13

Secure and Privacy-Preserving Identity and Access Management in CREDENTIAL

Peter Hamm[1], Stephan Krenn[2] and John Sören Pettersson[3]

[1]Goethe University Frankfurt, Germany
[2]AIT Austrian Institute of Technology GmbH, Austria
[3]Karlstad University, Sweden
E-mail: peter.hamm@m-chair.de; stephan.krenn@ait.ac.at;
john_soren.pettersson@kau.se

In an increasingly interconnected world, establishing trust between end users and service providers with regards to privacy and data protection is becoming increasingly important. Consequently, CREDENTIAL, funded under the European Union's H2020 framework programme, was dedicated to the development of a cloud-based service for identity provisioning and data sharing. The system aimed at offering both high confidentiality and privacy guarantees to the data owner, and high authenticity guarantees to the receiver. This was achieved by integrating advanced cryptographic mechanisms into standardized authentication protocols. The developed solutions were tested in pilots from three critical sectors, which proved that high user convenience, strong security, and practical efficiency can be achieved at the same time through a single system.

13.1 Introduction

Over the last decade, the availability and use of the Internet as well as the demand for digital services have massively increased. This demand has already reached critical and high assurance domains like governmental services, healthcare, or business correspondence. Those domains have particularly high requirements concerning privacy and security, as they are processing highly sensitive user data, and thus they need to be harnessed with various mechanisms for securing access.

Handling all the different authentication and authorization mechanisms requires user-friendly support provided by identity management (IdM) systems. However, such systems have recently experienced a paradigm shift themselves. While classical IdM systems used to be operated locally within organizations as custom-tailored solutions, nowadays identity and access management are often provided "as a service" by major cloud providers from different sectors such as search engines, social networks, or online retailers. Connected services can leverage the user identity base of such companies for authentication or identification of users.

In addition, many of these service providers do not only allow users to authenticate them towards a variety of cloud services, but also enable them to store arbitrary other, potentially sensitive, data on their premises, and share this data with other users in a flexible way, while giving the owner full control over who can access their data.

Unfortunately, virtually all existing solutions suffer from at least one of the following two drawbacks. Firstly, upon authentication a service provider (a.k.a. relying party) is only ensured by the IdP service that a user's attributes (e.g., name, birth data, etc.) are correct, but it does not receive any formal authenticity guarantees that these attributes were indeed extracted from, e.g., a governmentally-issued certificate. That is, the relying party needs to make assumptions about the trustworthiness of the IdP, which may not be desired in case of high-security domains. Secondly, users often do not get formal end-to-end confidentiality guarantees in the sense that the data storage and IdP do not have access to their data. In particular, for the IdP aspect this is technically necessary as otherwise the IdP could not vouch for the correctness of the claimed attributes. However, this introduces severe risks, e.g., in case of security incidents such as data leaks.

13.1.1 CREDENTIAL Ambition

The main ambition of the CREDENTIAL project was to overcome these limitations by designing and implementing a cloud-based identity and access management system which upholds privacy and data confidentiality at all times while simultaneously giving the relying party high and formal authenticity guarantees on the received data.

More precisely, the system aims to put users into full control over their data. They can share digitally signed data with relying parties in its entirety or in parts, thereby realizing the minimum disclosure principle.

Furthermore, all exchanged data is encrypted end-to-end, without the cloud-service provider being able to access the data. By being able to plausibly deny having access to the data, the service provider is able to build his business strategy around this advantageous security property. At the same time, the relying parties is guaranteed that the data they received from the identity provider is authentic and was indeed issues, e.g., by a public authority, thereby reducing the necessary amount of trust into the IdP with regards to the correctness of the provided data. This also holds true if only parts of a signed document are shared with the relying party.

13.2 Cryptographic Background

Before being able to describe how CREDENTIAL achieved its main ambition, we will briefly recap the necessary cryptographic primitives on a high level. For more detailed background information, we refer to the original literature.

