OLYMPUS: towards Oblivious identitY Management for Private and User-friendly Services

Rafael Torres Moreno*, Jorge Bernal Bernabe*, Antonio Skarmeta*, Michael Stausholm†,
Tore Kasper Frederiksen†, Noelia Martínez‡, Nuno Ponte§, Evangelos Sakkopoulos¶, Anja Lehmann‖
*Department of Information and Communications Engineering
University of Murcia, Spain
{rtorres, jorgebernal, skarmeta}@um.es
†Alexandra Instituttet, Dennmark
{michael.stausholm, tore.frederiksen}@alexandra.dk
‡Logalty, Spain
noelia.martinez@logalty.com
§Multicert, Portugal
nuno.ponte@multicert.com
¶Scytales, Sweden
sakkopul@unipi.gr
‖IBM Research, Switzerland
anj@zurich.ibm.com

***Abstract*—The OLYMPUS EU project is addressing the challenges associated to the use of privacy-preserving identity management solutions by establishing an inter-operable European identity management framework, based on novel cryptographic approaches applied to currently deployed identity management technologies. In particular, OLYMPUS employs distributed cryptographic techniques to split up the role of the online IDP over multiple authorities, so that no single authority can impersonate or track its users. This paper describes the IdM ecosystem being developed in the scope of OLYMPUS, including its main building blocks, requirements and use cases.**

***Index terms*—** Privacy, security, identity management, iot, digital identities, identity derivation, oblivious cryptography

I. Introduction

Current Authentication and Identity Management (IdM) mechanisms have difficulties to meet the demanded security and privacy requirements, while keeping usability levels. Single Sign On systems (SSO) [1] based on technologies such as OAuth [2] or SAML [3] have barely evolved and reveal several drawbacks for managing identity information in a reliable and privacy manner. At best, websites verify email addresses and phone numbers by sending one-time codes. Age verification, which should be a common use case given the amount of age-restricted material offered online, is usually performed by verifying a credit card number, even though credit cards were never meant for this purpose and are available also to teenagers in many countries.

Several countries have started issuing electronic identity cards in an attempt to remedy this situation. Electronic identity cards usually come in the form of smart-cards that are cumbersome to use in combination with personal electronic devices such as phones, tablets, and laptops. Also, national identity cards from different countries are usually incompatible, forcing web services to choose which countries they want to support. Unification frameworks developed in EU projects such as STORK have not yet found wide deployment.

In this context, usernames and passwords are still the most popular way to authenticate users online. Users have a hard time remembering and managing all their different passwords, though, so they choose weak passwords and reuse the same password across many different services.

Traditional solutions introduce a single-point-of-failure in the system, since the IDP is involved in every authentication to a service provider. The IdP becomes a Big Brother that can track the browsing behavior of their users and link their accounts across different services.

To fill this gap, the European project OLYMPUS [4] (ObLivious Identity and Management for Private and User-friendly Services) is devising a privacy-preserving identity management solution based on novel cryptographic approaches applied to currently deployed identity management technologies. In particular, Olympus will employ distributed cryptographic techniques to split up the role of the online IdP over multiple authorities, so that no single authority can impersonate or track its users. The system prevents user impersonation by using distributed cryptographic techniques. Furthermore, it establishes solid links between citizens' physical and digital identities and the derivation of additional digital identities to enable privacy-preserving transactions backed by strong identities for citizens.

To ease integration of the Olympus identity management system into existing technologies and deployments, the system minimizes the requirements on user hardware, offering user-friendly authentication using passwords or biometrics, without requiring trusted hardware or software.

Olympus framework is under development and being validated and tested in two main use cases. The first one is

related to online eCommerce scenarios that require strong authentication and high level of assurance and trust, whereas the second use case is intended to minimize the data that is revealed to a merchant when buying restricted goods and services using a mobile ID credential such as the mobile Driving Licence (mDL).

