# Privacy-Preserving Identity Management and Applications to Academic Degree Verification

Jorge Bernal Bernabe, Jesús García-Rodríguez, Stephan Krenn, Vasia Liagkou, Antonio Skarmeta, Rafael Torres

# Privacy-Preserving Identity Management and Applications to Academic Degree Verification*

Jorge Bernal Bernabe[1], Jesús García-Rodríguez[1], Stephan Krenn[2], Vasia Liagkou[3], Antonio Skarmeta[1], and Rafael Torres[1]

University of Murcia, Murcia, Spain
{jorgebernal,jesus.garcia15,skarmeta,rtorres}@um.es
AIT Austrian Institute of Technology, Vienna, Austria
stephan.krenn@ait.ac.at
Computer Technology Institute and Press "Diophantus", Patras, Greece
liagkou@cti.gr

**Abstract.** This paper summarizes the contents and presentations held at a workshop at the IFIP Summer School on Privacy and Identity Management 2021, focusing on privacy-preserving identity management. In this document, we first introduce the necessary background on privacy-preserving identity management, including core cryptographic concepts. We then present a demonstrator scenario which benefits from the use of such technologies. Finally, we present a distributed privacy-preserving identity management framework offering an even higher level of security and privacy than previous work.

**Keywords:** attributed-based credentials · privacy-preserving identity management · workshop

## 1 Introduction

Attribute-based credential systems, or *ABC-systems*, allow for strong yet privacy-preserving user authentication. In such a system, *users* can receive digital certificates (*credentials*) on pieces of the personal information (*attributes*) from an *issuer*. Such personal information may, for instance, include a user's first name, surname, nationality, or date of birth. A user can now use a credential to prove to a *verifier* that it possesses certain attributes, without the need to reveal more information than what is absolutely necessary. For instance, a verifier might require that a user has a specific age, e.g., in order to receive an age discount. The user can now selectively reveal only her date of birth to the verifier, while keeping all other identifying information private, in a way that guarantees to the verifier that the revealed date of birth had indeed been certified by the issuer. Even more, certain schemes even allow a user to prove predicates over her attributes, e.g., allowing her to prove that she is older than 65 years, without revealing the precise birth date, thereby further increasing the privacy level.

* Authors are listed in alphabetical order, cf. https://www.ams.org/profession/leaders/CultureStatement04.pdf.

Attribute-based credential systems have initially been envisioned by Chaum almost 40 years ago [12,13], and have received significant attention since then, resulting in a variety of different schemes, supporting different functionalities. The most widely known solutions are Microsoft's UProve [6,25] and IBM's Identity Mixer [7,9,10]. However, a large body of related work has been carried out over the last decades, including formal frameworks for ABCs [8], schemes allowing users to anonymously delegate parts of their rights to other users [2,3,11,14], issuer-hiding credential schemes allowing user to remain anonymous across multiple issuers [4], ABC systems with distributed issuers [18,32], ABCs bound to hardware tokens [1], cloud-based ABCs [21,23], or distance-bounding schemes [5].

Furthermore, ABC systems have been analyzed in the context of various application scenarios, including car rental [7], vehicular ad-hoc networks (VANETs) [17], ticketing systems [22], eHealth [26], or course evaluation in high schools [24,31].

*Outline.* The structure of this paper also follows the structure of the workshop held at the IFIP Summer School. In Section 2, we will introduce the fundamental concepts and cryptographic background of attribute-based credential systems to give an intuition on how such schemes work. In Section 3, we then introduce a demonstration scenario in the educational context, and present results from an initial user study carried out within the CyberSec4Europe project. Then, in Section 4, we introduce the OLYMPUS framework for distributed privacy-preserving identity management. We finally conclude in Section 5.

## 2 Concepts and Technologies

In this section, we will first introduce the basic processes and security and privacy properties of an ABC system, and then introduce the cryptographic building blocks from which such schemes can be built, and provide the basic intuition of the construction underlying most such schemes.

### 2.1 Entities and Processes

Figure 1 gives an overview of the different types of entities in an attribute-based credential system. The different processes in such a scheme can be described as follows:

**Key generation.** In a first step, all parties may generate local key material such as digital signature keys or encryption keys, depending on their role in the system. In most existing instantiations of ABC systems, in particular verifiers do not have a need for cryptographic keys.

**Issuance.** In the issuance phase, users may request certificates on personal attributes. Depending on the specific scenario, the issuer may certify arbitrary, self-claimed attributes, or perform rigorous validations, e.g., requiring in-person checks at an authority. After having agreed on the attributes to be certified, the user and the issuer engage in a potentially interactive protocol, at the end of which the user obtains a credential.

