Security and Privacy in the TeSLA Architecture

Christophe Kiennert[1], Malinka Ivanova[2], Anna Rozeva[2], Joaquin Garcia-Alfaro[1]

[1] Institut Mines-Telecom, Institut Polytechnique de Paris, France
{kiennert,garcia_a}@telecom-sudparis.eu
[2] Department of Informatics, Technical University of Sofia, Bulgaria
{m_ivanova,arozeva}@tu-sofia.bg

Abstract. In this chapter, we address security and privacy aspects in TeSLA, from a technical standpoint. The chapter is structured in three main parts. Firstly, we outline the main concepts underlying security in TeSLA, with regards to the protection of learners' data and the architecture itself. Secondly, we provide an empirical analysis of a specific deployment in one of the members of the consortium. Some representative aspects such as security levels in terms of storage, processing and transfer are analyzed in the deployment of TeSLA at the Technical University of Sofia. In the third part, we address identity management issues and outline additional efforts we consider worth exploring.

Keywords: Authentication, Authorship, Security, Public Key Infrastructures, X.509 Certificates, Anonymity, Privacy, GDPR..

1 Introduction

TeSLA aims at providing learners with an innovative environment, which allows them to take assessments remotely, thus avoiding mandatory attendance constraints. From a technical standpoint, TeSLA has been designed as a flexible architecture, in which traditional learning management systems and virtual learning environments are seen as the main entry points of an educational platform. The architecture itself is comprised of several entities, some of them located at the institution side, establishing communications with the learning environments or with external tools embedded into the learners' browsers; others belonging to a separate domain independent of the institution. Securing such architecture consisted in expressing the security needs regarding sensitive and personal data on the one hand, and analyzing threats both on hosts and network on the other. Moreover, the choices made on security measures ensured that TeSLA is compliant with existing technical standards and recommendations (ISO 2013), (OWASP 2013), (ANSSI 2016), (IEEE Standards 2018), and also with legal requirements, such as the European General Data Protection Regulation (EUR-Lex 2016).

From a security perspective, the main properties ensured by TeSLA are authentication, authorship, confidentiality and integrity. Authentication aims at proving an entity's identity to another party; authorship consists in proving the

identity of the creator of a piece of work; confidentiality consists in encrypting data to prevent information disclosure to unauthorized parties; and integrity aims at preventing fraudulent data alteration. Over the network, the most convenient way to implement these three traditional security properties was to deploy the well-known Transport Layer Security (TLS) protocol (Dierks & Rescorla 2008), which allows entities to authenticate to each other and creates a secure tunnel with data encryption and integrity check.

Authentication in TLS does not rely on passwords, but on X.509 certificates . These certificates rely on asymmetric cryptography, and create an association between a public key and an identity. Any entity can authenticate itself via the certificate, as long as it owns the associated private key, which is never transmitted over the network. The certificate management requires a Public Key Infrastructure (PKI), in which specific trusted entities, called Certification Authorities, are in charge of the certificate delivery.

As we will see in the first part of this chapter, TeSLA comes with a PKI to manage X.509 certificates within the TeSLA domain on the one hand, and within the institution domain on the other. This way, communication between the various entities of the TeSLA architecture can be entirely secured, in all the three dimensions aforementioned (i.e., authentication, confidentiality, and integrity). Other aspects that have been carefully taken into account in TeSLA are in terms of data protection from a privacy perspective. In fact, the identity of the learners is never disclosed within the TeSLA domain. The architecture has been conceived to respect sensitive data of the learners, for both legal and ethical reasons. In a nutshell, the enforcement of privacy in TeSLA consists in minimizing the personal information retrieved from learners during their interactions with the system, as well as encrypting and anonymizing the data exchanged or stored in the databases whenever required. In the end, the TeSLA architecture provides the learner with pseudo-identifiers, which hide the learner's genuine identity when taking e-assessment activities.

In this chapter, we elaborate further on all the aforementioned security and privacy aspects, and provide additional elements for further research perspectives and discussions. More specifically, Section 2 outlines the main concepts underlying the TeSLA architecture from a technical perspective. Section 3 reports a practical hands-on analysis conducted by members of the consortium during the pilot phases of the project. Section 4 discusses additional enhancements towards enhanced privacy features in future TeSLA releases. Finally, Section 5 concludes the chapter. Some parts of this chapter have been previously published in, (TeSLA 2016).

2 Technical Security Features in TeSLA

2.1 Security Problems and Use Cases

Specific security problems related to e-assessment systems in the eLearning literature point out the following question (Thamadharan & Maarop 2015), (Apampa, Wills & Argles 2009): "*How can learners and educators be confident that the e-assessment system can be trusted so that it can detect cheating attempts*?" To properly answer the

above question, we shall first raise concerns about situations in which a precise e-assessment system can be misused.

