Anonymous Certification for an e-Assessment Framework

Christophe Kiennert, Nesrine Kaaniche, Maryline Laurent, Pierre-Olivier Rocher, and Joaquin Garcia-Alfaro(✉)

SAMOVAR, Télécom SudParis, CNRS, Université Paris-Saclay, Paris, France
garcia_a@telecom-sudparis.eu

Abstract. We present an anonymous certification scheme that provides data minimization to allow the learners of an e-assessment platform to reveal only required information to certificate authority providers. Attribute-based signature schemes are considered as a promising cryptographic primitive for building privacy-preserving attribute credentials, also known as anonymous credentials. These mechanisms allow the derivation of certified attributes by the issuing authority relying on non-interactive protocols and enable end-users to authenticate with verifiers in a pseudonymous manner, e.g., by providing only the minimum amount of information to service providers.

Keywords: Attribute-based signatures · Attribute-based credentials · Privacy · Bilinear pairings · Anonymous certification · e-Assessment applications

1 Introduction

E-Assessment is an innovative form for the evaluation of learners' knowledge and skills in online education, as well as in blended-learning environments, where part of the assessment activities is carried out online. As e-assessment involves online communication channel between learners and educators, as well as data transfer and storage, security measures are required to protect the environment against system and network attacks. Issues concerning the security and privacy of learners is a challenging topic. Such issues are discussed under the scope of the TeSLA project (cf. http://www.tesla-project.eu/ for further information), a EU-funded project that aims at providing learners with an innovative environment that allows them to take assessments remotely, thus avoiding mandatory attendance constraints.

In [16], security of the TeSLA e-assessment system were analyzed and discussed. A security proposal for securing the TeSLA platform according to the General Data Protection Regulation (GDPR) [11] was proposed. With respect

N. Kaaniche and M. Laurent—Member of the Chair Values and Policies of Personal Information.

H. Lipmaa et al. (Eds.): NordSec 2017, LNCS 10674, pp. 1–16, 2017.
https://doi.org/10.1007/978-3-319-70290-2_5

to the protection of learners' data, and more specifically in terms of learners' certification techniques, it was highlighted the necessity of enhancing the framework with privacy-preserving attribute credentials, in order to allow learners to authenticate with verifiers in a pseudonymous manner. Indeed, an open educational system like TeSLA has to be properly secured with classical measures, such as authentication, data ciphering and integrity checks, in order to mitigate cyber-attacks that may lead to disastrous consequences, such as data leakage or identity theft.

To meet the GDPR recommendations, it is also necessary to ensure a reasonable level of privacy in the system. Security and privacy are very close domains, and yet important differences have to be highlighted, since it is possible to build a very secure system that fails to ensure any privacy properties. Security, from a technological standpoint, consists in guaranteeing specific requirements at different levels of the architecture, such as confidentiality, integrity or authentication. It mainly targets the exchange and storage of data, which in the case of TeSLA may contain some traces of learner's biometric data, the learner's assessment results, and other sensitive information. In contrast with security, privacy consists in preventing the exploitation of metadata to ensure that no personal information leakage will occur. However, it always remains mandatory to comply with legal constraints, which may prevent full anonymization of the communications. Therefore, the main objective of privacy, from a technological perspective, is to reveal the least possible information about the user's identity, and to prevent any undesired traceability, which is often complex to achieve.

In the context of TeSLA, several privacy technological filters have been included in the underlying design of the architecture. The randomized TeSLA identifier (TeSLA ID for short) associated to each learner is a proper example. This identifier is used each time the learner accesses TeSLA, hence ensuring pseudo-anonymity to every learner—full anonymity not being an option in TeSLA for legal reasons. Yet, a randomized identifier alone cannot protect the learners against more complex threats such as unwanted traceability. The system can still be able to link two different sessions of the same learner. A technical solution that could be integrated in the TeSLA architecture to handle such issues is the use of anonymous certification.

Anonymous certification allows users to prove they are authorized to access a resource without revealing more than they need about their identity. For example, users can be issued with certified attributes that may be required by the system verifier, such as *older than 18*, or *lives in France*. When the users want to prove that they own the right set of attributes, they perform a digital signature based on the required attributes, allowing the system verifier to check if a precise user is authorized, sometimes without even knowing precisely which attributes were used.

Such an approach could be integrated in several points of the TeSLA architecture where it is not necessary to identify the learner. For example, to access course material on the VLE, it should be enough to prove that the learner comes from an allowed university and is registered for this course. That way, it becomes

impossible for the VLE (Virtual Learning Environment) to follow the studying activity of each learner, while still letting the learners access the course material. Similarly, when a student has taken an assessment, the student's work can be anonymously sent to anti-cheating tools (such as anti-plagiarism). With anonymous certification, each tool might receive a request for the same work without being able to know which learner wrote it, but also without being able to correlate the requests and decide whether they were issued by the same learner.

Therefore, anonymous certification might prove to be a solid and innovative asset to enhance privacy in TeSLA, and to prevent traceability of the learners whenever it is not required. This paper reports an anonymous certification scheme that addresses the aforementioned challenges. It allows the learners of an e-assessment platform to reveal only required information to certificate authority providers. It builds on attribute-based signature schemes and allows the derivation of certified attributes by issuing authorities. The resulting construction provides a non-interactive protocol that allows the e-assessment users to authenticate with verifiers by providing only the minimum amount of information to service providers.