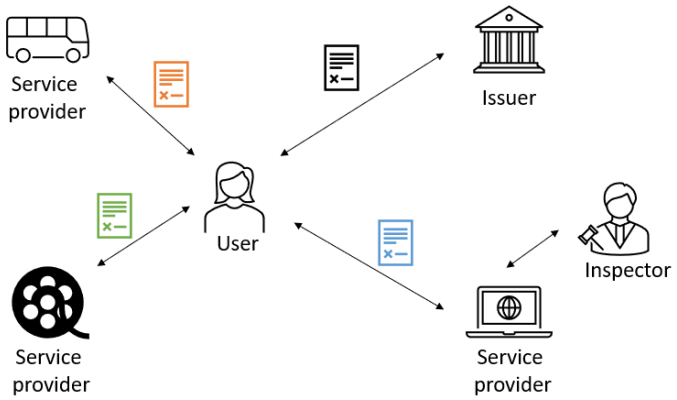


**Fig. 1.** Overview of entities in an ABC system.

**Presentation.** In order to authenticate towards a service provider (also known as relying party or verifier), the user and the service provider agree on a so-called *presentation policy*, which, among others, defines the issuer accepted by the service provider, as well as the attributes to be revealed. The user then derives a *presentation-token* from her credential which she sends to the service provider, who may now decide to accept or reject the user's presentation.

While these processes exist in any ABC system, also the following steps are available in many schemes found in the literature:

**Inspection.** In order to prevent abuse of anonymous authentication, a predefined party, known as *inspector*, may open presentation tokens, thereby revoking the user's anonymity. The inspector can then compute a cryptographic proof that a given presentation token was issued by a specific user. The rules under which the inspector may be contacted by a service provider need to be agreed upfront with the user.

**Revocation.** Upon abuse, loss, or theft of a credential, different entities in the system may request revocation of a given credential, in which case any future attempt to authenticate using the given credential will let the service provider reject the presentation token.

Furthermore, additional processes and features can be found in the literature, including, e.g., advanced issuance, where attributes can be carried over from one credential to another without the issuer learning anything about the attribute, except for the fact that it was already including in a previous credential belonging to the same user.

### 2.2 Security and Privacy Goals

In the following, we provide informal descriptions of the security goals that need to be achieved by an ABC system. For formal definitions, we refer to the original literature, e.g., Camenisch et al. [8].

**Correctness.** This property requires that the ABC system functions as intended. That is, if all parties behave honestly during the key generation and issuance phases, a user will always be able to derive a presentation token for a given presentation policy, which will be accepted by the service provider.

**Unforgeability.** Intuitively, this property requires that no user is able to derive a valid presentation token for a given presentation policy, unless she has previously obtained a credential satisfying the presentation policy from the issuer. A bit more formally, we assume that an adversary may request arbitrary credentials on attributes of his choice, and also request arbitrary presentation tokens from other users, e.g., by taking the role of a corrupted service provider. Eventually, the adversary outputs a presentation token for a presentation policy of his choice. We now say that an ABC scheme is unforgeable, if the adversary is unable to generate a valid presentation token, if none of the obtained credentials satisfies the policy. Note that this notion of unforgeability implicitly also covers replay attacks.

In the case that the ABC system supports revocation, the adversary may decide which credentials to revoke, and also succeeds with a forgery if he only knows revoked credentials satisfying the given presentation policy.

**Privacy.** Privacy in an ABC system covers multiple flavours. Firstly, privacy guarantees that the service provider does not gain any information about undisclosed attributes. Secondly, it requires that even if the service provider and the issuer collude or are controlled by the same entity, they will not be able to re-identify the user, i.e., it is infeasible to link issuance and presentation sessions, except by the information explicitly disclosed during these phases. Finally, privacy guarantees unlinkability of different presentation sessions by the same user. That is, a service provider cannot distinguish two presentation tokens from the same user from two presentation tokens computed by different users, as long as the attributes revealed during presentation are the same for these two users.

Note that this latter property is not available in all ABC systems such as, e.g., UProve [6,25], where presentations of the same credentials can be linked and thus privacy is only guaranteed if credentials are only used once.

Besides these mandatory requirements, many ABC systems also give additional security guarantees. For instance in the case of inspection, non-frameability guarantees that no set of colluding users, issuers, and inspectors, are able to generate a presentation token which, when opened by the inspector, will link to a certain user outside this set. However, a detailed description of these advanced properties is beyond the scope of this workshop summary.

### 2.3 Cryptographic Building Blocks

In the following we briefly describe the two central cryptographic primitives that are typically being used when constructing ABC systems, and give some intuition how such systems are often constructed.