From an educational point of view, several situations can source the problems. The main one is often referred to as the recognition of the learner's identity. In case learner's identity is being used by someone else, rather than the real learner to be assessed, we can refer to identity misuse, which leads to the following use cases:

- E-assessment could occur in a controlled environment, such as a university building under educator supervision, and it is a common case in universities with blended-learning. In this situation, the misuse of the system is possible when an educator is responsible for a big number of learners and the educator does not recognize their faces. Then, additionally the educator must check, e.g., the learner's national card, to be sure of their real identity.
- It is also possible that the e-assessment process gets performed in uncontrolled environment outside the university building where the educator does not have any control on learners' identity. This is the typical situation for online learning environments, in which the educator must be sure that the assessed learner is the same as the one from the declared personal data.

In the two aforementioned cases, a fair e-assessment process can be compromised if learner's identity changes. We consider the problem of assuring identity authentication as the main challenging problem to address by the e-assessment process. By applying a suitable authentication mechanism (Laurent & Bouzefrane 2015), the educator can ensure the identity of the assessed learner no matter where the assessment is located, hence avoiding the necessity of checking the identity periodically, as this can be time consuming.

If during the e-assessment process, private or sensitive data are transmitted, a second major problem arises. This is related to the disclosure of sensitive information to unauthorized parties. Regarding this issue, the following two use cases are defined:

- During an e-assessment process, learners may share more data than needed. Here, the role of the educator is very important, because he has to design the assessment scenarios in a way that will collect only the data needed to ensure a successful assessment process. The learners should not have to provide information that does not concern either the educator, or the improvement of the teaching and learning process, or the formation of the final mark. For example, if the educator starts a forum topic that is part of e-assessment scenario, this must exclude problems for discussion by learners that will reveal more private or sensitive data. The collection of any additional data will foster options for information disclosure.
- Learners' or educator's information can be stolen in result of the internal or external intervention of a malicious user and the e-assessment might be compromised. The loss of information of learners' achievements in this case will not allow the educator to form the final learners' marks. As a result, learners may have to take the assessment activities again and the educator has to mark them

again. Before that, the educator has to prepare new variants of the same assessment activities. It is time consuming and is an overload task for learners and educators. Of course, learners' data can be potentially stolen in traditional assessment environments, but in online assessment the information is much more vulnerable.

The two aforementioned use cases make the possibility for information disclosure very high, especially when data is transmitted from one system component to another, or from one organization to another. This can cause difficulties during the e-assessment process. This second problem concerns data confidentiality. It requires data protection and access control, to avoid the disclosure of data to unauthorized parties. Since the e-assessment data are stored in records and databases, fraudulent alteration of data must be addressed. Data modification leads to serious e-assessment problems for learners and educators. The following use cases are identified:

- An adversary (learner, faculty, university staff, etc.) can gain unauthorized access to the educational records and databases, in order to modify private or sensitive information (e.g., the outcomes of a quiz activity). This leads to a confusing situation and unclear picture for the educator.
- An adversary with unauthorized access to the e-assessment tasks before they are assigned to learners, could modify or distribute them to learners (e.g., for financial profit). The e-assessment process may lose its meaning which is to evaluate and measure the real learners' knowledge and skills.
- It may also be possible for the adversary to corrupt or delete part or the whole assessment information. This creates difficulties for the learners and the educator.

In all those aforementioned cases, the main challenging problem concerns data integrity, i.e., how to assure that data is secured in the case of fraudulent data alteration.

2.2 Integration of Security Measures in the TeSLA Architecture

The TeSLA architecture[1] is comprised of several entities (see Figure 1), some of them located in a cloud infrastructure, and shared among several institutions; some others deployed individually at an institutional level (e.g., one per university). Regardless of the location of each entity, TeSLA must secure the establishment of communications between entities such as Learning Management Systems (LMS) and Virtual Learning Environment (VLE), as well as with external tools embedded into the learners' browsers. Securing such architecture is a complex task. It consists in expressing all the security needs regarding sensitive and personal data on one hand, and analyzing threats and security levels on both hosts and network elements on the other. The choices made on the underlying security properties of the TeSLA architecture must also follow requirements in terms of learners' privacy, as those expressed by General

[1] More detailed information related to the TeSLA architecture can be found in Chapter 4: Engineering Cloud-based Technological Infrastructure to Enforce Trustworthiness.

Data Protection Regulation (GDPR) directives for all individuals within the European Union and the European Economic Area (EUR-Lex 2016). In a nutshell, this requires that the architecture guarantees (1) the ability to ensure the confidentiality and integrity of system communications and related services; and (2) ability to guarantee proper pseudonymization process of all user identities; and (3) ability to guarantee and appropriate protection of all the personal data stored or processed by the system as well.

Consequently, the security services provided by the TeSLA architecture concern the enforcement of authentication and protection of both communications and data storage. Authentication aims at proving an entity's identity to another party, leading to providing enough guarantees in terms of confidentiality and integrity. In turn, confidentiality consists in protecting data to prevent information disclosure to unauthorized parties. Integrity aims at preventing fraudulent data alteration. Over the network, the most convenient way to implement these security services is to use the TLS (Transport Layer Security) protocol (Dierks & Rescorla 2008), which allows entities to authenticate to each other and creates a secure tunnel with data encryption and integrity checks.

