CREDENTIAL: A Framework for Privacy-Preserving Cloud-Based Data Sharing

Felix Hörandner*, Stephan Krenn†, Andrea Migliavacca‡, Florian Thiemer§, and Bernd Zwattendorfer¶
*Graz University of Technology, Graz, Austria
felix.hoerandner@iaik.tugraz.at
†AIT Austrian Institute of Technology GmbH, Vienna, Austria
stephan.krenn@ait.ac.at
‡Lombardia Informatica S.p.A., Milan, Italy
andrea.migliavacca@cnt.lispa.it
§Fraunhofer FOKUS, Berlin, Germany
florian.thiemer@fokus.fraunhofer.de
¶Stiftung Secure Information and Communication Technologies, Graz, Austria
bernd.zwattendorfer@iaik.tugraz.at

***Abstract*—Data sharing – and in particular sharing of identity information – plays a vital role in many online systems. While in closed and trusted systems security and privacy can be managed more easily, secure and privacy-preserving data sharing as well as identity management becomes difficult when the data are moved to publicly available and semi-trusted systems such as public clouds. CREDENTIAL is therefore aiming on the development of a secure and privacy-preserving data sharing and identity management platform which gives stronger security guarantees than existing solutions on the market. The results will be showcased close to market-readiness through pilots from the domains of eHealth, eBusiness, and eGovernment, where security and privacy are crucial. From a technical perspective, the privacy and authenticity guarantees are obtained from sophisticated cryptographic primitives such as proxy re-encryption and redactable signatures.**

***Keywords*-data sharing; identity management; proxy re-encryption;**

I. Introduction

Data sharing plays a vital role in online applications. In particular, in the cloud computing context data storage and sharing gained huge popularity over the past years. Main advantage of such services is that data can be easily accessed and shared anytime with arbitrary clients. If sensitive data such as personal data needs to be shared, these data need special protection. This requirement is especially important in security-sensitive areas of applications such as eHealth, eBusiness, and eGovernment. While insensitive data can be easily shared using the offered software services of various existing cloud providers, the sharing of security-sensitive data becomes more difficult. The reasons are that security and privacy are still one of the main issues of cloud computing [1], [2]. To bypass these issues, some cloud providers already offer services that allow the sharing of data in encrypted format. However, in these cases the provider is usually always in possession of the decryption key [3] and might be able to inspect data. CREDENTIAL is therefore aiming on the development of a secure and privacy-preserving data sharing platform that puts the user under full control of her decryption key while still being able to share personal data in a secure and privacy-preserving manner over systems with limited trust such as public clouds.

One special case of data sharing is identity management (IdM), where personal and identity information is shared during authentication processes. While at the beginning identity management was mainly limited to inter-organizational approaches within a single domain, over the time more sophisticated federated approaches emerged, allowing the identification and authentication across organizational domains or even national borders. Typical examples enabling identity federation across domains are the Security Assertion Markup Language (SAML) [4], OpenID Connect [5], or WS-Federation [6]. The EU co-funded projects STORK (Secure Identities Across Borders Linked) [7] and STORK 2.0 paved the way for secure identity federation and authentication across national borders in Europe. Currently, the regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS regulation) [8], which entered into force in 2014, and its supporting documents set both the legal and technical basis for the cross-border acceptance of electronic identities (eIDs) within the EU boundaries.

From an architectural perspective, several identity management models have already emerged over time [9], [10], [11]. Basically, all these models follow a similar conceptual approach involving three key actors: user, service provider (SP), identity provider (IdP) [12]. Typically, in an identity management scenario, a *user* wants to access a protected resource at a *service provider*. To facilitate access and to lower the efforts for the service provider, usually an *identity provider* takes over and handles the identification and authentication process of the user for the service provider. Thereby, the user identifies and authenticates at the identity provider and after successful authentication the identity provider transfers relevant identity and authentication information to the service provider for access decision making. The data transfer between identity provider and service provider is usually carried out

using well-established identity protocols such as SAML or OpenID Connect. All these actors share a common trust relationship.