**Digital signatures.** A digital signature scheme [20] is a cryptographic mechanism for ensuring the integrity and authenticity of a message. To do so, a signer generates runs a key generation algorithm, obtaining a secret and a public key. Using the secret key, the signer can now compute signatures on arbitrary messages, which can then be validated by a verifier using the signer's public key.

The unforgeability property of a signature scheme ensures that no adversary, having seen arbitrarily many signatures on messages of his choice, may come up with a valid signature on a previously unsigned message. Sometimes, a stronger notion of unforgeability is needed, requiring that the adversary cannot generate generate fresh signatures on previously signed messages either.

**Zero-knowledge proofs of knowledge.** A zero-knowledge proof of knowledge [11, 16, 19, 27] is a cryptographic protocol which allows a prover to convince a verifier that she knows a secret piece of information, without revealing anything more than what is already revealed by the statement itself. For instance, the prover may prove that she knows $x$ such that $y = g^x$ in some cyclic group where the discrete logarithm problem is hard, without revealing any information about $x$. In the context of ABC systems, we usually consider non-interactive zero-knowledge proofs, where the prover locally computes a proof, and sends it to the verifier, without the need for additional communication rounds.

The intuition behind many ABC systems, including, e.g., [4, 7, 9, 10], is now as follows. In the key generation phase, the issuer generates a key pair for a digital signature scheme. Upon issuance, the user and the issuer agree on a set of attributes $(a_1, \ldots, a_n)$, and the issuer computes a digital signature $\sigma$ on $(a_1, \ldots, a_n)$. When computing a presentation token which discloses attributes $(a_i)_{i \in D}$, the user derives a zero-knowledge proof of knowledge $\pi$, proving that she knows a digital signature $\sigma$ on $(a_1, \ldots, a_n)$, while keeping $\sigma$ and $(a_i)_{i \notin D}$ private. The service provider then simply checks the validity of the zero-knowledge proof.

To add inspection, the inspector computes a key pair for a public key encryption scheme. Upon issuance, a unique user identifier is embedded as an additional attribute $a_{n+1}$, and the presentation token is enhanced as follows: the user computes a ciphertext $c$, and then generates a proof $\pi$ showing that the user knows a signature $\sigma$ on $(a_1, \ldots, a_n, a_{n+1})$, such that $a_{n+1}$ is also contained in $c$; again, all information except for $(a_i)_{i \in D}$ are kept private.

Similarly, for revocation, on possibility is to embed a revocation handle as attribute $a_{n+2}$, and let the revocation authority publish a list of revoked attributes. The user can then extend the proof $\pi$ to additionally show that the revocation handle embedded in her credential is not contained in the given list. For details on constructions, we refer to the original literature.

## 3 Demonstration Case and Piloting Results

In this section, we will now introduce the concrete use case which is currently under ongoing development within the H2020 CyberSec4Europe project[1], and present feedback from an initial user study which. While we only give a high-level summary here, we refer to the full reports for more details [28–30].

### 3.1 Demonstrator Background and Specification

In the early 2010s, a number of forged university degrees among civil servants was identified in Greece [15], where companies sold "degrees" on the Internet without requiring the buyer to do anything more than pay a fee. One way to combat this fraud could be the use of digital university certificates, which provide formal and tamper-proof proof of the courses taken and degrees obtained by a student. Motivated by the aforementioned incidents, the aim of this demonstrator within the H2020 CyberSec4Europe project is therefore to develop a platform that allows attribute-based credentials to be obtained from the university when passing an exam or obtaining a degree. These credentials can then be used in various scenarios, some of which are being developed as demonstrators within the project.

For example, when applicants apply for a PhD position at a university, they need to prove that they have certain degrees (e.g. a Bachelor's or Master's degree in a relevant field) and have taken certain courses to meet the formal requirements. To ensure the impartiality of the process at later stages, applicants may only want to prove that they meet the requirements, but not disclose any other sensitive information. For example, to avoid discrimination on the basis of age or gender, the applicant may wish to disclose their degree but not their full name, date of birth or the date on which the degree was issued; similarly, other forms of discrimination can be avoided by, for example, concealing the university that awarded the degree. Similar needs may arise when applying for a job where certain academic requirements must be met. Again, applicants may wish to withhold certain information, at least during the initial formal assessment of suitability, and only disclose it if invited. This also reduces the risk for the employer, as it never collects sensitive information about unsuccessful applicants, which could then be shared in the event of a data breach. Finally, anonymous credentials can also be useful, e.g., to prove to a public authority that courses have been taken with a sufficient number of ECTS credits to receive certain types of study allowance. However, again, it is not necessary to disclose the exact courses, grades, or number of ECTS credits taken.

