Towards the Adoption of Secure Cloud Identity Services

Alexandros Kostopoulos
Hellenic Telecommunications
Organization R&D
Athens, Greece
alexkosto@oteresearch.gr

Evangelos Sfakianakis
Hellenic Telecommunications
Organization R&D
Athens, Greece
esfak@oteresearch.gr

Ioannis Chochliouros
Hellenic Telecommunications
Organization R&D
Athens, Greece
ichochliouros@oteresearch.gr

John Sören Pettersson
Karlstad University
Karlstad, Sweden
john_soren.pettersson@kau.se

Stephan Krenn
AIT Austrian Institute of Technology
Vienna, Austria
stephan.krenn@ait.ac.at

Welderufael Tesfay
Goethe University Frankfurt
Frankfurt, Germany
welderufael.tesfay@m-chair.de

Andrea Migliavacca
Lombardia Informatica S.p.A.
Milan, Italy
andrea.migliavacca@cnt.lispa.it

Felix Hörandner
Graz University of Technology
Graz, Austria
felix.hoerandner@iaik.tugraz.at

ABSTRACT

Enhancing trust among service providers and end-users with respect to data protection is an urgent matter in the growing information society. In response, CREDENTIAL proposes an innovative cloud-based service for storing, managing, and sharing of digital identity information and other highly critical personal data with a demonstrably higher level of security than other current solutions. CREDENTIAL enables end-to-end confidentiality and authenticity as well as improved privacy in cloud-based identity management and data sharing scenarios. In this paper, besides clarifying the vision and use cases, we focus on the adoption of CREDENTIAL. Firstly, for adoption by providers, we elaborate on the functionality of CREDENTIAL, the services implementing these functions, and the physical architecture needed to deploy such services. Secondly, we investigate factors from related research that could be used to facilitate CREDENTIAL's adoption and list key benefits as convincing arguments.

CCS CONCEPTS

•**Security and privacy →Access control;** *Cryptography; Authentication; Privacy-preserving protocols;* Usability in security and privacy;

KEYWORDS

Data sharing, access control, identity management, user adoption, proxy re-encryption

ACM Reference format:
Alexandros Kostopoulos, Evangelos Sfakianakis, Ioannis Chochliouros, John Sören Pettersson, Stephan Krenn, Welderufael Tesfay, Andrea Migliavacca, and Felix Hörandner. 2017. Towards the Adoption of Secure Cloud Identity Services. In *Proceedings of ARES '17, Reggio Calabria, Italy, August 29-September 01, 2017,* 7 pages.
DOI: http://dx.doi.org/10.1145/3098954.3104061

ARES '17, Reggio Calabria, Italy
© 2017 Copyright held by the owner/author(s). 978-1-4503-5257-4/17/08…$15.00
DOI: http://dx.doi.org/10.1145/3098954.3104061

1 INTRODUCTION

With increasing mobility and Internet use, the demand for digital services has increased and already reached critical domains, with high security and privacy requirements. Handling all the different authentication and authorization mechanisms requires user-friendly support, which can be efficiently provided by digital *identity management* (IdM). IdM is currently experiencing a paradigm shift, and, under the given change, current solutions fall short in many aspects. Until recently, IdM was mainly a local issue and most organizations operated their own, custom-tailored IdM systems within the organization's domain boundaries.

The transformation in the IdM world goes hand in hand with the tremendous shift to cloud computing that has shaped the ICT world during the last years. Identity management has not remained unaffected in this respect. By now, numerous IdM systems and solutions are available as cloud services, providing identity services to applications operated both in closed domains and in the public cloud. This service model is often referred to as *Identity* (and Access) *Management as a Service* (IDMaaS). Popular examples for cloud IDMaaS providers are companies from the sectors of social networks (Facebook, LinkedIn), search engines (Google), business solutions (Microsoft, Salesforce) or online retailers (Amazon). However, currently no satisfactory approaches exist which allow the privacy-preserving storage and advanced sharing of identity data by cloud service providers.

