Secure and Privacy-Friendly Storage and Data Processing in the Cloud

Pasquale Chiaro, Simone Fischer-Hübner, Thomas Gross, Stephan Krenn, Thomas Lorünser, Ana Garcí, Andrea Migliavacca, Kai Rannenberg, Daniel Slamanig, Christoph Striecks, et al.

Secure and Privacy-Friendly Storage and Data Processing in the Cloud

Pasquale Chiaro[1], Simone Fischer-Hübner[2], Thomas Groß[3], Stephan Krenn[4], Thomas Lorünser[4], Ana Isabel Martínez Garcí[5], Andrea Migliavacca[6], Kai Rannenberg[7], Daniel Slamanig[4], Christoph Striecks[4], and Alberto Zanini[6]*

[1] InfoCert, Milan, Italy
pasquale.chiaro@infocert.it
[2] Karlstad University, Karlstad, Sweden
simone.fischer-huebner@kau.se
[3] University of Newcastle upon Tyne, Newcastle upon Tyne, United Kingdom
thomas.gross@newcastle.ac.uk
[4] AIT Austrian Institute of Technology GmbH, Vienna, Austria
{firstname.lastname}@ait.ac.at
[5] ETRA Investigacion y Desarrollo, S.A., Valencia, Spain
amartinez.etraid@grupoetra.com
[6] Lombardia Informatica S.p.A, Milan, Italy
andrea.migliavacca@cnt.lispa.it, alberto.zanini@lispa.it
[7] Goethe University Frankfurt, Frankfurt, Germany
kai.rannenberg@m-chair.de

Abstract. At the IFIP Summer School 2017, the two H2020 projects CREDENTIAL and PRISMACLOUD co-organized a workshop dedicated to introducing the necessary background knowledge and demonstrating prototypes of privacy-preserving solutions for storing, sharing, and processing potentially sensitive data in untrusted cloud environments. This paper summarizes the given presentations and presents the discussions and feedback given by the workshop attendees, including students and senior researchers from different domains as well as relevant non-academic stakeholders such as public data protection agencies.

Keywords: Privacy ⋄ Data protection ⋄ Demonstration

1 Introduction

Storing, sharing, and processing data in the cloud play vital roles in many everyday scenarios, ranging from private data vaults and company backups over identity and access management (IAM) to eHealth and eBusiness. However, besides the many benefits of the cloud setup such as cost-effectiveness and scalability, many of these applications pose very high security and privacy requirements to the solutions in use as data owners have no control over how their data is

* The projects contributing to this work have received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644962 (PRISMACLOUD) and 653454 (CREDENTIAL).

used once it is released to the cloud. Consequently, a large body of work on privacy-enhancing technologies has been proposed by the academic community, and many results have reached a high maturity level; however, as pointed out by Lorünser et al. [1], a large fraction of these results is purely academic and does not sufficiently address the needs of users and service providers, and thus does not get adopted in the real world.

The ambition of the two large-scale European Horizon 2020 (H2020) research and innovation actions PRISMACLOUD[8] and CREDENTIAL[9] is to close this gap for certain cryptographic primitives, by developing promising candidates for integration into commercial cloud offerings. This is achieved by involving all relevant stakeholders in the design process. Based on their inputs, a careful selection of cryptographic technologies was made, and efficient and secure first prototype implementations were developed. To showcase the usability and usefulness of these prototypes, they were then integrated into multiple pilot scenarios coming from the real world.

After already having held independent workshops at the IFIP Summer Schools 2015 [2] and 2016 [3], the two projects organized a joint workshop in 2017, in order to raise awareness of their solutions, and to receive feedback and inputs on the developed pilots. During the remaining runtime of the projects, this feedback will be used to further improve the developed tools in order to guarantee that they indeed serve the needs of real users and cloud service providers, and to adequately address any concerns, specific requirements, or ideas.

This paper summarizes the content of this workshop, and gives an overview of the discussions with students and senior researchers from different domains, legal experts, and other relevant non-academic stakeholders.

1.1 Outline

This document is structured as follows. After briefly explaining the challenges of identity management in the cloud in Section 2, Section 3 briefly summarizes the main ambitions of the two projects CREDENTIAL and PRISMACLOUD. Section 4 then gives detailed descriptions of five pilots executed in the two projects, two from CREDENTIAL and three from PRISMACLOUD. A summary of the feedback given by the workshop participants and the projects' advisory board members is then given in Section 5. Finally, we briefly conclude in Section 6.

2 Cloud Privacy & Identity Management

In the following, we give an introduction to privacy-friendly and trustworthy identity management. We discuss the privacy and security issues of typical federated identity management architectures, namely over-identification and the "Calling Home" problem, and present possible solutions to both of them.

[8] https://prismacloud.eu/
[9] https://credential.eu/

Over-identification occurs, when users need to present credentials, that contain more information than needed to justify the respective access claim, e.g., when an ID card is presented to prove legal age often the precise birth date is presented, while a certified Boolean statement, that the person is of legal age, would be satisfactory and would avoid misuse of the birth date information.

The "Calling Home" problem is caused by credentials, that are always double-checked with the issuer, which causes a lot of information there, which user is using which credentials for which service at which point in time. It can also be caused by situations in which users need to ask for a credential on the spot, exactly when they need it.