Paper Organization—Section 2 surveys some related work. Section 3 provides a short description of the mathematical details of our proposed anonymous certification mechanism. Section 4 presents a description of the TeSLA architecture, provides a use case towards validating our anonymous certification mechanism. Section 5 briefly discusses some details of the ongoing implementation of the solution and details about the security levels of the proposal. Section 6 concludes the paper.

2 Related Work

Privacy-preserving authentication mechanisms, called also anonymous certification schemes, are based on advanced cryptographic primitives, such as anonymous credentials, minimal disclosure tokens, self-blindable credentials, group signatures, sanitizable signatures or attribute-based signatures [3,4,6,8,10,14,28].

In these schemes, users obtain certified credentials for their attributes from trusted issuing organizations and later derive, without further assistance from any issuing authority, presentation tokens that reveal only the required attribute information that might be verified by the verifier under the issuing organization's public key. Well-known examples include Brands scheme [4], mainly relying on blind signatures, and Camenisch-Lysyanskaya scheme, using group signatures [6], which have been implemented in Microsoft U-Prove and IBM Identity Mixer, respectively.

Attribute-based signature schemes (ABS for short) are considered as a promoting cryptographic primitive for building privacy-preserving attribute credentials [19]. To use ABS, a user shall possess a set of attributes and a secret signing key per attribute. The signing key must be provided by a trusted authority. The user can sign, e.g., a document, with respect to a predicate satisfied by the set of

attributes. Several ABS schemes exist in the related literature, considering different design directions. This includes ABS solutions in which (i) the attribute value can be a binary-bit string [13,18,19,21,23] or general-purpose data structures [29]; (ii) ABS solutions satisfying access structures under threshold policies [13,18,23], monotonic policies [19,29] and non-monotonic policies [21]; and (iii) ABS solutions in which the private keys associated to the attributes are either issued by a single authority [19,23,29] or by a group of authorities [19,21].

Kaaniche and Laurent present in [14] a complete anonymous certification scheme, called $\mathcal{HABS}$, and constructed over the use of ABS. In addition to common requirements such as *privacy* and *unforgeability*, $\mathcal{HABS}$ is designed with three additional properties: (i) signature traceability, in order to grant some entities the ability of identifying the user originating an ABS signature; (ii) issuing organization unlinkability, to avoid that colluding ABS authorities link user requests sharing a single public key; and (iii) mitigation of replayed sessions, by imposing the use of random nonces and secure timestamps.

In [26,27], some of the requirements imposed by $\mathcal{HABS}$ are questioned by Vergnaud. The concrete realization of the $\mathcal{HABS}$ primitive is presented as unsatisfactory with regard to the unforgeability and privacy properties under the random oracle model. $\mathcal{PCS}$ [15], built over $\mathcal{HABS}$, addresses the limitations pointed out by [26,27] is used in this paper as the underlying construction deployed as an AC scheme of TeSLA.

The work by Aïmeur et al. in [1,2] discusses about the necessity of extended analysis of security and privacy techniques for e-learning systems. E-learning systems are presented by Aïmeur et al. as a composition of Internet-based protocols and tools, that require from well-established cryptographic techniques, in order to allow learners to perform on-line studies while preserving a minimum of privacy requirements. The authors survey in their work a list of security challenges to address, as well as some common threats to the privacy of the learners. A high-level overview of research examples in terms of attribute-based encryption and anonymous credentials is reported—without providing any explicit construction.

3 Anonymous Certification (AC) Construction

3.1 Background

In [9], Chaum introduced the notion of Anonymous Credentials (AC). Camenisch and Lysyanskaya fully formalized the concept in [6,7]. AC, also referred to as privacy-preserving attribute credentials, involve several entities and procedures. It fulfills some well-identified security and functional requirements. In the sequel, we first present some further details about the type of entities and procedures associated to traditional AC schemes. Then, we provide our specific AC construction.

3.1.1 Entities

An AC involves several entities. Figure 1 identifies several AC entities. Some entities, such as the *user*, the *verifier* and *issuer* are mandatory, while other

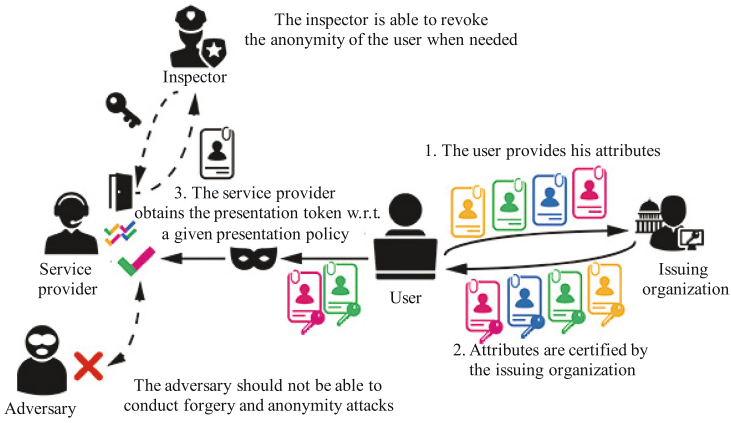

Fig. 1. Traditional AC entities

entities, such as the *revocation authority* and the *inspector* are optional [5]. These entities can be defined as follows:

- The *user* is the central entity, whose interest is to have privacy-preserving access to services, offered by service providers, known as *verifiers*. The user has first to collect credentials from various *issuing organizations*. Then, he selects the appropriate information from credentials, to present to the requesting verifier, under the presentation token.
- The verifier protects access to a resource or service that it offers by imposing restrictions on the credentials that users have to own and the information from these credentials that users must present to access the service. The verifier restrictions are referred to as *presentation policy*. The user generates from his credentials a *presentation token* that contains the required information and the supporting cryptographic evidence.
- The issuing organization issues credentials to users, while attesting the correctness of the information contained in the credential with respect to the user. Notice that before issuing a credential, the issuer may have to authenticate the user.
- The *revocation authority* has to revoke issued credentials and maintain the list of valid credentials in the system. So that, these credentials can no longer be used to derive presentation tokens. Both the user and the verifier have to obtain the most recent revocation information from the *revocation authority* to generate, respectively verify, presentation tokens.
- The *inspector* is a trusted entity, which has the technical capabilities to, when needed, remove the anonymity of a user.

3.1.2 Procedures

As depicted in Fig. 1, privacy-preserving ABC systems mainly rely on two main procedures (i.e., *issuance* and *presentation*).

The issuance of a credential is an interactive protocol, between the user and the issuing organization. At the end of this phase, the issuing organization provides a *signed* credential to the user, certifying the validity of the contained information. A user may have several credentials, each asserting some collection of attributes.

The presentation phase starts when a user requests access to the service provider's resources. Indeed, the verifier sends to the user the presentation policy, that describes which proofs must be sent, and which information from the credential(s) have to be revealed. The user then checks the combination of credentials that fulfill the policy in order to generate the response, referred to as *presentation token*, then sent to the verifier. Thus, a presentation token may reveal information about the user (reveal attribute values), but also prove certain facts about some other attributes (while hiding the values), such as proving that the birth date is earlier than a given day.

During a presentation procedure, the user may also need to prove not only that he possesses certain attribute values, but also that the credentials certifying those attributes have not been revoked.

3.1.3 Security and Functional Requirements

Privacy preserving authentication systems have to fulfill the following security requirements:

- ***anonymity*** – the user must remain anonymous during the authentication process.
- ***unforgeability*** – a party that does not belong to the set of authorized users should not be able to successfully run the protocol with the verifier.
- ***unlinkability*** – this property is important to preserve the privacy of users. Two sub-proprieties have to be identified: *issue-show unlinkability*, ensuring that any information gathered during the credential issuing cannot be used to later link the credential to its issuance while proceeding to its verification, and *multi-show unlinkability*, guarantying that multiple presentation sessions w.r.t. the same credential should not be linked.

Additionally, privacy preserving attribute-based credentials have to ensure several functional features, namely revocation, inspection and *selective disclosure*. The selective disclosure property refers to the ability provided to users, to present to the verifier partial information extracted or derived from their credentials.

3.2 Our Construction

In this section, we present our precise anonymous certification scheme, in order to extend the e-assessment framework reported in [16]. The solution is based on

an existing attribute-based signature scheme previously presented in [15]. Our construction relies on the following list of algorithms:

– SETUP—It takes as input the security parameter ξ and returns the public parameters *params*. The public parameters are considered an auxiliary input to all the algorithms.

Global Public Parameters params – the SETUP algorithm first generates an asymmetric bilinear group environment $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \hat{e})$ where $\hat{e}$ is an asymmetric pairing function such as $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$.

The random generators $g_1, h_1 = {g_1}^{\alpha}, \{\gamma_i\}_{i\in[1,U]} \in \mathbb{G}_1$ and $g_2, h_2 = {g_2}^{\alpha} \in \mathbb{G}_2$ are also generated, as well as $\alpha \in \mathbb{Z}_p$ where U denotes the maximum number of attributes supported by the span program.

We note that each value γ_i is used to create the secret key corresponding to an attribute a_i.

Let $\mathcal{H}$ be a cryptographic hash function. The global parameters of the system are denoted as follows:

$$params = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \hat{e}, p, g_1, \{\gamma_i\}_{i\in[1,U]}, g_2, h_1, h_2, \mathcal{H}\}$$

– KEYGEN—It returns a pair of private and public keys for each participating entity (i.e., issuing organization and user). In other words, the user has a pair of keys (sk_u, pk_u) where sk_u is chosen at random from $\mathbb{Z}_p$ and $pk_u = {h_1}^{sk_u}$ is the related public key. The issuing organization also holds a pair of secret and public keys (sk_o, pk_o). The issuing organization secret key sk_o relies on the couple defined as $sk_o = (s_o, x_o)$, where s_o is chosen at random from $\mathbb{Z}_p$ and $x_o = {g_1}^{s_o}$. The public key of the issuing organization pk_o corresponds to the couple $(X_o, Y_o) = (\hat{e}(g_1, g_2)^{s_o}, {h_2}^{s_o})$.
– ISSUE—It is executed by the issuing organization. The goal is to issue the credential to the user with respect to a pre-shared set of attributes $\mathcal{S} \subset \mathbb{S}$, such that $\mathbb{S}$ represents the attribute universe, defined as: $\mathcal{S} = \{a_1, a_2, \cdots, a_N\}$, where N is the number of attributes such that $N < U$.