In response, CREDENTIAL [5, 7, 12, 17] intends to develop, test and showcase innovative cloud-based services for storing, managing, and sharing digital identity information and other critical personal data. The security of these services relies on the combination of strong hardware-based multi-factor authentication with end-to-end encryption representing a significant advantage over current password-based authentication schemes. The use of sophisticated cryptography schemes, such as proxy re-encryption [3] and

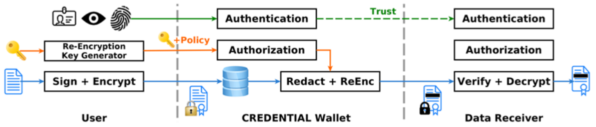

Figure 1: CREDENTIAL conceptual architecture [1, 10]

redactable signatures [14], enables a secure and privacy preserving information sharing network for cloud-based identity information in which even the identity provider cannot access the data in plaintext and hence protect access to identity data. The *CREDENTIAL Wallet* is the central component of the tools and components developed. Our goal is to extend the application of the CREDENTIAL approach to a comprehensive cloud system and to existing solutions by using and exploiting recognized standards and protocols.

In this paper, we focus on the adoption of CREDENTIAL by service providers and end-users. To provide context, we also clarify CREDENTIAL's architecture and user cases. Our main contribution can be split into two parts:

Firstly, we elaborate on how the CREDENTIAL concept can be adopted in terms of implementation and deployment. We introduce CREDENTIAL's main functions and outline their implementation by presenting groups of services as well as their composition. Also, we map those services to physical resources and investigate aspects for a successful cloud deployment, such as reliability and scalability.

Secondly, we explore factors that could facilitate the adoption of CREDENTIAL. Based on a survey of related research on adoption especially of technologies, we identify relevant concepts and potential factors to boost CREDENTIAL's adoption. Finally, taking these aspects into account, we present benefits of the CREDENTIAL solution.

1.1 Outline

The paper is organized as follows: Section 2 presents the main stakeholders and their interactions, as well as the conceptual CREDENTIAL architecture. Section 3 focuses on the functional spit and the provided services. In Section 4, we describe how the logical architecture is interpreted into the physical one. Section 5 investigates three use cases in order to demonstrate how the CREDENTIAL technology can be deployed in diverse contexts. In Section 6, we consider the potential factors that could boost the adoption of the CREDENTIAL Wallet. We conclude our remarks in Section 7.

2 ECOSYSTEM AND ARCHITECTURE

CREDENTIAL's basic architecture is based on the integration of cryptographic mechanisms involving three key components namely a *user*, the *CREDENTIAL Wallet*, and a *data receiver*, as shown in Figure 1.

The CREDENTIAL Wallet stores user data and identity data in a secure cloud. It is a cloud platform, which offers sharing of those user data with other participants or service provider in a secure way and preserving user privacy. The Wallet comprises an identity and access management (IAM) system, performing authentication and providing authorization to access those data. In particular, IAM system implements a multi-factor authentication and authorizes access to data stored. This leads to two main advantages:

- proxy re-encryption system does not expose plain data, therefore confidentiality of data shared and stored by CREDENTIAL Wallet in the cloud is ensured;
- once a re-encryption key is available for some specific set of data as specified by the user, these data can be shared with specified receivers even if the user or his/her client application are not available.

The CREDENTIAL architecture consists of the following three actors: Firstly, an *external Identity Provider* can be embedded to offer authentication functionality for end users. Secondly, the *end-user* owns data that might be securely stored or shared with other account-holders in the CREDENTIAL Wallet. He/she has the absolute control over the data flow of his/her personal and sensitive data. A client application in the user's domain handles cryptographic operations involving the user's private key, such as signing or generating a re-encryption key. Finally, the *data receiver*, that can be either *another CREDENTIAL user* or a *service provider*, reaches data stored in or authentication assertions issued by the CREDENTIAL Wallet and can perform arbitrary data processing.

The data sharing process involves the actors of CREDENTIAL's basic architecture in the following steps:

(1) The user authenticates at the Wallet to get read and write permission to her Wallet account, which are used to upload signed and encrypted data.
(2) To later share this data, the user generates a re-encryption key towards a selected data receiver in her trusted domain. Along with this key, the user defines a policy defining which data may be disclosed to which entity and installs it at the Wallet.
(3) When an authorized receiver tries to access the user's data, not required parts are redacted and the remaining parts are transformed into ciphertext for the data receiver by using the re-encryption key.
(4) Finally, the data receiver is able to decrypt the data and verify the signature on the disclosed parts.

3 FUNCTIONAL SPLIT AND PROVIDED SERVICES

After presenting the overall architecture and the main workflow, we present the main functionalities, as well as the services provided by the CREDENTIAL platform.