Technical solutions for addressing these issues include the following: partial identities, attribute-based credentials (especially Privacy-ABCs) and redactable signatures for cloud identity management:

Partial identities and identities as such are defined in ISO/IEC 24760 [4] as a "set of attributes related to an entity". Partial identities support the building of identity management systems, that enable users to select the appropriate attributes for the respective situation and so help against over-identification.

Attribute-based credentials (especially Privacy-ABCs) enable the user to have the relevant attributes certified without having to recur to the original certifiers of the attributes: If a set of attributes is certified in a Privacy-ABC the certified users can choose their own subset of attributes as needed and derive the certificate themselves from the original one. More details on the nature and the trialling of Privacy-ABCs in real life scenarios can be found, e.g., in Rannenberg et al. [5].

Redactable signatures for cloud identity management as developed in the CREDENTIAL project enable the editing of encrypted credentials (e.g., to protect them when stored in a cloud-based identity management system). So redactable signatures enable the editing of Privacy-ABCs.

Further approaches for a more privacy-friendly Internet and respective cloud services are:

- Decentralisation;
- Minimum disclosure;
- Strong sovereign assurance tokens (e.g. smart cards, if appropriate mobile devices).

3 Project Overview

The following section briefly explains the approaches of CREDENTIAL and PRISMACLOUD to address them.

3.1 Privacy-Friendly IAM with CREDENTIAL

CREDENTIAL is an innovation action dedicated to the design and implementation of a privacy-preserving platform for sharing of authenticated data, including identity and access management scenarios, thereby directly addressing the problem of overidentification and partially adressing the "calling home" problem [6,7].

The security and privacy of the developed platform, the so-called CREDENTIAL Wallet, is mainly based on two cryptographic building blocks, *redactable signatures* and *proxy re-encryption*. Redactable signatures [8] allow the signer to define parts of the message which can later be blanked out by any party knowing the message and the signature. That is, any party, not requiring access to the secret signing key, can later remove (subsets of the) redactable parts of the message and simultaneously adapt the signature such that the obtained signature still certifies the authenticity of the revealed information. On the other hand, proxy re-encryption [9] is an extension of traditional public key encryption schemes, where a dedicated third party (the *proxy*) can transform ciphertexts encrypted for a user A to ciphertexts encrypted for a user B, without itself every gaining access to the plain data. This is achieved by letting A use his secret key and (depending on the concrete scheme being used) B's public or secret key to compute a so-called re-encryption key, which is then sent to the proxy and can only be used for re-encryption but not decryption.

The overall approach of CREDENTIAL now is as follows. Users can obtain certificates on personal attributes from an issuer who signs them using a redactable signature scheme. The encrypted attributes together with the signature are then uploaded to the CREDENTIAL Wallet. Furthermore, when a user first wants to authenticate himself towards a specific service provider, the user computes a re-encryption key from his own public key to the service provider's public key, and stores this re-encryption key in his account at the CREDENTIAL Wallet. Now, for subsequent authentications, the Wallet re-encrypts only those attributes that the user does chooses to reveal to the service provider and redacts the remaining ones. By doing so, the service provider will still be convinced that the revealed attributes have not been altered, hereby solving the problem of over-identification similar to attribute-based credentials systems [10,11,12]. The approach is also illustrated in Figure 1.

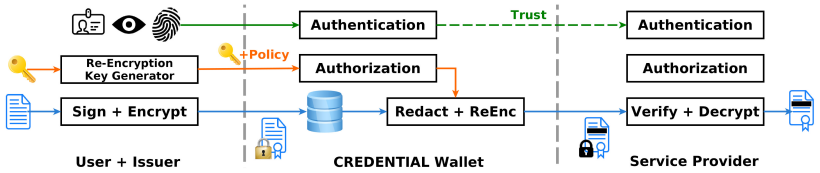


Fig. 1: The CREDENTIAL approach, adapted from Karegar et al. [6].

The CREDENTIAL approach is not directly susceptible to the "calling home" problem as the issuer is not contacted upon authentication. However, the CREDENTIAL Wallet as a central entity is contacted upon every authentication process, and therefore learns which service a user accesses at which time. A partial solution to this problem, where the Wallet only learns that a user is authenticating to *some* service but not to which one, was recently suggested by Krenn et al. [13].

The feature set and usability of the CREDENTIAL Wallet is demonstrated using use case scenarios from the domains of eGovernment, eBusiness, and eHealth, cf. also Section 4.

3.2 PRISMACLOUD Overview and Applications

PRISMACLOUD is a research and innovation action dedicated to enabling secure and trustworthy cloud-based services by improving and adopting novel tools from cryptographic research [14,15]. Cloud computing raised the need for application of cryptography to be more secure and privacy-friendly. However, the adoption of cryptography for modern information and communication (ICT) technologies is not hampered by the lack of technical feasibility, but more by accompanying factors like usability, missing knowledge in IT security community, and regulation.

The PRISMACLOUD approach is to propose a layered architecture of secure and trustworthy cloud-based services that utilizes strong and novel cryptographic primitives and tools to be adapted to several real-world applications. This layered approach is illustrated in Figure 2.