13.2.1 Proxy Re-encryption

In conventional public key encryption schemes, a user Alice holds a public key pk_A and a corresponding secret key sk_A. Now, when another user Bob wants to send a message to Alice, he encrypts a message m under pk_A, and sends the resulting ciphertext c_A to Alice, who then can decrypt the ciphertext using her secret key. Unfortunately, this technique is not practical for data sharing applications: assume that Alice stores her confidential data in an encrypted form on a cloud platform. Now, in order to share the data with Bob and Charlie, she would need to download the ciphertexts, decrypt them locally, and encrypt them again under the right public keys, say pk_B and pk_C.

This challenge is overcome by proxy re-encryption, originally introduced by Blaze et al. [3], and later refined by Ateniese et al. [1] and Chow [6], among others. Using those schemes, Alice can use her secret key and a receiver's public key to compute a re-encryption key $rk_{A \to B}$. Using this key, a proxy can translate a ciphertext c_A encrypted for Alice into a ciphertext c_B for Bob, without learning any information about the message contained in the ciphertext beyond what is already revealed by the ciphertext itself (e.g., the size of the message).

Within CREDENTIAL, proxy re-encryption is used to enable end-to-end encrypted data sharing without negatively affecting usability or efficiency on the end-user side, as the computation is outsourced to the CREDENTIAL Wallet.

13.2.2 Redactable Signatures

Traditional digital signature schemes allow the receiver of a signed message to verify the authenticity of the document. That is, a signer first uses his secret signing key *sk* to sign a message *m*, obtaining a signature *sig*. Now, a receiver, having access to *m*, *sig*, and the signer's public verification key *vk* can verify that the message has not been altered in any way since the signature has been generated. In particular, any editing or deletion of message parts would be detected, as the verification process would fail.

While this is a very useful primitive in many applications, it is often too restrictive when developing privacy-preserving applications. For instance, when aiming for selective disclosure in authentication processes, the holder of a signed electronic identity document is not able to blank out the information he does not want to reveal to the receiver.

Redactable signatures [16] solve this problem. In such schemes, the signer can label blocks of a message *m* as admissible when creating a signature *sig*. Now, any party having access to *m* and *sig* can redact admissible message blocks and update the signature to a signature that will still verify for the altered message, without requiring any secret key material. However, no other modifications than redacting admissible blocks (such as deletion of other blocks or parts of blocks, or arbitrary updates to the messages) can be performed without breaking the validity of the signature. Thus, the receiving party can rest assured that the received data blocks are authentic and have been signed by the holder of the secret key.

13.3 Solution Overview

To realize the project's ambition, the project consortium developed a cloud-based platform called the CREDENTIAL Wallet. Users can access and manage their account using a mobile application, the CREDENTIAL App.

In the following, we describe the main steps performed by the actors involved in the CREDENTIAL authentication flow:

- A user obtains a digital certificate on his attributes from an issuer, which could be a public authority attesting the user's birth date or nationality, but also a service provider signing the expiration date of a subscription. This is done by letting the issuer sign the user's attributes using a redactable signature scheme.
- The user then encrypts the received certificate using his public encryption key and uploads this data to the CREDENTIAL Wallet.

- When a relying party – either another user or a service provider – requests access to the user's data for the first time, the user computes a re-encryption key from his public key to that of the relying party. To do so, the user employs the CREDENTIAL App, which fetches the receiver's public key, while the user's secret key is locally stored. The App then sends the re-encryption key to the CREDENTIAL Wallet, where it is stored in a dedicated key storage component. For subsequent access requests from the same relying party no fresh key material needs to be generated until a potential key update.
- Now, when the relying party accesses the data, the user receives a notification through the CREDENTIAL App. The user selects which attributes to reveal to the relying party and which ones to blank out. Having received the selection, the CREDENTIAL Wallet redacts the defined attributes and re-encrypts the resulting ciphertext for the receiver.
- Having received the re-encrypted and redacted data, the relying party decrypts the ciphertext using its own secret key and verifies the signature on the received attributes. If the verification succeeds, the receiver is ensured that the revealed information was indeed signed by the issuer, and continues, e.g., by granting the user access to the request resource. If the verification fails, authentication was unsuccessful and the relying party aborts.

An overview of the described data flow is given in Figure 13.1. In the case that a user wants to share non-authentic data with another user, the process is simplified, in the sense that all steps related to signature generation, redaction, and verification are omitted.