3.1 Functionalities

The main functionalities of the CREDENTIAL Wallet can be grouped in three main categories:

Account Management: These services focus on the whole account life-cycle and access management. A user can create a new account that involves the creation of its proxy-re-encryption enabled key material and an account association on the CREDENTIAL Wallet. Furthermore, the user can perform various management functionalities like showing an activity protocol on its data or delegate access rights to its data.

Identity Management: These functionalities are focusing on integrating identity data stored within the CREDENTIAL Wallet in the authentication mechanisms towards other service providers. The use of proxy-re-encryption technologies allows sharing the identity data in the CREDENTIAL Wallet in a secure and privacy aware way.

Data Sharing: Such functionalities focus on storing, reading and sharing of user data that is assigned to the CREDENTIAL Wallet. The user data is protected by encryption and the data being shared is never disclosed to the CREDENTIAL Wallet itself.

3.2 Services

An initial classification has been made in order to group related services:

Cryptographic Services: This service type comprises all services that are related to the management of cryptographic material and its usage to protect data.

Data Management Services: Such services include everything dealing with the management of the data and the policies to access it. When another user's data is requested, this service transforms the ciphertext for the data owner into ciphertext for the requester.

Account and Identity Management Services: These services deal with credentials, accounts and identity and attributes management. Particularly, the authentication service in the server side is responsible to, in base to some pre-established credentials such as a key-pair, determine if the end-user trying to access the Wallet is the owner of such credentials. The account management service is responsible for handling the life cycle of CREDENTIAL accounts. The access management service controls the access to the users' data by managing and evaluating requests against user-defined policies.

Auditing and Notification Services: This category includes horizontal services that are not specifically related to the management of data, accounts or cryptographic material. In particular, the auditing service will store, in compliance with current legislation framework and in consonance with privacy requirements, information regarding attempted access and authorizations to access stakeholders' data. The Notification Service is responsible for recognizing events that happens on the CREDENTIAL Wallet and notify users according to their preferences. Users can customize various notification settings and get notifications on their devices.

Figure 2 shows all the logical components and the main relationships of CREDENTIAL architecture. From participant's site, the available services include *decryption*, *re-encryption key generation*, *key generation*, *authentication*, *encryption*, *sign*, *personal trust store*, and *notification*. Regarding the CREDENTIAL cloud infrastructure, a set of services run either for the *Data Repository* or/and for the *Participant Index*. Such services may include *participant data search*, *attribute*, *redactor*, *authentication*, *participant search* and *registration*, as well as *notification*, *audit trail*, and *authorization*.

4 PHYSICAL ARCHITECTURE

Our next step is focused on mapping the CREDENTIAL logical architecture to the physical one. In particular, this section describes the physical nodes where CREDENTIAL technology/components are being deployed. We propose a reference physical architecture taking into account the functionalities and services presented in Section 3, but also general non-functional requirements such as availability, reliability (fault-tolerance), performance (throughput), and scalability. While this reference architecture is general and cloud platform independent, we present an operational environment supported by an open source solution for private and public clouds, such as OpenStack, that can be instantiated and adapted for pilot-specific needs.

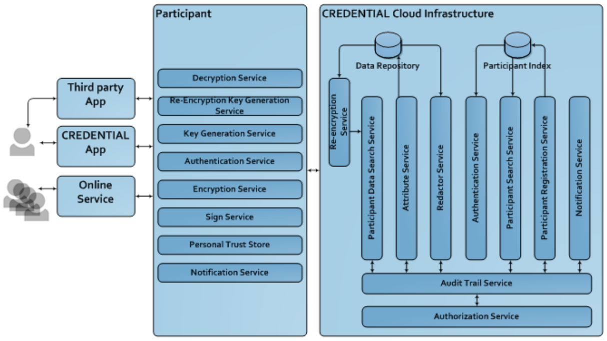

Figure 2: Logical architecture and services

Besides the development components [7], there are additional "commodity" components that must be integrated in the generic physical architecture (e.g. network, physical storage, etc.). Being this the reference architecture, multiple instances/configurations of it are expected (e.g., for development and testing, for the deployment of the system for various sites, for different customers, etc.). Hence, the mapping of the development components to the physical nodes needs to be highly flexible and have a minimal impact on the scalability of the CREDENTIAL Wallet.