### 3.2 The CyberSec4Europe Demonstrator

On a high level, the architecture chosen for the CyberSec4Europe demonstrator follows a natural approach, as can be seen in Figure 2. The university serves as

[1] https://cybersec4europe.eu

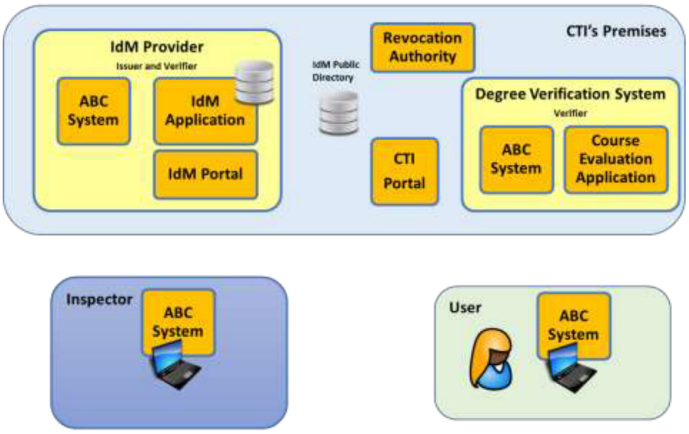


**Fig. 2.** High-level overview of the CyberSec4Europe architecture.

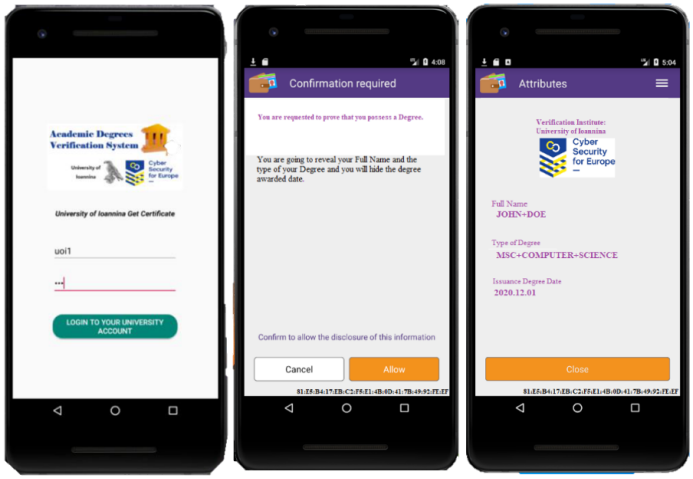


**Fig. 3.** Impressions of the graphical user interface.

the identity provider, and employs all components necessary for issuing credentials to a user, who locally stores the received credentials. The Degree Verification System, as part of the job application portal, will later verify all presentation tokens received from a user during an application process. The inspector has currently not been implemented yet within our demonstrator, but will be located in a separate entity, which may or may not be controlled by the issuer.

On the user side, a mobile app was implemented, which allows the user to obtain and manage her credentials, and which can be used to derive presentation tokens when revealing sensitive information to a service provider. Some impressions of this application are given in Figure 3.

### 3.3 Evaluation Phase

In a first piloting round, the developed pilot was tested with 42 participants with different backgrounds (i.e., BSc and MSc candidates) to give feedback regarding usability, perceived privacy, etc. The participants had mainly computer science related backgrounds, however, without a special focus on cyber security. Future versions of the demonstrator case will also seek for feedback from participants with other backgrounds. About 67% of the participants were male and 33% were female. The age ranged from 22 years to 35 years, with an average of 28 years.

After an introduction to the technology and the demonstrator scenario, the participants were requested to perform a variety of tasks, such as obtaining digital credentials, and applying for a PhD position at the university. Subsequently, the participants were asked to answer a questionnaire which was divided into three main blocks:

- The first set of questions aimed to understand whether the overall setup of the demonstrator was easy to understand, and whether the tasks where clearly communicated and explained to the students. Furthermore, we aimed at finding out whether from an efficiency and usability point of view, the developed solutions were acceptable.
- The second set of questions aimed at understanding whether participants understood the privacy guarantees of the developed solution. Furthermore, we tried to find out whether participants are willing to trust such solutions, and whether they understand the added value of the technology for the specific use case, but also in general.
- Finally, we asked whether it was clearly understood which attributes were actually revealed to the job application portal, and whether participants see the potential benefit in increasing compliance of service providers using privacy-enhancing identity management systems, in order to comply with legal regulations such as the GDPR.