Layer 1 (Primitives). PRISMACLOUD is focusing on a broad range of cryptographic primitives on the lowest layer, including attribute-based credential systems for privacy-preserving user authentication [10,11,12], secret sharing for secure distributed storage of data at rest [17,18], malleable signature schemes for controlled modifications of authenticated data [8,19,20,21], or graph signatures for topology certification [22]. Malleable signatures are a super set of redactable signatures, that allow for even advanced functionality besides the redaction of signed messages. Secret sharing on the other hand allows for secure distribution of sensitive data. Thereby, the message is split into shares and distributed to many cloud databases. Inherently, the system has redundancy in the sense that only a fraction of the cloud databases is needed to reconstruct the message. Graph signatures encode graph data structure into the underlying digital signature scheme in a way that for all components of a graph (i.e., edges, vertices, labels), proof-of-knowledge properties can be stated. Together with attribute-based credentials, malleable signatures tackle the over-identification and "Calling home" problems.

Layer 2 (Tools). On the next layer, the primitives from Layer 1 are included into more complex tools. For example, attribute-based credentials and malleable signatures are used as building blocks for Flexible Authentication with Selective Disclosure and Verifiable Data Processing, respectively. Further, the Topology Certification tool is presented in more detail in Section 4.5.

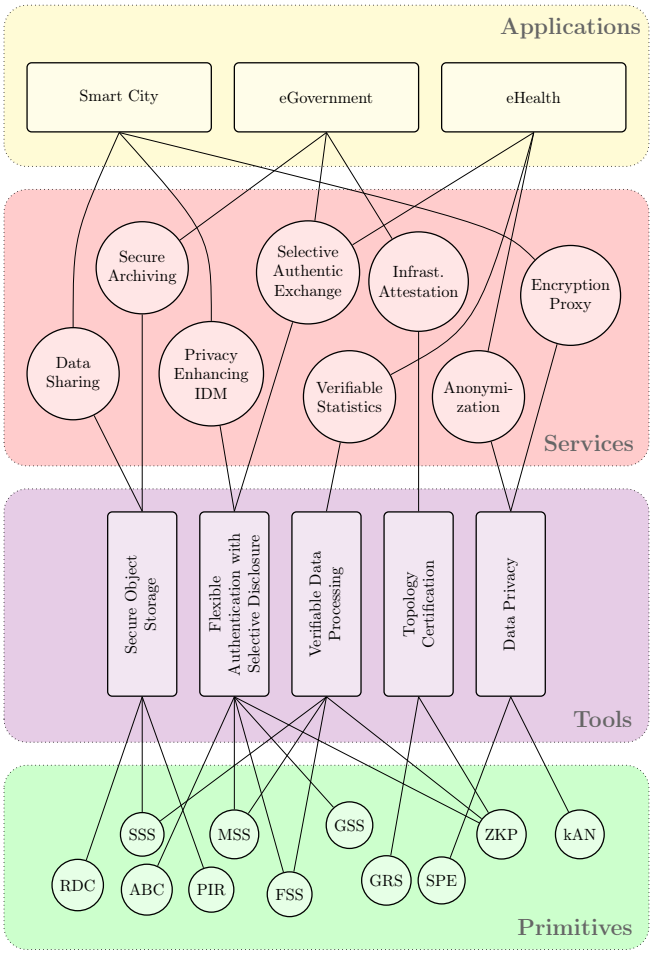


Fig. 2: The layer approach of PRISMACLOUD from Lorünser et al. [16].

Layer 3 (Services). On the service layer, the tools from the Layer 2 are the building blocks for more advanced functionalities. For example, Flexible Authentication with Selective Disclosure and Verifiable Data Processing are used as building blocks for Privacy Enhancing Identity Management (IDM) and Verifiable Statistics, respectively. Furthermore, Secure Archiving is derived from Secure Object Storage (cf. also Section 4.4) and directly serves as a example for the Decentralization approach mentioned in Section 2.

Layer 4 (Applications). The application layer deploy the services from Layer 3 in real-world scenarios such as Smart City, eGovernment, and eHealth, cf. also Section 4.3.

Note that in contrast to Layers 1 and 2, almost no cryptographic knowledge is needed any more on Layers 3 and 4, making them also accessible to software

developers and product designers without requiring deep mathematical background.

PRISMACLOUD also has a strong focus on human computer interaction (HCI) design patterns, the implementation of modular and reusable software libraries, and the design of cloud services that can be seamlessly integrated into existing software applications via the layered approach. This holistic approach enables PRISMACLOUD to achieve its main ambition, namely to enable end-to-end security and privacy for cloud users without negatively impacting usability neither for users nor for service providers.

4 Pilots and Discussions

The following section introduces some of the pilots designed, implemented, and executed within PRISMACLOUD and CREDENTIAL. Furthermore, it summarizes the feedback, questions, suggestions, and concerns received from the workshop participants, who were able to get hands-on experience of the pilots during the IFIP Summer School 2017.

4.1 eGovernment Pilot (CREDENTIAL)

The CREDENTIAL eGovernment pilot focuses on identity management to authenticate citizens towards services provided by public authorities. Based on standardized protocols such as SAML or OpenID Connect, the service provider can request authentication and identity attributes from the CREDENTIAL Wallet. By requesting the user's consent for granting the service provider access to the requested data, the user is given full transperancy and control over which data is requested and revealed; furthermore, because of the encryption technology being used, the CREDENTIAL Wallet never obtains access to the user's attributes in an unencrypted form. The pilot not only enables authentication via national eID solutions, but also cross-border authentication according to the eIDAS regulation, aims at high interoperability with existing authentication protocols, and minimizes the integration effort on the service provider's side.

