), so that he can forward a subset of the blood test value to a dietitian (verifier) instead of revealing the complete test results.

During the discussion, the group was very closely following the suggested protocol. First opportunities and challenges of malleable signatures in the chosen E-Heath scenario in regard to privacy, trust and usability were brainstormed and discussed. Then, the group discussed and jointly elicited requirements for utilizing opportunities and addressing concerns that were highlighted earlier in the discussion.

(C) Highlights of features and issues

Opportunities

On the discussion on how in this scenario malleable signatures can enhance privacy, trust, security, the following aspects were raised:

- More control for data subjects: Privacy can be enhanced, as it gives the data subject/redactor more control over what information to disclose to the verifier and what data they would like to redact. Hence, they can enforce data minimization.
- There is usually a trust relationship between the patient and the nurse and doctor. Even if the nurse or doctor make a selection of what data fields can be redacted, it will still give the patient control over some of his data that are redactable, i.e. this enhances his privacy.
- Trust can be enhanced, as the verifier can assume that the data is authentic.
- It is easier to exercise control for users if they can do it directly electronically instead of requesting signed redacted data offline.
- If users are trusted to keep control over their data and to do the redactions themselves instead of requesting the nurse or doctor to do so, third parties (verifiers) could still trust

the correctness of the document if it contains a malleable signature by the nurse. Hence, trust and ease of use will be enhanced.
- Patients may put more trust into the health care provider, if they get options to control their data.

Concerns

Concerns that were brought up in regard to privacy, trust, usability:

- Trust has to be put in the specialist (nurse or doctor) to decide what fields could be redacted.
- Increased patient control may also put more burden and responsibility on the users.
- It can be debated whether patients should really have full electronic access to their medical dossiers, as they may not always be able to interpret all details and consequences correctly.
- Doctors or nurses must be trusted to make competent decisions in regard to the amount of information that can be redacted by different patients.
- In case that the signer has full control over which types of values can be redacted, the patient's degree of control is by this limited.
- If the redactor cannot be authenticated (i.e., in technical terms: the redaction operation is "unkeyed"), the verifier may lack trust in the redaction, e.g. may not be sure that really only information that was not needed in a certain context was redacted by authorized persons. Moreover, the patient may repudiate.
- If it is possible that the doctor can do the redaction and later claim that the patient did so, this may create privacy and trust issues.
- If the signer who is in charge of sampling the blood test creates a malleable signature on the blood test that authorizing the patient concerned to do redactions on his blood test, then the identity of the patient may leak to the signer. However, for privacy reasons it is the practice that blood tests should be submitted anonymously.
- Patients may not feel competent enough to do redactions themselves. For example, if they redact too much information, it may endanger their safety. They may therefore want to delegate this task to a trusted third party. However, accountability for the redaction may in this case be at stake.
- It may affect trust if the verifiers cannot distinguish the cases when data has been redacted from documents or not. Also privacy may be affected if the fact that information has been redacted (i.e. that the patient chose to hide certain medical values) can be hidden.
- Doctors, verifiers or patients may not trust the claim that malleable signatures will really work as claimed.
- Solutions that rely on PKIs (public key infrastructures) inherently have several usability issues.

(D) Elicited Requirements

The following list includes a number of requirements for enhancing privacy, trust and usability that were jointly suggested by the workshop participants:

- **R1A** It must be possible for the patient to delegate redactions to a specialist that he trusts; In this case, the delegatee must be accountable for his actions.
- **R1B** The redactor should be accountable (i.e., the redaction operation should be a "keyed" operation).

- **R1C** Even if the redactor can be made accountable, there should be a possibility that the redactor can be anonymous or pseudonymous to the signer (so that the anonymity of blood tests can be guaranteed).
- **R1D** In dependence of the case, the redaction should be "visible" or "invisible" to the verifiers, i.e. in some cases the very fact that data was redacted should be hidden.
- **R1E** Usable guidelines and support are needed for informing users about how much information is advisable to redact in which cases taking both privacy and patient safety criteria into consideration.
- **R1F** The user interface should be based on suitable metaphors and HCI concepts and complementing tutorials for illustrating how the system works for promoting user trust in the claimed functionality of malleable signatures.

Further requirements addressing issues raised in the discussion are:

- **R1G** The definition of fields that can be redacted should follow the data minimisation principle while considering the patient's safety. Doctor and nurses need guidelines and support on how to define redactable fields while following these principles.
- **R1H** The handling of signing and verifying keys and operations must be made easy and safe.

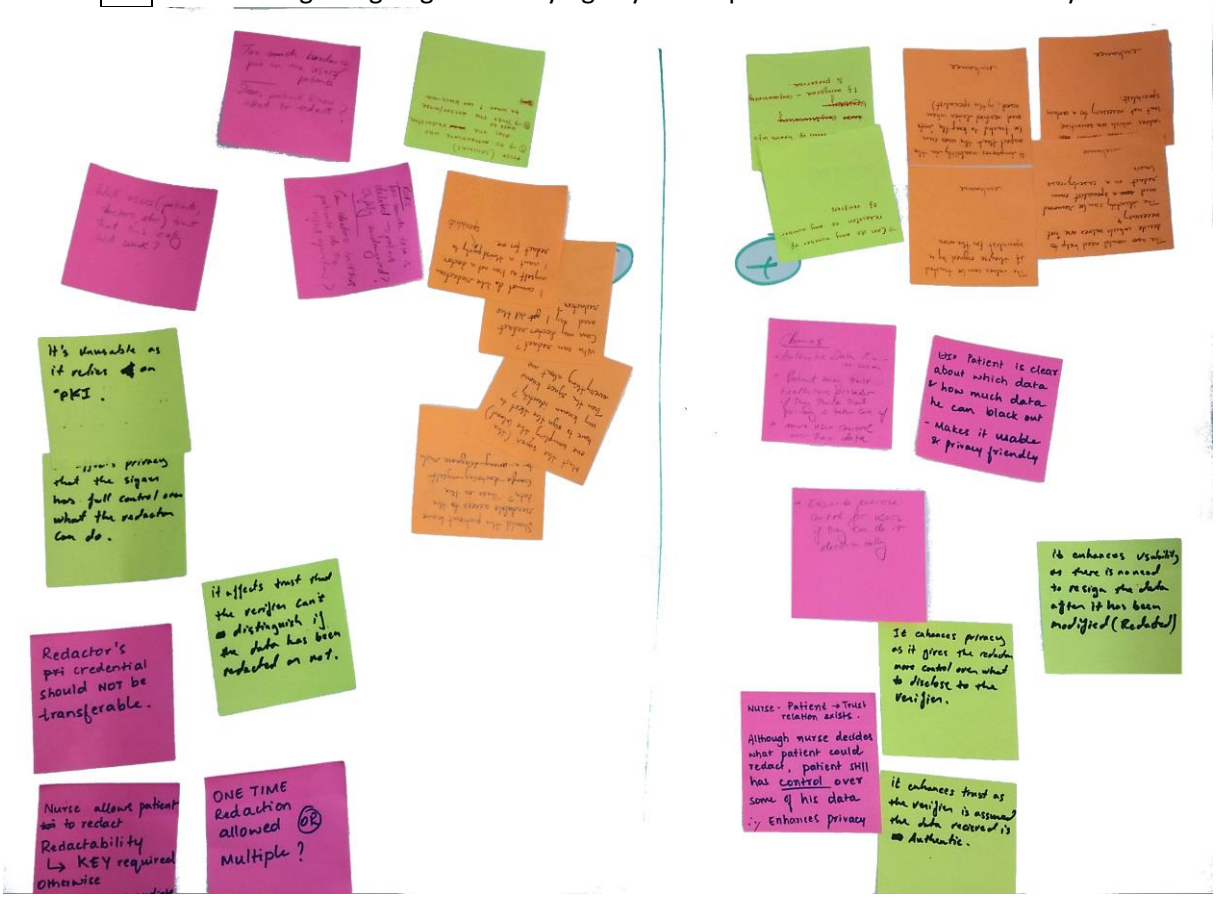

Figure 12: Brainstorming notes on opportunities and concerns by focus group one.

Focus Group No. 2:

(A) Brief summary of participants, number, background/experience

There were five participants in total who took part in the discussion of this group, three from computer privacy and security and two from cognitive science background. One main issue was related to different levels of experience of participants, which have hindered some discussion flows and interactivity, however many points of view were raised and discussed.

(B) General description of the discussion in relation to the scenarios and functions (which scenarios, functions)

When choosing case scenarios, debates regarding issues with reasons behind choosing a specific scenario and applicability of the chosen scenario. There was a discussion on how plausible this scenario is, and whether the scope is too narrow. Eventually, smart city and handicap parking was chosen as a preliminary case scenario. Debatable discussion regarding the cryptographic functions' usefulness concluded with using attribute-based signatures to sign GPS coordinates as a claim of a handicapped person on a specific parking spot.