On a high level, the feedback received from participants was positive, however showing slight biases, e.g., depending on the participants' background and age, which will be further addressed in the next revision of the demonstrator case. For detailed evaluation result, we refer to Sforzin and Bobba [30].

## 4 The OLYMPUS Framework

In this section, we give an overview on the identity management solution developed in the H2020 OLYMPUS project[2], and how it is applied to the use case that we are reviewing. This solution aims to offer advanced Single Sign (SSO) capabilities with special attention to privacy aspects. Concretely, the main focus is addressing the issues that traditional SSO solutions have in that respect, that mostly are caused by the fully trusted Identity Provider (IdP) that becomes a single point of failure:

[2] olympus-project.eu/

- A compromised (or malicious) IdP can impersonate users, gaining full access to all their accounts and personal data. Also, the user's login credentials are jeopardized.
- A compromised (or malicious) IdP can forge identities, effectively bypassing access control mechanisms of service providers that trust the IdP for authentication.
- The IdP can track user behaviour, learning about which services the user interacts with and when they do it.

To tackle the root of the problem, the OLYMPUS identity management system distributes the task of the IdP among several partial identity providers. As the collaboration of all of them is necessary for performing their role, compromising one (or even all but one) identity provider is not enough to gain control over the system and carry out the aforementioned attacks. Apart from this, novel cryptographic mechanisms are applied to further mitigate the security risks and to boost user privacy and their control over their identity. As general and different scenarios as possible: minimizing hardware requirements, two complementary approaches, compatible (as much as possible) with standards and traditional technologies. Also, user-friendly (as it is a common issue of cryptographic approaches).

- Minimizing the requirements on user hardware, offering user-friendly authentication using passwords without requiring trusted hardware or software.
- A novel system compatible with traditional technologies that respects users' privacy while remaining user-friendly is obtained

The OLYMPUS solution is completely open-source, and can be found in the project's public repository[3]. There, you can find all the necessary code to deploy your own identity providers, as well as the library code for clients and verifiers. The project's documentation is linked within the repository, but you can also start to get used to the code base and its concepts through a guided use case demonstration available in a separate repository[4].

### 4.1 OLYMPUS architecture and roles

The ecosystem of the OLYMPUS identity management system (overview in Figure 4, more details in [32]) involves three main participants: the virtual Identity Provider (vIdP), the user client and the relying party (RP).

**Virtual IdP** : It is a set of entities (partial IdPs) that collaborate to perform the role of identity provider. Each partial IdP has three modules for the main functionalities:
  - Distributed authentication: account management and user login through password verification (and potentially multi-factor authentication). It is also a key component in the enrolment process, in which attributes from trusted external attribute providers are linked to the account.

[3] https://bitbucket.alexandra.dk/projects/OL/repos/olympus-identity/
[4] https://bitbucket.alexandra.dk/projects/OL/repos/usecase-3/

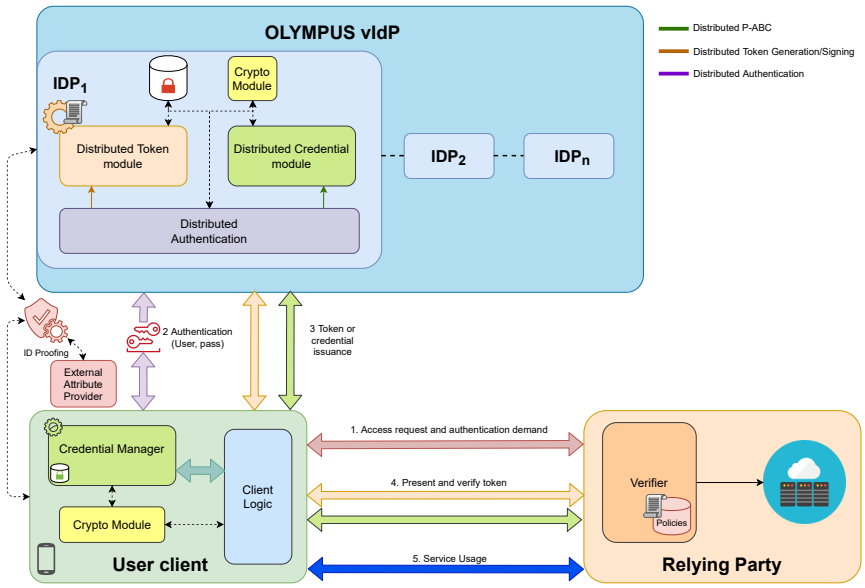


**Fig. 4.** Simplified version of the OLYMPUS architecture.

- Distributed credential module: Generates credential shares for the distributed p-ABC scheme. Each share is generated independently by each partial IdP (i.e., no communication or explicit collaboration is needed during the process).
- Distributed token module: Generates token shares (RSA-like signature shares), which are part of the OLYMPUS "online" approach, leveraging PESTO.