The ISSUE algorithm takes as input the public key of the user pk_u, the set of attributes $\mathcal{S}$ and the private key of the issuing organization sk_o. It also picks an integer r at random and returns the credential C defined as:

$$C = (C_1, C_2, \{C_{3,i}\}_{i\in[1,N]}) = (x_o \cdot [{pk_u}^{s_o \mathcal{H}(\mathcal{S})^{-1}}] \cdot {h_1}^r, {g_2}^r, \{{\gamma_i}^r\}_{i\in[1,N]})$$

where $\mathcal{H}(\mathcal{S}) = \mathcal{H}(a_1)\mathcal{H}(a_2)\cdots\mathcal{H}(a_N)$ and ${\gamma_i}^r$ represents the secret key associated to the attribute a_i, where $i \in [1, N]$.
– OBTAIN—It is executed by the user. It takes as input the credential C, the secret key of the user sk_u, the public key of the issuing organization pk_o and

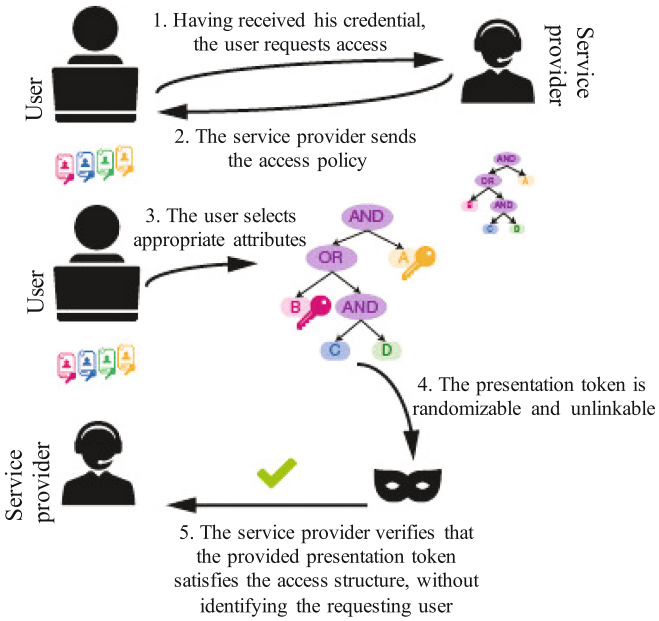

Fig. 2. ABS for the support of AC (Presentation Procedure)

the set of attributes $\mathcal{S}$. The algorithm returns 1 if Eq. 1 holds true; or 0, otherwise.

$$\hat{e}(C_1, g_2) \stackrel{?}{=} X_o \cdot \hat{e}(g_1^{sk_u \mathcal{H}(\mathcal{S})^{-1}}, Y_o) \cdot \hat{e}(h_1, C_2) \tag{1}$$

– SHOW ↔ VERIFY: this two-party algorithm is illustrated by Fig. 2. The different algorithms are defined as follows:

- VERIFY: this algorithm is executed by the verifier upon receiving an authentication request from a user. In a first step, it outputs the presentation policy, including a randomized message $\mathtt{M} = {g_1}^m$, a predicate Υ and the set of attributes that have to be revealed. In the following, we note that:
  * m should be different for each authentication session to prevent replay attacks,
  * $\mathcal{S}_R$ denotes the set of attributes revealed to the verifier and $\mathcal{S}_H$ denotes the set of non-revealed attributes, such as $\mathcal{S} = \mathcal{S}_R \cup \mathcal{S}_H$,
  * Υ is represented by an LSSS access structure (M, ρ), where M is an $l \times k$ matrix, and ρ is an injective function that maps each row of the matrix M to an attribute.
- SHOW: The SHOW algorithm takes as input the user secret key sk_u, the credential C associated to the attribute set $\mathcal{S}$ for pk_u, the message $\mathtt{M}$ and the predicate Υ. The showing process is as follows:
  1. The user first randomizes his credential in the following way: it selects uniformly at random an integer $r' \in \mathbb{Z}_p$ and sets:

$$\begin{cases} C'_1 = C_1 \cdot {h_1}^{r'} = x_o \cdot [{pk_u}^{s_o \mathcal{H}(\mathcal{S})^{-1}}] \cdot {h_1}^{r+r'} \\ C'_2 = C_2 \cdot {g_2}^{r'} = {g_2}^{r+r'} \\ C'_{3,i} = C_{3,i} \cdot {\gamma_i}^{r'} = {\gamma_i}^{r+r'} \end{cases}$$

The resulting credential C' is set as follows:

$$C' = (C'_1, C'_2, \{C'_{3,i}\}_{i\in[1,N]}) = (x_o \cdot [{pk_u}^{s_o \mathcal{H}(\mathcal{S})^{-1}}] \cdot {h_1}^{r+r'}, {g_2}^{r+r'}, \{{\gamma_i}^{r+r'}\}_{i\in[1,N]})$$