Insert Figure 1 here

Figure 1. The TeSLA architecture.

Authentication in TLS relies on the use of X.509 certificates (ITU 2016), which, in turn, use asymmetric cryptography, and create an association between a public key and an identity. Any entity can authenticate itself via its certificate, as long as it owns the associated private key, which is never transmitted over the network. The certificate management requires a Public Key Infrastructure (PKI) (Cooper et al.2005)], in which specific trusted entities, called Certification Authorities (CA), are in charge of certificate delivery. The TeSLA architecture has its own PKI, to manage the certificates within the TeSLA domain on one hand; and within the institution domain on the other. This way, the communications between the various entities of the architecture can be entirely secured.

Some of the aforementioned elements and mechanisms are elaborated further in the following sections as a summary of the main actions and guidelines followed during the design phase of the TeSLA architecture. Such actions and guidelines are the result of a careful analysis conducted by the technical members of the TeSLA project, to guarantee that the resulting architecture follows generic best practices and well-established security standards (see (ISO 2013), (OWASP 2013), (ANSSI 2016), (IEEE Standards 2018) and citations thereof, for further details).

2.3 TLS and PKI-based Communication

The TeSLA architecture guarantees that traditional information security properties such as confidentiality, integrity and authentication are always respected. This is achieved as follows: (1) use of TLS to secure all the exchanges between components

of the architecture; (2) deployment of a PKI associated to the TeSLA architecture; (3) enforcement of mutual authentication between all the components of the architecture.

The TLS protocol ensures confidentiality, integrity, authentication and non-repudiation altogether for two communicating entities. The protocol consists of two phases: the handshake, during which the security parameters are negotiated (in particular, cipher and hash algorithms (Menezes, van Oorschot, & Vanstone 2011). The communicating entities are hence authenticated (either mutually or one-way). In the second phase, a secure tunnel is established between the two communicating entities, ensuring that all data are properly encrypted and cannot be modified by an attacker during transmission. Symmetric keys are used to encrypt all the TLS exchanges. The keys are automatically and dynamically generated during the initial handshake of the TLS protocol.

TLS-based authentication requires X.509 digital certificates, which are managed by the PKI. The principle of a certificate is to assess the link between an entity and its public key, through a TTP (Trusted Third Party) called a Certificate Authority (CA). The CA digitally signs certificates itself, or delegates the signature activity to intermediate entities. The validation of a certificate during the authentication process includes the following steps: (i) check the expiration date of the certificate; (ii) verify the signature of the certificate; (iii) check if the signing CA is recognized as a trusted CA; (iv) check if the certificate has not been revoked.

The PKI model proposed for the TeSLA architecture is available in (Kiennert, Rocher et al. 2017). The PKI secures, for instance, all the exchanges with biometric instruments, i.e., those TeSLA components in charge of evaluating data to assess learner's identity and authorship (see Section 2.1, second use case: "*the educator must be sure that the assessed learner is the same as the one from the declared personal data*"). More information about the use of PKI certificates is provided in the following sections.

2.3.1 Certificate Management

The PKI model proposed in (Kienert, Rocher et al. 2017) for the TeSLA architecture identifies the following four representative certificate authorities: (i) TeSLA CA; (ii) TeSLA Intermediate CA; (iii) Institution CA; and (iv) Institution Intermediate CA.

Firstly, the TeSLA CA is the top certificate authority regarding the TeSLA PKI. Basically, this certificate authority is only used once, to sign the TeSLA intermediate CA signature request. It is recommended to use this certificate as scarcely as possible (ISO 2013), (Dierks & Rescorla 2008). Then, the TeSLA intermediate CA signs the Institution CAs certificates (one for each institution) and delivers the client and server certificates for the TeSLA components. The Institution CA is the top certificate authority regarding the institution based TeSLA components. For security purposes, the use of the certificate associated to the Institution CA is minimized, e.g., it is used only once, to sign the Institution intermediate CA signature request. As for the TeSLA CA certificate, it is also recommended to use it as scarcely as possible. Finally, the Institution Intermediate CA is used to deliver client and server certificates of the

architecture components (e.g., backend components of TeSLA system and its corresponding databases).

2.3.2 Revocation Lists

The TeSLA PKI shall maintain, update and provide secure access to two main revocation lists (Cooper at al 2008): (i) the revocation list associated to the TeSLA CA; and (ii) the revocation list associated to the TeSLA intermediate CA. Each institution using its corresponding CAs has to manage, update and provide secure access to two revocation lists: the revocation list associated to the Institution CA, and the revocation list associated to the Institution intermediate CA.

With respect to the secure connections between the TeSLA components, the certificate validity must be checked with respect to their revocation lists. A certificate may indeed be valid (i.e., not expired and with a correct signature), but marked as revoked. Finally, the use of the Online Certificate Status Protocol (OCSP) (Santesson et al. 2013) has also been included at the core PKI functionality of TeSLA, for obtaining the revocation status of X.509 digital certificates.