**User client** : Provides common identity functionalities (registration, authentication, managing attributes...), abstracting from the distributed nature of the IdP. Apart from application logic and flows, it is in charge of cryptographic operations (like combination of signature shares) and secure management of credentials.

**Relying party** : Accepts OLYMPUS tokens (PESTO or p-ABC) for user authentication in order to perform attribute-based access control. The relying party will define and communicate policies that must be fulfilled for granting access (e.g., being over 18 or revealing the user's name).

### 4.2 Application to the Use Case

The OLYMPUS virtual IdP is a great asset for ensuring privacy preservation for end users in the university use case. In particular, the p-ABC approach can be used to replace the Idemix [7] credentials used in the first-phase pi-

lot, taking advantage of the improvements of OLYMPUS as an identity management system. More concretely, the p-ABC used in OLYMPUS is based on Pointcheval-Sanders multi-signatures (PS-MS), which are more efficient than the Camenisch-Lysyanskaya (CL) signatures used in Idemix. Additionally, PS-MS allow distributed issuance and the setup phase for the cryptography can be done independently by each partial identity provider. With the distribution of the IdP, we gain security against impersonation and forgery attacks. What is more, partial IdPs can be controlled by different legal entities, which leads to more beneficial conditions in terms of privacy and data control from the viewpoint of regulations like GDPR. However, it is true that deployment and management of the group of IdPs becomes more complex, especially in the case where multiple legal entities are involved, as agreements and contracts must be reached. Apart from the direct benefits of using the distributed scheme, the OLYMPUS infrastructure brings other technical advantages. First, it offers user-friendly account management and authentication, giving users familiar options like passwords and two-factor authentication. Also, the implementation is being integrated with W3C Verifiable Credentials specification, an emerging standard for representing digital credential, which encourages interoperability and adoption. However, Idemix has some functionalities that can be useful depending on the use case and are not supported by the current OLYMPUS implementation.

- Blind issuance, where the issuer does not learn user attributes but only commitments over them (blindly signs them).
- Other proof types, like (non)-membership.
- Credential revocation and inspection

Nevertheless, following a modular approach these functionalities are also technically possible (some theoretical work has already been done in this direction) using the OLYMPUS tools.

## 5 Conclusion and Future Work

In this workshop, we presented the conceptual foundations of privacy-preserving identity management solutions. We then presented a concrete application scenario in the educational domain which is currently under development within the H2020 CyberSec4Europe project. We presented first evaluation results, and ongoing developments based on the results of the H2020 OLYMPUS project, which can achieve additional security and privacy guarantees compared to the previous iteration.

Using the synergies of these two projects not only allows us to enhance the demonstration case within CyberSec4Europe, but also improves and evolves the OLYMPUS identity management system with new capabilities. First, we aim to establish a trusted public information framework for IdPs, users and relying parties based on Distributed Ledger Technologies (first approximation can be found in [33]). In addition, we are working on adding new functionalities to the framework, enabling fine-grained credential revocation and adding support for credential inspection.

**Acknowledgements.** The work leading to this workshop was funded by the European Union under the H2020 Programme Grant Agreement No. 830929 (CyberSec4Europe) and No. 786725 (OLYMPUS).