2. As the attributes of the user in $\mathcal{S}$ satisfy Υ, the user can compute a vector $\boldsymbol{v} = (v_1, \cdots, v_l)$ that also satisfies $\boldsymbol{v}M = (1, 0, \cdots, 0)$.
3. For each attribute a_i, where $i \in [1, l]$, the user computes $\omega_i = {C'_2}^{v_i}$ and calculates a quantity B that depends on $\{C'_{3,i}\}_{i\in[1,N]}$ such that $B = \prod_{i=1}^{l} (\gamma'_{\rho(i)})^{v_i}$.
4. Afterwards, the user selects a random r_m and computes the couple $(\sigma_1, \sigma_2) = (C'_1 \cdot B \cdot \mathtt{M}^{r_m}, {g_1}^{r_m})$. Notice that the user may not have knowledge about the secret value of each attribute in Υ. If this happens, v_i is set to 0, so to exclude the necessity of this value.
5. Using now the secret key of the user, it is possible to compute an accumulator on non-revealed attributes as follows:

$$A = {Y_o}^{\frac{sk_u \mathcal{H}(\mathcal{S}_H)^{-1}}{r_m}}$$

The user returns the presentation token $\Sigma = (\Omega, \sigma_1, \sigma_2, C'_2, A, \mathcal{S}_R)$, that includes the signature of the message $\mathtt{M}$ with respect to the predicate Υ, and where $\Omega = \{\omega_1, \cdots, \omega_l\}$ is the set of committed element values of the vector $\boldsymbol{v}$, based on the credential's item C'_2.

- VERIFY: In a second step, given the presentation token Σ, the public key of the issuing organization pk_o, the set of revealed attributes $\mathcal{S}_R$, the message m and the signing predicate Υ, the verifier first computes an accumulator A_R such as $A_R = {\sigma_2}^{\mathcal{H}(\mathcal{S}_R)^{-1}}$. Then, it picks uniformly at random $k-1$ integers $\mu_2, \cdots, \mu_k$ and calculates l integers $\tau_i \in \mathbb{Z}_p$ for $i \in \{1, \cdots, l\}$ such that $\tau_i = \sum_{j=1}^{k} \mu_j M_{i,j}$ where $M_{i,j}$ is an element of the matrix M. It accepts the presentation token as valid (i.e.; outputs 1) if and only if Eq. 2 holds:

$$\hat{e}(\sigma_1, g_2) \stackrel{?}{=} X_o \hat{e}(A_R, A) \hat{e}(h_1, C'_2) \prod_{i=1}^{l} \hat{e}(\gamma_{\rho(i)} {h_1}^{\tau_i}, \omega_i) \hat{e}(\sigma_2, {g_2}^{m}) \qquad (2)$$

4 E-learning Use Case for $\mathcal{PCS}$

In this section, we describe how anonymous certification relying on attribute-based signatures may be integrated into an e-learning environment to enhance the learners' privacy. We first present the TeSLA architecture for e-learning and e-assessment, before detailing in which parts of the architecture anonymous certification may be implemented.

4.1 TeSLA Architecture

The TeSLA project aims at providing an e-learning environment that integrates secure e-assessment, in order to allow the learners to take assessments remotely while providing the necessary countermeasures to prevent cheating.

The TeSLA architecture is comprised of several components that may belong to two domains: the university domain and the TeSLA domain. Components that belong to the university domain must be present in the network of each university willing to make use of the TeSLA e-assessment framework, while components that belong to the TeSLA domain are completely independent of the university network. The two domains do not share data unless explicitly stated. The TeSLA domain contains the following components:

- The TeSLA E-assessment Portal (TEP), which acts as a service broker that gathers and forwards requests to the TeSLA components.
- The TeSLA Portal, that aims at gathering statistics regarding the e-assessment activities.
- Instruments that analyze the biometric samples and send their analysis results back to the client side.

The university domain contains the following components:

- A Virtual Learning Environment (VLE), which can be provided by a classic Learning Management System (LMS) such as Moodle[1].
- A plugin integrated to the VLE that acts as a client side interface with the TeSLA components.
- Various tools integrated to the VLE that send requests and data to the TeSLA components through the plugin. There are three categories of tools: the learner tool, the instructor tool, and external tools. The learner tool and instructor tool are respectively designed to take or setup an e-assessment. External tools are in charge of sampling the learner's biometric data and sending them to TeSLA instruments for evaluation, as part of the anti-cheating countermeasures.
- The TeSLA Identity Provider (TIP), which is in charge of generating an anonymized identity for each learner, called TeSLA ID, to be used in the communication with TeSLA components.

The TeSLA architecture is represented in Fig. 3. The communications between the components are secured by the TLS protocol [22], deployed on the whole architecture with mutual authentication, hence ensuring confidentiality and integrity of every data exchange. The underlying Public Key Infrastructure for TLS deployment and management is detailed in [16].

Taking an e-assignment in this architecture first requires to log in on the VLE that contains the client-side plugin. The learner can require the e-assignment using the learner tool available on the VLE as a third-party tool. The learner

[1] https://moodle.org/.