Due to the increasing take up of cloud computing because of its easy data sharing capabilities in various – also security-sensitive – areas, secure identity management gets more and more importance in the cloud domain too. Identity management systems in the cloud – often also referred to as Identity Management as a Service (IdMaaS) – can benefit from several advantages the cloud itself can offer. For instance, cloud computing provides higher scalability, elasticity, and cost savings, since no in-house infrastructure needs to be hosted and maintained [13]. Similar to traditional identity management systems, several cloud identity management models have already evolved over the past years. All have their advantages and disadvantages as shown in [14]. Nevertheless, all these cloud identity management models lack in privacy when deployed in a public cloud. Privacy is one of the main issues of cloud computing [1], [2], in particular when taking a public cloud as underlying deployment model such as for an identity management systems. While in traditional identity management models the operator of the identity management system is usually assumed to be fully trusted with respect to privacy, this assumption does not hold anymore when operating the identity management system in a public cloud. In fact, public cloud providers are able to inspect arbitrary data (e.g. identity data) if the stored data are not encrypted. Such cloud providers are considered to be semi-trusted and acting honest-but-curious [15]. Even if the cloud provider works correctly, it might be curious in inspecting stored or processed data.

To bypass the privacy issue in existing data sharing platforms and in particular for identity management systems in public clouds, CREDENTIAL proposes a new approach where identity data is treated in encrypted format only when stored in or transferred to public clouds. Thereby, the cloud provider does not get access to any sensitive data. In addition, CREDENTIAL will enhance existing cloud data sharing and identity management solutions by supporting secure and hardware-based two-factor authentication mechanisms.

II. About the Project

The overall vision of CREDENTIAL is to develop and showcase innovative cloud-based services for storing, managing, and sharing identity information or other personal data with a demonstrably higher level of security than current existing solutions. CREDENTIAL will thereby rely on novel cryptographic mechanisms such as proxy re-encryption [16] or redactable signatures [17] to be applied in cloud identity management scenarios. Furthermore, CREDENTIAL will improve current insecure password-based authentication schemes by adapting strong hardware-based multi-factor authentication mechanisms in cloud set-ups. In the following, we describe the basic approach and underlying principles of CREDENTIAL.

A. Objectives

The CREDENTIAL consortium developed five objectives to be addressed during the project phase to meet the overall CREDENTIAL vision of privacy-preserving cloud-based identity management solutions. Briefly, the five objectives are:

- Adapt novel cryptographic mechanisms to securely store and share (identity) data in the cloud
- Enhance existing cloud authentication mechanisms by strong hardware-based multi-factor mechanisms
- Design and develop a user-friendly and portable cloud identity and data management architecture
- Create secure and portable implementations
- Evaluate and pilot the results in pre-production environments in different domains

The use of novel cryptographic mechanisms will protect confidentiality, integrity, and authenticity of data in the cloud. This will also preserve user's privacy by applying mechanisms to efficiently re-encrypt and share encrypted data as well as providing selective disclosure features. Insecure password-based authentication mechanisms will be substituted by strong hardware-based multi-factor mechanisms. The developed data sharing platform and identity provider will follow state-of-the-art security and privacy by design principles. By taking up well-established standards and protocols, CREDENTIAL components will be easy to integrate into existing solutions requiring minimum modifications only. Finally, CREDENTIAL results will be intensively tested and evaluated in near operational pilots in three different domains (e-Government, e-Health, e-Business).

B. Base Technologies

The use of proxy re-encryption and redactable signatures allows to mitigate privacy obstacles for data sharing and identity management systems in public cloud deployments. Proxy re-encryption protects the confidentiality of personal data and enables secure end-to-end encrypted data sharing. Redactable signatures ensure data integrity and authenticity by providing selective disclosure mechanisms at the same time. In the following, amongst others assessed within CREDENTIAL, the two base technologies of CREDENTIAL are briefly described.

Proxy Re-Encryption: A proxy re-encryption (PRE) scheme [16] is a public key encryption scheme that allows a semi-trusted proxy to transform a ciphertext c_A created with a public key pk_A of party A into another ciphertext c_B of party B. The transformed ciphertext c_B can be decrypted by party B using her private key sk_B. The transformation of ciphertext c_A into ciphertext c_B is carried out using a re-encryption key $rk_{A\rightarrow B}$, which can be created out of sk_A and pk_B. During the transformation, the proxy neither gets access to the plaintext nor to the decryption keys.

Redactable Signatures: A redactable signature (RS) scheme [17] allows the removal of parts of a signed message by any party without invalidating the original signature. For achieving that, access to the signers

secret key is not required. In other words, parts of a signed message can be blacked out without invalidating the signature.

C. Basic Architecture

The basic architecture of CREDENTIAL follows the common conceptual approach for identity management systems involving three key actors: user, service provider (SP), and identity provider (IdP) [12]. If not concerned with identity management but sharing of arbitrary potentially sensitive data, the SP can be thought of as the data receiver, and the IdP can be thought of as the CREDENTIAL data sharing platform (or *wallet*).

Figure 1 illustrates the basic architecture involving all key stakeholders. All stakeholders rely on CREDENTIAL technology and thus are CREDENTIAL-enabled. In the following, we briefly describe a simple identification and authentication process using CREDENTIAL.