Regarding the IoT scenarios, Olympus is also a promising approach. Nowadays, IoT devices consume services inside and outside their home networks. Providing protection and additional privacy-preservation properties to these devices can be done through Olympus. However, the particularities of these IoT scenarios should be taken into account by the IdM system. For example, strong IoT device authentication is required to ensure connected devices on the IoT can be trusted. Consequently, each IoT device needs a unique identity when the device attempts to connect its home network. With this unique ID, the identity managers can track each device throughout its life-cycle and if the device shows an unexpected behavior revoke its privileges. Additional requirements authentication systems available for IoT devices, such as Trusted Platform Module (TPM), X.509 certificates or symmetric cryptography must be taken into account when applying the Olympus approach, as there is no user interaction of devices accessing the services.

This paper presents the Olympus ecosystem, along with its main requirements, use cases, and building blocks. It shows the benefits of the Olympus solution to strengthen the security and trust in online identity-related processes, increasing user's privacy by employing distributed cryptographic techniques to split up the role of the online IdP over multiple authorities so that no single authority can impersonate or track its users.

The rest of this paper is structured as follows. Section II describes the state of the art in the research field. Section III describes the requirements of the project. Section IV is devoted to the explanation of Olympus identity management. Section V delves into the use of cases evaluation and security analysis. Section VI put the focus on IoT scenarios and their particularities. Finally, Section VII concludes the paper with the conclusions obtained.

II. State of the art

Traditional identity systems are based on the use of entities called Identity Providers (IdP). An identity provider creates, maintains and manages identity information about users while providing authentication services to Relaying parties (RP). IdPs enable the use of Single Sign-On (SSO) processes, allowing users to only perform the authentication process once.

In that sense, traditional solutions, such as SAML [3], OAuth [2], OpenID [5] try to provide security and privacy solutions in this kind of federated online scenarios.

Traditional identity solutions such as SAML [3], OAuth [2] or OpenID [5] are widely used solutions that try to manage authentication processes in the best possible way; however, with regard to privacy, they have significant shortcomings.

In that sense, the systems are evolving so that the user retakes control over their data, improving their privacy. With this objective, new concepts such as self-sovereign identity or privacy by design are being introduced [6].

Anonymous Credential Systems (ACS) allows a minimum disclosure of personal attributes, with privacy by design features. These systems rely on attributed based credential and cryptographic operations to generate Zero-knowledge proofs (ZKP) with which is possible to provide pseudo-anonymity, anonymity, and minimum disclose features over the data.

Identity Mixer, proposed by Camenisch et al. [7], is a cryptographic protocol for privacy-preserving authentication and transfer of certified attributes. It allows user authentication without divulging any personal data.

Furthermore, recent proposals such as ABC4Trust EU Project [8] or ReliAble euRopean Identity EcoSystem (ARIES) [9] have been using this kind of novel cryptographic tools. The first one for the use case of buying restricted goods and the second one, adding biometrics and virtual identifications generation for strong authentication processes.

However, due to the complexity of these systems and lack of compatibility with current IdM's standards, they have not had broad adoption. The lack of user-friendly tools makes them a scarcely extended solution.

The approach proposed by the Olympus project, unlike the previous proposals, is to solve the problem of compatibility with traditional systems while adding functionality to avoid IdP impersonation. This approach frees the user from heavy tasks and takes privacy by design directly to the identity providers.

Result of this combination, a novel system compatible with traditional technologies that respect the privacy of users while remains user-friendly is obtained.

Next, in section III, the concept of Oblivious Identity Management is introduced.

III. OLYMPUS Requirements

Main requirements established in OLYMPUS framework are listed below:

- **No Impersonation by IdPs**: when an adversary successfully assumes the identity of one of the legitimate parties. In this approach, a coalition of less than a threshold number of IdPs will not be able to impersonate the user. That is, IdPs cannot issue access tokens for any RP.
- **Short-lived authentication tokens:** user should employ short-lived access tokens after authenticating to the system. They can be configured to last for anywhere from a few minutes to several hours. After the credentials expire, the IdPs no longer recognizes them or allows any kind of access.
- **Unlikablity across RPs**: user identity cannot be linked across different RPs. Access tokens cannot be linked. Different pseudonyms in different RPs. Which means that within the system from the attacker's perspective, items of interest are no more and no less related after his observation than they are related concerning his apriori knowledge.