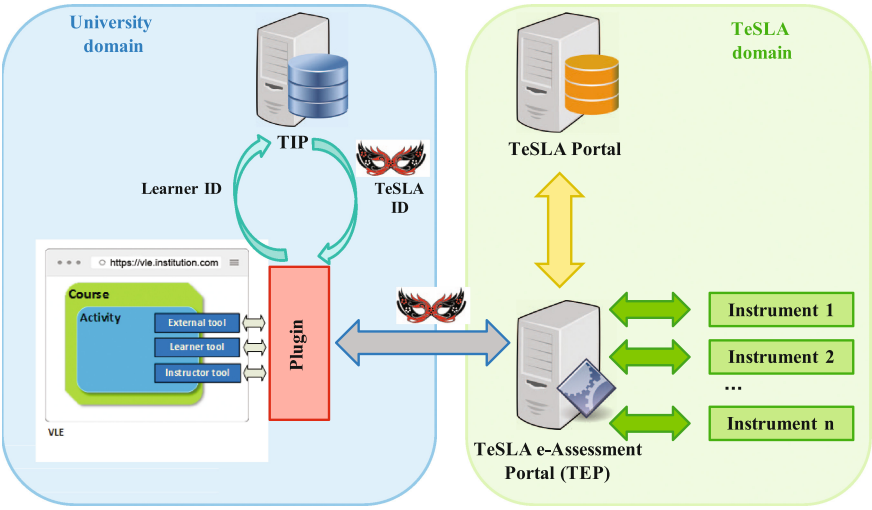

Fig. 3. Simplified TeSLA architecture representation

tool sends a request through the plugin to the TEP. The incoming request does not contain the name of the learner, but only the TeSLA ID, that the plugin requested from the TIP. Then, the TEP fetches the e-assignment in its database and sends it back to the VLE, where the learner will take the assignment while external tools sample biometric data that will be regularly sent to instruments for anti-cheating analysis.

4.2 Pseudonymity

A project for secure e-assessment such as TeSLA does not make it possible to implement full anonymity for the learners. Indeed, the very nature of the assessment makes it mandatory to store the association between the examinee number (e.g., the TeSLA ID) and the real name of the learner. Therefore, in such context, only partial anonymity, i.e. pseudonymity can be provided to learners during exchanges with the TeSLA components.

In this architecture, pseudonymity is ensured with a randomized TeSLA identifier named TeSLA ID, which becomes the learner's identity within the TeSLA domain. Therefore, no TeSLA component has ever access to the learner's true identity.

The TeSLA ID is generated by the TIP component as a random number computed according to version 4 of the UUID standard [17]. The matching between the learner's identity and the TeSLA ID is stored in the TIP database. The TIP database is placed at the university side and is not accessible from TeSLA. The TIP database shall be shared with all the VLEs. Since any interaction between the university domain and the TeSLA domain involve the plugin on one hand, and the TEP on the other hand, it is sufficient to make sure that any request

sent to the TEP through the plugin is first redirected to the TIP to retrieve the learner's TeSLA ID and use it in place of the learner's identity. Notice that the TeSLA ID enables pseudonymity for all learners, who can take e-assessments without revealing their identity to the TeSLA system. However, it should be noted even though the learners are anonymized with respect to the e-assessment system, it is not enough to prevent the acquisition and correlation of personal data by the system. For example, the TeSLA ID does not ensure multi-session unlinkability, since the e-assessment system is obviously able to know when the same learner is logging in over two different sessions and gather data about this learner's actions, even without knowing his identity. Anonymous certification, as described in Sect. 3, is a solution that ensures many more privacy properties than a simple anonymized identifier. In the next subsection, we describe how the system can be integrated to an e-learning environment such as TeSLA.

4.3 Integrating Anonymous Certification to TeSLA

The purpose of anonymous certification is to perform anonymous access control, in order to certify that users are allowed to access a resource because they own some attributes required by the verifier. However, the verifier only knows that the users' attributes match the policy, without necessarily knowing which attributes they own exactly.

Therefore, anonymous certification cannot be used in a context where it is necessary to perform authentication in order to identify a specific user. Obviously, it can be adapted to such a situation by requiring the user identifier as an attribute that must be revealed, but it loses its interest by doing so. In the context of TeSLA, it means that anonymous certification cannot be used during e-assessment itself, since the e-assessment needs to be associated to the unique identifier of a learner.

However, anonymous certification can be naturally added to the VLE. Indeed, a LMS generally aims at informing learners about courses they registered at, and letting them access the course material. In both cases, the VLE does not need to identify the learner in a unique way, but only needs to prove that the learner is authorized. In this case, the following attributes could be defined and used to decide whether to authorize a learner:

- The university where the learner is enrolled
- The courses at which the learner registered

These attributes are enough to let every learner access to the VLE pages he is entitled to visit, without proceeding to an usual, nominative authentication (even using a pseudonym or an anonymized identifier). Thus, learners might be able to access the course document at any time without any possibility for the VLE to log and profile the learners' activity. This can be a significant advance for learners' privacy since learners may for example abhor to let the system know at which hours they are awake, and at which moment they accessed the course material.

Likewise, it is also possible to enhance the privacy of e-assignments' post processing. When an e-assignment is completed by a learner, it must first be sent to a number of external anti-cheating instruments, that will for example check if the assignment contains plagiarism. Instead of transmitting requests associated to the learner's TeSLA ID, the requests can be anonymized and authorized with anonymous certification. The attributes may be defined similarly as above. On top of preventing each instrument from profiling students based on their TeSLA ID, the unlinkability property of the anonymous certification scheme guarantees that two different instruments will not be able to know that the request was emitted from the same learner. This greatly limits the possibility for the instruments to correlate data, i.e., it enhances the learners' privacy.

5 Implementation and Security Details of $\mathcal{PCS}$

We briefly discuss in this section the ongoing implementation of the proposal reported in this paper, as well as some remarks about the security level of $\mathcal{PCS}$.