(C) Highlights of features and issues

Points regarding features and concerns of the scenario discussed were:

- Inspection measures versus linkability problem, there was a discussion on what is required to be considered and done in regards to this tradeoff.
- Verifying credentials in the Cloud, which hardware and software to be considered from the users' side, in this case the discussion focused on the smart mobile phone.
- A main concern on whether there is a need to use the Cloud at all for this use case scenario
- Some concern whether the application might give a false sense of privacy, where users might not be aware of the extent of data they are exposing.
- Denial of service (DoS) issues, and distributed denial of service attacks were included in the scenario, since sabotaging users might need to be hindered by the application, allowing users to anonymously reserve all parking places.
- Fraud and fault issues, discussion on how users can still lend out the handicap privileges despite the applications' main functions.
- Usability issues with the app in comparison to the handicap card. The latter requires no effort on the behalf of the user, whereas the first is more demanding.

(D) Elicited Requirements

- **R2A** Trust requirements for the users: need of evaluators and transparency.
- **R2B** User privacy requirement, by maintaining control of identifiers and credentials.
- **R2C** Each user must possess a credential that is securely stored on a mobile device, and a provably correct anonymous credentials protocol and implementation (validation + verification).
- **R2D** Suitable UI and tutorials so that users can be aware of the systems functions and limitations
- **R2E** Payment requirement, even a little in order to mitigate DoS.
- **R2F** Revocation should be possible; temporary impaired/handicapped people (doctors/physicians can issue revocation)
- **R2G** Fraud inspection means are needed
- **R2H** Important verifiers' availability and integrity (no corruption or coercion)
- **R2I** Application should be for general purposes, many attributes, and not just for being handicapped.
- **R2J** Usability: less credentials to handle for easy decision making and less interferences with driving.
- **R2K** Mobile application needs to be generic, for usability and appeal.

Figure 13: Opportunities and concerns brainstormed by focus group two.

Focus Group No. 3:

(A) Brief summary of participants, number, background/experience

The 5 group members consisted of a senior researcher in applied cryptography, a researcher and 2 PhD students in privacy and security related work within computing science, and a research engineer on privacy policies specification and their enforcement within a cloud computing environment.

(B) General description of the discussion in relation to the scenarios and functions (which scenarios, functions)

In this group, the e-health scenario was chosen, and the discussion focused on the application of malleable signature schemes. In particular, the discussion was about "blacking out fields" from medical data. In the beginning, there were some issues that needed clarification by the moderator (as there were questions from the participants of which were answered in the second part of the workshop). Afterwards, the discussion identified positive aspects of applying such schemes, e.g., more efficient processes (less interaction steps are required) and no longer requiring the signer if we want to give away authentic data to another party (offline feature). Nevertheless, the focus was more on the related problems and thus focused on what one would need to do in order to make such schemes applicable in practice.

It was identified that it is very important to specify redaction rules of how signed messages/documents are allowed to be redacted/modified. Thereby, it could be problematic if redacted versions of a document would be used in various different areas (e.g., e-health and outside e-health) - as this makes it hard to specify in which context which redactions are allowed. This could

then lead to a redacted document that could be misused in the respective other area. Technically, one could counter this problem by using redaction policies (i.e., using a formal specification language to exactly specify what is allowed) and it should clearly (formally) define what is allowed to do in which context (it seems, however, that this is a highly non-trivial task). Policies could also support users (signers as well as redactors) to eliminate human errors and make such redaction tools easier to handle. Another problem that was identified in context of users is that users (signers) may not be able to comprehend what data to "mark" as being redactable. Consequently, it seems that for practical applications there is an inevitable need for policy and software support tool.

(C) Highlights of features and issues

Features and concerns:

- Eliminate human errors and make such redaction tools easier to handle.
- Concern regarding redacted versions of a documents that could be used in various areas (e.g., e-health and outside e-health), which would make it difficult to specify which context which redactions are allowed.
- Redacted documents that could be misused in the respective other area
- Users (signers) may not be able to comprehend what data to "mark" as being redactable.

(D) Elicited Requirements

- ❖ **R3A** Important to specify redaction rules of how signed messages/documents are allowed to be redacted/modified.
- ❖ **R3B** Using redaction policies (i.e., using a formal specification language to specify what is allowed) and it should clearly define what is allowed to do in which context.
- ❖ **R3C** practical applications – strong need for policies and software support tools

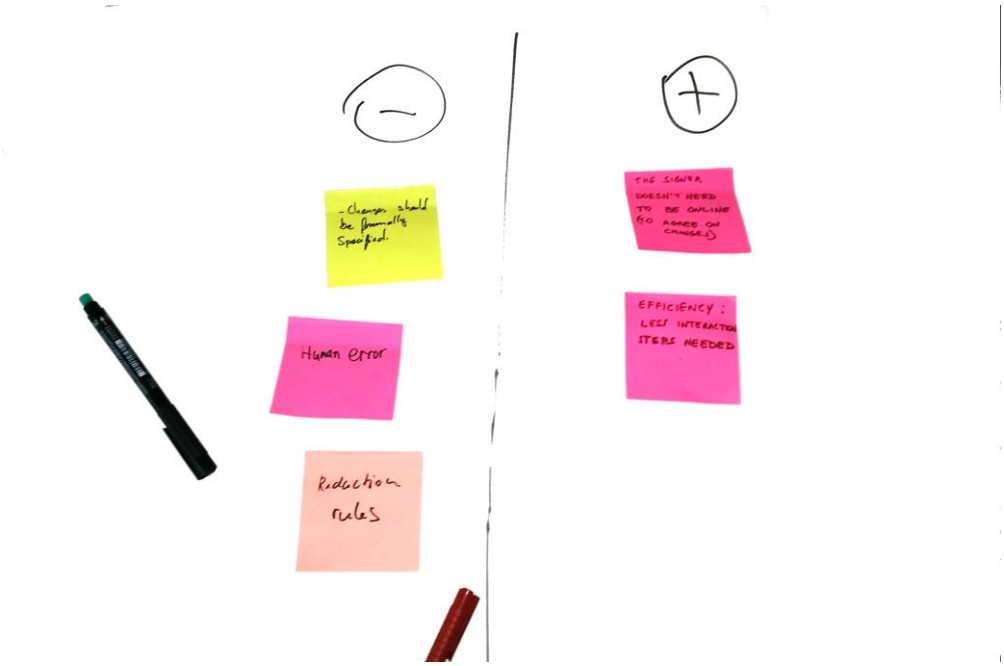

Figure 14: Opportunities and concerns brainstormed by focus group three.

Focus Group No. 4:

(A) Brief summary of participants, number, background/experience

The group consisted of (1) an associate professor of privacy enhancing protocols and privacy by design in the Netherlands, (2) a principal research scientist in the Security and Cloud Research Lab with a focus on privacy enhancing technologies, accountability and the cloud, (3) a research engineer involved in developing a monitoring framework for cloud assurance and accountability, and (4) a PhD student working on data pseudonymization and anonymization.

(B) General description of the discussion in relation to the scenarios and functions (which scenarios, functions)

In general, the group attempted to analyse all scenarios, but discussion got caught up on signatures. It started with detailed explanation of redactable signatures and the health use-case. The use of malleable signatures and verifiable computation in the blood test use case was then discusses. Participants saw the need for the suggested tools; however confidentiality was pointed out to be more critical issue than authenticity. There was doubt about the use case and participants thought the introduction of a trusted third party is dangerous. A concern regarding the danger of the third party adding not the right values to influence the result to their own favor, this scenario only makes sense, if the final signature can also be used to verify that the right values have been included in the computation. Reasons why ABC is necessary and what can be done with it were discussed. There was a concern regarding the smart city use case with the electronic version of the disable batch, which was the fear that it is still possible to link GPS or other metadata to anonymous credentials, e.g., license plate.

(C) Highlights of features and issues

Features and concerns:

- Unclear what happens if redactor is the user?
- If many field should be redactable, how can the user know which are redactable?
- Why should user trust third party that he redacts the info he wants to be removed (confidentiality)?
- Need for blacking out in some situations, e.g. anonymous data sharing in health care applications;
- Anonymity is doubted, since inferences can be made by metadata;
- Difference between Malleable signatures and ABCs unclear;
- For the distributed storage case, participants saw an opportunity to further compute on the data in such a setting which would be another advantage of such system;

(D) Elicited Requirements

- **R4A** Different scenarios for redactors are needed; if redactor=user, then use ABCs
- **R4B** Need for proactively introducing redactable fields.
- **R4C** Address the need for third parties, and improve means for trusting them (confidentiality).
- **R4D** Need for additional means to protect against re-identification and aid anonymization and pseudo anonymization.
- **R4E** Define advantage of redactable signatures over ABCs.
- **R4F** Need for good technical arguments for trusting distributed storage systems.
- **R4G** Need to address scalability, what if many fields should be redactable.