A bit more precisely, the eGovernment pilot considers a user owning a CREDENTIAL account that already contains a set of authentic data items. The user wants to authenticate himself towards a service hosted by Lombardia Informatica S.p.A. (LISPA), a public-capital service company in northern Italy. Specifically, we assume that the user wants to authenticate himself towards SIAGE, a web portal used to request tax breaks and other types of fiscal advantages. When browsing to the login page, the user has the option to choose CREDENTIAL as an identity provider, and is then redirected to an URL published by the OpenAM component in charge of initiating the authentication flow according to the OAuth2 standard. The user then receives a notification on his mobile phone listing all the required and optional attributes SIAGE wants to access for authentication and the subsequent process, and can decide whether or not to disclose these values, cf. Figure 3. In case the user gives his consent, the requested data

Fig. 3: eGovernment pilot.

is re-encrypted by the CREDENTIAL Wallet and sent to SIAGE, who can then decrypt the data and verify its authenticity.

4.2 eBusiness Pilot (CREDENTIAL)

Many business processes can nowadays be performed online. However, there is often a trade-off between security and usability: that is, systems that are easy to use often do not sufficiently protect security and privacy, while safer processes often partially sacrifice usability. The CREDENTIAL eBusiness pilot addresses some of the most often performed processes and provides privacy-friendly, secure, and usable solutions for authentication and Single Sign-On (SSO), purchase processes and online form subscription, and forwarding of encrypted communication. The first scenario is strongly related to the authentication use case in the eGovernment pilot presented in Section 4.1. The second scenario reliefs users from having to enter all their personal information like name, date of birth, or address everytime they subscribe to a service; rather, the user's information that is already stored in the CREDENTIAL Wallet can automatically be filled into the registration forms. In the following we will put our main focus on the third scenario on encrypted communication.

InfoCert is an Italian organization offering trust based business solutions for organisations and businesses to interact with customers and citizens. Among others, InfoCert offers Legalmail, an email service realizing legally binding mail exchange. The goal of CREDENTIAL is to add an end-to-end encryption layer to Legalmail. However, due to the legal properties of the communication it is important to support proper mail forwarding possibilities for such mails. This is because an email is legally considered delivered once it reaches the recipients mailbox, independent of whether it was read or not; thus, in the case of a longer

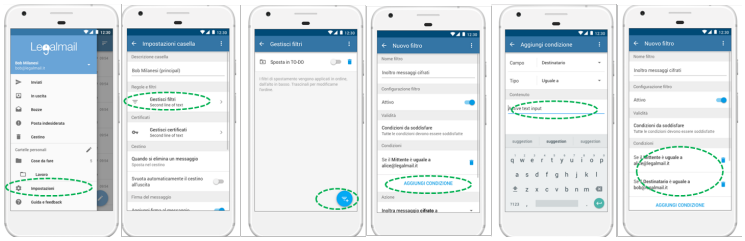


Fig. 4: eBusiness pilot.

absence, it might happen that the receiver otherwise misses important deadlines or similar. However, using the standard forwarding capabilities of the mail server is not sufficient for encrypted emails for obvious reasons: either, the delegatee cannot decrypt the received message, or the original receiver would have to share his secret keys with the substitute. Within CREDENTIAL, this problem is addressed by using proxy re-encryption [9], where the receiver can deposit a re-encryption key that allows the mail server to translate the cipher text into an encryption under the delegatee's public key without itself learning the plain message.

After explaining the scenario, interactive mockups were used to show how Legalmail users can setup the encrypted mail forwarding within a slightly extended Legalmail app. Figure 4 shows how a user first accesses into the setup section, then selects "filter setting" and "add new filter", finally defines the forwarding rules.

Discussion and feedback. Considering that Legalmail was new to all workshop participants, the received feedback was quite interesting: both technical and not technical attendees agreed about the perceived value of a legally binding communication. They also founded coherent the need to enhance the security in sharing some kind of sensitive information. Furthermore, several concrete suggestions on how to improve the user interfaces and experience were made by the workshop participants.

4.3 Smart-City Pilots (PRISMACLOUD)

During the tutorial, demos of two PRISMACLOUD pilots applied within the smart-city environment SIMON[10] were shown. Each of them integrates one secure cloud service, developed inside the PRISMACLOUD project. SIMON is another European project dedicated to remove and prevent barriers that cause problems for persons with disabilities when using products, services and public infrastructure. One goal of SIMON is to ensure that only disabled persons are able to park in reserved lots in a city. Instead of only putting the parking card into the car, the disabled person first uses the SIMON mobile application and the smart-parking card

[10] http://simon-project.eu/

for marking the location in which he/she is parking. As parking cards are very easy to duplicate, SIMON help authorities and end users to fight fraud, because operators can check if the smart card is duplicated. In Figure 5, screenshots of the end-user's mobile parking application are given.