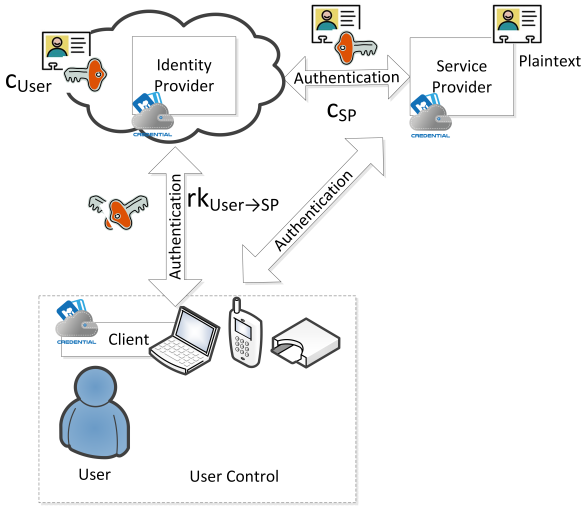

Figure 1. CREDENTIAL Basic Architecture

For simplification, as a prerequisite we assume that the user has already stored personal identity data at the identity provider in the cloud. In the CREDENTIAL scenario, these personal data are not stored in plain but rather encrypted. To allow the user to stay in maximum control of her data, the data are stored encrypted for the user only (by using her private key pk_{User}). This means that only the user herself is able to decrypt the data using her decryption key sk_{User}. According to Figure 1, the encrypted user data is denoted as c_{User}.

If the user wants to access a protected resource at the service provider, the user is delegated to the identity provider to carry out identification and authentication. For authentication, the user relies on strong CREDENTIAL-enabled hardware-based two-factor authentication mechanism. During the authentication process, the user also generates a re-encryption key $rk_{User \rightarrow SP}$ out of sk_{User} and pk_{SP}, which is further provided to the CREDENTIAL-enabled identity provider in the cloud. The CREDENTIAL-enabled identity provider takes the re-encryption key and re-encrypts c_{User} for the service provider resulting in c_{SP}. After that, the re-encrypted data c_{SP} is transferred to the service provider using standardized identity protocols such as SAML or OpenID Connect. Since the user data was re-encrypted for the service provider, the CREDENTIAL-enabled service provider is now able to decrypt c_{SP} using its private key sk_{SP}. The resulting plaintext can be used for granting or denying access to the protected resource.

Depending on the encrypted data structures, the described process flow can be enhanced by selective disclosure features using redactable signatures. Thereby, the user is able to redact certain parts of her identity and thus only a minimum data set might be transferred to the service provider, while still being able to ensure integrity and authenticity of that data set.

Compared to traditional identity management systems and identity management systems in the cloud CREDENTIAL mitigates the privacy risk introduced by honest-but-curious cloud providers. By the use of proxy re-encryption and redactable signatures, personal identity data are treated in encrypted format only, the user stays under full control of her data, and only selective identity data can be disclosed.

D. Deployment Options

According to the CREDENTIAL objectives, the CREDENTIAL consortium wants to create secure and portable implementations. To stay flexible in terms of portability and deployment, CREDENTIAL defined a set of generic actors and components that can be arbitrarily arranged together and applied in different scenarios. This flexibility allows for different implementation and deployment options, enabling the set-up of new cloud identity management systems or just enhancing existing ones to increase privacy.

CREDENTIAL will provide two different deployment options:

1) CREDENTIAL will design and implement individual software libraries that can be easily integrated into existing identity management systems and products. Thereby, existing products can be CREDENTIAL-enabled and the privacy features of these products can be increased.
2) CREDENTIAL will design and implement a comprehensive cloud identity management system that can be easily deployed in and ported between different cloud platforms. This comprehensive solution combines different software components to support the pilot evaluation. However, the comprehensive solution will be generic enough to be applied in different scenarios beyond the ones the described in the following sections.

III. Pilots

As mentioned earlier, the results and findings of CREDENTIAL will be showcased and demonstrated by means of pilots from the domains of eHealth, eBusiness, and eGovernment. In the following, we give a short introduction to those pilots.

A. eHealth Pilot

The e-Health pilot covers sharing of medical data between patients and practitioners. The pilot integrates in the treatment of patients who are suffering diabetes 1 and 2. The following scenario covers the definition of therapy goals and continuous tracking of progress towards these goals. It is the baseline storyboard for the CREDENTIAL eHealth proof-of-concept which covers the initialization of the covered care episode and continuously repeated activities. The practitioner will collect core vital data (height, weight, blood pressure, ...) from the patient and stores them encrypted with CREDENTIAL technology in the patient's Personal Health Record (PHR). The patient can grant access rights to the practitioners who are involved in her treatment which allows them to read data from the PHR and to share information with the patient. The patient will be equipped with a glucometer, continuously measures her medical data and publish the data automatically via her smartphone into the PHR.