- **R4H** Avoid linkability through additional data (ABCs)

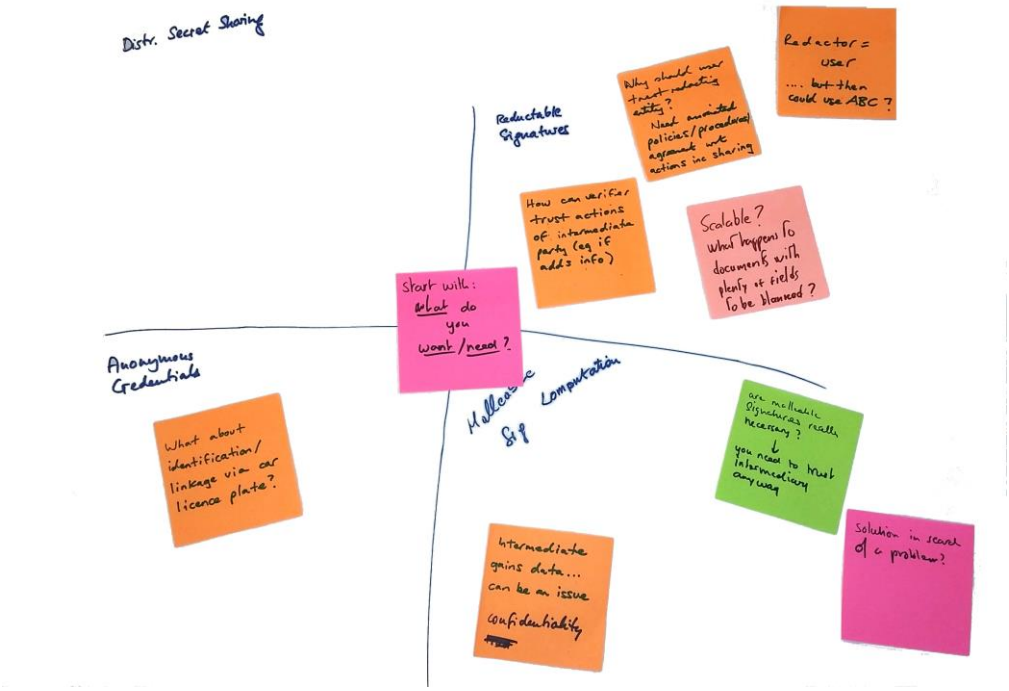

Figure 15: Opportunities and concerns brainstormed by focus group four.

8. Conclusion Legal, Social, and HCI-related requirements

8.1. Summary of Requirements

The totality of the requirements elicited and extracted through analysis in this deliverable is presented in Table 5. All requirements are indexed with a requirement number (in the first column of the table) that other PRISMACLOUD activities can later refer to. The requirement reference numbers with the prefix RL refers to the legal requirements on malleable signatures. The prefix RS are used for social requirements from Chapter 6. Then for the use cases, the reference numbers with the prefix RH refer to requirements elicited for health care use cases, the prefix RG are used for requirements elicited for e-Government, and RSC refers to requirements for the Smart City use cases (these requirements are also described under the same reference numbers in more details in Table 2, Table 3, and Table 4). The prefixes R1, R2, R3, R4 refer to the requirements elicited by focus groups 1, 2, 3, and 4 (as also listed and described in section 7.1.4).

In the last column with the heading “Topology”, we specify the nature of the requirements to indicate by which type of developers the requirements should be addressed. UI/Usability requirements will be of importance for the UI development and HCI work, while system requirements will be more generally important for the design of systems and use cases, and User/Human Factors may be of importance for both the UI design/HCI work and the design of systems and use cases. General requirements for PRISMACLOUD solutions need to be addressed on a higher level, particularly by organisational means, standardisation or certification.

Some requirements in Table 5 are directly related to system use. Suggestions for how these requirements might be fulfilled by the user interfaces have been derived simultaneous with the requirements analysis that we did for the interviews. These suggestions for possible UI solutions are presented in Table IV in Appendix VI.

Table 5: Summary of end user and HCI-related requirements

Requirement reference number	**Requirement**	**Topology**
Legal requirements for malleable and functional signatures: For an electronic signature (***ES***) to be legally considered an advanced electronic signature (***AS***), it needs to fulfil RL1 – RL4:		
RL1	- uniquely linked to the signatory;	SYSTEM REQ.
RL2	- capable of identifying the signatory;	SYSTEM REQ.
RL3	- created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control;	SYSTEM REQ.
RL4	- linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;	SYSTEM REQ.
Additional legal requirements for malleable and functional signatures: Furthermore, for an electronic signature (***ES***) to be legally considered a qualified electronic signature (***QS***), which is the highest legal recognition, it needs also to fulfil RL5-RL6:		
RL5	- created by a qualified electronic signature creation device (***QD***); and	SYSTEM REQ.
RL6	- based on a qualified certificate for electronic signatures (***QC***).	SYSTEM REQ.
Social requirements relates to trust and acceptance:		
RS1	Users must understand the extent to which they can act under pseudonyms	USER/HUMAN FACTOR REQ.
RS2	Users should trust that one can manage in a life-long way the information associated with different identities	USER/HUMAN FACTOR REQ.
RS3	Users should be able to put the right scope to distrust	USER/HUMAN FACTOR REQ.
RS4	Users should be made aware of trustworthy assessments of trustworthiness	UI & USABILITY REQ.

RS5	Users must believe that organizational and technical resources exist to support the use of the system ("external control")	USER/HUMAN FACTOR REQ.
RS6	Perceived security and privacy should be high enough to motivate adoption	USER/HUMAN FACTOR REQ.
RS7	User should be aware of the problem and abstract solutions	USER/HUMAN FACTOR REQ.
RS8	Users should understand what technology implements abstract solutions	USER/HUMAN FACTOR REQ.
RS9	There should be privacy/security guarantees	GENERAL REQ.
Requirements relating to use cases:		
RH1	Need for login and authentication when someone wants to sign a document and shall be made easy and unobtrusive.	USER/HUMAN FACTOR REQ.
RH2	Need for some "functional" benefits from logout/login for users' incentives.	UI & USABILITY REQ.
RH3	Personal log-in is required for personal accountability.	USER/HUMAN FACTOR REQ.
RH4	Redacting ("blacking out") information and other pseudonymisation or anonymization functions shall happen by default (in the background of the system) as hospital personnel do not see the need for such measures directly, but they may anyhow appreciate them if these functions are there.	SYSTEM REQ.
RH5	The UI shall remind the user of code of conduct. Incentives and risks in the health sector needs to be made clear.	USER/HUMAN FACTOR REQ.
RH6	Need to make use for the branding of systems that are important.	GENERAL REQ.
RH7	Need for incidence reporting tools, which are able to respond to questions about incidents, giving feedback to end users.	GENERAL REQ.
RH8	IT incidents in the Cloud shall be detectable and accountable.	GENERAL REQ.

RH9	Need for private Cloud run by the respective authority (e.g., Landstinget in Sweden).	GENERAL REQ.
RH10	General benefits, risks, limitations of Cloud Computing needs to be mediated to the users.	UI & USABILITY REQ.
RH11	Need for clear responsibility differentiations; people need to be aware of the systems functions and limitations, and redaction roles.	UI & USABILITY REQ.
RH12	Need for means to prevent staff from peeping.	GENERAL REQ.
RH13	Need for an independent body to verify trustworthiness.	GENERAL REQ.
RH14	Need to standardize input, possibly via format preserving encryption. (The data requirement behind this is that medical records shall be searchable and different web services shall be able to speak to each other).	SYSTEM REQ.
RH15	Backup services shall be readily available.	SYSTEM REQ.
RH16	Need to be open to patients and transparent, so that patients can have access to their own data.	UI & USABILITY REQ.
RH17	Access rights need to be reconfigured. Give more control to patients over the access to their records.	UI & USABILITY REQ.
RH18	Available patient data shall be relevant for each user.	GENERAL REQ.
RH19	Need for blocking of data after expiration of retention period. Ex. If cloud storage is based on secret sharing, data can be practically deleted from the Cloud if shares are deleted.	SYSTEM REQ.
RG1	Need for usable privacy policies for informing users about the location of cloud servers and jurisdictions that will apply.	UI & USABILITY REQ.
RG2	Logs and other accountability measures shall be accessible in an understandable format for responsible public officers.	USER/HUMAN FACTOR REQ.
RG3	Electronic signatures shall be easy to use.	USER/HUMAN FACTOR REQ.