The CREDENTIAL Wallet's physical architecture takes into account the following concepts and aspects:

- The CREDENTIAL Wallet' underlying infrastructure will consist of physical, virtual, and automation components.
- The starting point for the CREDENTIAL Wallet – independently of application specific characteristics – is the physical data center, control, and hardware.
- CREDENTIALfis reference architecture is required to achieve the correct level of resiliency and redundancy, including power and security aspects of the underlying infrastructure.
- The underlying platform is critical to consider as it is the foundation of the services that are built and delivered with high quality and reliability.
- The hardware platform consists of physical servers to provide the underlying compute, memory, and local disk needed to support the infrastructure needs of cloud.
- Storage consists of a variety of different speeds and sizes of Serial Advanced Technology Attachment (SATA), Serial Attached SCSI (SAS), and solid-state (SSD) disks. These disks can be local to the storage infrastructure.

According to these aspects, we deploy CREDENTIAL's Wallet main components (IAM and Data Services) in replicated virtual

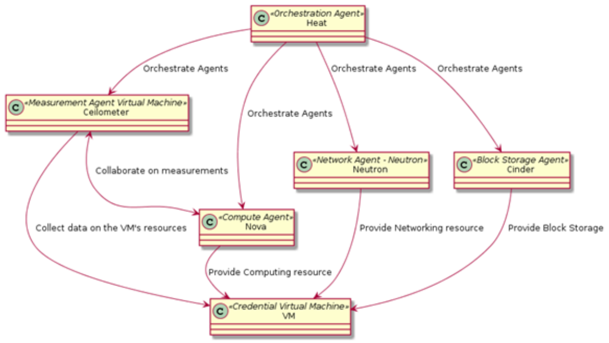
«Orchestration Agent»
Heat
«Measurement Agent Virtual Machine»
Ceilometer
«Network Agent - Neutron»
Neutron
«Block Storage Agent»
Cinder
«Compute Agent»
Nova
«Credential Virtual Machine»
VM
Orchestrate Agents
Orchestrate Agents
Orchestrate Agents
Orchestrate Agents
Collaborate on measurements
Collect data on the VM's resources
Provide Networking resource
Provide Block Storage
Provide Computing resource

Figure 3: Overview of cloud provider modules

nodes that will support high availability requirements for CREDENTIAL Wallet's services. Beyond this additional redundancy, failover and load balancing mechanisms will be proposed to address high availability and avoid data loss in CREDENTIAL Wallet services.

Figure 3 shows an overview of OpenStack modules that can build VMs with the appropriate resources and the deployment setup of CREDENTIAL infrastructure. The OpenStack modules can be grouped or split in one or more physical nodes, depending on the requirements, use and load of the system(s) or service(s) to be hosted.

Given the flexibility a cloud can have and give to a virtualized environment, it can facilitate both *horizontal* and *vertical scaling*. Horizontal scaling means that the scaling is performed by adding more machines into the available pool of resources whereas vertical scaling or scaling up means that scaling is performed by adding more power (CPU, RAM) to an existing machine, noting that vertical scaling often involves downtime.

Regarding databases, horizontal scaling is often based on partitioning of the data i.e. each node contains only part of the data, in vertical scaling the data resides on a single node and scaling is done through multi-core, i.e. spreading the load between the CPU and RAM resources of that machine.

Additionally, cloud environments have developed mechanisms that can also apply auto-scaling, either horizontally or vertically based on sets of rules. In the OpenStack platform, this can be achieved with the utilization of HEAT and Ceilometer modules.

However, the CREDENTIAL architecture has the business logic and the data split in separate VMs (see Figure 4), which allows adding either more VMs or increase certain hardware characteristics of a specific VM, depending on the given load, number of active users, availability and security requirements, etc. Given the fact that most of the functionality resides in the CREDENTIAL Wallet VM, such as web server, authentication, authorization, certificate generation etc., it is expected that it may need to be more provisioned for CPU and memory, while the DB VMs more provisioned for HD space.

5 USE CASES

To showcase the provided benefits of the CREDENTIAL Wallet and to demonstrate how a higher security and privacy can be achieved by the means of the CREDENTIAL Wallet, three different use cases are considered in the domains eGovernment, eHealth and eBusiness [7]. Each use case brings different challenges for CREDENTIAL technologies. The eGovernment use case targets Identity Management, the eHealth use case targets sharing of sensitive medical data across multiple users and the eBusiness use case targets sharing of data with service providers. By considering use cases from different domains, we highlight the potentials for widespread adoption of the CREDENTIAL Wallet.