According to the German S3 Guideline for diabetes treatment [18], the patient and her doctor shall define and document individual therapy goals for the patient. These goals shall be measurable and consider the specific situation of the patient. Therapy goals should be oriented towards best clinical practice and evidence. In particular therapy goals should be defined for the following parameters:

Data collected by the patient:

1) Lifestyle (e.g. average steps per day)
2) Blood sugar
3) Body weight
4) Blood pressure

Data collected by the physician:

1) HbA1c
2) LDL Cholesterol
3) Abdominal girth
4) Creatinin
5) Microalbumin

The CREDENTIAL e-Health use case will focus on providing data to patient centric apps which allow the patient and her care providers to track therapy progress in accordance to the defined therapy goals. For this the agreed care goals on the parameters listed above will be electronically captured and stored as a document in a secure data store protected by proxy-re-encryption mechanisms. Access to this document can be granted to other actors by either the patient or the family doctor.

Diabetes patients may use various homecare devices for tracking their blood sugar level, weight and blood pressure. In addition more lifestyle oriented devices such as pedometers may be utilized for tracking physical activity. Continua Health Alliance [19] and other international initiatives for integrating personal health devices developed various reference architectures for connecting personal health and lifestyle devices to health records and data analysis services. An evolution of the Continua reference architecture that matches best with recent developments

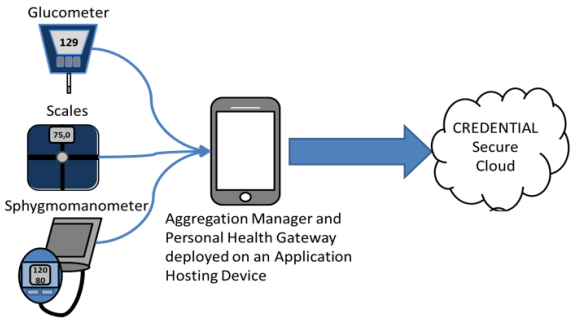

Figure 2. Reference architecture for the e-Health pilot

in mHealth is the Danish Reference Architecture for Collecting Health Data from Citizens [20] which explicitly considers multi-step processing of monitored data and therefore allows for an easy integration of gateways and security appliances. This approach best matches the CREDENTIAL architectural presettings because it defines clear integration points for the CREDENTIAL security services (e.g. deploying the proxy re-encryption service within a WAN device).

In the state of the art, medical data stored in a PHR is protected by a record key r. The record key is the shared secret among all participants who are allowed to access the PHR. If a participant is allowed to access the PHR the record key has to be encrypted for her. This is done by the patient and can be achieved when the patient visits her practitioner and gives consent that she is currently in a treatment relationship with the practitioner and that she is allowed to access her PHR. In this process the record key r_{prac} is created with the practitioners public key and signed by the patient. The PHR can verify the consent given by the patient and registers r_{prac} in the key set of the patient's record. Now the practitioner is able to read data from the patient's record.

With the introduction of proxy-re-encryption mechanisms the record key r is not encrypted for every participant but only for the patient herself. The individual **process steps** in order to share medical data are described in the following lines:

1) **Request Access Rights:** The practitioner sends a Access Rights Request to the patient. The patient verifies the request and obtains the public key pk_{prac} from the practitioner. The key can be provided in the request or the patient request the key through a Public Key Infrastructure (PKI).
2) **Grant Access Rights:** The patient creates a re-encryption key $rk_{patient \rightarrow prac}$ by using her private key $sk_{patient}$ and the practitioner's public key pk_{pract}. She signs the re-encryption key and sends it to the PHR. The PHR is able to verify the originator of the re-encryption key and thus access to the PHR is granted for the practitioner. Access rights are registered in the access control system of the PHR.
3) **Read Data:** The practitioner requests a data set from the PHR. The access control system checks

for given access rights and for a re-encryption key $rk_{patient \rightarrow prac}$. If the access rights are evaluated successfully and a re-encryption key was found the PHR re-encrypts the record key r with $rk_{patient \rightarrow prac}$ and obtains r_{prac}. Then, r_{prac} and the requested resource is returned to the practitioner. The practitioner decrypts the record key with her own private key and decrypts the requested record with the record key r.

The use of proxy re-encryption **adds value for the patient** in form of transparency and usability.