RG4	Citizens and officers shall be able to easily find and evaluate e-ID offers.	USER/HUMAN FACTOR REQ.
RG5	Consistency shall remain through chain of services.	UI & USABILITY REQ.
RG6	System input controls are sensitive to personal data and replaces such input in free format with aliases.	SYSTEM REQ.
RG7	Need to prompt users to check what anonymity level is needed, when sending a document.	USER/HUMAN FACTOR REQ.
RG8	Accountability tools shall be available to check cloud services.	SYSTEM REQ.
RG9	Benefits of new solutions shall also include benefits for individual users, not only the organisations procuring the systems. (Compare RH2)	UI & USABILITY REQ.
RG10	Procurer shall be able to verify cloud service performance (in various respects).	SYSTEM REQ.
RSC1	There needs to be a backup solution in case that the anonymous reservation does not work.	SYSTEM REQ.
RSC2	The user needs to get an electronic proof that he has successfully reserved a parking slot.	GENERAL REQ.
RSC3	UI shall consider evaluation and auditing functions for the user.	UI & USABILITY REQ.
RSC4	Performances shall also be taken into account if the solution applies to large data set transfer.	SYSTEM REQ.
RSC5	PRISMACLOUD solution shall be designed to be used by IaaS provider as a service to be offered to business user purchasing resources.	SYSTEM REQ.
RSC6	PRISMACLOUD solution shall be designed in a modular way, allowing to be deployed totally/partially in a large number of scenarios.	SYSTEM REQ.
RSC7	PRISMACLOUD solution shall be designed as a software layer which can be deployed over actual cloud layers in a non-disruptive way.	SYSTEM REQ.
RSC8	All verification tools shall deliver the same result. Protocols need to be standardised.	SYSTEM REQ.

RSC9	Need for limitations and expirations; data should only be usable for a definite period of time.	SYSTEM REQ.
RSC10	Only necessary data shall be stored, the coordination points are unlinkable.	SYSTEM REQ.
Further requirements:		
R1A	It shall be possible for the patient to delegate redactions to a specialist that he trusts.	GENERAL REQ.
R1B	The redactor shall be accountable (i.e., the redaction operation should be a “keyed” operation) and there shall be a possibility that the redactor can be anonymous or pseudonymous to the signer (so that the anonymity of blood tests can be guaranteed).	SYSTEM REQ.
R1C	In dependence of the case, the redaction shall be “visible” or “invisible” to the verifiers, i.e. in some cases the very fact that data was redacted should be hidden.	UI & USABILITY REQ.
R1D	Usable guidelines and support are needed for users about how much information is advisable to redact in which cases taking both privacy and patient safety criteria into consideration.	UI & USABILITY REQ.
R1E	The user interface shall be based on suitable metaphors and HCI concepts and complementing tutorials for illustrating how the system works for promoting user trust in the claimed functionality of malleable signatures.	UI & USABILITY REQ.
R1F	The definition of fields that can be redacted shall follow the data minimisation principle while considering the patient’s safety. Doctor and nurses need guidelines and support on how to define redactable fields while following these principles.	SYSTEM REQ.
R1G	The handling of signing and verifying keys and operations shall be made easy and safe.	USER/HUMAN FACTOR REQ.
R2A	Trust requirements for the users, need for evaluators and transparency.	UI & USABILITY REQ.
R2B	Need to maintain control of identifiers and credentials for users’ privacy.	GENERAL REQ.
R2C	Each user shall possess a credential that is securely stored on a mobile device, and a provably correct	SYSTEM REQ.

	anonymous credentials protocol and implementation (for validation & verification),	
R2D	Suitable UI and tutorials are needed so that users can be aware of the systems functions and limitations	USER/HUMAN FACTOR REQ.
R2E	Need for payment requirement, even a little in order to mitigate DoS.	SYSTEM REQ.
R2F	Revocation shall be possible; temporary impaired/handicapped people (doctors/physicians can issue revocation).	SYSTEM REQ.
R2G	Need for fraud inspection means.	GENERAL REQ.
R2H	Need for verifiers' availability and integrity (no corruption or coercion).	GENERAL REQ.
R2I	Application shall be for general purposes, many attributes, and not just for being handicapped.	GENERAL REQ.
R2J	Need for fewer credentials to handle by the user, for easy decision making, no interference with driving.	USER/HUMAN FACTOR REQ.
R2K	Mobile application needs to be generic, for usability and appeal.	USER/HUMAN FACTOR REQ.
R3A	Need to specify redaction rules of how signed messages/documents are allowed to be redacted/modified.	USABLITY AND UI REQ.
R3B	Need to use redaction policies (i.e., using a formal specification language to specify what is allowed) and it shall clearly define what is allowed to do in which context.	GENERAL REQ.
R3C	Practical applications – strong need for policies and software support tool.	GENERAL REQ.
R4A	Need for different scenarios for redactors; in case a redactor is a user, then use ABCs.	GENERAL REQ.
R4B	Need for proactively introduce redactable fields.	USER/HUMAN FACTOR REQ.
R4C	Need for third parties, and improve means for trusting them (confidentiality).	GENERAL REQ.

R4D	Need for additional means to protect against re-identification and aid anonymization and pseudo anonymization.	GENERAL REQ.
R4F	Need for good technical arguments for trusting distributed storage systems.	GENERAL REQ.
R4G	Need to address scalability, what if many fields should be redactable.	SYSTEM REQ.
R4H	Need to avoid linkability through additional data (ABCs)	SYSTEM REQ.

8.2. Final discussion

This deliverable presents the legal, social, end user and HCI-related requirements that we have elicited for the PRISMACLOUD project in the first 9 project months, which should guide the development of PRISMACLOUD use cases, user interfaces and technical solutions to be developed by the projects.

For this deliverable, we have used different methods for eliciting requirements at different levels of detail. For deriving legal and social requirements, we conducted an analysis of the European legal framework on electronic signature legislation and a literature review, which both resulted in high level requirements in regard to the legal status and social factors influencing trust and acceptance, as summarized below. For a more in depth analysis of end user and HCI-related requirements, we conducted semi-structured interviews, surveys and focus groups, which resulted in a list of more detailed and more specific requirements.

The main conclusions of our requirement elicitation work can be summarized as follows:

The legal standing of malleable signatures (MS) has been analysed with respect to the latest signature legislation on EU level (eIDAS) in chapter 5. An MS – in form of the signatories original signature or in the form of derived signature generated either with an additional key (keyedMS) or without an additional key (unkeyedMS) by the authorised third party – can be a qualified electronic signature (QS) in the sense of article 3 section 12 jo. 3 section 11 jo. 26 eIDAS depending on the cryptographic implementation. This is the highest level of assurance awarded by the eIDAS after meeting six requirements. This gives the document with the MS the same legal standing as a document signed with a handwritten signature and it cannot be denied access to the court's proceedings.

The actual value of this malleably signed document is determined by the actual case and its applicable legislation as well as evidentiary value legislation of the EU Member State. Apart from standard cryptographic security properties, like unforgeability, it is especially the cryptographic property of public non-interactive accountability which allows the cryptographic implementation of a MS to technically function like existing legally well recognised digital signature algorithms, like RSA with SHA2.

We note that allowing any party to modify certain well-definable parts of the signed document subsequently might aid usability, it however complicates appointing liability to the Sanitizer. Therefore, we advise to use a keyedMS, which allows identifying the Sanitizer by its derived signature (ds) - which can be technically made to comply also with the requirements for a QS - making the Sanitizer technically and legally accountable for occurred subsequent modifications.

The literature reviews conducted in chapter 6 on social and other factors determining technology acceptance demonstrated a host of different circumstances influencing the adoption of advanced mechanism for security control and identity management. Some are of course outside the scope of the PrismaCloud project. Others qualify for further interrogation within the frames of the scenarios developing within the project, such as: understandability of the extent to which they can act under pseudonyms; trust that one can manage in a life-long way the information associated with different identities; awareness of trustworthy assessments of trustworthiness; perception of external control; perceived security and privacy; and privacy/security guarantees.

During the course of the interviews conducted (reported in chapter 7), there has been reoccurring trends (and conclusions that can be drawn from it), that are worth the mentioning among the participants opinions regarding privacy and security in the cloud. It was apparent that while users /user representatives would appreciate the offered functionality of many PRISMACLOUD functions, it may be difficult to understand for them what functions would need to be invoked for what services. Hence, one of the main conclusions is to implement the principle of "privacy by default", where the benefits of secure cryptographic functions are acquired by default while hiding any technical implementation details and keeping the processes in the background, thus minimizing interferences and efforts that users have to take to perform those functions.

There was a noticeable need for clear policies and guidelines, using tutorials and UIs that are user friendly, in order to provide users with awareness regarding their data's privacy and security while clarifying their responsibility in regards to solutions which would provide them with more control over their data.

Another important notion is in branding and standardization; trust in government that is very high in Sweden, trust in doctors, trust in researcher, etc., which can be used in order to gain users' trust in prospective solutions. When it comes to the Cloud, a noticeable attitude towards the location of the Cloud servers was important; they would use the Cloud it was private, local, regional, or EU-based.