5.1 Implementation Details

Available at http://j.mp/PKIPCSgit as a multi-platform `C++` software code, and mainly based on existing cryptographic libraries such as PBC [25] and MCL [24], the construction is available online to facilitate understanding, comparison and validation of the solution. Special attention has been paid to the nature of the elliptic curves required to validate the operations of the construction in Sect. 3. We recall that Anonymous Credentials (AC) are built on top of Attribute-Based Cryptography, which makes use of pairing-friendly elliptic curves, i.e., elliptic curves that satisfy certain conditions [12]. For instance, the degree of immersion of such curves. Some parts of the implementation and testing of the elliptic curve operations are based on either Ate or Tate pairing implementations (cf., for instance, the *Ate Pairing over Barreto-Naehrig Curves* implementation, available at https://github.com/herumi/ate-pairing). Extended versions of the Miller algorithm [20] from [12] are used to computing the pairings. Precise examples, and data computed to verify the security of the construction, are available at http://j.mp/PKIPCSgit as well.

5.2 Security Level Sketch of Our Proposal

We recall that brute-force attacks consist in checking all possible keys until the correct one is discovered (i.e., with a key of length k bits, there are 2^k possible keys). Thus, k denotes the security level in symmetric cryptography. In public-key cryptography, the security level of an algorithm is defined with respect to the hardness of solving a mathematical problem such as the Discrete Logarithm Problem (DLP). The time required to resolve the DL problem is much less important than trying the 2^k keys by a brute-force attack. For instance, a 1024-RSA key-length bits provides a 80 key-length equivalent key of a symmetric algorithm.

In order to generate security parameters for each security level of the $\mathcal{PCS}$ proposal, we shall investigate the structure of $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$. The attribute-based signature scheme depends on the pairing function $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \leftarrow \mathbb{G}_T$. Let $\mathcal{E}(\mathtt{F}_q)$ denote an elliptic curve [12] defined over the finite prime field $\mathbb{F}_q$ of order q. $\mathbb{G}_1$ is a finite additive subgroup of $\mathcal{E}(\mathtt{F}_q)$, $\mathbb{G}_T$ is a finite multiplicative subgroups of $\mathcal{E}(\mathtt{F}_{q^k})$ with order equal to p, such as k is the embedding degree of the curve $\mathcal{E}(\mathtt{F}_{q^k})$ relatively to p.

k defines the type of pairing function (type A, E, D, G) with respect to PBC library [25]. As such, the security level is related to the hardness of solving the DLP in the group $\mathbb{G}_T$. Let the order of G1 be the ECC key and the order of $\mathbb{G}_T$ be $p = q * k$. In order to generate the security parameters using PBC library, it is necessary to know the *rbit* order of $\mathbb{G}_1$ and the *qbit* order of $\mathtt{F}_q$. Table 1 shows the equivalent sizes of *rbits* and *qbits* for three considered security levels.

Table 1. Equivalent key sizes for some representative security levels (in bits)

Security level	Pairing type	$\mathbb{G}_T$ Size	$\mathtt{F}_q$ Size	$\mathbb{G}_1$ Size
80	A	1024	512	160
80	E	1024	1024	160
$\geq$80	D	1050	175	167
$\geq$80	G	1080	108	103
112	A	2028	1024	224
112	E	2048	2048	224
$\geq$112	D	2082	347	332
$\geq$112	G	3010	301	279
128	A	3072	1536	256
128	E	3072	3072	256
$\geq$128	D	3132	522	514
$\geq$128	G	5250	525	487

From Table 1, we notice that the computation duration of pairing functions, while considering different security levels, should be taken into consideration while implementing $\mathcal{PCS}$, since the size of $\mathbb{G}_T$, $\mathtt{F}_q$ and $\mathbb{G}_1$ groups size, mainly depend on the selected security level. For our $\mathcal{PCS}$ construction, the security level depends on the sensitivity level of handled e-learners data.

6 Conclusion

We have detailed an anonymous certification scheme for e-assessment systems. The proposed construction revisits an existing mechanism based on homomorphic attribute-based signatures, and offers a selective disclosure of features to enable anonymous certification of learners of an e-assessment system. A precise

use case has been presented, and an ongoing implementation of the approach discussed. Perspectives of future work include extending the framework for additional use cases, as well as an exhaustive performance reporting of the full C++ implementation of the construction, will be released at http://j.mp/PKIPCSgit.

Acknowledgements. This work is supported by the H2020-ICT-2015/H2020-ICT-2015 TeSLA project *An Adaptive Trust-based e-assessment System for Learning*, Number 688520. The authors graciously acknowledge as well the support received from the Chair Values and Policies of Personal Information of the Institut Mines-Télécom.