- **Hiding RPs from IdP**: IdPs only know that an authentication process is taking place. They cannot know which user accesses which service. Use of pseudonyms.
- **User-side hardware-software environment avoidance:** users should not be required to make use of hardware or software environments on their devices to protect the credentials. No credentials are stored in the user part.
- **Interoperable with existing IdM technologies**: compatibility with identity management standards such as SAML, OpenID and OAuth.
- **Optional support of anonymous credential Systems**: e.g. Privacy-ABCs such as Idemix.
- **Credentials might be linked to soft-proofs**: including biometrics, location information, and contextual information of the mobile device.
- **Data-minimization**: limit personal data collection, storage, and usage to data that is relevant, adequate, and absolutely necessary for carrying out the purpose for which the data is processed.
- **Oblivious and Distributed IdM deployment**: IdPs should split their responsibilities and tasks across several virtual ones to minimize security and privacy risks.

IV. Oblivious Identity Management

The overall idea is to distribute the responsibility of the identity provider between several entities, called virtual Identity Providers (vIdPs). These might either be distinct identity providers or virtual entities run by the same identity provider. We need each of these virtual entities to run on distinct physical machines, at different physical locations, with different system admins and operating systems. Because of this, we get that the effort required by an attacker to compromise each of these is almost the same as currently required by an attacker to compromise a full identity provider, that does not use the Olympus framework. The reason is that the Olympus framework will require that all these systems be compromised before an attacker can do anything useful; be it constructing fake sign-on tokens, or even trying to brute-force a user's password.

Assume that a user has registered with an identity provider (or providers) running the Olympus framework. Then when a user wishes to sign on to a service at a relying party, it executed a protocol with the vIdPs, which will result in it learning a one-time token that it can pass on to a relying party. The relying party can then verify the token and accepts it if it trusts the identity provider(s). We illustrate this flow in Fig. 1.

A. Main Building blocks

The Olympus framework takes its point of departure in the notion of *threshold* cryptography. A type of cryptography where secrets and other cryptographic material is shared between several parties. The sharing works in such a way that knowing less than all shares do not give any information away about the secret. It is this idea that makes it possible to achieve enhanced security by using a set of n vIdPs rather than a single one. However, this in itself is not enough, as for example

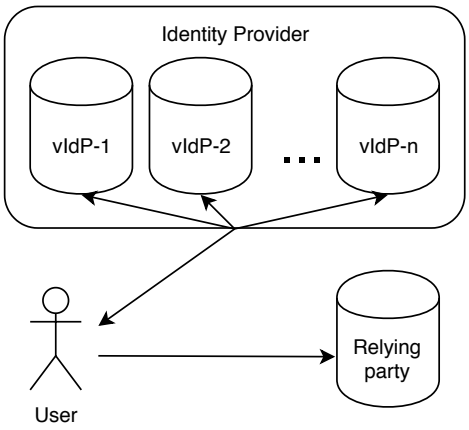

Fig. 1: Illustration of the Olympus framework.

sharing a hashed password in a threshold scheme will still not allow the vIdPs to verify said password without it existing in plain in their memory at some point in time. Fortunately, several techniques exist to achieve this, which we leverage in the Olympus framework [10], [11]. In particular, we take significant inspiration from the PASTA framework [11], which is composed of a threshold signature scheme and a threshold oblivious pseudorandom function (TOPRF).

In a threshold signature scheme, the private signing key is shared among the n vIdPs s.t. they each can compute a partial signature, all of which can then be combined by a user who knows all the partial signatures. This is achievable because of the mathematical structures in many popular signature schemes such as RSA [12] or (EC)DSA [13]. Thus the signature resulting from the combination is standard and can be verified by parties who are not aware that it was constructed based on a threshold signature scheme. A bit more formally we consider the setting where vIdP i holds private signing key share k_i and can compute a partial signature on the message m as $\mathrm{Sign}_{k_i}(m) = x_i$. All of these can then be combined $\mathrm{Combine}(x_1, \ldots, x_n) = x$ which can be verified using a public key p by computing $\mathrm{Verify}_p(x, m) = \textsc{accept}$ if and only if x was a legal signature on m.