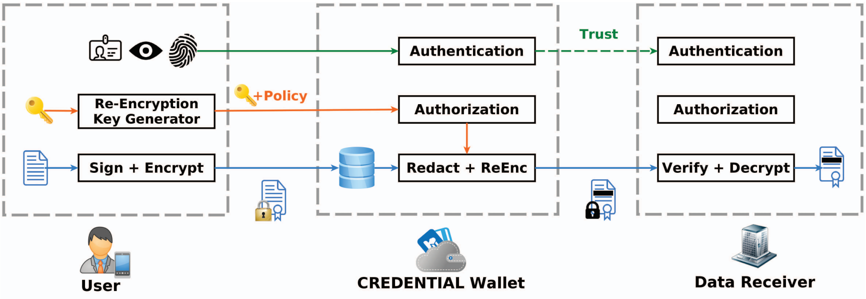

Figure 13.1 Abstract data flow in CREDENTIAL [10].

13.3.1 Added Value of the CREDENTIAL Wallet

The described data flow and implementation of the CREDENTIAL Wallet brings various benefits for all actors in the ecosystem of identity and access management [2, 11].

Benefits for end users. The end users of the CREDENTIAL Wallet benefit in various ways from the fact that the CREDENTIAL Wallet and all related components are under the privacy-by-design principle. For instance, the necessary trust into the IdP provider can be significantly reduced, as the provider does no longer have access to any of the user's data; besides protecting against internal threats such as malicious system administrators, this also shields the user against security incidents such as data leaks because of active attacks or during hardware decommissioning. Users are put back into full control over their data and can selectively disclose parts of their identity information to the service provider. This is enforced on a technical and not on a policy level. Furthermore, the user needs to access his or her secret key material when granting a relying party access to his attributes for the first time, but not for subsequent authentications. In particular, the user can store his or her secret key on a trusted mobile device, but does not need to carry it with them, e.g., when leaving for vacation. Finally, due to the implemented multi-factor authentication mechanisms, accessing a service from an insecure device (e.g., a shared PC) under the control of a potential adversary does not enable the adversary to impersonate the user for subsequent authentications to the same or other services.

Benefits for CREDENTIAL Wallet providers. Compared to traditional providers of identity and access management systems, providers of the CREDENTIAL Wallet benefit from the end-to-end encryption mechanisms used in our solution, and they can build their business models around our increased security features and guarantees. By not having access to sensitive user data, the liability risk is reduced significantly, and it becomes easier to comply with legal regulations such as the General Data Protection Regulations (GDPR).

Benefits for relying parties. The main benefit for relying parties is that they receive formal authenticity guarantees on the data they receive, by being able to verify that the data they receive was indeed cryptographically signed by a valid issuer. Consequently, they can significantly reduce the necessary trust into the identity provider. Furthermore, the CREDENTIAL Wallet was designed with maximum interoperability with existing industry standards for entity authentication (e.g., OAuth) in mind. This simplifies the integration into existing schemes substantially compared to other solutions following an ad-hoc design.

13.4 Showcasing CREDENTIAL in Real-World Pilots

A main objective of the CREDENTIAL project was not only to design the CREDENTIAL Wallet, improve and adapt the required technologies, and develop the necessary components, but also to evaluate the usability, stability, and efficiency of the applications in different real-world application domains from critical sectors.

In the following, we give a brief overview of the different pilot domains and our conclusions based on representative pilot users. Preliminary descriptions of the pilots can also be found in [8, 11].

13.4.1 Pilot Domain 1: eGovernment

CREDENTIAL's eGovernment pilot considered citizens and professionals who wish to authenticate themselves towards services offered by a public authority in a highly transparent way that gives them full control over which data goes where. More precisely, the project partners integrated the CREDENTIAL Wallet into SIAGE, a web portal hosted by our project partner Lombardia Informatica S.p.A. When visiting SIAGE's login page, users were offered to connect using their CREDENTIAL account. When selecting this option, they were redirected to an OpenAM component developed within the project, and an OAuth2 authentication flow was initiated. The users received a notification on their mobile phone and were asked to accept the information requested by the SIAGE system for authentication. Upon approval, the CREDENTIAL Wallet re-encrypted and redacted the appropriate user attributes before forwarding the resulting authentication token to SIAGE, which decrypted the data and verified its authenticity.