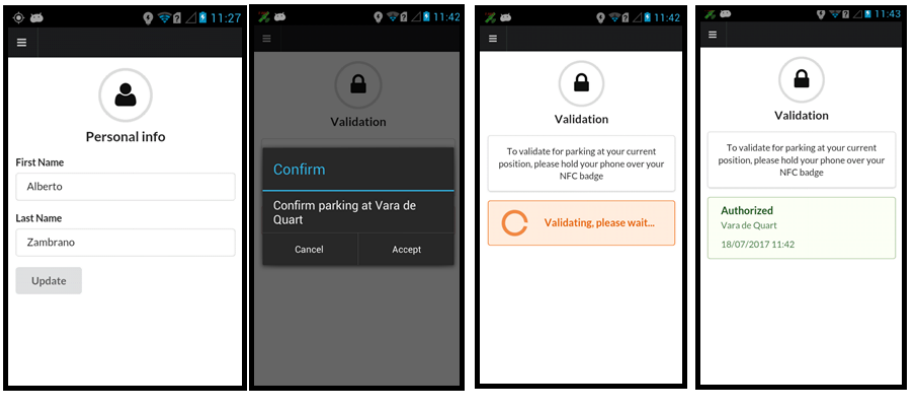
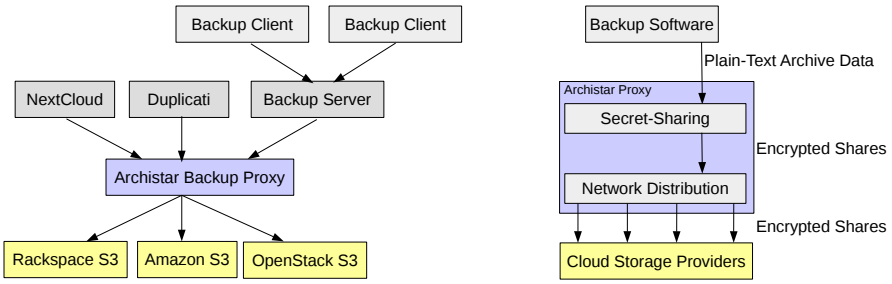


Fig. 5: SIMON application for end users.

The first demo showed the PRISMACLOUD Encryption Proxy (EP) service integrated in SIMON. Since SIMON is in the cloud, the first problem it deals with is the treatment of sensitive data. SIMON is managing sensitive data such as personal information, which do not have to be accessible to other people except for the dedicated end users. This EP service encrypts sensitive data on the fly, leaving non-sensitive data not encrypted. Therefore, the messages and the information stored on the database contain non-sensitive data in clear text and sensitive data in encrypted format.

The second demo showed the integration of Privacy Enhancing Identity Manager (PIDM) service in SIMON. Another problem of SIMON in the cloud is that the user's personal identifier is sent in clear for each operation, so users are identified. This is a big problem due to legal implications. In SIMON, city areas or neighborhood are defined and users have permissions to park in lots belonging to those areas that they belong to. The PIDM has been integrated in order to anonymize those operations. The user's identifier is replaced in messages by a proof of belonging to the area in which the lot is; thus, the system does not know which user is going to park. It only knows that a user which has permission for the area is going to park. The proof is generated by cryptographic mechanisms in the service, i.e., by means of suitable group signatures [23].

Discussion and feedback. During the presentation, students were very interested in the two demos and some technical question were asked. The first point of discussion was where personal data or private keys have to be stored and it was necessary to explain that the private keys belong to the end user, so they are



(a) High-level network system overview. (b) Example data-flow from backup client.

Fig. 6: High-Level network system overview and example data-flow from backup clients to the cloud storage servers.

generated and stored on the mobile memory, and the smart-card only has the firmed message in order to be checked by the parking operator. The second point was related to how to decide what is sensitive in any application. In the case of SIMON is mainly the user's personal information. Finally, students appreciated that all these cryptographic resources have use in an practical environment, due they usually deal with theoretical problems.

4.4 Distributed Storage Pilot (PRISMACLOUD)

During the tutorial the PRISMACLOUD solution for secure object storage in distributed multi-cloud settings [14] was shown. In order to protect data at rest in the cloud, the project builds on secure information dispersal, i.e., secret sharing techniques, which achieves security, integrity and availability at the same time in a very flexible and efficient way [24,25].

To give users easy access to the developed technologies, a secure archiving service (SA or SAaaS) specifically tailored to the needs of trustworthy backups was implemented [16]. Its functional key features were motivated from our eGovernment use case and it has been designed to support most commonly encountered cloud backup scenarios. The general idea of the secure archiving service is to provide an extremely reliable and secure storage back-end which can be easily hosted and used. The archiving use case focuses on data retention over long time periods and can even provide full quantum safe security when combined with adequate transport layer encryption, e.g., like in [26,27].

The prototype provides compatibility with multiple providers and legacy systems to support hybrid cloud storage scenarios which integrate local storage with public cloud offerings in a seamless way. Therefore, the Simple Storage System (S3) industry standard was chosen as main API and the service was made compatible with this standard on both sides, the back-end provider side as well as the front-end client side. Additionally, because we avoid the use of active components on the provider side, deployment can be very straight forward [28].

Overall, the service acts as a proxy [29] and the basic architecture is shown in Figure 6a as well as the data flow model in Figure 6b. It is part of the Archistar software framework [30] and supports the following main features: increased data privacy and availability, prevention from vendor lock-in, keyless (credential based) operation, reduced data remanence, long-term security support, support for multimodal encryption, support for remote auditing, plug-in replacement for legacy systems.