The TOPRF implements the idea of a pseudorandom function, PRF, shared between the n vIdPs so that they must work together to compute $\mathrm{PRF}(m) = y$ on message m. However, this must also be done obliviously, meaning that none of the vIdPs are allowed to learn m or y. Like the case for threshold signatures, each of the vIdPs will get a share of a private key; $k_1, \ldots, k_n$. The user who wishes to query the TOPRF on m will first encode this using some randomness ρ. That is by computing $\mathrm{Enc}_\rho(m) = x$. The user then sends x to the servers who compute their shares of the PRF output; $\mathrm{Eval}_{k_i}(x) = y_i$. They send this back to the user who can then combine this into the PRF output; $\mathrm{Combine}(y_1, \ldots, y_n) = y$.

Based on these components the overall PASTA scheme can be described as follows:

Setup The vIdPs setup a threshold signing scheme among themselves and publish the public verification key p.

Sign-up The user constructs private keys for a TOPRF and distributes these to the vIdPs along with an encoding of its password, pwd, using the TOPRF.

Request When the user wish to get a token m signed by the identity provider, it picks some fresh randomness ρ and computes $\mathrm{Enc}_\rho(\mathsf{pwd}) = x$ and sends this, along with m, to the vIdPs. Based on this the vIdPs constructs an encrypted share of their partial signatures such that only the party who supplied the key shares for the TOPRF, and possessing the password, will be able to decrypt. The vIdPs sends their encrypted shares of the partial signatures to user, who decrypts them, reconstructs the token signature and passes this on to the relying party, who can then verify it based on the identity provider's public key.

Unfortunately, the PASTA framework does not give unlinkability between tokens issued to the same party. The first step in fixing this is to randomize the token to be signed in some way unknown to the vIdPs but known to the user, such that the user can remove this randomness before sending the token and its signature to the relying party. This can be achieved using something known as *blind signatures* [14]. It consists of the user picking some randomness and randomizing the message that the identity provider should sign. Because of a specific structure in the randomness, the user can remove the randomness from the token while keeping the signature valid, before returning the token to the relying party. Such random signatures can be implemented on top of standard signature schemes such as RSA. Formally we can express this as $\mathrm{Blind}(m) = m'$ and $\mathrm{Unblind}(x') = x$ where $x' = \mathrm{Combine}(x'_1, \ldots, x'_n)$ with $x'_i = \mathrm{Sign}_{k_i}(m')$ for $i = 1, \ldots, n$.

A problem with blind signatures is that the identity provider now obliviously signs *whatever* a user gives it. This is an issue if the user is malicious. For example, it could make the identity provider sign a token saying the user is older than he or she actually is. To prevent this, another cryptographic tool, known as zero-knowledge proof, comes into play. A zero-knowledge proofs allows a party to prove that it knows something, called a *witness*, without leaking any non-public information about what it knows. This means that, based on some public information, it is possible for a party to prove that it knows some relatable information which is hard to compute. Concretely this could be that the public information is a SHA-256 digest and the witness is a pre-image of it. The public information could also be an element of a large prime group and the witness the discrete logarithm of this element.

B. Scheme Outline

With the above discussion in mind we can now describe the overall structure of the Olympus distributed identity provider framework:

a) Setup: Run the setup phase of PASTA to get the public verification key p. Get this certified by a certificate authority and distribute it on a channel publicly accessible to potential relying parties.

b) Sign-up: Out-of-band the user proves its identity and attributes towards the vIdPs. Next, based on the user's password it executes the sign-up step of PASTA.