References

1. Aïmeur, E., Hage, H.: Preserving learners' privacy. In: Nkambou, R., Bourdeau, J., Mizoguchi, R. (eds.) Advances in Intelligent Tutoring Systems. SCI, vol. 308, pp. 465–483. Springer, Heidelberg (2010). doi:10.1007/978-3-642-14363-2_23
2. Aïmeur, E., Hage, E., Onana, F.S.M.: Anonymous credentials for privacy-preserving e-learning. In: 2008 International MCETECH Conference on E-Technologies, pp. 70–80. IEEE (2008)
3. Belenkiy, M., Camenisch, J., Chase, M., Kohlweiss, M., Lysyanskaya, A., Shacham, H.: Delegatable anonymous credentials. Cryptology ePrint Archive, Report 2008/428 (2008)
4. Brands, S.A.: Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press, Cambridge (2000)
5. Camenisch, J., Krenn, S., Lehmann, A., Mikkelsen, G.L., Neven, G., Pederson, M.O.: Scientific comparison of ABC protocols: Part i - formal treatment of privacy-enhancing credential systems (2014)
6. Camenisch, J., Lysyanskaya, A.: An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 93–118. Springer, Heidelberg (2001). doi:10.1007/3-540-44987-6_7
7. Camenisch, J., Mödersheim, S., Sommer, D.: A formal model of identity mixer. In: Kowalewski, S., Roveri, M. (eds.) FMICS 2010. LNCS, vol. 6371, pp. 198–214. Springer, Heidelberg (2010). doi:10.1007/978-3-642-15898-8_13
8. Canard, S., Lescuyer, S.: Protecting privacy by sanitizing personal data: a new approach to anonymous credentials. In: Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, ASIA CCS 2013. ACM, New York (2013)
9. Chaum, D.: Security without identification: transaction systems to make big brother obsolete. Commun. ACM **28**(10), 1030–1044 (1985)
10. Chaum, D., van Heyst, E.: Group signatures. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 257–265. Springer, Heidelberg (1991). doi:10.1007/3-540-46416-6_22
11. European Council: Proposal for a regulation of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. In General Data Protection Regulation (2016)
12. Hankerson, D., Menezes, A., Vanstone, A.: Guide to Elliptic Curve Cryptography. Springer Science & Business Media, New York (2006)
13. Herranz, J., Laguillaumie, F., Libert, B., Ràfols, C.: Short attribute-based signatures for threshold predicates. In: Dunkelman, O. (ed.) CT-RSA 2012. LNCS, vol. 7178, pp. 51–67. Springer, Heidelberg (2012). doi:10.1007/978-3-642-27954-6_4

14. Kaaniche, N., Laurent, M.: Attribute-based signatures for supporting anonymous certification. In: Askoxylakis, I., Ioannidis, S., Katsikas, S., Meadows, C. (eds.) ESORICS 2016. LNCS, vol. 9878, pp. 279–300. Springer, Cham (2016). doi:10.1007/978-3-319-45744-4_14
15. Kaaniche, N., Laurent, M., Rocher, P.-O., Kiennert, C., Garcia-Alfaro, J.: $\mathcal{PCS}$, a privacy-preserving certification scheme. In: Garcia-Alfaro, J., Navarro-Arribas, G., Hartenstein, H., Herrera-Joancomartí, J. (eds.) ESORICS/DPM/CBT-2017. LNCS, vol. 10436, pp. 239–256. Springer, Cham (2017). doi:10.1007/978-3-319-67816-0_14
16. Kiennert, C., Rocher, P.O., Ivanova, M., Rozeva, A., Durcheva, M., Garcia-Alfaro, J.: Security challenges in e-assessment and technical solutions. In: 8th International Workshop on Interactive Environments and Emerging Technologies for eLearning, 21st International Conference on Information Visualization, London, UK (2017)
17. Leach, P.J., Salz, R., Mealling, M.H.: A Universally Unique IDentifier (UUID) URN Namespace. RFC 4122, July 2005
18. Li, J., Au, M.H., Susilo, W., Xie, D., Ren, K.: Attribute-based signature and its applications. In: ASIACCS 2010 (2010)
19. Maji, H.K., Prabhakaran, M., Rosulek, M.: Attribute-based signatures. In: Kiayias, A. (ed.) CT-RSA 2011. LNCS, vol. 6558, pp. 376–392. Springer, Heidelberg (2011). doi:10.1007/978-3-642-19074-2_24
20. Miller, V.S.: Use of elliptic curves in cryptography. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 417–426. Springer, Heidelberg (1986). doi:10.1007/3-540-39799-X_31
21. Okamoto, T., Takashima, K.: Efficient attribute-based signatures for non-monotone predicates in the standard model. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 35–52. Springer, Heidelberg (2011). doi:10.1007/978-3-642-19379-8_3
22. Rescorla, E., Dierks, T.: The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246, August 2008
23. Shahandashti, S.F., Safavi-Naini, R.: Threshold attribute-based signatures and their application to anonymous credential systems. In: Preneel, B. (ed.) AFRICACRYPT 2009. LNCS, vol. 5580, pp. 198–216. Springer, Heidelberg (2009). doi:10.1007/978-3-642-02384-2_13
24. Shigeo, M.: MCL - Generic and fast pairing-based cryptography library, version: release20170402. https://github.com/herumi/mcl
25. Stanford University: PBC - The Pairing-Based Cryptography Library, version: 0.5.14. https://crypto.stanford.edu/pbc/
26. Vergnaud, D.: Comment on "attribute-based signatures for supporting anonymous certification" by N. Kaaniche and M. Laurent (ESORICS 2016). IACR Cryptology ePrint Archive (2016)
27. Vergnaud, D.: Comment on attribute-based signatures for supporting anonymous certification by N. Kaaniche and M. Laurent (ESORICS 2016). Comput. J. 1–8, June 2017
28. Verheul, E.R.: Self-blindable credential certificates from the Weil pairing. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 533–551. Springer, Heidelberg (2001). doi:10.1007/3-540-45682-1_31
29. Zhang, Y., Feng, D.: Efficient attribute proofs in anonymous credential using attribute-based cryptography. In: Chim, T.W., Yuen, T.H. (eds.) ICICS 2012. LNCS, vol. 7618, pp. 408–415. Springer, Heidelberg (2012). doi:10.1007/978-3-642-34129-8_39