2.3.3 Cryptographic Keys

We conclude this section with a quick overview regarding the security procedures that have to be applied when a private key is disclosed, as suggested in (Barker 2016) and (ANSSI 2016). Possible incidents are classified in terms of critical levels (in which zero represents the most critical one, i.e., the one with the highest priority).

- Level 0 - If the TeSLA CA private key has been compromised, then the whole system is compromised. The whole TeSLA PKI has to be recreated, and all the certificates and CAs that had previously been generated must be revoked.
- Level 1 - If the TeSLA Intermediate CA private key has been compromised, then the TeSLA CA has to revoke this certificate. All the certificates that were signed by the TeSLA Intermediate CA have also to be revoked. On the other hand, if a client/server private key associated to a certificate signed by the TeSLA Intermediate CA has been compromised, then the TeSLA Intermediate CA has to revoke this certificate.
- Level 2 - If the Institution CA private key has been compromised, then the TeSLA Intermediate CA has to revoke this certificate. All the certificates that were signed by the Institution CA have also to be revoked.
- Level 3 - If an Institution Intermediate CA private key has been compromised, then the TeSLA Institution CA has to revoke this certificate. All the certificates that were signed by the Institution Intermediate CA have also to be revoked. Likewise, if a client/server private key associated to a certificate signed by the Institution Intermediate CA has been compromised, then the Institution Intermediate CA has to revoke this certificate.

Finally, the CA certificates use RSA keys with a modulus of at least 4096 bits (Menezes, van Oorschot & Vanstone 2011), (ANSSI 2016) and (Barker 2016). The validity is fixed to ten years maximum (also limited by the TeSLA license validity period). Client and server certificates use RSA keys with a modulus of at least 2048 bits [ANSSI 2016) and (Barker 2016). The validity is fixed to one year. Attention must be paid to certificate management to prevent architecture malfunctioning, e.g., new certificate emission to clients and servers before their actual certificates expire.

3 Security Evaluation of a Representative TeSLA Deployment

In this section, we provide an empirical security hands-on analysis of the deployment of TeSLA at the Technical University of Sofia (TUS for short) (Baró-Solé et al. 2018). The analysis builds upon an existing methodology (Ivanova & Rozeva 2017), provided by TUS for the verification of secure web services and applications. The analysis focuses on the e-assessment environment at TUS, involving Moodle (Kumar & Dutta 2011), complemented by the TeSLA release deployed at TUS for the pilots of the TeSLA project. The criteria, parameters and underlying tools for the evaluation used during the analysis support multi-criteria decision-making and are based on fuzzy set theory and fuzzy logic.

3.1 Aims and Background

3.1.1 Fuzzy sets and fuzzy logic

An online environment implementing variety of web services is always vulnerable to various threats and attacks. The correct evaluation of its security status is a complex task, due to difficulties in considering and proper identification of all the factors that influence it. Decision-making and tasks concerning security issues have to be performed based on incomplete information provided by experts. Such information is mainly in form of natural language statements involving linguistic variables, i.e. “High”, “Medium”, “Low”, rather than numbers. Cases like these require dealing with approximations of numbers, which are close to a given real number, rather than with crisp real numbers and crisp intervals. Classic mathematical description and formalization turns out to be inapplicable to such knowledge, expressed in natural language statements, referred to as fuzzy statements.

An approach providing for finding optimal decision by such expert systems, which has been adopted for the evaluation of the security status of TeSLA online environment is based on the fuzzy set theory. It states the conceptualization of fuzzy statements by appropriate fuzzy sets in R (real numbers set) in order to treat them as fuzzy numbers. It has been widely adopted in decision support, knowledge based and expert systems. It has become the background of methodology designed at conceptual level (Ivanova & Rozeva 2017), which addresses managers, technical professionals and other authorities involved in securing the online environment in an organization. It has been implemented for performing empirical analysis of the security level of the deployment of TeSLA in the online virtual learning environment at TUS.

Fuzzy set (Zadeh 1965) Ã of set X is defined by its membership function μÃ: X→ [0,1] as x→ μÃ (x)∈ [0,1]. The fuzzy membership function μÃ (x) indicates the degree of belonging of x ∈ X to Ã. Value 0 corresponds to absolute non-membership and value 1 to full membership. For set X with elements x1, x2, ... xn, the fuzzy set Ã = {(x1, μ (x1)), (x2, μ (x2)), ... (xn, μ (xn))}. Fuzzy sets can be represented by different kinds of membership functions. The most popular variant of membership function is the "triangle" one, as it provides for the simplification of calculations performed upon fuzzy sets. The triangular membership function (Porebski & Straszecka 2016), depends on three scalar parameters a, c (lower and upper bound) and b (mean value) and is defined as (1):

$$\mu_A(x) = \begin{cases} \frac{x-a}{b-a}, & a \le x \le b \\ \frac{c-x}{c-b}, & b < x \le c \\ 0, & a < x, x > c \end{cases} \quad (1)$$