The pilot was executed using internal IT professionals for technical evaluations, and external focus groups to analyse the usability and perceived security aspects of the solution. The overall opinion of the users was very positive throughout all user groups. A detailed description of the pilot execution is also given in [17].

We want to stress that the analysed functionalities also demonstrate the technical feasibility and efficiency of the CREDENTIAL technologies in the context of many other eGovernment procedures beyond pure authentication, including aspects such as paper de-materialization. Imagine for example an employer who is willing to issue pay slips electronically. This employer, taking the role of the issuer in the authentication case, could sign the pay slip using a redactable signature scheme and label the different blocks of the pay slip as admissible. Now, when a user wants to request financial advantages from Lombardy region through the SIAGE system, he could log in as described above, and then decide to share those parts of the pay slip that are needed for receiving the requested support. For instance, if the support solely depends on gross income, the notification on the mobile phone would request obligatory access only to this data, and the user could decide to blank out information such as spent vacation days or reimbursements of actual travel costs. The data flows would be fully analogous to the authentication flow, and the service provider only needs to integrate the needed CREDENTIAL libraries.

13.4.2 Pilot Domain 2: eHealth

The eHealth pilot focused on secure remote data sharing between diabetes patients and their physicians [14]. To do so, two dedicated mobile applications for patients and doctors, respectively, have been developed.

The patient's app offers a convenient way for users to import medical data from devices such as glycosometers or scales. Like existing healthcare applications, users can browse through their history and get visual representations of their measurements. Whenever a user imports a new value and wishes to store it in its patient healthcare record (PHR), this access request is processed by a dedicated component developed within the project, cf. Figure 13.2. This so-called interceptor component redirects all requests through the CREDENTIAL Wallet. Technically, the patient's data is encrypted using a symmetric encryption scheme. The symmetric key is then encrypted employing the user's proxy re-encryption key and stored in their CREDENTIAL Wallet account. When selecting a treating doctor, the patient's application computes a re-encryption key from the patient to the doctor and deposits it in the CREDENTIAL Wallet's key store. Now, using the doctor's app, a diabetologist or general practitioner can access the encrypted key in the patient's account. The CREDENTIAL Wallet re-encrypts the ciphertext and the doctor receives the secret key that was used to encrypt the data in the PHR. After accessing the encrypted data in the PHR, the doctor can decrypt the data and analyse the patient's measurements.

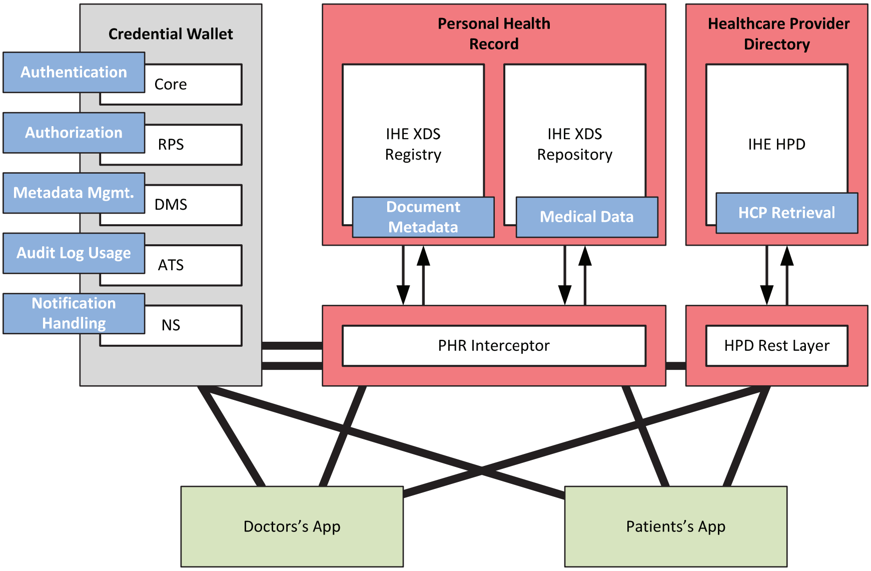

Figure 13.2 Architecture of the CREDENTIAL eHealth pilot (cf. also [14]).