## References

1. Baldimtsi, F., Camenisch, J., Hanzlik, L., Krenn, S., Lehmann, A., Neven, G.: Recovering lost device-bound credentials. In: Malkin, T., Kolesnikov, V., Lewko, A.B., Polychronakis, M. (eds.) Applied Cryptography and Network Security - 13th International Conference, ACNS 2015, New York, NY, USA, June 2-5, 2015, Revised Selected Papers. Lecture Notes in Computer Science, vol. 9092, pp. 307–327. Springer (2015), https://doi.org/10.1007/978-3-319-28166-7_15
2. Belenkiy, M., Camenisch, J., Chase, M., Kohlweiss, M., Lysyanskaya, A., Shacham, H.: Randomizable proofs and delegatable anonymous credentials. In: Halevi, S. (ed.) Advances in Cryptology - CRYPTO 2009. Lecture Notes in Computer Science, vol. 5677, pp. 108–125. Springer (2009), https://doi.org/10.1007/978-3-642-03356-8_7
3. Blömer, J., Bobolz, J.: Delegatable attribute-based anonymous credentials from dynamically malleable signatures. In: Preneel, B., Vercauteren, F. (eds.) Applied Cryptography and Network Security - ACNS 2018. Lecture Notes in Computer Science, vol. 10892, pp. 221–239. Springer (2018), https://doi.org/10.1007/978-3-319-93387-0_12
4. Bobolz, J., Eidens, F., Krenn, S., Ramacher, S., Samelin, K.: Issuer-hiding attribute-based credentials. In: Conti, M., Stevens, M., Krenn, S. (eds.) Cryptology and Network Security - CANS 2021. Lecture Notes in Computer Science, Springer (2021), (to appear)
5. Bosk, D., Bouget, S., Buchegger, S.: Distance-bounding, privacy-preserving attribute-based credentials. In: Krenn, S., Shulman, H., Vaudenay, S. (eds.) Cryptology and Network Security - CANS 2020. Lecture Notes in Computer Science, vol. 12579, pp. 147–166. Springer (2020), https://doi.org/10.1007/978-3-030-65411-5_8
6. Brands, S.: Rethinking Public Key Infrastructure and Digital Certificates – Buildingin Privacy. Ph.D. thesis, Eindhoven Institute of Technology (1999)
7. Camenisch, J., Herreweghen, E.V.: Design and implementation of the *idemix* anonymous credential system. In: Atluri, V. (ed.) ACM Conference on Computer and Communications Security - CCS 2002. pp. 21–30. ACM (2002), https://doi.org/10.1145/586110.586114
8. Camenisch, J., Krenn, S., Lehmann, A., Mikkelsen, G.L., Neven, G., Pedersen, M.Ø.: Formal treatment of privacy-enhancing credential systems. In: Dunkelman, O., Keliher, L. (eds.) Selected Areas in Cryptography - SAC 2015. Lecture Notes in Computer Science, vol. 9566, pp. 3–24. Springer (2015), https://doi.org/10.1007/978-3-319-31301-6_1
9. Camenisch, J., Lysyanskaya, A.: A signature scheme with efficient protocols. In: Cimato, S., Galdi, C., Persiano, G. (eds.) Security in Communication Networks, Third International Conference - SCN 2002. vol. 2576, pp. 268–289. Springer (2002), https://doi.org/10.1007/3-540-36413-7_20
10. Camenisch, J., Lysyanskaya, A.: Signature schemes and anonymous credentials from bilinear maps. In: Franklin, M.K. (ed.) Advances in Cryptology - CRYPTO 2004. Lecture Notes in Computer Science, vol. 3152, pp. 56–72. Springer (2004), https://doi.org/10.1007/978-3-540-28628-8_4

11. Chase, M., Lysyanskaya, A.: On signatures of knowledge. In: Dwork, C. (ed.) Advances in Cryptology - CRYPTO 2006. Lecture Notes in Computer Science, vol. 4117, pp. 78–96. Springer (2006), https://doi.org/10.1007/11818175_5
12. Chaum, D.: Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM **24**(2), 84–88 (1981), http://doi.acm.org/10.1145/358549.358563
13. Chaum, D.: Security without identification: Transaction systems to make big brother obsolete. Commun. ACM **28**(10), 1030–1044 (1985), https://doi.org/10.1145/4372.4373
14. Crites, E.C., Lysyanskaya, A.: Delegatable anonymous credentials from mercurial signatures. In: Matsui, M. (ed.) Topics in Cryptology - CT-RSA 2019. Lecture Notes in Computer Science, vol. 11405, pp. 535–555. Springer (2019), https://doi.org/10.1007/978-3-030-12612-4_27
15. ekathimerini.com: Minister admits number of civil servants with forged degrees was exaggerated (2013), https://www.ekathimerini.com/news/154846/minister-admits-number-of-civil-servants-with-forged-degrees-was-exaggerated/
16. Fiat, A., Shamir, A.: How to prove yourself: Practical solutions to identification and signature problems. In: Odlyzko, A.M. (ed.) Advances in Cryptology - CRYPTO '86. Lecture Notes in Computer Science, vol. 263, pp. 186–194. Springer (1986), https://doi.org/10.1007/3-540-47721-7_12
17. de Fuentes, J.M., González-Manzano, L., Serna-Olvera, J., Veseli, F.: Assessment of attribute-based credentials for privacy-preserving road traffic services in smart cities. Pers. Ubiquitous Comput. **21**(5), 869–891 (2017), https://doi.org/10.1007/s00779-017-1057-6
18. García-Rodríguez, J., Torres Moreno, R., Bernal Bernabe, J., Skarmeta, A.: Implementation and evaluation of a privacy-preserving distributed abc scheme based on multi-signatures. Journal of Information Security and Applications **62**, 102971 (2021), https://www.sciencedirect.com/science/article/pii/S2214212621001824
19. Goldwasser, S., Micali, S., Rackoff, C.: The knowledge complexity of interactive proof-systems (extended abstract). In: Sedgewick, R. (ed.) ACM Symposium on Theory of Computing - STOC '85. pp. 291–304. ACM (1985), https://doi.org/10.1145/22145.22178
20. Goldwasser, S., Micali, S., Rivest, R.L.: A digital signature scheme secure against adaptive chosen-message attacks. SIAM J. Comput. **17**(2), 281–308 (1988), https://doi.org/10.1137/0217017
21. Haböck, U., Krenn, S.: Breaking and fixing anonymous credentials for the cloud. In: Mu, Y., Deng, R.H., Huang, X. (eds.) Cryptology and Network Security - CANS 2019. vol. 11829, pp. 249–269. Springer (2019), https://doi.org/10.1007/978-3-030-31578-8_14
22. Han, J., Chen, L., Schneider, S., Treharne, H., Wesemeyer, S.: Privacy-preserving electronic ticket scheme with attribute-based credentials. IEEE Trans. Dependable Secur. Comput. **18**(4), 1836–1849 (2021), https://doi.org/10.1109/TDSC.2019.2940946
23. Krenn, S., Lorünser, T., Salzer, A., Striecks, C.: Towards attribute-based credentials in the cloud. In: Capkun, S., Chow, S.S.M. (eds.) Cryptology and Network Security - CANS 2017. Lecture Notes in Computer Science, vol. 11261, pp. 179–202. Springer (2017), https://doi.org/10.1007/978-3-030-02641-7_9
24. Liagkou, V., Metakides, G., Pyrgelis, A., Raptopoulos, C.L., Spirakis, P.G., Stamatiou, Y.C.: Privacy preserving course evaluations in greek higher education institutes: An e-participation case study with the empowerment of attribute based