Fuzzy numbers, defined by triangular membership function are referred to as triangular fuzzy numbers. A fuzzy number is denoted by a triplet (a, b, c).
The basic operations on triangular fuzzy numbers $\tilde{A}_1$ (a_1, b_1, c_1) and $\tilde{A}_2$ (a_2, b_2, c_2) are defined as follows:

Addition +: $\tilde{A}_1 \oplus \tilde{A}_2 = (a_1 + a_2, b_1 + b_2, c_1 + c_2)$,
Subtraction -: $\tilde{A}_1 \ominus \tilde{A}_2 = (a_1 - c_2, b_1 - b_2, c_1 - a_2)$,
Multiplication x: $\tilde{A}_1 \otimes \tilde{A}_2 = (\min(a_1a_2, a_1c_2, c_1a_2, c_1c_2), b_1b_2, \max(a_1a_2, a_1c_2, c_1a_2, c_1c_2))$.
Comparison ≤: $\tilde{A}_1 \le \tilde{A}_2 \rightarrow (a_1, b_1, c_1) \le (a_2, b_2, c_2)$.
Mean $m(\tilde{A}) = 1/3(a + b + c)$,
Variance $\sigma(\tilde{A}) = 1/18(a^2+b^2+c^2-ab-ac-bc)$

Fuzzy numbers are implemented in fuzzy logic, which is an approach for computing, based on partial, i.e. truth to a certain degree and not on the absolute truth (true / false). This is close to real life cases where a lot of imprecise data is generated. It provides for representation of generalized human cognitive abilities in software solutions. Fuzzy logic involves building fuzzy IF-THEN rules as a way for formalizing human natural language and facilitating decision-making. Sample fuzzy rule is IF x is A THEN y is B, where A and B are linguistic values defined by fuzzy sets, x and y are input and output variables. The input to the rule is a crisp value x, which is transformed into fuzzy set by applying a specialized function. The procedure is referred to as fuzzification. The output to the rule is a fuzzy set assigned to the output variable y, which is turned into a crisp number after performing the reverse transformation called defuzzification.
The process involving fuzzy logic based inference on expert knowledge simulates human reasoning by implementing relatively simple mathematical concepts.

3.1.2 Fuzzy logic algorithm for empirical security analysis

The main goal of the algorithm is the identification of the influence of selected criteria and parameters that are most relevant for assuring high security level of the virtual learning environment with TeSLA deployment at TUS. Performance ratings and importance weights for them are defined by using fuzzy numbers. Fuzzy logic is implemented in the decision-making process, as suggested in (Ansari, Mittal & Chandna 2010). Fuzzy performance-importance index of each criterion and parameter is calculated to facilitate the improvement the security level of the TeSLA e-Assessment environment.

A. Criteria definition

Criteria that are relevant to the security degree of the services related to TeSLA deployment at TUS are defined. Figure 2 presents the hierarchical relationship of a global criterion (GC), criteria (C_i) and their parameters (P_i).

Insert Figure 2 here

Figure 2. Criteria and parameters for security evaluation of TeSLA deployment

B. Definition of security level scale with triangular fuzzy numbers for criteria boundaries.

C. Definition of linguistic variables with triangular fuzzy numbers for rating the performance and weighing the importance of the security criteria and parameters.

D. Security evaluation by experts and aggregation of the obtained fuzzy numbers for performance-ratings and importance-weights (Equation 2).

$$a = \sum_{i=1}^{3} a_i /3\ ,\ b = \sum_{i=1}^{3} b_i /3,\ c = \sum_{i=1}^{3} c_i /3 \quad (2)$$

E. Calculation of the fuzzy indexes of criteria C_i and their parameters.

The fuzzy indexes of each criterion C_i are calculated by Equation (3):

$$WR = \sum_{i,j=1}^{n} W_{ij}\, R_{ij} / \sum_{i,j=1}^{n} W_{ij}, \quad (3)$$

where W_{ij} are the importance-weights of parameters, and R_{ij} are the performance-ratings.

F. Calculation of the fuzzy security index for the global criterion. Match the result obtained as triangular fuzzy number to the linguistic variable corresponding to the respective security level in the scale from **B.**

G. Validation of the security level determined in **F** by the Euclidean distance of the global criterion to each security level.

The Euclidean distance is the distance between two triangular fuzzy numbers X ($x1$, $x2$, $x3$) and Y ($y1$, $y2$, $y3$). It is calculated by Equation (4) (cf. [CHK08] and citations thereof, for further details):

$$D(X,Y) = \sqrt{\frac{1}{6}[(x_1 - y_1)^2 + 4(x_2 - y_2)^2 + (x_3 - y_3)^2]} \quad (4)$$

The calculated security level corresponds to the minimal value of the Euclidean distance and its linguistic value is obtained from the scale, defined in **B**.

H. Calculation of the performance-importance indices and rating scores of all parameters of the security criteria for suggesting the ones that could be improved.