Usability: If the record key r has to be changed the patient has to create for each participant a new encrypted record key. With the use of proxy-re-encryption the PHR can simply re-encrypt the record key without any activity performed by the patient.

Transparency: If a practitioner receives new key material the patient does not have to generate a new re-encryption key. The practitioner can simply create a re-encryption key from her old key material to the new one.

B. eBusiness Pilot

This pilot covers the use case of email delegation.

Multiple scenarios motivate the recipients' need to delegate their emails to other persons. In the following we present two scenarios. Firstly, even during vacation, a person might receive official communication that requires a reaction in a limited timeframe. In this scenario, it would be beneficial if another person would be able to read those official emails and to induce a reaction, for example by contacting the original recipient via other means of communication. Secondly, businesses also face communication problems when employees leave for vacation. Again, it is important that another employee is able to act as substitute by answering incoming emails.

However, encryption represents a challenge when delegating emails. As emails often contain senstitive information, such as official documents or business secrets, the end-to-end confidentiality of the content has to be ensured with encryption. Therefore, the sender encrypts outgoing emails for one or multiple recipients. Consequently, these mails can not directly be delivered to another receiver who was authorized by a specified receiver to act as a substitute.

Currently, two approaches allow to delegate emails that are protected by traditional encryption, as illustrated in figure 3. Firstly, the sender encrypts the email for the original receiver (OR) and transmits the resulting in ciphertext C_{OR} via the mail server. This receiver then decrypts her email and encrypts it again for another receiver, giving the ciphertext C_{DR}. The mail server forwards this email to the delegated recipient (DR), who is finally able to decrypt and therefore respond to the email. Secondly, the original recipient could hand her private key sk_{OR} the delegated recipient and advises the mail server to automatically forward her mails to this substitute. Consequently, the email encrypted by the sender for the original receiver is forwarded to the delegated recipient, who uses the original receiver's private key sk_{OR} to decrypt the email.

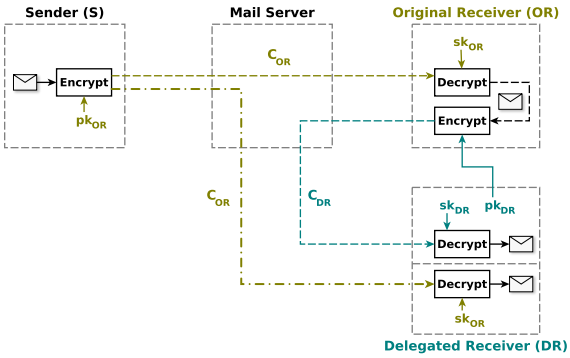

Figure 3. Email Delegation with Traditional Encryption. sk_X and pk_X denote the private key and public key of entity X, respectively. C_X represents a ciphertext encrypted for X.

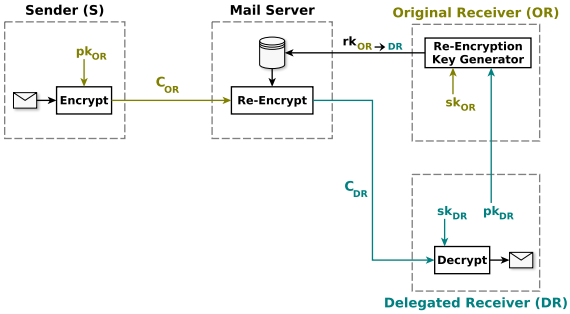

Figure 4. Email Delegation with Credential Technologies. sk_X and pk_X denote the private key and public key of entity X, respectively. C_X represents a ciphertext encrypted for X. $rk_{X \rightarrow Y}$ is a re-encryption key from X to Y.

However, two issues remain in the before described approaches with traditional encryption, namely availability and trust. Those issues severely limit the applicability of these approaches in a real-world deployment. Firstly, if the original recipient is not available, for example because she is on vacation, she is also not able to decrypt and encrypt emails that can be passed on to her substitute. Secondly, users do not want to expose their private key material to environments or people they do not completely trust.

By applying CREDENTIAL technology, email delegation can be implemented, which solves the issues of approaches that use traditional encryption. Proxy re-encryption allows a recipient (delegator) to delegate decryption rights to another entity (delegatee) by generating a re-encryption key. A proxy then uses this re-encryption key to translate ciphertext for the delegator to ciphertext for the delegatee. Also, as the proxy does not learn the underlying plaintext in any intermediate step of the re-encryption process, the ciphertexts confidentiality is ensured.