Furthermore, the doctor can also provide feedback to the patient, e.g., by adding lab values such as HbA1c, or provide treatment recommendations.

After overcoming initial stability and efficiency problems, the feedback received from the external users and doctors was highly positive, in particular concerning the perceived security guarantees of the developed solution. One of our main conclusions is that it is possible to provide sophisticated end-to-end security solutions to the user in a way that is almost fully transparent and does not negatively affect usability.

13.4.3 Pilot Domain 3: eBusiness

The eBusiness pilot, documented in detail by Pallotti et al. [13], covered three use cases. The first use case allowed users to securely authenticate themselves towards an eCommerce platform, while the second use case enabled them to retrieve their data from the CREDENTIAL Wallet and share it with a service provider to subscribe to new services. From a technical point of view, these use cases are closely related to the eGovernment pilot described above, and we will focus on the third use case in the following.

In this use case, CREDENTIAL's proxy re-encryption libraries were integrated into InfoCert's Legalmail application, a certified mail service providing the same level of legal assurance as paper-based registered mail. The use case addressed the issue of forwarding encrypted emails to a deputy in case of absence: using classical email encryption technologies, the sender would need to be notified that the intended receiver is currently unavailable and would have to resend the mail to the defined deputy. The only way to avoid this additional interaction would then be to share the receiver's secret decryption key with the deputy, which however poses significant security risks and requires very high trust assumptions. Using proxy re-encryption, a Legalmail client can define a deputy, and deposit a re-encryption key at the mail server. Upon receiving an encrypted mail, the message is re-encrypted and forwarded to the deputy, who can decrypt the mail using his own secret key. While the sender does not need to be actively involved in this process, he still received a notification for transparency reasons.

The test users involved in the piloting phase showed genuine interest in the added security provided by CREDENTIAL. The possibility of exchanging confidential messages with a certified mail service has been highly appreciated. In addition, the pilot was able to show that the CREDENTIAL Wallet is not only able to provide meaningful features "as a whole", but also that single components of the system can successfully be integrated in other contexts.

13.5 Conclusion and Open Challenges

CREDENTIAL's main ambition was to develop a privacy-preserving and end-to-end secure and authentic data-sharing platform with integrated identity provisioning functionalities. To achieve this goal, the project consortium analysed, improved, and integrated security technologies from different domains including cryptography, multi-factor authentication, among others. Furthermore, the entire development process was accompanied by privacy experts to guarantee privacy-by-design and privacy-by-default, as well as by usability experts to ensure that end users are able to efficiently and conveniently interact with the system. Finally, the developed CREDENTIAL Wallet was tested through pilots within the highly sensitive domains of eGovernment, eHealth, and eBusiness, where the real-world usability and applicability of the developed solutions has been successfully proven.

13.5.1 Recommendations on Usability and Accessibility

Within the project, also ways to facilitate the adoption of privacy-friendly solutions for identity management and data sharing were studied. It turned out that users are often unaware of the privacy-issues with existing IdP solutions. Our analyses suggest that video tutorials can be an efficient way to inform users: statistical tests showed significant differences in the correctly identified advantages between participants who received a tutorial on single sign-on and those who did not, and also perceived usability increased of a more elaborate user interface which supported them in making more informed decisions [9].

Regarding accessibility, we believe that the European Directive 2016/2012 on the accessibility of websites and mobile applications of public sector bodies will inspire a development where assistive technology can seamlessly merge with IdP apps. A mobile application for the CREDENTIAL Wallet is an intermediary for the services benefitting from the Wallet's service. Thus, the public sector bodies – which all have to live up to the Directive – must rely on IdP services that also meet the requirements of the Directive. This will in its turn make it easy for service providers from the private sector to provide high levels of accessibility, as they benefit from users using these IdPs. Furthermore, the accessibility analysis provided within the CREDENTIAL project [7] can serve as an example for future developers of apps for services like the CREDENTIAL Wallet. One should also realise that further legal analysis might be needed from the public-sector side of its liabilities in accessible interactive communication.