c) Request: When the user wish to get a token m signed by the identity provider it computes $\mathrm{Blind}(m) = m'$, picks some fresh randomness ρ and computes $\mathrm{Enc}_\rho(\mathsf{pwd}) = x$ and sends (x, m') to the vIdPs. It then executes a zero-knowledge proof with each of the vIdPs, proving that it knows m s.t. $\mathrm{Blind}(m) = m'$ and that m has the form for a legal token for this specific user. Based on (x, m') the vIdPs constructs an encrypted share of its partial signature such that only the party who supplied the key shares for the TOPRF and possessing the password will be able to decrypt. The vIdPs sends their encrypted shares of the partial signatures to the user, who decrypts them, reconstructs the token signature, x' and computes $\mathrm{Unblind}(x') = x$. It then passes the token and signature x on to the relying party, who can then verify it based on the identity provider's public key.

V. Use cases

The purpose of this use case, outlined in Fig. 4, is to demonstrate minimal and selective disclosure of personal information based on international standards as ISO 18013 (Driver's License). While until now a Driver's License is usually either in paper or card, ISO 18013 part 5 [15] is under development aiming to standardize an alternative form factor of a Driver's License to a smartphone. This is currently the leading path towards standardizing any identification document for a smartphone using multiple popular contactless transmission interfaces widely available such as QR, NFC, and BLE [16].

Particularly, we focus on demonstrating the use case of a citizen willing to buy an age restricted good or service (for example, a bottle of wine), using the mobile Driver's License (mDL) as an electronic version of one's ID document. This approach strengthens citizen privacy, because instead of disclosing the full dataset of the mDL, the user may only share the appropriate information about age, making proof that he or she is older or younger than a certain age.

Fig. 2: mobile Driver's License Use Case Overview

Based on ISO 18013-5 early committee draft [15], we focus on the interface between:

1) The mDL holder (e.g. driver or citizen) and the mDL verifier (e.g. merchant) and
2) The mDL verifier and the Issuing Authority (IA) that usually hold the primary registry of mDL holder's information.

At the moment the approach is designed for face to face encounters which are identified as *attended cases* by ISO

18013-5. In attended cases, any mDL verification shall be made by a verifier person or entity, as opposed to unattended systems.

In the proposed use case, the target audience would be individuals needing to be verified by relying parties such as merchants or officers, in order to access and/or receive age-restricted services and/or products that require the individual to be above or below a certain age.

We anticipate that smartphone users may need to perform age verification in front of relying on parties up to several times per week (estimated 1-5 per week). In the case of a verifier that has to perform age verification to its customers, the frequency of use may increase up to multiple times per day depending on the number of customers.

The mDL use case is designed in order to assist privacy preservation during face to face ID verifications. In this way, mDL is seen as a catalyst in facilitating daily and practical implementation of data protection laws for data minimization such as EU GDPR [17].

A. *Credit file*

The overall idea is to create an online platform where SMEs, self-employed and legal or natural individuals can create and manage their credit file and their standardized rating for financial entities.

Nowadays, when a customer needs financing, the financial entity requires the user's identification, access to external databases to collect and validate customer data, a credit risk evaluation, and, if it is granted, establishing a contractual credit relationship. As for the new EU General Data Protection regulation, before knowing if the contractual relationship will be performed, it is required for the client to give consent for providing the personal data signing one or more documents and for the financial entity to keep the consent and the personal data for several years. Within this use case, the goal is to ease this process for both sides, in a way that allows them to exchange the minimal required information until the financial entity approves the request.

The purpose of this use case is to change the current paradigm. Instead of providing all the customer's information at the first step of the relationship, the financial entity will receive an anonymous credit file containing the minimal required amount of financial information, bound to a pseudonym, that allows them to evaluate the user's suitability. The anonymization of financial information prevents the financial entity from having access to the user's personal data before performing an actual contractual relationship. This promotes the user's privacy and at the same time reduces the bank's need to process sensitive information to accommodate GDPR compliance.

Once the financial information contained in the credit file is evaluated, the bank must produce a binding response based solely on the data in the credit file, hence the financial entity can not discriminate between potential customers on any non-relevant information. If the bank decides that the user's information is suitable for producing an offer/contract, the customer can use the pseudonym to reveal his or her identity to the financial entity and start a contractual relationship.