The individual process steps illustrated in figure 4 are described in the following lines:

1) **Activate:** Before leaving for vacation, the original recipient generates a re-encryption key $rk_{OR \rightarrow DR}$ that can be used to transform her ciphertext for a delegated recipient. For this operation, the original

recipient requires her own private key sk_{OR} as well as the delegatee's public key pk_{DR}. Then, the original recipient activates the delegation, by handing this re-encryption key to the mail server. This concludes the one-time setup phase.

2) **Send:** A sender encrypts the email addressed to the original recipient with the recipient's public key pk_{OR}. The resulting ciphertext C_{OR} is then transmitted to the mail server.
3) **Forward:** Upon receipt of an incoming email, the mail server checks whether the addressee activated the delegation of her emails. If so, the server retrieves the deposited re-encryption key $rk_{OR \to DR}$. Subsequently, the mail server acts as proxy by using this key to translate the incoming encrypted email C_{OR} to a re-encrypted email C_{DR} for the delegatee. This re-encrypted email is then sent to the delegated receiver.
4) **Receive:** Finally, the delegatee receives the re-encrypted email C_{DR}. With her private key sk_{DR}, the delegated receiver is able to decrypt the email's contents.

The use of proxy re-encryption adds value for the users, as it not only solves the trust and availability issues of traditional re-encryption but also equips the receiver with more control over her granted delegation.

Availability: After generating the re-encryption key, the delegator is not involved in the delegation process anymore. Therefore, the delegator also does not have to be available at the time an encrypted email for her is re-encrypted for the delegatee.

Trust: The delegator does not have to reveal her private key to any external entity or environment. This private key is only required to required to generate a re-encryption key, which can be done locally by the delegator.

Control: The delegator has intuitive control over the delegation. Only this delegator is able to enable re-encryption by generating a re-encryption key from her private key material and distributing the re-encryption to the mail server. Also, the delegation can be suspended by advising the mail server to delete the re-encryption key, for example when returning from vacation.

Additionally, the solution applying CREDENTIAL technology presents added value for service providers. Email solutions with traditional encryption suffer from trust and availability issues which prevent the adoption of delegation functionality. By using proxy re-encryption, service providers not only offer end-to-end confidentiality, but also the ability to securely delegate mails to other users, which is a highly desired advantage in multiple scenarios. Therefore, this distinguishes CREDENTIAL-enabled service providers from traditional solutions by providing a considerable competitive advantage.

In future work, we will concentrate on conditional proxy re-encryption (C-PRE) to limit the delegated decryption rights. With C-PRE [21], messages are tagged with a condition during encryption. A re-encryption key is only able to re-encrypt such a ciphertext if it satisfies the ciphertext's condition. Furthermore, in advanced C-PRE schemes with fine-grained policy [22] it is possible to define a policy over multiple conditions that has to be fulfilled in order to perform the re-encryption. Those types of proxy re-encryption could be used in the email delegation use case, to precisely control the delegated decryption rights. For example, senders could tag their messages with keywords, such as `urgent` or `marketing`, and the current month, like `April 2016`. Then, the original recipient generates a re-encryption key, that allows to translate encrypted mails for her delegatee, only if the message was sent during her vacation `Mai 2016` and it is `urgent`. Therefore, the original recipient would enjoy fine-grained over her delegation. Initial considerations to use such conditional proxy re-encryption schemes seem promising.

C. eGovernment Pilot

eGovernment consists of the introduction of ICT technologies into public administrations for providing services in a more innovative and usable way. The level of interaction depends on different involved actors. This could be between citizens and government, or between different public authorities, or between government and the business/industrial world.

One of the main goals of eGovernment is to provide to the citizen a portfolio of public services with high accessibility, cost-effectiveness, efficiency, transparency, and security. Many of these public services require a digital identity (or eID) of the citizen to perform personal identification (authentication) and access rights assessment (authorisation).

One of the scenarios considered in CREDENTIAL is the following: a citizen of country A living in country B needs to interact with some public authority in country B, e.g., in order to pay her taxes.

1) **Authentication:** In a first step, the user would use her national eID card of country A to authenticate herself to the tax portal of country B; this cross-border authentication is performed using STORK [7] or eIDAS [8] technology.
2) **Data sharing:** The CREDENTIAL platform is now used to host authentic personal data that goes beyond the data that is stored on the national eID card. For instance, such data might include pay slips or certificates of registration. The user can now grant the tax authority of country B access to this data by storing a re-encryption key for the tax authority.

A high-level message flow of the use case is depicted in Figure 5.