The results of the post-questionnaire survey show that there is quite an agreement that that cloud services are not fulfilling users' expectations in regards to privacy and data security. The results also showed that the interviewees found that cryptography could ameliorate current solutions to such an extent that there would be a higher adoption of cloud services. The follow up questionnaire confirmed that cryptography is mediator of trust in cloud services but also pointed to a series of other trust factors such as certification schemes and privacy policies.

Finally, the focus groups confirmed the need of usable guidelines, suitable metaphors and policies clarifying the roles, rights and restrictions of actors in malleable signature and templates for enforcing such restrictions. Besides, potential security, trust and accountability issues and possible countermeasures and related requirements were discussed.

9. References

[1] European Commission, "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures," *Official Journal of the European Communities, L 013,* pp. 12-20, 2000.

[2] European Commission, "Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC," *Official Journal of the European Communities, L 257,* pp. 73-114, 2014.

[3] J. Angulo, S. Fischer-Hübner and J. Pettersson, "General HCI principles and guidelines for accountability and transparency in the cloud (Deliverable D:C-7.1)," A4Cloud Project, 2013.

[4] H. Bernard, Research methods in cultural anthropology, CA: Sage Newbury Park, 1988.

[5] B. Dziminski and C. Reed, D:B-5.2 Report on legal and regulatory dependencies for effective accountability and governance, vol. D25.2, 30/09/2014.

[6] T. Lorünser, A. Happe and D. Slamanig, "ARCHISTAR: Towards Secure and Robust Cloud Based Data Sharing," *IEEE 7th International Conference on Cloud Computing Technology and Science, CloudCom 2015, Vancouver, November 30 - December 3,* 2015.

[7] D. Slamanig and C. Hanser, "On Cloud Storage and the Cloud of Clouds Approach," *ICITST-2012,* pp. 649-655, 2012.

[8] A. Shamir, "How to Share a Secret," *Commun. ACM 11 Vol 22,* pp. 612-613, 1979.

[9] J. Müller-Quade and D. Unruh, "Long-Term Security and Universal Composability," *J. Cryptology,* vol. 23, no. 4, 2010.

[10] D. Demirel, D. Derler, C. Hanser, H. Pöhls, D. Slamanig and G. Traverso, PRISMACLOUD D4.4: Overview of Functional and Malleable Signature Schemes, 2015.

[11] M. Walfish and A. J. Blumenberg, "Verifying Computations without Reexecuting Them," *Commun. ACM,* vol. 58, no. 2, pp. 74-84, 2015.

[12] D. Catalano, "Homomorphic Signatures and Message Authentication Codes," *SCN,* pp. 514-519, 2014.

[13] T. Groß, "Signatures and Efficient Proofs on Committed Graphs and NP-Statements," *Financial Cryptography,* 2015.

[14] J. Camenish, A. Lehmann and G. Neven, "Electronic Identities Need Private Credentials," *IEEE Security,* vol. 10, pp. 80-83, 2012.

[15] L. Sweeney, "K-anonymity: a model for protecting privacy," *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems,* vol. 5, pp. 557-570, 2002.

[16] A. Meyerson and R. Williams, "On the complexity of optimal k-anonymity," *Symposium on Principles of Database Systems, PODS '04, New York, U.S.A.,* 2004.

[17] E. Commission, ”Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of person-al data and on the free movement of such data,” 1995.

[18] E. Commission, ”Proposal for a Regulation of the European Parlia-ment and of the Council on the protection of individual with regard to the pro-cessing of personal data and on the free movement of such data (General Data Protection Regulation),” 15. December 2015.

[19] K. H. (ed.), D:B-5.1 White paper on the proposed data protection regulation, A4Cloud Project, 2014.

[20] C. Millard, Cloud Computing Law, Oxford University Press, 2013.

[21] H. C. Pöhls, *PhD thesis: Increasing the Legal Evidentiary Value of Private Malleable Signatures,* Passau, Germany: University of Passau (to be published), 2016.

[22] H. Pöhls, S. Peters, K. Samelin, J. Posegga and H. de Meer, "Malleable Signatures for Resource Constrained Platforms," *Information Security Theory and Practice. Security of Mobile and Cyber-Physical Systems,,* pp. 18-33, 2013.

[23] S. Fischer-Hübner, J. S. Pettersson and J. Angulo, "HCI Requirements for Transparency and Accountability Tools for Cloud Service Chains," in *Accountability and Security in the Cloud: First A4Cloud Summer School held in Malaga, Spain, on June 2-6, 2014*, Malaga, Spain, Springer, 2015, pp. 81-113.

[24] O. O’Neill, A Question of Trust., Cambridge: CUP, 2002.

[25] C. Wamala, "Does IT count?: complexities between access to and use of information technologies among Uganda's farmers," *Sort,* vol. 20, no. 50, 2010.

[26] H. Lacohée, S. Crane and A. Phippen, "Trustguide: Final Report," *Trustguide,* October 2006.

[27] C. Marshall and J. Tang, "That Syncing Feeling: Early user experiences with the cloud," in *Proceedings of the Designing Interactive Systems Conference. ACM*, 2012.

[28] S. Bødker, N. Mathiasen and M. G. Petersen, "Modeling is not the answer!: designing for usable security," *Interactions,* vol. 19, no. 5, pp. 54-57, September/October 2012.

[29] J. Angulo, S. Fischer-Hübner, E. Wästlund and T. Pulls, "Towards usable privacy policy display and management," *Information Management & Computer Security,* vol. 20, no. 1, pp. 4-17, 2012.

[30] I. Ion, N. Sachdeva, P. Kumaraguru and S. Capkun, "Home is safer than the cloud!: privacy concerns for consumer cloud storage," in *Proceedings of the Seventh Symposium on Usable Privacy and Security*, Pittsburg, PA, USA. ACM. 13:1, 2011.

[31] C. Andersson, J. Camenisch, S. Crane, S. Fischer-Hübner, R. Leenes, S. Pearson, J. Pettersson and D. Sommer, "Trust in PRIME," *Proceedings of the 5th IEEE International Symposium on Signal Processing and IT,* vol. Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology, 2005.

[32] D. Shin, "User centric cloud service model in public sectors: Policy implications of cloud services," *Government Information Quarterly,* 2013.

[33] S. Pearson, "Privacy, Security and Trust in Cloud Computing," in *Privacy and Security for Cloud Computing*, Springer, 2013, pp. 3-42.

[34] A. Voida, J. S. Olson and G. M. Olson, "Turbulence in the Clouds: Challenges of Cloud-Based Information Work," in *CHI 2013: Changing Perspectives*, Paris, France, 2013.

[35] A. N. Joinson, U.-D. Reips, T. Buchanan and C. Paine Schfield, "Privacy, trust, and selfdisclosure online," *Human–Computer Interaction,* vol. 25, no. 1, p. 1–24, 2010.

[36] C. Lancelot Miltgen and D. Peyrat-Guillard, "Cultural and generational influences on privacy concerns: a qualitative study in seven European countries," *European Journal of Information Systems,* vol. 23, pp. 103-125, 2014.

[37] H. Smith, T. Dinev and H. Xu, "Information privacy research: an interdisciplinary review," *MIS Quarterly,* vol. 35, no. 4, p. 989–1015, 2011.

[38] Y. Li, "Empirical studies on online information privacy concerns: literature review and an integrative framework," *Communications of the Association for Information Systems,* vol. 28, no. 28, p. 453–496, 2011.

[39] (EEC-net), "Trust marks report 2013," European Consumer Centres Network, Karlstad, 2013.

[40] A. Joinson and L. Piwek, "Technology and the formation of socially positive behaviours," in *Beyond Behaviour Change*, F. Spotswood, Ed., Bristol, Policy Press, 2016.

[41] European Union, "Special Eurobarometer 431. Data Protection," European Union, 2015.

[42] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS quarterly,* pp. 319-340, 1989.

[43] V. Venkatesh and F. D. Davis, "A theoretical extension of the technology acceptance model: Four longitudinal field studies," *Management science,* vol. 46, no. 2, pp. 186-204, 2000.

[44] V. Venkatesh and H. Bala, "Technology acceptance model 3 and a research agenda on interventions," *Decision Sciences,* vol. 39, no. 2, pp. 273-315, 2008.

[45] S. AlAwadhi and A. Morris, "The Use of the UTAUT Model in the Adoption of E-government Services in Kuwait," in *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*, IEEE Computer Society, 2008, p. 219.

[46] V. Venkatesh, J. Y. Thong and X. Xu, "Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology," *MIS quarterly,* vol. 36, no. 1, pp. 157-178, 2012.

[47] M. Lallmahamood, "An Examination of Individual's Perceived Security and Privacy of the Internet in Malaysia and the Influence of this on their Intention to Use E-commerce: Using an Extension of the Technology Acceptance Model," *Journal of internet banking and commerce,* vol. 12, no. 3, pp. 1-26, 2007.