Since the financial entity and credit file platform does not communicate directly, all data is passed through the customer, hence we focus on the interfaces:

1) Between the financial entity and the customer.
2) Between the customer and the credit file platform.

First, the user, in the initial website, selects a specific profile that determines the types of request that are available, defining a list of the minimum required information needed to make a financial evaluation for the requested profile. If the user validates this information list to be provided, a QR code, containing a machine-readable description of the data that the credit file platform will need to provide, will be generated.

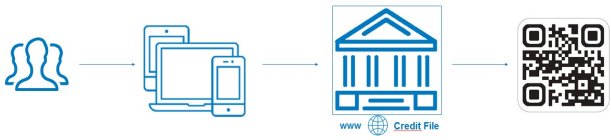

Fig. 3: Financial entity and customer interaction

Then, the user scans the QR code displayed in the financial entity website with a smartphone, uses an external app to authenticate against an external, traditional IdP and obtains an access token. This token is sent to the Credit File platform with the information from the QR code with the purpose to obtain the financial report on behalf of the user. Once the report is retrieved, the anonymization is performed extracting the relevant information from the financial report, binding the token to the user's actual identity and the credit file is signed digitally. This anonymized financial report is then sent to the financial entity for its evaluation. When the evaluation is ready, a push notification is sent to the user's mobile device to inform that the response is ready to be read.

Fig. 4: User and credit file interaction

VI. OLYMPUS APPLICABILITY IN IOT SCENARIOS

In IoT scenarios, devices are unattended and password-based systems are not appropriate. Instead, authentication technologies based on X.509 certificates, Trusted Platform Modules (TPM) and/or symmetric cryptography with shared keys, are commonly used.

Olympus aims to offer a privacy-preserving solution for users when accessing online services or, in the IoT case, when an intelligent device access to a third party service. In that sense, the authentication of these devices is an essential requirement that must occur directly between the IoT device and its Identity Manager, without end-user intervention. For

applying the Olympus approach in IoT, two phases can be distinguished:

- **Bootstrapping and registration/discovery**: This phase is performed against an Identity/Key Manager in its home network, where the IoT device authenticates itself (using, for instance, a pre-installed certificate from the vendor), and through an identity manager that is able to trace it and identify it unequivocally. Proposals such as ARMY [18] have already addressed this process in a privacy-aware way in IoT environments.
- **Authentication of the IoT device in an external service through Olympus**: In this phase, the IoT device makes use of the cryptographic material obtained during the configuration process in such a way that it is able to perform the processes (enrollment, authentication) in Olympus, as it is explained in section IV.B and benefit from the minimal information disclosure, privacy-preserving techniques and unlinkability through IdP when it makes use of a third party service.

While bootstrapping phase in the home network is outside the scope of Olympus, phase two is applicable. In contrast to the cases previously shown, the reuse of the cryptographic material obtained during the first phase is mandatory because the IoT device does not have the ability to use a password-based system. Once the cryptographic material has been obtained, the Olympus proposal takes action as previously shown, minimizing the data disclosure and being interoperable with standard technologies.

VII. Conclusions

This paper has presented the Olympus ecosystem, along with two well-differentiated use cases. In addition, its applicability to IoT scenarios is considered taking into account the special requirements of this kind of scenarios. Olympus proposes an identity management solution compatible with traditional systems while adding new privacy features and improving the security of scenarios. With this objective, a set of requirements have been identified, such as, for instance, IdP impersonation avoidance, short life credentials or unlikablity.

To fulfill these requirements, the use of Oblivious Identity Management is proposed. This approach performs identity management in a distributed manner. By this way, the traditional IdP is eliminated as the only point of failure, preventing an attacker from being able to impersonate the identity manager unless it compromises a number greater than a certain threshold of these new Olympus IdP entities. Despite the structural privacy improvements proposed, end users can still use the system transparently and in a user-friendly way, and therefore, only a user-password combination is required while the benefits of the SSO still applies in the architecture.