13.5.2 Open Challenges

During the project duration, many challenges regarding design, efficiency, or understanding of user attitudes were successfully overcome. Nevertheless, we would like to briefly discuss two remaining challenges in the following.

Metadata privacy. From a technical point of view, metadata privacy is one of the main challenges that still needs to be addressed in cloud-based solutions such as the CREDENTIAL Wallet. While fundamental aspects such as linkability of authentication processes in cloud-based solutions were successfully addressed [12], the CREDENTIAL Wallet may still be able to infer sensitive information, e.g., who is sharing data with whom, or which data is accessed by whom and how often. The cryptographic literature contains several approaches to tackle these challenges, such as private information retrieval (cf. [4] and reference therein) or oblivious transfer (cf. [15] and the references given there). However, to the best of our knowledge, all existing solutions are currently too inefficient for large-scale deployment in real-world systems or would render the entire system too expensive.

Establishing business models for privacy. A major challenge we faced during the CREDENTIAL project relates to establishing sustainable business models for privacy-preserving solutions. At the current point in time, many major identity provider solutions – offered by, e.g., major search engine or social network providers – are free for the end user in the sense that no subscription fee needs to be paid, but the providers in turn gain substantial amounts of data about the user and build their business models around this. Furthermore, several studies have shown that while end users prefer privacy-preserving solutions in different scenarios, they are often not willing to pay for this feature. The successful commercialization of privacy-enhancing systems such as the CREDENTIAL Wallet would thus require a change of thinking on the cloud service provider and on the end user side, which could be triggered by legal regulations such as the General Data Protection Regulation (GDPR) or information campaigns to raise the users' awareness for privacy-related issues. Alternatively, especially for critical domains such as eHealth or eGovernment, we believe that also public authorities (e.g., ministry of health) could be potential providers of the CREDENTIAL Wallet, where the deployment and maintenance costs do not need to be paid directly by the end users.

Acknowledgements

The CREDENTIAL (Secure Cloud Identity Wallet) project leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653454.

The authors would like to thank all partners of the CREDENTIAL consortium for their efforts and work during the entire project duration and beyond. Finally, the authors are grateful to the editors for their efforts during the preparation of this book.

References

[1] Giuseppe Ateniese, Kevin Fu, Matthew Green, Susan Hohenberger. *Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage*. In NDSS 2005. The Internet Society. 2005.

[2] Charlotte Bäccman, Andreas Happe, Felix Hörandner, Simone Fischer-Hübner, Farzaneh Karegar, Alexandros Kostopoulos, Stephan Krenn, Daniel Lindegren, Silvana Mura, Andrea Migliavacca, Nicolas Notario McDonnell, Juan Carlos Pérez Baún, John Sören Pettersson, Anna E. Schmaus-Klughammer, Evangelos Sfakianakis, Welderufael Tesfay, Florian Thiemer, and Melanie Volkamer. *D3.1 – UI Prototypes v1*. CREDENTIAL Project Deliverable. 2017.

[3] Matt Blaze, Gerrit Bleumer, and Martin Strauss. *Divertible Protocols and Atomic Proxy Cryptography*. In EUROCRYPT 1998 (LNCS), Kaisa Nyberg (Ed.), Vol. 1403. Springer, 127–144. 1998.

[4] Ran Canetti, Justin Holmgren, Silas Richelson. *Towards Doubly Efficient Private Information Retrieval*. In TCC (2) 2017 (LNCS), Yael Kalai and Leonid Reyzin (Eds.), Vol. 10678. Springer, 694–726. 2017.

[5] Pasquale Chiaro, Simone Fischer-Hübner, Thomas Groß, Stephan Krenn, Thomas Lorünser, Ana Isabel Martínez Garcí, Andrea Migliavacca, Kai Rannenberg, Daniel Slamanig, Christoph Striecks, and Alberto Zanini. *Secure and Privacy-Friendly Storage and Data Processing in the Cloud*. In IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2.2 International Summer School 2017 (IFIP AICT), Marit Hansen, Eleni Kosta, Igor Nai-Fovino, and Simone Fischer-Hübner (Eds.), Vol. 526. 153–170. 2018.