[48] W. Nasri and L. Charfeddine, "Factors affecting the adoption of Internet banking in Tunisia: An integration theory of acceptance model and theory of planned behavior," *The Journal of High Technology Management Research,* vol. 23, no. 1, pp. 1-14, 2012.

[49] T. Herath, R. Chen, J. Wang, K. Banjara, J. Wilbur and H. R. Rao, "Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service," *Information Systems Journal,* vol. 24, no. 1, pp. 61-84, 2014.

[50] Z. Benenson, A. Girard and I. Krontiris, "User acceptance factors for anonymous credentials: An empirical investigation," *WEIS, Delft: Workshop on the Economics of Information Security,* pp. 1-12, 2015.

[51] P. A. Wang, "Information security knowledge and behavior: An adapted model of technology acceptance," in *Education Technology and Computer (ICETC), 2010 2nd International Conference on*, 2010, pp. V2-364-V2-367.

[52] E. Wästlund, J. Angulo and S. Fischer-Hübner, Evoking Comprehensive Mental Models of Anonymous Credentials, vol. Open Problems in Network Security, C. e. al., Ed., Springer, 2012.

[53] J. Angulo and E. Wästlund, Exploring touch-screen biometrics for user identification on smart phones, vol. Privacy and Identity Management for Life, C. e. al., Ed., Srpinger, 2012.

[54] L. Carter and F. Bélanger, "The utilization of e-government services: citizen trust, innovation and acceptance factors*," *Information systems journal,* vol. 15, no. 1, pp. 5-25, 2005.

[55] M. Chase, M. Kohlweiss, A. Lysyanskaya and S. Meiklejohn, "Malleable Signatures: Complex Unary Transformations and Delegatable Anonymous Credentials," *IACR Cryptology ePrint Archive,* p. 1, 2013.

[56] F. Höhne, H. C. Pöhls and K. Samelin, "Rechtsfolgen editierbarer Signaturen," *Datenschutz und Datensicherheit,* vol. 36, no. 7, pp. 485-491, 2012.

[57] V. Venkatesh, M. G. Morris, G. B. Davis and F. D. Davis, "User acceptance of information technology: Toward a unified view," *MIS quarterly,* pp. 425-478, 2003.

[58] C. Brzuska, H. C. Pöhls and K. Samelin, "Non-Interactive Public Accountability for Sanitizable Signatures,," *Proc. of the 9th European PKI Workshop: Research and Applications (EuroPKI 2012),* p. 178, 2012.

[59] H. De Meer, H. C. Pöhls, J. Posegga and K. Samelin, "Scope of Security Properties of Sanitizable Signatures Revisited," *Proc. of the 8th International Conference on Availability, Reliability and Security (ARES 2013),* pp. 188-197, 2013.

[60] I. S. Organisation, "ISO 9241-210 Human-Centred Design," International Standard Organisation, 2010.

[61] E. Wästlund, J. Angulo and S. Fischer-Hübner, Evoking Comprehensive Mental Models of Anonymous Credentials, vol. Open Problems in Network Security, C. e. al., Ed., Springer, 2012.

10. ANNEX I: Interview guide for semi-structured interviews

Tuesday, October 20, 2015

Interview guide

To the interviewer:

Reminder: The consent form needs to be edited to fit your organization!

1. First of all, not all questions need to be answered. If there was no response, the sub sections of questions can be skipped.
2. Responses that are experiences and examples from the interviewees are strongly encouraged.
3. All odd information is valuable.
4. Results tables demonstrate how we would like the results to be documented; you have the freedom to choose the way you would like to fill the fields in those tables.

"How to" Interview:

1. Sign the consent form
2. Record interview if it is consented
3. Give introduction
4. Part A Questions
5. Part B (choose one of the cases)
    a. Show figure
    b. Explain case
    c. Ask questions
6. Part C Questions
7. Give out Questionnaire
8. Acknowledgments

After Interview:

1. Refine notes and from recordings (if it was recorded)
2. Translate (if English was not used) and fill in the results table
3. Send back to UKARL

1 | Page

Tuesday, October 20, 2015

Interview

Consent form taken and signed

Consent for recording

Introduction to the interview <2-3 minutes>

We are [a research group at Karlstad University] participating in an EU project called "PrismaCloud –Privacy and Security Maintaining services in the Cloud "(Horizon 2020). One main focus is on digital signatures functions from a cryptographic perspective; the development of new schemes, their uses and challenges, for ensuring that data stored in the cloud will be kept confidential and will (verifiably) only be processed in an authorized manner.[1]
At this stage, we are interested in interviewing stakeholders to gain an understanding of their current status regarding procedures, systems, and uses of signed documents. We also would like to explore the opinions and perspectives of PrismaCloud cryptographic solutions for more secure signature solution and verifiable computing and authenticity.
This interview would be semi-structured and would take approximately an hour. First we will discuss the general status of your organization in regards to authenticating documents; next we will introduce a case scenario to facilitate further inquiry.

Part A: General Inquiry <10-15 minutes>

1.	In your organization, (what means do you use) how do you authenticate documents/data physically and or digitally?
2.	Do you share information with parities outside your organization? How?
3.	Do you use Cloud Services? Why? Which ones?
4.	What systems do you use for authentication/verification? Can you give a short description?
4.1.	What are the perceived pros and cons of the system?
4.2.	Is it considered Private/secure? Is it protected against unauthorized users?
4.3.	From your experience has there been any incidents regarding security/privacy?
5.	What actors are involved in the process, and what levels of authority are they given?

[1] i.e., computation will be verifiable and (signatures on) results will only be authentic if authorized

Tuesday, October 20, 2015

Table 1: Results for Part A (General Inquiry)

A	1.	2.	3.	4.	4.1.	4.2.	4.3.	5.	-	-
	a. Physical documents authentication means b. Digital documents authentication means	a. Sharing information outside organization b. Means	a. Response b. Reason C. Examples	a. System used by the organization for authenticating documents/data	a. Pros of the system b. Cons of the system	a. Response b. Extra info.	List of incidents jeopardizing security /privacy	List of actors involved in the system and their level of authority	List of additional information points	List of comments of the interviewers
1.*	..	..	..	..						

Tuesday, October 20, 2015

Part B: Case scenarios <20-25 minutes>

One of the following cases is to be chosen for each interview.

Option i: Health care part (1/2)

Hand out figure printout

Description

Consider a case, where a patient goes to the doctor for a routine check-up and takes an extensive blood test. The blood test is taken by the doctor's nurse and the results are uploaded to the portal and are digitally signed by the nurse. The doctor has access to the complete blood test results.

NEXT>> the patient visits a dietitian, who requires few specific fields of the blood test. The patient doesn't want to reveal all fields from the extensive blood test. So the patient selects the mandatory fields from the extensive blood test for the dietitian to see and "blacks-out" the other fields.

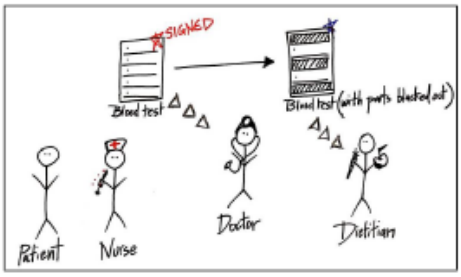

Figure 1: blood test use case

Alternative similar case:

Consider a case, where a patient goes to the doctor for a routine check-up and takes an extensive blood test. The blood test results and diagnosis report are uploaded to the portal and are digitally signed by the doctor. The doctor has access to the complete blood test results.

NEXT>> the patient wants a second opinion from another doctor on her results. The patient doesn't want to reveal the diagnosis fields from the report. So the patient selects the blood test results for the second doctor to see and "blacks-out" the diagnosis fields.

1. In your opinion, is the blood test that was viewed by the dietitian still verified/authentic, i.e. is the nurse's signature still valid? Why/why not?
   - 1.1. Would you trust claims that signatures for parts of the document are still valid?
2. Are there similar examples/cases in your organization, where parts of a document are modified/edited out?
   - 2.1. How does your system handle modifications?
   - 2.2. How does your system guarantee that modified documents will have a valid signature?
3. From your experience, what other signature related issues/incidents can you share?

Option i: Health care part (2/2)

Hand out figure printout

Description

Consider a case, where a patient has a smart phone training application that uses the sensors on the phone/wearable device to monitor and collect personal data of the patient. The patient would like to share only activity progress information of the data collected by the application.