credentials. In: Preneel, B., Ikonomou, D. (eds.) Privacy Technologies and Policy - First Annual Privacy Forum, APF 2012, Limassol, Cyprus, October 10-11, 2012, Revised Selected Papers. Lecture Notes in Computer Science, vol. 8319, pp. 140–156. Springer (2012), https://doi.org/10.1007/978-3-642-54069-1_9
25. Paquin, C., Zaverucha, G.: U-prove cryptographic specification v1.1 (revision2). Technical report, Microsoft Corporation (Apr 2013)
26. Pussewalage, H.S.G., Oleshchuk, V.A.: An anonymous delegatable attribute-based credential scheme for a collaborative e-health environment. ACM Trans. Internet Techn. **19**(3), 41:1–41:22 (2019), https://doi.org/10.1145/3338854
27. Schnorr, C.: Efficient identification and signatures for smart cards. In: Brassard, G. (ed.) Advances in Cryptology - CRYPTO '89. Lecture Notes in Computer Science, vol. 435, pp. 239–252. Springer (1989), https://doi.org/10.1007/0-387-34805-0_22
28. Sforzin, A.: D5.1 – Requirements analysis of demonstration cases phase 1. H2020 CyberSec4Europe project deliverable (2020), available at https://cybersec4europe.eu/
29. Sforzin, A.: D5.2 – Specification and set-up demonstration case phase 1. H2020 CyberSec4Europe project deliverable (2020), available at https://cybersec4europe.eu/
30. Sforzin, A., Bobba, R.: D5.3 – Validation of demonstration case phase 1. H2020 CyberSec4Europe project deliverable (2021), available at https://cybersec4europe.eu/
31. Stamatiou, Y.C., Benenson, Z., Girard, A., Krontiris, I., Liagkou, V., Pyrgelis, A., Tesfay, W.: Course evaluation in higher education: the patras pilot of abc4trust. In: Rannenberg, K., Camenisch, J., Sabouri, A. (eds.) Attribute-based Credentials for Trust: Identity in the Information Society, pp. 197–239. Springer (2015), https://doi.org/10.1007/978-3-319-14439-9_7
32. Torres Moreno, R., Bernal Bernabé, J., García Rodríguez, J., Frederiksen, T.K., Stausholm, M., Martínez, N., Sakkopoulos, E., Ponte, N., Skarmeta, A.F.: The OLYMPUS architecture - oblivious identity management for private user-friendly services. Sensors **20**(3), 945 (2020)
33. Torres Moreno, R., García-Rodríguez, J., Bernal Bernabe, J., Skarmeta, A.: A trusted approach for decentralised and privacy-preserving identity management. IEEE Access **9**, 105788–105804 (2021)