Performance-importance indices FPII are calculated by Equation (5):

$$FPII = [(1,1,1) \ominus W'_{ij}] \otimes PRI, \quad (5)$$

where W'_{ij} is the importance-weight fuzzy number of all the parameters with reversed places of fuzzy values and PRI is their matched performance-rating fuzzy number. FPII numbers are then matched to crisp rating scores by using Equation (6):

$$RS = (x_1 + 2x_2 + x_3)/4, \quad (6)$$

The minimal values of the rating scores indicate which parameters must be addressed as vulnerabilities that could compromise the security status.

3.2 Results of empirical security analysis

B → The security status of the TeSLA deployment environment at TUS is evaluated at five levels. The linguistic variables and the fuzzy numbers that have been chosen to define the boundaries of each security level are shown in Table 1.

	Security Levels				
Linguistic Variable	NS (non-secure)	PS (poorly secure)	MS (moderately secure)	S (secure)	VS (very secure)
Fuzzy Set	(0, 0.6, 1.2)	(1, 1.6, 2.2)	(2, 2.6, 3.2)	(3, 3.6, 4.2)	(4, 4.5, 5)

Table 1. Linguistic variables and Fuzzy numbers of defined security levels.

C→ The security criteria and parameters' rating of performance and weighing of importance are performed with linguistic variables and fuzzy numbers defined in Table 2. A scale from 0 to 5 is chosen for each fuzzy set definition. The importance-weights range from 0 to 1.

R (Performance Rating)			**W (Importance Weighting)**	
Linguistic Variable	**Fuzzy Set**		**Linguistic Variable**	**Fuzzy Set**
P (Poor)	(0, 0.6, 1.2)		Very low (VL)	(0, 0.12, 0.24)

F (Fair)	(1, 1.6, 2.2)		Low (L)	(0.2, 0.32, 0.44)
G (Good)	(2, 2.6, 3.2)		Medium (M)	(0.4, 0.52, 0.64)
VG (Very Good)	(3, 3.6, 4.2)		High (H)	(0.6, 0.72, 0.84)
E (Excellent)	(4, 4.5, 5)		Very High (VH)	(0.8, 0.9, 1)

Table 2. Performance-ratings and importance-weights of the criteria and parameters.

D→ The rating of performance **R** and weighing the importance **W** of the security criteria and parameters have been obtained by surveying three experts involved in the TeSLA system pilots at TUS as software and security professionals. Sample expert evaluation in terms of the linguistic variables is shown in Table 3.

Criterion C_i	**Weight W_i**	**Parameter P_{ij}**	**Weight W_{ij}**	**Rating R_{ij}**
C1	VH	P01	VH	E
		P02	VH	E
		P03	VH	E
		P04	VH	E
		P05	H	VG
		P06	VH	VG
		P07	VH	E
		P08	VH	VG

Table 3. Performance-ratings and importance- weights expert vote.

Excerpt of the three votes for criterion C1 and parameters P01 and P02 represented as fuzzy numbers is presented in Table 4.

Criterion C_i	**Weight W_i**	**Parameter P_{ij}**	**Weight W_{ij}**	**Rating R_{ij}**
C1	(0.7, 0.85, 1)	P01	(0.5,0.7, 0.85)	(3, 4, 5)
	(0.7, 0.85, 1)		(0.7,0.85, 1)	(4, 5, 6)
	(0.7, 0.85, 1)		(0.7,0.85, 1)	(4, 5, 6)
		P02	(0.5,0.7, 0.85)	(4, 5, 6)
			(0.5,0.7, 0.85)	(3, 4, 5)
			(0.7, 0.85, 1)	(4, 5, 6)
		…	…	…

Table 4. Excerpt of votes for performance and importance of criteria and parameters.

The votes for all criteria and parameters have been aggregated (Equation 2). The definitions of the obtained ratings **R** and weighs **W** for all parameters are presented in Table 5.

C1			**C2**		
P_{ij}	**R_{ij}**	**W_{ij}**	**P_{ij}**	**R_{ij}**	**W_{ij}**
P01	(4, 4.5, 5)	(0.8, 0.9, 1)	P09	(4, 4.5, 5)	(0.8, 0.9, 1)
P02	(4, 4.5, 5)	(0.8, 0.9, 1)	P10	(4, 4.5, 5)	(0.8, 0.9, 1)
P03	(4, 4.5, 5)	(0.8, 0.9, 1)	P11	(4, 4.5, 5)	(0.8, 0.9, 1)
P04	(4, 4.5, 5)	(0.8, 0.9, 1)	P12	(4, 4.5, 5)	(0.8, 0.9, 1)
P05	(3, 3.6, 4.2)	(0.6,0.7,0.8)	P13	(4, 4.5, 5)	(0.8, 0.9, 1)
P06	(3, 3.6, 4.2)	(0.8, 0.9, 1)	P14	(4, 4.5, 5)	(0.8, 0.9, 1)
P07	(4, 4.5, 5)	(0.8, 0.9, 1)	P15	(4, 4.5, 5)	(0.8, 0.9, 1)