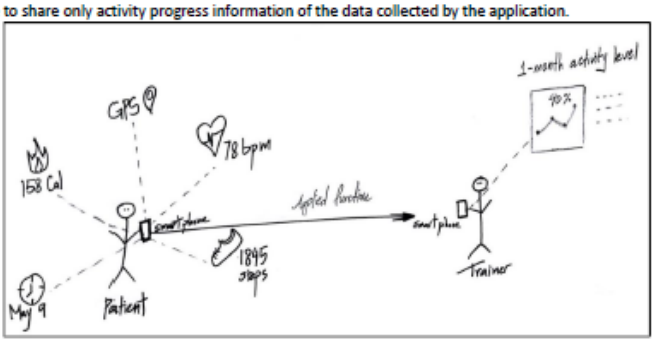

Figure 2: monitor application use case

Tuesday, October 20, 2015

4. Do you see the benefit of this case (providing applied functions data instead of raw data)? Why?
5. What similar functions can you foresee in your organization? Examples?

Table 2: Results from Part B.i (Health care)

B.i	1. a. Response/ opinion b. Reasons	1.1. a. Response b. Extra info.	2. List of similar examples/cases	2.1. Means of handling modifications	2.2. Means of validity verification	3. List of experiences/ issues/incidents	4. a. Response b. Reason c. Extra info.	5. a. List of similar functions b. Examples	- List of additional information points	- List of comments of the interviewers
1.*	..	..	..	..						

Tuesday, October 20, 2015

Option ii: Smart City

Hand out figure printout

Description

Consider a case, where handicaps are required to use either their regular phones or smart phones to validate themselves for handicap parking. When using a regular phone, a control station by the parking will be used to authorize the parking with SMS. When using a smart phone, the parking APP would use the NFC badge (digital identification) and GPS location for identification.

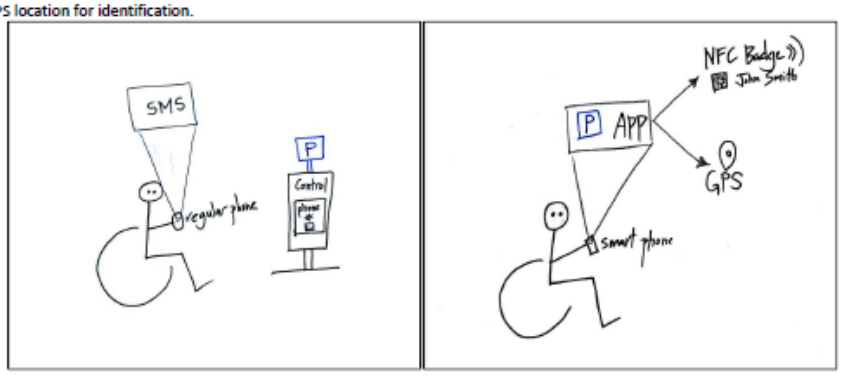

Figure 3: Handicap parking authorization using regular phone (left) or smart phone (right)

1. In your opinion, do you think that this application supports or jeopardizes security? To whom (actors involved)? Why?
2. Do you think that this application supports or jeopardizes privacy? To whom? Why?
3. What do you think is the minimal information to be disclosed?
4. Would you trust a technical solution that claims that users could securely authorize themselves for being eligible for this service without leaking any other information?
4.1. What concerns would you have in such solution?

Tuesday, October 20, 2015

5. From your experience, what other security/privacy related issues/incidents can you share?

Table 3: Results for Part B.ii (Smart City)

B.ii	1. a. Response b. Actors involved c. Reasons	2. a. Response b. Actors involved c. Reasons	3. Response	4. Response	4.1. Concerns	5. List of experiences/ issues/incidents	- List of additional information points	- List of comments of the interviewers
1.*	..	..	..	..				

Tuesday, October 20, 2015

Option iii: E-government part (1/2)
No figure available **Description** For disaster recovery and backup purposes, IT providers of governmental institutions split their databases into multiple parts (shares) that are stored at independent cloud providers. Consider a case where a disaster occurs, and a potential data loss is at risk. To reconstruct data, only a predefined subset of shares stored at different cloud providers would be required, e.g., 4 shares out of 7.
1. Do you have disaster protection mechanisms? What are they?
1.1. Do they protect against data loss?
2. Do you have any data recovery mechanisms? What are they? How does it address confidentiality of backups?
3. Do you see benefits in such solutions? Would you use such backup/data-sharing setup? Why/why not?

Option iii: E-government part (2/2)
No figure available **Description** Consider a case where a forest fire occurs. Later the government has produced a report that includes personal information, e.g. about victims or rescue workers, and potentially other classified information (all signed) regarding the cause and the incident response procedure. The conclusions are signed by relevant experts. Based on this, the intention is to release a report to the public where one wants to anonymize all personal information and classified information, but keep the electronic signed conclusions.
4. In your opinion, is the report released that was viewed by the public is still verified/authentic i.e., is the original signature still valid? Why/why not?
4.1. Would you trust claims that the signatures will still be valid for the document after all personal information has been "blacked-out"?
5. Are there similar examples/cases in your organization, where parts of a document are modified/edited out, while validity for the unmodified parts should be maintained?
5.1. How does your system handle modifications? 5.2. How does your system guarantee that modified documents will have a valid signature?
6. From your experience, what other signature related issues/challenges can you share?

Tuesday, October 20, 2015

Table 4: Results for Part B.iii (E-Government)

B.iii	1.	1.1.	2.	3.	4.	4.1.	5.	5.1.	5.2.	6.	-	-
	a. Response b. mechanisms	Response	a. Response b. Data-recovery mechanisms	a. Response b. Reason	a. Response / opinion b. Reasons	a. Response b. Extra info.	List of similar examples/cases	Means of handling modifications	Means of validity verification	List of experiences/ issues/incidents	List of additional information points	List of comments of the interviewers
1.*	..	..			..	..	..	..				

Part C: Requirements follow up <10- 15 minutes>

1. In your perspective, for a system dealing with digital signatures, what are the fundamental requirements does the system need to fulfill in order for it to be considered trustworthy? Secure? Private? Authentic?
2. What are your general concerns when it comes to security/privacy in Cloud services (outsourcing)?
3. What are security requirements for your organization for using the Cloud services (outsourcing)?
4. What are your thoughts/expectations on authenticity of data and verified computations in the Cloud?
5. Would you trust that contractual agreements, certification and auditing schemes will be sufficient for ensuring security for data outsourced to the cloud? Or would you put more trust on crypto-based security solutions?

Table 5: Results for Part C

C	1.	2.	2.	3.	4.	5.	-	-

Tuesday, October 20, 2015

	List of requirement for a. Trust b. Security c. Privacy d. Authenticity	Security concerns in the cloud	Privacy concerns in the cloud	Security requirement in the Cloud	Thoughts and expectations for authenticity	Response	List of additional information points	List of comments of the interviewers
1.*	..	..	..	..				

Hand out Questionnaire

11. ANNEX II: Consent Form

CONSENT FORM

Within the scope of the EU H2020 project PRISMACLOUD on "Privacy and Security Maintaining Services in the Cloud", [Karlstad University] is conducting interviews with different stakeholders for eliciting requirements for PRISMACLOUD services.

Elicited requirements will be published in a project deliverable in November 2015 and possibly also in research papers and/or reports.

If you consent, the interviews will be recorded electronically or manually. All recording will be stored safely at [Karlstad University] and will be deleted at the latest by the end of November 2015 when the project deliverable will have been published. Privacy rules according to the [Swedish] Data Protection Act and the EU Data Protection Directive 95/46/EC will be followed.

No personal data will be published at any time, unless we will get your consent for publishing your name or any other identifying data about you in reports/articles. In this case, you will receive the deliverable/reports/articles for reviews before you will be asked to provide your consent.

You have the right to withdraw your consent at any time, request access to your data and demand the deletion or correction n of the material recording your interview or any other personal data relating to you.

[ ] I consent that data about collected during the interview can be processed under the conditions described above.

Name, date

Signature.

[ ] I consent that my interview can be recorded electronically.

Name, date

Signature.

12. ANNEX III: Post-Interview Survey Questions

POST-INTERVIEW SURVEY

Role in organization/Area of work: Date:

Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	*I Don't Know*
In our organization						
User privacy is sufficiently addressed						
We could use improvements to support user privacy						
Security is sufficiently addressed						
We could use improvements to support security of data						
Usability is sufficiently addressed						
In the Cloud (Cloud-outsourcing)						
We are currently using/would like to use Cloud services as they are						
There is a lack of understanding Cloud services and processes						
Safety is more important than Privacy						
We base our trust mainly on contractual agreements and policies						
We have concerns dealing with Cloud services regarding user privacy and security						
We are satisfied with current Cloud services from Privacy and security perspectives						
User privacy is more crucial if data is stored in the Cloud						
Data security is more crucial if data is stored in the Cloud						
Cryptographic solutions						
I have a fair Idea about how cryptographic solutions can enhance security/privacy						
Cryptographic secure solutions would significantly increase our trust in Cloud services						
If data security and user privacy are improved we are more likely to use/trust Cloud services						
List few words that describe Cloud services to you: **General comments about the interview in general and/or topics discussed:**						

13. ANNEX IV: Survey Questions

SURVEY 1/2

Q1a: Please choose the type of your organization (choose one)

☐ Academia (Research Organization) ☐ Industry

Q1b: Do you consider your organization as Critical Infrastructure (e.g. Bank, Public Administration, Utility Provider, Government) (choose one)?