In this example, the user already wants to file her tax declaration before all official payroll statements from the employer have already been uploaded to the CREDENTIAL wallet. Therefore, the tax authority can file a data request at the wallet in order to be notified once all necessary documents are in place. Now, the employer uses

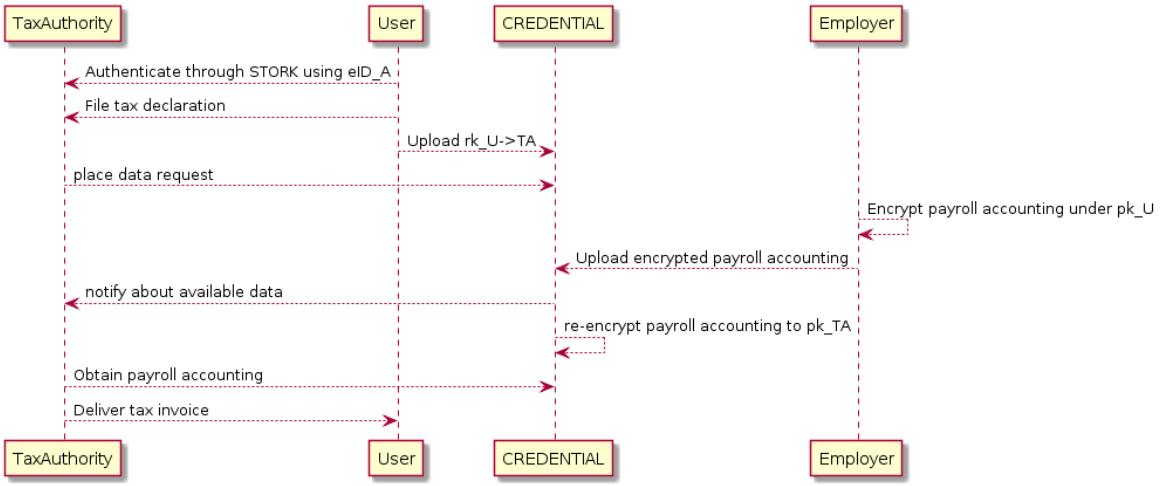

Figure 5. Data flow of the eGovernment use case.

the public key pk_U of the user to encrypt the payroll accountings and uploads them to the server. Once they have been received, they are re-encrypted to the public key of the tax authority using $rk_{U \to TA}$ filed by the user. Finally, the tax authority gets notified about the availability of the documents, and can issue the final tax invoice to the user, directly or again through the CREDENTIAL wallet. Note that in this scenario, the user does not need to be online any more after filing her tax declaration.

In another manifestation of the eGovernment use case, a user might be interested in granting a public authority access to only specific parts of a document. For instance, for receiving family allowance, it might be necessary to prove to the authority that a child is indeed studying at a university—but it might not be necessary to reveal the concrete grades or attended courses. In this case, the university could sign a certificate of studies using a redactable signature scheme, and upload it to the CREDENTIAL wallet, again encrypted under pk_U. Also, the user would again generate a re-encryption key $rk_{U \to A}$ for the authority. However, now instead of re-encrypting and purely forwarding the ciphertext to the authority, the CREDENTIAL wallet would now first redact the requested parts of the document. By only revealing the necessary information to the authority, the privacy of the user would be respected, while the authority would still be assured about the authenticity of the received data.

In summary, the eGovernment use case provides the following **added value to users and authorities**:

Usability: By granting all involved stakeholders access to the CREDENTIAL wallet, the user does not need to be online in all steps any more. Also, as access rights can also be granted to documents that will only be added in the future by storing the respective re-encryption keys, the timings of certain processes can be made more flexible.

Privacy+Authenticity: The combination of proxy cryptography and redactable signatures allows to enhance the privacy of users, while still guaranteeing the authenticity of (the revealed parts of) documents to the receiver.

Mobility: By having a central repository for storing, re-encrypting, and redacting official documents, the user can conduct transactions with public authorities from any device, independent of her location. Yet, the confidentiality of the stored data is protected by strong cryptographic mechanisms, so that the cloud provider cannot learn the content of the encrypted documents.

IV. Conclusion

Migrating services and applications into the cloud comes with the cost of privacy and security issues. In contrast, by using cloud services users and service providers can benefit from several advantages. We showed how pilots in three different domains can integrate proxy-re-encryption and redactable signature technology in their workflows so that they can profit from cloud advantages by still maintaining their security and privacy needs.

In the e-Health domain we showed how existing solutions for storing sensitive medical data can support practitioner and patients in the treatment of there diseases by using proxy-re-encryption technology.

A proposal for enhancing encrypted mail was made by highlighting how proxy-re-encryption defines new use cases that are not feasible with current state-of-the-art technology because they would break with security, privacy and usability needs.