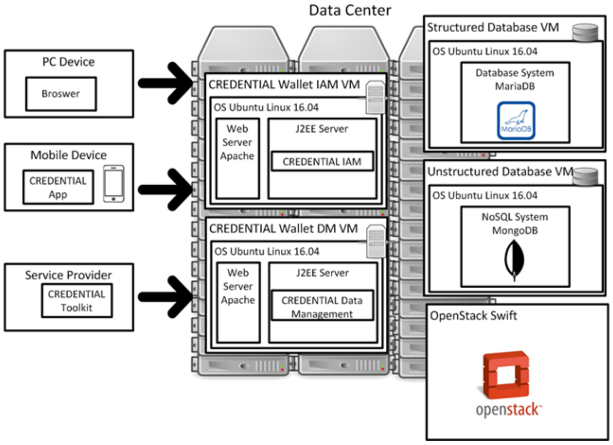

Figure 4: IAM and data management (DM) components

For the definition of the use case activities were considered both technological aspects and the possibility for users to recognize the advantages of privacy management systems. Each use case was designed considering the environment of specific domains and their constraints, such as for the eGovernment the infrastructure of Lombardy Region and for the eBusiness the Infocert products and services infrastructure. The eHealth domain has less technological and architectural constrains because a new solution is deployed.

The use case definition has therefore focused on designing a process where the user can "touch" the potential advantage of the CREDENTIAL Wallet compared to existing privacy management systems. This issue is important because the citizens normally do not have an exact perception about their own privacy and its connection to the different identity management systems.

The definition of such a comprehensive use case scenario has allowed us to tackle key challenges about privacy, in particular for the health data exchange, which strengthens the potentials of the widespread adoption of the CREDENTIAL Wallet.

For a detailed specification of the pilots we refer to [4].

5.1 eGovernment

The eGovernment use case is mainly oriented on secure authentication in a cloud environment using an ecosystem of Identity Providers (IdP) who join the CREDENTIAL project. Secure authentication covers at least two key factors: user is authenticated in a secure way (using a secure device) and user data are handled and transmitted over the network with confidentiality and security.

This use case focuses on identity management to authenticate citizens and assess their eligibility for a service, based on sensitive identity attributes. Standardized identity protocols such as

SAML or OpenID Connect should be used in CREDENTIAL’s identity management data sharing process. Within this protocol, the service provider (i.e., the data receiver) triggers the process by requesting authentication and identity attributes from the identity provider (i.e., the CREDENTIAL Wallet). In our pilot we intend to enable authentication not only via national eID solutions, but also cross-border authentication according to the eIDAS regulation. The CREDENTIAL Wallet reacts to the user consent and generates a re-encryption key, whilst the service provider receives re-encrypted attributes disclosed in a selective way.

5.2 eHealth

The eHealth use case focuses on secure data sharing between patients, doctors, and further parties, in the field of Type 2 Diabetes. In particular, the process applies to patients, which can use mobile devices to record their health data, those data are collected by a CREDENTIAL eHealth mobile app which remotely stores them in the CREDENTIAL Wallet. This data sharing approach offers several advantages to the patient, such as enhanced privacy by minimizing disclosed data, having a continuous control of health data, as well as saving time and money for personal visits.

Stakeholders of the CREDENTIAL eHealth piloting scenario are doctors, medical personnel, health insurance companies and patients. In particular, a Personal Health Record (PHR) will be available for all stakeholders to store patient data. By encrypting data using CREDENTIAL confidentiality protection means prior to storing data to the PHR, full end-to-end encryption can be achieved where only an authorized consumer of the medical data is able to decrypt the data. Providing such end-to-end encryption from data provisioning until data consumption is a prerequisite in some countries – e.g., Germany – for sharing health data via a cloud infrastructure. By this, CREDENTIAL is aimed as an enabler for establishing cost-effective and scalable cloud storage in healthcare.

5.3 eBusiness

Today many business processes in several market sectors can be performed online. But there is always a trade-off between security and usability: in fact, often the online services that are simple for users do not guarantee the right level of security and privacy.