☐ Yes ☐ No

Q2: Which role best describes your position in your organization (choose multiple)?

☐ Management ☐ Researcher ☐ Engineer ☐ Consultant

☐ Other (please indicate) ……..

Q3: Where is your organization based (choose one)?

☐ Austria ☐ another EU Country ☐ USA

☐ Other (please indicate) ……..

Q4: Which of the following do you consider your organization (choose multiple)?

☐ Cloud service provider ☐ None

☐ Cloud service user ☐ Others ……..

Q5: Which of the following applies for your organization (choose multiple)?

☐ Cloud user/provider with own virtual Infrastructure

☐ Cloud user/provider with own physical Infrastructure

☐ Other ……..

☐ Infrastructure is shared between independent sub/units/departments/subsidiaries inside my organization

☐ Infrastructure is (partially) outsourced to a 3rd party

☐ None

Q6: Do you agree that Cloud service providers can be trusted in handling user data if (choose one per line):

Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	*I Don't Know*
The cloud service provider is certified by a third party						
The cloud service provider is operated in a certified computing center						
The cloud service provider explains how it meets the agreed upon privacy policy						
The cloud service provider uses cryptographic functions and schemes for making computing verifiable						
The cloud service provider is placed in Europe and complies with European privacy law and regulations						

Q7: In your opinion, what factor do you think are important for Cloud service users to trust in Cloud service providers (open question)?

Q8: What are the reasons that would lead you to distrust cryptographic solutions? What practical hindrances would you foresee in implementing cryptographic solutions (open question)?

SURVEY 2/2

Q9: How important do you consider the following Security related aspects when it comes to cryptographic solutions? (Order the following from 1 (top priority) to 6 (least priority), i.e., using each number once)

Attribute =>	Integrity	Usability	Confidentiality	Availability	Anonymity/ Privacy	Accountability/ Verifiability
Priority order (1-6)						

Q10: Which of the following concepts would you prefer for secure services?
Please prioritize your top three: 1 (top priority) to 3 (least priority), using each number once

- ☐ A security level indicator for your service, without details of the underlying infrastructure
- ☐ Cryptographic solutions to protect authenticity and confidentiality of data end-to-end
- ☐ Security Guideline for cloudification
- ☐ Other ……..

Q11: Do you have concerns about moving your data to the Cloud?
Please prioritize your top three: 1 (top priority) to 3 (least priority), using each number once

- ☐ Someone tampering (i.e. modifying or stealing) my data
- ☐ Privacy limitation due to the legislative disadvantages (e.g. American patriot Act)
- ☐ No, I do not have any concerns moving data

Q12: As a Cloud user what of the following would you prefer to be fulfilled from a Cloud provider?
Please prioritize your top three: 1 (top priority) to 3 (least priority), using each number once

- ☐ Cloud providers that are certified (e.g. security, auditing or other certificates)
- ☐ Cloud providers that implements trust concepts and strategies
- ☐ Cloud provider that only support SLA
- ☐ None, I just want to exploit the benefits of Cloud provider

Q13: As a Cloud user, how would you fulfill your duty to control the cloud provider?
Please prioritize your top three: 1 (top priority) to 3 (least priority), using each number once

- ☐ On-Site Audit
- ☐ Not at all
- ☐ Choose a certified Cloud provider
- ☐ Other (please indicate) ……..

Q14: Which of the following are prior concerns to you from your role (Cloud provide / Cloud user)?
Please prioritize your top three: 1 (top priority) to 3 (least priority), using each number once

- ☐ Security/Privacy
- ☐ High scale processing
- ☐ Standardization
- ☐ Implementing Trust strategies and concepts
- ☐ Auditing
- ☐ Certification
- ☐ Legal concerns
- ☐ Monitoring
- ☐ Other (please indicate) ……..

Q15: Which of the following would you like to use for establishing security/privacy concepts inside a cloud environment?
Please prioritize your top three: 1 (top priority) to 3 (least priority), using each number once

- ☐ Customizable security/privacy mechanisms
- ☐ Aligning with the security and privacy related standards
- ☐ Security/privacy certification
- ☐ Service Level Agreements
- ☐ Other (please indicate) ……..

Contact: info@seccrit.eu

14. ANNEX V: Focus Group Agenda

Agenda

Part 1: Introduction (10 minutes)

- Introduction to the workshop agenda
  - Materials: sketches and post-it, write everything down
  - Flexibility, new ideas and critique is welcome
- Divide into groups
- Know your group! (introduce yourself to your group members)

Part 2: Group discussions (25 minutes)

Task 1- Selecting a scenario (10 minutes)

- Choose one of the scenarios which were presented with the cryptographic functions (you can modify them or suggest a new scenario/function)
  #list of functions from Thomas and Daniels slides and Scenarios: (in a separate sheet of paper)
    1. E-health
    2. E-Government
    3. Smart City

Task 2- Perspective on the cryptographic functions (Cloud) (15 minutes)

- Discuss how the cryptographic function selected would enhance privacy, trust and usability
  - Each take 2 minutes and write down a post it
  - Go around each stick the post-its on the table
- Discuss concerns in regards to privacy, trust and usability
  - Each take 2 minutes and write down a post it
  - Go around each stick the post-its on the table

Part 3: Requirements (15 minutes)

- From your different perspectives and backgrounds, what requirements would Crypto need to fulfil in order to enhance trust in the Cloud?
  - Each take 5 minutes to write down on a post it
  - Go around, each reads their note and stick it on the table's paper

Part 4: Wrap up (10 minutes)

- Go rounds: Group summaries to other groups
- Closing and thanks
- Feedback and follow-ups

15. ANNEX VI: Suggestions for User Interface solutions

Some requirements in Table 5 are directly connected to system use. Suggestions for how these requirements might be satisfied by the user interfaces have been noted simultaneous with the requirements analysis. These (high-level) suggestions for UI solutions are presented in Table IV. They cover only requirements elicited during interviews.

Table VI: Examples of possible UI implementations for RH#, RG#, and RSC#.

RH#	**Example of possible UI implementations**
RH1	Example for easy login: unobtrusive biometrics (e.g., touch screen biometrics in combination with graphical passwords).
RH2	Example for functional benefit: The working context is preserved if they logout from one system and login to another one. (i8)
RH3	(This needs no example except what is given for RH1.)
RH4	Template for certain standardised documents defining attributes that will by default be redacted (e.g., when data is made available to researchers).
RH5	(No examples yet, but this is an interesting topic. Tutorials will not affect a person like the interviewee who will simply not watch such “nonsense”.)
RH6	The UI that relates to the “owner” (responsible organization) of the system.
RH7-8	UIs of incident reporting tools (based on functional signatures) should explain how incidents were detected based on deviations of the allowed operations for the Cloud.
RH9	The UI informs if a private Cloud controlled by the respective authority (e.g., via suitable clickable icons).
RH11	Tutorials and possibly a test to check patients’ / users’ understanding.
RH12	UI informs staff of how many patients accessed their log access during some period.
RH13	Intuitive clickable icons could visualize the states of trustworthiness. If clicked, the UI refers to signed documents that include results from regular functional tests.
RH14	Avoid free-format input but this can make for cumbersome systems. Another alternative is to have “spell checkers” (standards checker) suggesting expressions.
RH16	Secure and privacy friendly mobile applications providing functions for patients and interactivity. Usable transparency visualizing the essentials of logs and possible misuses.
RH17	Intuitive identity management UI paradigms supporting selective disclosure, such as the ones developed in the PrimeLife project based on an adapted card metaphor (see [52]).
RH18-19	Good systems would avoid answering inquiries about patients that are of no concern for a specific health worker. Thus no specific UI solution is needed.
RG#	**Example of possible UI implementations**
RG1	The UI should mediate prominently that an EU-based Cloud solution is used, e.g. by the use of appropriate icons (as were researched by the A4Cloud project, see [53]). Tutorial inside the system if the system user is a health authority.
RG5	UIs of each service provider automatically adjust to the UI theme that the user has chosen.
RG8	UI should allow to easily verify whether critical computations took place or not.
RSC#	**Example of possible UI implementations**
RSC1	UI has to inform about backup solutions.
RSC2	The UI has functionalities for viewing proofs and forwarding them to other parties.
RSC3-4	Proper guidelines to evaluate the crypto solution that can be tailored to different scenarios.
RSC9	Data subject is informed about the data retention periods, and whether the data will be deleted either manually of automatically after these periods.