Discussion and feedback. During prototype presentation the audience was particularly impressed by the ease of use and integration of the provided solution and saw a great potential for exploitation. Additionally, they recommended to think about a version where no single point of trust exist, if this is possible. They also liked the idea of making the software available as open source software, such that it can be reviewed by a larger audience. Furthermore, one participant mentioned that similar technology is already used in commercial high-end storage solutions for data centers, but no solutions for broad adoption or multi-cloud configurations exist, especially for small end medium enterprises, are known. Finally, the participants also recommended to look into the field of mix networks and the security modeling used there, which has many similarities that may be transferred to multi-cloud approaches.

Besides feedback on the technical integration, we were also interested in feedback on the perception of security in systems based on data splitting. In its very pure nature, the data security is solely based on non-collusion of cloud providers, which is a different security model from what we typically use today. During the discussions of the demo we therefore tried to find suitable configurations for such storage systems and also discussed the necessity of an additional cryptographic layer to protect from collusion attacks. The feedback was very valuable for us and will be included into the configurations guidelines we are currently preparing in PRISMACLOUD.

4.5 Infrastructure Certification Pilot (PRISMACLOUD)

The tutorial workshop offered an introduction to the Infrastructure Certification (IA) of PRISMACLOUD. The overall goal of the IA work is to enable the capacity to certify infrastructures, such as virtualized infrastructures in the Cloud in such a way that their security properties can be proven to others without disclosing sensitive data. Therein, this work follows the principles of *Confidentiality-Preserving Security Assurance*.

The core technical contributions presented in the workshop are the Topology Certification tool, called TOPOCERT, its underlying Graph Signature library and a demonstration functionality to prove the separation of machines by geo-separation, which we shall discuss in turn.

Confidentiality-preserving topology certification was first proposed in the work by Groß [22]. The core idea of this proposal is that an Auditor could issue a certificate on the topology on an infrastructure to the Provider, which is usable for subsequent zero-knowledge proofs of knowledge on a wide range of

security properties. This work is founded on earlier research on topology-based security assurance [31,32,33], which analyzes the configuration of infrastructures to determine components, sub-systems and their inter-connectivity and derives a graph representation for a security analysis. Confidentiality-preserving security assurance takes this method one step further in signing the graph representation for further proof protocols.

The graph signing and corresponding zero-knowledge proofs of knowledge are facilitated by a dedicated graph signature library. It realizes the cryptographic protocols between a Signer and a Recipient of graph signatures as well as between a Prover and a Verifier of the corresponding proofs of knowledge. Graph signatures were proposed by Groß [34] as a means to encode graph data structures into an underlying digital signature scheme, such that the components of the graphs, the vertices, edges and labels are still accessible to proofs of knowledge. In a first construction, this is facilitated by employing the Camenisch-Lysyanskaya signature scheme [35] and using techniques first introduced for the efficient encoding of credential attributes [36,37]. The first construction for graph signatures [34] has still a number of short-comings, most notably requiring the signing of one certificate per proof. However, it shows intriguing properties in that the signatures are general in that they could be used to answer a wide range of questions not known at signing time and expressive in that they could encode arbitrary statements from NP languages.

The tutorial workshop included an example application for *geo-location separation* [38]. The idea for that is that the Auditor could certify the physical geo-location of the physical hosts. In this case, we might think of the Auditor as a tamper-proof appliance, which can obtain a secure fix on its current geo-location. In this case, the Auditor could, for instance, label the physical machines of an audited infrastructure with labels denoting the UN countries these machines are located in. The geo-location separation proof protocols executed by the Prover and the Verifier would then convince the Verifier that the machines are in at least k different countries, without disclosing which countries are involved.

5 Advisory Board Feedback

The tutorial workshop ended with a panel of Advisory Board members of the two projects that provided feedback and suggestions for future directions and topics to be addressed by the projects. While in general the panelists appreciated the work presented, they raised a few issues.

One issue mentioned was that a cloudified approach as provided by the CREDENTIAL project relies on one central server, which even if all data are encrypted, still needs to be trusted, as it can monitor all traffic data, is able to derive meta information from them (e.g., it can profile the users' usages of different services - see also [3]) and represents one single point of failure. For users it might not be clear whether this cloudified approach can be fully trusted and it remains a challenge to communicate the trust assumptions to the users. Further research

should also address the questions what is meant by trust and distrust in the whole service solution. For this, the complete process of gaining, losing and re-establishing trust in the service needs to be considered.

Furthermore, it was discussed that Open Source (such as PRISMACLOUD's Archistar) would often be seen as a means for gaining user trust, as the code is openly published and can be reviewed by the users, and that it could be easier for the projects to put their solutions as open source into practice. However, it needs to be considered also that according to the EU General Data Protection Regulation (GDPR) it is not the software producer who is responsible for achieving Data Protection by Design. Pursuant Art. 25 GDPR, the responsibility for the implementation of appropriate technical and organisational measures, which are designed to implement data protection principles, rather lies with the controller. Art. 25 (3) mentions that approved certification mechanisms pursuant to Article 42 may be used as an element to demonstrate compliance of the controller with the Data Protection by Design requirements, and such privacy certification schemes could also be means for gaining or increasing user trust.

Another comment by the Advisory Board members concerned PRISMACLOUD's Smart City parking app. It was pointed out that restricting and framing it as an app for booking parking places for disabled users could mean that users that are installing and using the app could be easily associated as handicapped and thus be discriminated. Hence, the app should have a wider framing and should also provide features that would be useful also for non-disabled users.