The eBusiness use case focuses on the integration of modular libraries implementing CREDENTIAL’s technologies into existing solutions to provide additional value. In particular, it tackles the issue of forwarding encrypted mails, which are nowadays increasingly used by companies to protect data and products, when employees are not at work. In fact, according to the current legislation, an employee has to provide her private keys to access the company e-mail system to give the possibility to other colleagues to still read and eventually take over incoming mail. Through proxy re-encryption, an employee can generate a re-encryption key towards an authorized colleague and hand this key to the mail server before leaving. The mail server is then able to re-encrypt incoming mail during the worker’s absence and forward it to the authorized colleague.

6 CREDENTIAL WALLET ADOPTION

To what extent will people understand and appreciate the benefits offered by solutions like the CREDENTIAL Wallet?

Previous research efforts show that there is a general lack of understanding among users of different login solutions, and a lack of appreciation of identity providers, etc. We depict the main research frameworks for understanding the adoption drivers for new technologies and services in order to investigate the adoption of the CREDENTIAL Wallet.

The classical diffusion theory has increased our understanding of how innovations (e.g., a new protocol) spread within populations. Rogers’ diffusion of innovations theory [13] breaks the adoption process down into five stages. In the *knowledge* stage, the individual is exposed to the innovation, but lacks complete information about it. In the *persuasion* stage the individual becomes interested in the new idea and seeks additional information about it. The next stage is *decision*, where the individual mentally applies the innovation to his present and anticipated future situation, and then decides whether or not to try it. In the *implementation* stage the individual employs the innovation. Finally, in the *confirmation* stage the individual decides to continue the full use of the innovation.

Rogers also defines five categories of adopters. *Innovators* are the first individuals to adopt an innovation and they are willing to take risks. The second fastest group who adopt an innovation is called *early adopters. Early majority* represents those who adopt an innovation after a varying degree of time, which is significantly longer than the first two groups. *Late majority* represents the group that adopts an innovation after the average member of the society. Finally, *laggards* are the last who adopt an innovation.

Rogers furthermore presents five characteristics of an innovation. The *relative advantage* is the degree to which the new technology is better than a preceding one. *Compatibility* is the consistency with existing values, past experiences and needs. *Complexity* is the difficulty of understanding and use. A new technology is more likely to be adopted if it is compatible with existing practices of adopters, and is relatively easy to understand and use. *Trialability* is the degree to which it can be experimented with on a limited basis. Finally, *observability* is the visibility of its results.

The diffusion phenomenon has also been studied from a community point of view, focused on the economic value an innovation brings to potential adopters. This economic value to an adopter depends on the size of the existing network of adopters and the potential network of adopters. Katz and Shapiro [11] analyze the adoption of a new technology for cases where *network externalities* are significant. Adoption becomes more likely when the number of current adopters in the network increases.

There are also some other concepts mentioned by Katz and Shapiro that influence adoption of a new technology, i.e. the *development of a related technology infrastructure, economies of scale, communication channels* which could also help the process of diffusion of innovation, the presence of *sponsorship* which decreases the risk of adoption, etc. Hence, despite the fact that a new technology is considered to be superior to the incumbent, an adopter may still not adopt the innovation. For example, adopters may be unwilling to bear the incompatibility cost and the risk of being locked into the innovation before it reaches critical mass.

Last but not least, *information asymmetry* could lead to different incentives and strategic behaviors in the technology adoption game. In particular, Zhu and Weyant [16] present how asymmetric information affects firms' decisions to adopt a new technology, by using game theory. In particular, the authors compare two information structures under which two competing firms have asymmetric information about the future performance of the new technology. Zhu and Weyant conclude that equilibrium strategies under asymmetric information conditions are quite different from those under symmetric information conditions.

The theories presented above have mainly been used for studying the adoption of consumer products. However, the adoption of new Internet protocols and services, such as those developed within the CREDENTIAL project, is more complex than that of consumer products, and therefore requires more elaborated modeling. Several attempts have been made at studying the adoption of new Internet protocols and services.

In particular, the IAB has identified the most important factors that enhance or limit the success of a protocol based on several case studies [15]. Although a protocol design will not necessarily be able to incorporate all the proposed success factors, experience indicates that following some of them will improve the probability of success. The most important factors for the initial success are *filling a real need* and *being incrementally deployable*.

Hovav et al. [8] present a model of Internet standards adoption that identifies additional factors that influence adoption of a new technology, focused on the IPv6 protocol. *Development of a related technology infrastructure, economies of scale* and *amount of information available* could also help a new protocol to spread. Moreover, the presence of *sponsorship* will decrease the risk of adoption, and thus could positively influence the adoption rate and adoption extent of the new protocol.