[6] Sherman S. M. Chow, Jian Weng, Yanjiang Yang, and Robert H. Deng. *Efficient Unidirectional Proxy Re-Encryption*. In AFRICACRYPT 2010 (LNCS), Daniel J. Bernstein and Tanja Lange (Eds.), Vol. 6055. Springer, 316–332. 2010.

[7] Felix Hörandner, Pritam Dash, Stefan Martisch, Farzaneh Karegar, John Sören Pettersson, Erik Framner, Charlotte Bäccman, Elin Nilsson, Markus Rajala, Olaf Rode, Florian Thiemer, Alberto Zanini, Alberto Miranda Garcia, Daria Tonetto, Anna Palotti, Evangelos Sfakianakis, and Anna Schmaus-Klughammer. *D3.2 – UI Prototypes v2 and HCI Patterns*. CREDENTIAL Project Deliverable. 2018.

[8] Felix Hörandner, Stephan Krenn, Andrea Migliavacca, Florian Thiemer, and Bernd Zwattendorfer. *CREDENTIAL: A Framework for Privacy-Preserving Cloud-Based Data Sharing*. In ARES. IEEE Computer Society, 742–749. 2016.

[9] Farzaneh Karegar, Nina Gerber, Melanie Volkamer, Simone Fischer-Hübner. *Helping John to make informed decisions on using social login*. In SAC 2018, Hisham M. Haddad, Roger L. Wainwright, and Richard Chbeir (Eds.). ACM, 1165–1174. 2018.

[10] Farzaneh Karegar, Christoph Striecks, Stephan Krenn, Felix Hörandner, Thomas Lorünser, and Simone Fischer-Hübner. *Opportunities and Challenges of CREDENTIAL - Towards a Metadata-Privacy Respecting Identity Provider*. In IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6/SIG 9.2.2 International Summer School 2016 (IFIP AICT), Anja Lehmann, Diane Whitehouse, Simone Fischer-Hübner, Lothar Fritsch, and Charles D. Raab (Eds.), Vol. 498. 76–91. 2017.

[11] Alexandros Kostopoulos, Evangelos Sfakianakis, Ioannis Chochliouros, Jon Sören Pettersson, Stephan Krenn, Welderufael Tesfay, Andrea Migliavacca, and Felix Hörandner. *Towards the Adoption of Secure Cloud Identity Services*. In ARES. ACM, 90:1–90:7. 2017.

[12] Stephan Krenn, Thomas Lorünser, Anja Salzer, and Christoph Striecks. *Towards Attribute-Based Credentials in the Cloud*. In CANS 2017 (LNCS), Srdjan Capkun and Sherman S. M. Chow (Eds.), Vol. 11261. Springer, 179–202. 2018.

[13] Anna Pallotti, Luigi Rizzo, Romualdo Carbone, Pasquale Chiaro, and Daria Tonetto. *D6.6 – Test and Evaluation of Pilot Domain 3 (eBusiness)*. CREDENTIAL Project Deliverable. 2018.

[14] Anna Schmaus-Klughammer, Johannes Einhaus, and Olaf Rode. *D6.5 – Test and Evaluation of Pilot Domain 2 (eHealth)*. CREDENTIAL Project Deliverable. 2018.

[15] Peter Scholl. *Extending Oblivious Transfer with Low Communication via Key-Homomorphic PRFs*. In PKC (1) 2018 (LNCS), Michel Abdalla and Ricardo Dahab (Eds.), Vol. 10769. Springer, 554–583. 2018.

[16] Ron Steinfeld, Laurence Bull, and Yuliang Zheng. *Content Extraction Signatures*. In ICISC 2001 (LNCS), Kwangjo Kim (Ed.), Vol. 2288. Springer, 285–304. 2001.

[17] Alberto Zanini and Andrea Migliavacca. *D6.4 – Test and Evaluation of Pilot Domain 1 (eGovernment)*. CREDENTIAL Project Deliverable. 2018.