Finally, it was discussed and emphasized that in practice "pretty good" usable cryptographic and privacy solutions can already be very helpful for end users. Hence, the projects research should not only try to achieve provably secure solutions, but should also look at practical and usable solutions that provide good enough security for the majority of use cases.

6 Conclusion

Storing, sharing, and processing sensitive data in untrusted cloud environments is the central goal of the H2020 projects CREDENTIAL and PRISMACLOUD. This tutorial paper summarizes given presentations and demonstrations within a workshop at IFIP Summer School 2017 co-organized by both projects. In particular, the workshop aimed at introducing the necessary background knowledge and presenting prototype demonstrations of CREDENTIAL and PRISMACLOUD to a wider academic audience (e.g., students, senior researcher) as well as to participant from the non-academic field (e.g., public data protection agencies).

To this end, we briefly introduced the two projects and described the talks given within the workshop. Furthermore, all demonstration pilots were presented and findings discussed. Valuable feedback was gathered from the advisory-board members to enhance the further projects' development.

References

1. Lorünser, T., Krenn, S., Striecks, C., Länger, T.: Agile Cryptographic Solutions for the Cloud. e&i Elektrotechnik und Informationstechnik (2017)
2. Alaqra, A., Fischer-Hübner, S., Groß, T., Lorünser, T., Slamanig, D.: Signatures for Privacy, Trust and Accountability in the Cloud: Applications and Requirements. In Aspinall, D., Camenisch, J., Hansen, M., Fischer-Hübner, S., Raab, C.D., eds.: Privacy and Identity Management 2015. Volume 476 of IFIP Advances in Information and Communication Technology., Springer (2015) 79–96
3. Karegar, F., Striecks, C., Krenn, S., Hörandner, F., Lorünser, T., Fischer-Hübner, S.: Opportunities and Challenges of CREDENTIAL - Towards a Metadata-Privacy Respecting Identity Provider. In Lehmann, A., Whitehouse, D., Fischer-Hübner, S., Fritsch, L., Raab, C.D., eds.: Privacy and Identity Management 2016. Volume 498 of IFIP Advances in Information and Communication Technology., Springer (2016) 76–91
4. ISO/IEC: ISO/IEC 24760: A Framework for Identity Management – Part 1: Terminology and Concepts, Part 2: Reference Framework and Requirements, Part 3: Practice. http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html (2011–2016)
5. Rannenberg, K., Camenisch, J., Sabouri, A., eds.: Attribute-based Credentials for Trust: Identity in the Information Society. Springer (2015)
6. Hörandner, F., Krenn, S., Migliavacca, A., Thiemer, F., Zwattendorfer, B.: CREDENTIAL: A Framework for Privacy-Preserving Cloud-Based Data Sharing. In: ARES 2016, IEEE Computer Society (2016) 742–749
7. Kostopoulos, A., Sfakianakis, E., Chochliouros, I.P., Pettersson, J.S., Krenn, S., Tesfay, W., Migliavacca, A., Hörandner, F.: Towards the Adoption of Secure Cloud Identity Services. In: ARES 2017, ACM (2017) 90:1–90:7
8. Johnson, R., Molnar, D., Song, D., Wagner, D.: Homomorphic Signature Schemes. In Preneel, B., ed.: CT-RSA 02. Volume 2271 of LNCS., Springer (2002) 244–262
9. Blaze, M., Bleumer, G., Strauss, M.: Divertible Protocols and Atomic Proxy Cryptography. In Nyberg, K., ed.: EUROCRYPT 98. Volume 1403 of LNCS., Springer (1998) 127–144
10. Chaum, D.: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Commun. ACM **24** (1981) 84–88
11. Chaum, D.: Security Without Identification: Transaction Systems to Make Big Brother Obsolete. Commun. ACM **28** (1985) 1030–1044
12. Camenisch, J., Krenn, S., Lehmann, A., Mikkelsen, G.L., Neven, G., Pedersen, M.Ø.: Formal Treatment of Privacy-Enhancing Credential Systems. In Dunkelman, O., Keliher, L., eds.: SAC 2015. Volume 9566 of LNCS., Springer (2015) 3–24
13. Krenn, S., Lorünser, T., Salzer, A., Striecks, C.: Towards Attribute-Based Credentials in the Cloud. In Chow, S.S., Capkun, S., eds.: Cryptology and Network Security – CANS 2017. (2017) (to be published).
14. Lorünser, T., Rodriguez, C., Demirel, D., Fischer-Hübner, S., Groß, T., Länger, T., des Noes, M., Pöhls, H., Rozenberg, B., Slamanig, D.: Towards a New Paradigm for Privacy and Security in Cloud Services. In Cleary, F., Felici, M., eds.: Cyber Security and Privacy. Volume 530 of Communications in Computer and Information Science. Springer International Publishing (2015) 14–25
15. Lorünser, T., Länger, T., Slamanig, D.: Cloud Security and Privacy by Design. In Katsikas, S.K., Sideridis, A.B., eds.: E-Democracy Citizen Rights in the World of the New Computing Paradigms. Volume 570 of Communications in Computer and Information Science. Springer International Publishing (2015) 202–206