In the study by Joseph et al. [9], an economic model based on *users' utility* is used to study the adoption of new network protocols and services. The model incorporates various factors, such as *user and network benefits*, and *switching costs*, and discusses the *impact of converters* on the adoption of new Internet protocols and services. Key findings include that new Internet protocols and services need to withstand a period of decreasing total system utility till a *critical mass* of users is reached.

Technology Acceptance Model (TAM) has also gained more popularity within the information systems community. TAM was first proposed by F. D. Davis [6] in his pioneering work in this domain. According to TAM, users' actual use of a given technology is influenced directly or indirectly by the user's behavioral intentions, attitude, perceived usefulness of the system, and its perceived ease of use. TAM was developed in further versions which elaborate what external factors affect intention and actual use through mediated effects on perceived usefulness and perceived ease of use. TAM provides a basis with which one traces how external variables influence belief, attitude, and intention to use of a given technology.

The aforementioned models could improve our understanding, as well as guide the design and implementation – and even the presentation – of mechanisms enhancing the adoption of the CREDENTIAL services. The stages Rogers speaks of are naturally initially met by communication activities. The CREDENTIAL project includes a work package especially designed for this, and there is an advisory board that helps tuning the communication for a good reception among a variety of stakeholders in the European Union. Also activities within the three pilots mentioned in Section 5 facilitates awareness-raising within their sectors and also makes trialability and observability possible.

At the same time it is necessary to understand that the stage of *decision* is not reached without a mix of the factors mentioned by Rogers and the other authors appearing as favorable to each potential adopter. The mix may differ from one group of stakeholder to another. The adoption of protocols will take different courses and can be severely hindered if there are not easy steps where the CREDENTIAL technology can be first implemented. The eGovernment and eBusiness pilots show how it can be deployed within existing infrastructures where citizens and public authorities can adopt it within existing processes while at the same time gain a potential for an increased digitization of these activities, leading to an economy of scale.

Thus, individual partners in the CREDENTIAL project have expressed specific ideas for adoption condition. Klughammer, active in the eHealth pilot, explains that clinics have to adopt first, then it easy to get patients to adopt, but the other way will not work. The argument comes from experience in telemedicine: people do not use telemedicine software when they are healthy or very sick. Rather, patients who are willing to use telemedicine are those who have a chronic disease. This is one reason why CREDENTIAL selected a Diabetes Use Case. But even when there are patients with chronic diseases they need some kind of incentive to use telemedicine. These incentives have to be provided by somebody. That could be the practitioner, the clinic or the health insurance. Incentives can be of various kinds: less traveling which saves time and money, better diagnosis, better treatment, or simply being reimbursed by the health insurance when taking part in such a project. Thus questions of sponsorship also affects switching costs, incremental deployment, among other factors. This demonstrates the sectors-specific nature of the mix of factors that influence adoption.

Table 1 provides a concise overview of the most important benefits that users can expect from the tools and technologies developed within CREDENTIAL, in order to highlight what system-related features may influence usersfi adoption incentives. In [2, Section 6] there are several literature reviews of uptake (or lack thereof) of different technologies.

7 CONCLUSIONS AND FUTURE WORK

The main goal of the CREDENTIAL project is to develop a privacy-preserving data sharing platform with integrated identity provider, which can be used to share authenticated data without the wallet learning any of the user's personal information. This paper concentrates on the adoption of CREDENTIAL by service providers and end-users: Firstly, we described the main functionalities of the CREDENTIAL system, as well as the overall logical and physical architecture. Secondly, we investigated potential factors that could boost CREDENTIAL's adoption and considered them in a list of concrete benefits that may serve as convincing arguments.

In future work, the functionality and added-value of these services will be showcased by concrete pilots from the domains of