P08	(3, 3.6, 4.2)	(0.8, 0.9, 1)	P16	(3, 3.6, 4.2)	(0.8, 0.9, 1)
			P17	(3, 3.6, 4.2)	(0.8, 0.9, 1)

C3		
$\mathbf{P}_{ij}$	$\mathbf{R}_{ij}$	$\mathbf{W}_{ij}$
P18	(4, 4.5, 5)	(0.8, 0.9, 1)
P19	(4, 4.5, 5)	(0.8, 0.9, 1)
P20	(3, 3.6, 4.2)	(0.8, 0.9, 1)
P21	(3, 3.6, 4.2)	(0.8, 0.9, 1)
P22	(3, 3.6, 4.2)	(0.6, 0.7, 0.8)
P23	(3, 3.6, 4.2)	(0.8, 0.9, 1)

Table 5. Aggregated fuzzy sets for ratings and weights of the parameters.

E→ The fuzzy indices of each criterion C_i are calculated (Equation 3) by considering the influence of the respective parameters.

The fuzzy numbers of criterion C1 using the values in Table 5 are obtained as follows:

$C_1 = [5 \otimes (0.8, 0.9, 1) \otimes (4, 4.5, 5) \oplus 2 \otimes (0.8, 0.9, 1) \otimes (3, 3.6, 4.2) \oplus (0.6, 0.72, 0.84) \otimes (3, 3.6, 4.2)]/[7 \otimes (0.8, 0.9, 1) \oplus (0.6,0.72, 0.84)] = (3.65, 4.18, 4.71)$.

For C2 and C3, the following fuzzy indices are obtained:

$C_2 = (3.78, 4.3, 4.82)$, from the aggregated values for parameters P09 to P17;
$C_3 = (3.35, 3.91, 4.47)$, from the aggregated values for parameters P18 toP23.

F→ The global criterion index is obtained in a similar way as the indices of C1, C2 and C3, i.e., $GC = (3.59, 4.13, 4.7)$. It summarizes the influence of the criteria and their parameters with respect to security of the TeSLA system deployment at TUS. The obtained result in terms of fuzzy values is matched to the corresponding linguistic variable of the security level described in Table 1, and it is characterized as *very secure* deployment.

G→ The Euclidean distance of the global criterion GC to each security level (Equation 4) is presented in Table 6. The linguistic value of the security level (cf. Table 1) is determined by the minimal value of the calculated Euclidean distance The minimal value is D(GC, VS)=0.038, which corresponds to security level denoted as *very secure*. This result validates the security level, obtained in **F**.

D(GC, VS)	D(GC, S)	D(GC, MS)	D(GC, PS)	D(GC, NS)
0.038	0.383	1.187	1.796	2.503

Table 6. Euclidean distance from global criterion to each security level.

H→ Identification of criteria and parameters that could be improved for enhancing the security level. For this purpose, Fuzzy Performance-Importance Indices are calculated (Equation 5). FPII of parameter P01 is obtained as follows:

$FPII = [(1,1,1) \ominus (1, 0.9, 0.8)] \otimes (4, 4.5, 5) = (0, 0.45, 1).$

The calculated value (Equation 6) is the rating score. The RS index of P01 is:

$RS = \frac{0+2.0.45+1}{4} = 0.475.$

The obtained Fuzzy performance-importance indices and rating scores of all parameters are presented in Table 7.

Parameter	**FPII (Fuzzy-Performance Importance Index)**	**RS (Rating Score)**
P01	(0, 0.45, 1)	0.475
P02	(0, 0.45, 1)	0.475
P03	(0, 0.45, 1)	0.475
P04	(0, 0.45, 1)	0.475
P05	(0.48, 1.01, 1.68)	1.04
P06	(0, 0.36, 0.84)	0.39
P07	(0, 0.45, 1)	0.475
P08	(0, 0.36, 0.84)	0.39
P09	(0, 0.45, 1)	0.475
P10	(0, 0.45, 1)	0.475
P11	(0, 0.45, 1)	0.475
P12	(0, 0.45, 1)	0.475
P13	(0, 0.45, 1)	0.475
P14	(0, 0.45, 1)	0.475
P15	(0, 0.45, 1)	0.475
P16	(0, 0.36, 0.84)	0.39
P17	(0, 0.36, 0.84)	0.39
P18	(0, 0.45, 1)	0.475
P19	(0, 0.45, 1)	0.475
P20	(0, 0.36, 0.84)	0.39
P21	(0, 0.36, 0.84)	0.39
P22	(0.48, 1.01, 1.68)	1.04
P23	(0, 0.36, 0.84)	0.39

Table 7. Fuzzy performance-importance indices and rating scores of parameters.