Regarding IoT scenarios, the approach provided by Olympus can be beneficial. The consumption of third-party services from devices that have many security limitations poses privacy risks, and through Olympus, it is feasible to improve this situation considerably while, at the same time, keep the existing authentication methods intact and compatible.

Acknowledgment

The project leading to this application has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 786725 (OLYMPUS project).

References

[1] J. De Clercq, "Single sign-on architectures," in *International Conference on Infrastructure Security*, pp. 40–58, Springer, 2002.

[2] D. Hardt, "The oauth 2.0 authorization framework," tech. rep., 2012.

[3] H. Lockhart and B. Campbell, "Security assertion markup language (saml) v2. 0 technical overview," *OASIS Committee Draft*, vol. 2, pp. 94–106, 2008.

[4] "Oblivious identity management for private and user-friendly services," 2019. https://www.olympus-project.eu/.

[5] D. Recordon and D. Reed, "Openid 2.0: a platform for user-centric identity management," in *Proceedings of the second ACM workshop on Digital identity management*, pp. 11–16, ACM, 2006.

[6] M. Langheinrich, "Privacy by design—principles of privacy-aware ubiquitous systems," in *International conference on Ubiquitous Computing*, pp. 273–291, Springer, 2001.

[7] J. Camenisch and E. Van Herreweghen, "Design and implementation of the idemix anonymous credential system," in *Proceedings of the 9th ACM conference on Computer and communications security*, pp. 21–30, ACM, 2002.

[8] A. Sabouri and K. Rannenberg, "Abc4trust: protecting privacy in identity management by bringing privacy-abcs into real-life," in *IFIP International Summer School on Privacy and Identity Management*, pp. 3–16, Springer, 2014.

[9] J. B. Bernabe, A. Skarmeta, N. Notario, J. Bringer, and M. David, "Towards a privacy-preserving reliable european identity ecosystem," in *Annual Privacy Forum*, pp. 19–33, Springer, 2017.

[10] J. Camenisch, A. Lehmann, and G. Neven, "Optimal distributed password verification," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-16, 2015* (I. Ray, N. Li, and C. Kruegel, eds.), pp. 182–194, ACM, 2015.

[11] S. Agrawal, P. Miao, P. Mohassel, and P. Mukherjee, "PASTA: password-based threshold authentication," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018* (D. Lie, M. Mannan, M. Backes, and X. Wang, eds.), pp. 2042–2059, ACM, 2018.

[12] V. Shoup, "Practical threshold signatures," in *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding* (B. Preneel, ed.), vol. 1807 of *Lecture Notes in Computer Science*, pp. 207–220, Springer, 2000.

[13] S. K. Langford, "Threshold DSS signatures without a trusted party," in *Advances in Cryptology - CRYPTO '95, 15th Annual International Cryptology Conference, Santa Barbara, California, USA, August 27-31, 1995, Proceedings* (D. Coppersmith, ed.), vol. 963 of *Lecture Notes in Computer Science*, pp. 397–409, Springer, 1995.

[14] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology: Proceedings of CRYPTO '82, Santa Barbara, California, USA, August 23-25, 1982*. (D. Chaum, R. L. Rivest, and A. T. Sherman, eds.), pp. 199–203, Plenum Press, New York, 1982.

[15] "Personal Identification – ISO Compliant Driving Licence – Part 5: Mobile Driving Licence application (mDL)," Draft Standard, International Organization for Standardization, Geneva, CH, Dec. 2018.

[16] E. Sakkopoulos, Z. Ioannou, and E. Viennas, "Mobile personal information exchange over BLE," in *9th International Conference on Information, Intelligence, Systems and Applications, IISA 2018, Greece, July 23-25, 2018*, pp. 1–8, IEEE Computer Society, 2018.

[17] European Parliament and Council of European Union, "Regulation (EU) no 2016/679," 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.

[18] J. L. Hernandez-Ramos, J. B. Bernabe, and A. Skarmeta, "Army: architecture for a secure and privacy-aware lifecycle of smart objects in the internet of my things," *IEEE Communications Magazine*, vol. 54, pp. 28–35, Sep. 2016.