With the e-Government pilot we are able to show how proxy-re-encryption can be integrated in traditional identity management systems. With the support of redactable signatures the usability and mobility of the user is increased.

References

[1] S. Pearson and A. Benameur, “Privacy, Security and Trust Issues Arising from Cloud Computing,” in *IEEE CloudCom*, Nov. 2010, pp. 693–702.

[2] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592, Mar. 2012.

[3] Institut, Frauenhofer, "SIT Technical Reports - On the Security of Cloud Storage Services," 2012. [Online]. Available: https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Cloud-Storage-Security_a4.pdf

[4] S. Cantor, J. Kemp, R. Philpott, and E. Maler, "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2 .0 - Errata Composite," OASIS, Tech. Rep., 2009.

[5] N. Sakimura, J. Bradley, M. Jones, B. de Medeiros, and C. Mortimore, "OpenID Connect Core 1.0," OpenID, Tech. Rep., Apr. 2014. [Online]. Available: http://openid.net/specs/openid-connect-core-1_0.html

[6] M. Goodner and A. Nadalin, "Web Services Federation Language (WS-Federation) Version 1.2," OASIS, Tech. Rep., 2009.

[7] H. Leitold and B. Zwattendorfer, "STORK: Architecture, Implementation and Pilots," in *ISSE 2010 Securing Electronic Business Processes*, 2011, pp. 1–11.

[8] European Commission, "Regulation (EU) No 910/2014 of the European Parliament and the council on electronic identification and trust services for electronic transactions in the internal market," pp. 1–42, 2014. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910\&from=EN

[9] M. Bauer, M. Meints, and M. Hansen, "D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems," FIDIS, Tech. Rep., 2005.

[10] A. Jø sang, M. Al Zomai, and S. Suriadi, "Usability and privacy in identity management architectures," in *ACSW '07 Proceedings of the fifth Australasian symposium on ACSW frontiers*, L. Brankovic, P. Coddington, J. F. Roddick, C. Steketee, J. R. Warren, and A. Wendelborn, Eds. Australian Computer Society, Inc. Darlinghurst, Australia, 2007, pp. 143–152.

[11] J. Palfrey and U. Gasser, "Digital Identity Interoperability and eInnovation," *Berkman Publication Series*, pp. 1–49, 2007.

[12] E. Bertino and K. Takahashi, *Identity Management: Concepts, Technologies, and Systems*. Artech House, 2011.

[13] R. Bohn, J. Messina, F. Liu, and J. Tong, "NIST Cloud Computing Reference Architecture," *2011 IEEE World Congress*, 2011. [Online]. Available: http://www.computer.org/portal/web/csdl/doi/10.1109/SERVICES.2011.105

[14] B. Zwattendorfer, T. Zefferer, and K. Stranacher, "An Overview of Cloud Identity Management-Models," in *10th International Conference on Web Information Systems and Technologies (WEBIST)*. SCITEPRESS Digital Library, 2014, pp. 82–92.

[15] Y. Chen and R. Sion, "On Securing Untrusted Clouds with Cryptography," in *Proceedings of the 9th annual ACM workshop on Privacy in the electronic society*, 2010, pp. 109–114.

[16] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *In EUROCRYPT*. Springer-Verlag, 1998, pp. 127–144.

[17] R. Johnson, D. Molnar, D. Song, and D. Wagner, "Homomorphic Signature Schemes," in *Topics in Cryptology - CT-RSA 2002*, vol. 28913, 2002, pp. 244–262.

[18] "German s3 guideline for diabetes type-1 and type-2 treatment," http://www.deutsche-diabetes-gesellschaft.de/fileadmin/Redakteur/Leitlinien/Evidenzbasierte_Leitlinien/NVL_Therapie_DM2_lang_Aug_13_geae_Nov_2014.pdf, accessed: 2016-04-29.

[19] The Continua Alliance. [Online]. Available: http://www.continuaalliance.org/

[20] "Reference architecture for collecting health data from citizens." [Online]. Available: http://sundhedsdatastyrelsen.dk/da/rammer-og-retningslinjer/om-referencearkitektur-og-standarder/referencearkitekturer

[21] J. Weng, R. H. Deng, X. Ding, C. Chu, and J. Lai, "Conditional proxy re-encryption secure against chosen-ciphertext attack," in *Proceedings of the 2009 ACM Symposium on Information, Computer and Communications Security, ASIACCS 2009*, 2009, pp. 322–332.

[22] L. Fang, W. Susilo, C. Ge, and J. Wang, "Interactive conditional proxy re-encryption with fine grain policy," *Journal of Systems and Software*, vol. 84, no. 12, 2011.