16. Lorünser, T., Slamanig, D., Länger, T., Pöhls, H.C.: PRISMACLOUD Tools: A Cryptographic Toolbox for Increasing Security in Cloud Services. In: 11th International Conference on Availability, Reliability and Security, ARES 2016, Salzburg, Austria, August 31 - September 2, 2016, IEEE Computer Society (2016) 733–741
17. Shamir, A.: How to Share a Secret. Communications of the ACM (1979)
18. Blakley, G.R.: Safeguarding cryptographic keys. AFIPS National Computer Conference (1979)
19. Ahn, J.H., Boneh, D., Camenisch, J., Hohenberger, S., Shelat, A., Waters, B.: Computing on Authenticated Data. In Cramer, R., ed.: TCC 2012. Volume 7194 of LNCS., Springer (2012) 1–20
20. Haber, S., Hatano, Y., Honda, Y., Horne, W.G., Miyazaki, K., Sander, T., Tezoku, S., Yao, D.: Efficient Signature Schemes Supporting Redaction, Pseudonymization, and Data Deidentification. In Abe, M., Gligor, V.D., eds.: ASIACCS 08, ACM (2008) 353–362
21. Camenisch, J., Derler, D., Krenn, S., Pöhls, H.C., Samelin, K., Slamanig, D.: Chameleon-Hashes with Ephemeral Trapdoors - And Applications to Invisible Sanitizable Signatures. In Fehr, S., ed.: PKC 2017, Part II. Volume 10175 of LNCS., Springer (2017) 152–182
22. Groß, T.: Efficient certification and zero-knowledge proofs of knowledge on infrastructure topology graphs. In: CCSW 14, ACM (2014) 69–80
23. Derler, D., Slamanig, D.: Fully-anonymous short dynamic group signatures without encryption. IACR Cryptology ePrint Archive **2016** (2016) 154
24. Krenn, S., Lorünser, T., Striecks, C.: Batch-verifiable Secret Sharing with Unconditional Privacy. In: Proceedings of the 3rd International Conference on Information Systems Security and Privacy - Volume 1: ICISSP,, INSTICC, ScitePress (2017) 303–311
25. Demirel, D., Krenn, S., Lorünser, T., Traverso, G.: Efficient and Privacy Preserving Third Party Auditing for a Distributed Storage System. In: 11th International Conference on Availability, Reliability and Security, ARES 2016, Salzburg, Austria, August 31 - September 2, 2016, IEEE Computer Society (2016) 88–97
26. Lorünser, T., Querasser, E., Matyus, T., Peev, M., Wolkerstorfer, J., Hutter, M., Szekely, A., Wimberger, I., Pfaffel-Janser, C., Neppach, A.: Security processor with quantum key distribution. In: Application-Specific Systems, Architectures and Processors, 2008. ASAP 2008. International Conference on, IEEE (2008) 37–42
27. Neppach, A., Pfaffel-Janser, C., Wimberger, I., Lorünser, T., Meyenburg, M., Szekely, A., Wolkerstorfer, J.: Key management of quantum generated keys in IPSEC. In: International Conference on Security and Cryptography SECRYPT 2008 July 26 2008 July 29 2008. SECRYPT 2008 - International Conference on Security and Cryptography, Proceedings, Inst. for Syst. and Technol. of Inf. Control and Commun. (2008) 177–183
28. Happe, A., Krenn, S., Lorünser, T. In: Malicious Clients in Distributed Secret Sharing Based Storage Networks. Springer International Publishing, Cham (2017) 206–214
29. Happe, A., Wohner, F., Lorünser, T.: The Archistar Secret-Sharing Backup Proxy. In: Proceedings of the 12th International Conference on Availability, Reliability and Security. ARES '17, New York, NY, USA, ACM (2017) 88:1—-88:8
30. Lorünser, T., Happe, A., Slamanig, D.: ARCHISTAR: Towards Secure and Robust Cloud Based Data Sharing. In: Cloud Computing Technology and Science (CloudCom), 2015 IEEE 7th International Conference on. (2015) 371–378

31. Bleikertz, S., Groß, T., Schunter, M., Eriksson, K.: Automated Information Flow Analysis of Virtualized Infrastructures. In: ESORICS 11, Springer (2011)
32. Bleikertz, S., Vogel, C., Groß, T.: Cloud Radar: near real-time detection of security failures in dynamic virtualized infrastructures. In: ACSAC 14, ACM (2014) 26–35
33. Bleikertz, S., Vogel, C., Groß, T., Mödersheim, S.: Proactive security analysis of changes in virtualized infrastructures. In: ACSAC 15. (2015)
34. Groß, T.: Signatures and efficient proofs on committed graphs and NP-statements. In: FC 15. (2015) 293–314
35. Camenisch, J., Lysyanskaya, A.: A signature scheme with efficient protocols. In Cimato, S., Galdi, C., Persiano, G., eds.: SCN 2002. Volume 2576 of LNCS., Springer (2003) 268–289
36. Camenisch, J., Groß, T.: Efficient attributes for anonymous credentials. In: ACM CCS 2008, ACM Press (2008) 345–356
37. Camenisch, J., Groß, T.: Efficient attributes for anonymous credentials. TISSEC **15** (2012) 4:1–4:30
38. Groß, T.: Geo-location separation of virtualized systems. Technical Report CS-TR, Newcastle University (2017)