Selective disclosure	Users have full control over which data should be revealed to which service provider. These rights can be adjusted dynamically and are enforced on a technical (not a policy) level.
Authentic data sharing	Users can share authentic (i.e., signed) documents with other users or stakeholders, while still being able to redact predefined parts of those documents without invalidating the signature. This puts back users into control over which data they want to reveal to whom also in the data sharing scenario.
Maximum cloudification	A personal device holding secret cryptographic key material is only needed when initially granting rights to a new service provider or data receiver. All other actions can be done fully only without requiring physical access to a personal device.
End-to-end confidentiality	The confidentiality of the user's data is guaranteed at any point in time. That is, the central CREDENTIAL Wallet is technically unable to learn the data stored in the Wallet, while the intended receiver in every interaction can do so.
Metadata privacy	Any two actions taken by a user are unlinkable even by colluding service providers if not intended otherwise by the user. In its final maturity level, the user's actions could even be widely hidden from the Wallet.
Platform independence	Even though only prototyped on Android systems, all developed libraries could also be ported to other operating systems and hardware settings. This way, a hardware vendor lock-in can be avoided.
Personal data safe	The Wallet can be used as a highly secure personal data and identity safe because of its high security and privacy guarantees.
Strong authentication	Due to strong 2FA methods (including, e.g., passwords, biometrics, secure devices, etc.), the risk of unauthorized access to the Wallet can be minimized.
Interoperability	Interoperability with existing authentication schemes like OAuth, etc. simplifies the integration into existing IAM solutions.

Table 1: Benefits of the CREDENTIAL Wallet solution [2]

eGovernment, eHealth, and eBusiness, which are currently under deployment. The CREDENTIAL Cloud Wallet has distinct features that may affect its adoption by end users. Our future work will also include mapping these features into acceptance factors to explain how the technology is perceived.

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.

REFERENCES

[1] Andreas Abraham, Jörg Caumanns, Enrico Francescato, Felix Hörandner, Elias Klughammer, Stephan Krenn, Thomas Lorünser, Andrea Migliavacca, Silvana Mura, Franco Nieddu, Nicolas Notario McDonnell, Christoph Rabensteiner, Simon Roth, Jetzabel Serna, Christoph Striecks, Florian Thiemer, Alberto Zanini, and Bernd Zwattendorfer. 2017. Assessment Report on Cryptographic Technologies, Protocols and Mechanisms. CREDENTIAL Deliverable D4.1. (2017).

[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. 2017. UI Prototypes v1. CREDENTIAL Deliverable D3.1. (2017).

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

[4] Nikolas Bompetsis, Jörg Caumanns, Pasquale Chiaro, Enrico Francescato, Agi Karyda, Alexandros Kostopoulos, Stephan Krenn, Andrea Migliavacca, Juan Carlos Pérez Baún, Luigi Rizzo, Anna E. Schmaus-Klughammer, Evangelos Sfakianakis, Florian Thiemer, and Alberto Zanini. 2017. Pilot Use Case Specification. CREDENTIAL Deliverable D6.1. (2017).

[5] CREDENTIAL. 2017. CREDENTIAL Secure Cloud Identity Wallet. https://credential.eu. (2017).

[6] Fred D. Davis. 1989. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly* 13, 3 (1989), 319–340.

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

[8] Anat Hovav, Ravi Patnayakuni, and David Schuff. 2004. A model of Internet standards adoption: the case of IPv6. *Inf. Syst. J.* 14, 3 (2004), 265–294.

[9] Dilip Antony Joseph, Nikhil Shetty, John Chuang, and Ion Stoica. 2007. Modeling the adoption of new network architectures. In *CoNEXT 2007*, Jim Kurose and Henning Schulzrinne (Eds.). ACM, 5.

[10] Farzaneh Karegar, Christoph Striecks, Stephan Krenn, Felix Hörandner, Thomas Lorünser, and Simone Fischer-Hübner. 2016. 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.

[11] M. Katz and C. Shapiro. 1986. Technology Adoption in the Presence of Network Externalities. *Journal of Political Economics* 94 (1986), 822–84.

[12] Nicolás Notario, Stephan Krenn, Bernd Zwattendorfer, and Felix Hörandner. 2016. CREDENTIAL: Secure Cloud Identity Wallet. *ERCIM News* 2016, 106 (2016).

[13] Everett M. Rogers. 2003. *Diffusion of innovations (5. ed.).* Free Press.

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

[15] D. Thaler and B. Aboba. 2008. What Makes for a Successful Protocol? RFC 5218. (2008).

[16] Kevin Zhu and John Weyant. 2003. Strategic Decisions of New Technology Adoption under Asymmetric Information: A Game-Theoretic Model. *Decision Sciences* 34, 4 (2003), 643–675.

[17] Bernd Zwattendorfer, Stephan Krenn, and Thomas Lorünser. 2016. Secure and Privacy-Preserving Identity Management in the Cloud. *ERCIM News* 2016, 104 (2016).