3.3 Evaluation and recommendations

The minimal values of the rating scores indicate which parameters must be addressed in terms of potential vulnerability for compromising the security status of the TeSLA deployment at TUS. Table 7 shows that the minimal value of rating score is 0.39, which is bounded to parameters P06, P08, P16, P17, P20, P21, P23. This means that special attention must be paid to the following criteria and specific

parameters, in order to assure proper maintenance of the security level obtained by the deployment of TeSLA at TUS:

- P06 (applying standards for security) and P08 (guidelines regarding security) referring to the criterion C1 (programming code);
- P16 (network monitoring) and P17 (security configuration) referring to criterion C2 (administration);
- P20 (home-working & mobile devices), P21 (rules for data usage) and P23 (managing incidents) referring to criterion C3 (policies).

In the context of TeSLA deployment in the virtual learning environment at TUS P08 implies the need for requirements and recommendations for the secure elaboration, adoption, administration and use of the TeSLA web services. P16 refers to the configuration of a firewall; traffic monitoring and understanding web services' proper functioning. In case of recognized problems vulnerabilities and possible threats and attacks should be detected. P17 implies proper certificate authorization management; efficient access control of different user categories, i.e. students, teachers, managers, administrative staff.

The obtained and validated result "very secure" of the fuzzy security index after performing fuzzy logic based empirical analysis of security issues indicated that the deployment of TeSLA at TUS is at sufficient security level. Another analysis result suggested some criteria and parameters subjected to further improvement in order to guarantee its maintenance at the required security level.

4 Identities and Privacy Management

As pointed out in Section 2 of this chapter, TeSLA provides numerous protection features to properly secure the exchange of learners' data from institutional and cloud domains, to third party services. To guarantee the high degree of security evaluated in Section 3, the learner identity managed by the TeSLA components must be seamlessly and securely linked to the identity in use in each context.

Notice that a single learner may have several digital identities. For instance, the identity provided by the university where the learner is registered. Usually, this identity is linked with learner data such as first and last names, date of birth, and visual data (e.g., learners' photography). When the learner accesses the new services provided by TeSLA, direct mapping is performed between login and personal data, if the connection is within the institutional domain. However, whenever the services refer to other domains (e.g., cloud domain or third party agents), the learner may have to make use of other digital identities needed to authenticate to these services. Since these identities all refer to the same learner, they cannot be decorrelated.

Several solutions exist to reduce the need for various credentials and refer to only one identity. The first one consists in adding third party services as plugins to the learning environments, and forwarding the necessary personal data to the services, based on the identity in use in the institutional domain. For instance, standards like

LTI (Learning Tools Interoperability) make these interactions possible (Durand & Downes 2009). A trust relationship is established between domains, e.g., using a shared secret that ensures the security of all the remaining exchanges based on the OAuth 1.0 standard (Leiba 2012).

The second solution, which is adapted to the case of third party services built independently from TeSLA, consists in relying on identity federation, implemented in several standards such as OpenID, SAML (*Security Assertion Markup Language*), or Shibboleth. Identity federation consists in delegating authentication to an identity provider. The user who wishes to access the service provider is redirected to the identity provider for authentication, where authorization token is generated to certify the authentication success. This token is then transmitted to the service provider, which allows the user to be regarded as authenticated. This way, in case of deploying TeSLA as a standalone service, the enforcement of authentication can be managed using traditional identity federation services, i.e., by simply allowing institutional domains to act as identity providers.

4.1 Use of Pseudonymous Identification in TeSLA

While the above standards provide the technological basis to link learner's identity with TeSLA, specific attention should be paid to privacy issues. As already anticipated in Section 1, the personal data associated to one's identity must be carefully managed during the association of entities and domains, e.g., to avoid the unauthorized disclosure of private information. In order to make it possible for the learner to take assessments without disclosing personal information, TeSLA provides pseudonymity management. Learners are authenticated and authorized in TeSLA without allowing TeSLA to know the real identity of the learner.

Anonymity is only partial in this context, since links between the TeSLA identifiers (hereinafter denoted as TesLA ID) and the learners' true identities remain available at institutional level (e.g., at the university domain). The precise approach, from a technical standpoint, is as follows. Each institution (e.g., university) generates a series of randomized Universally Unique IDentifiers (UUIDs) (TeSLA uses version four of the UUID standard (Leach 2005) for each learner. As such, the institution generating the UUIDs is the only entity able to make the link between a precise UUID and the records of the learner. Using public information, such as learner's e-mail address to generate a UUID using version 3 or version 5 of the UUID standard, is excluded for operational deployments, since it allows attackers to compute all the possible TeSLA IDs from the learner's directory, and deduce the link between learners' names and TeSLA IDs.

The UUIDs are stored in databases that are shared between all the remaining components of the TeSLA architecture (see Section 2). A dedicated component, i.e., the TeSLA Identity Provider, is mapped to the database in order to receive requests from the remaining TeSLA components. This provider is issued with learners' true identities, and replies with the corresponding UUID. The communication between TeSLA components (e.g., TeSLA plugins) and the identity provider is mutually authenticated with TLS (see Section 2). In case learners' authentication is certificate-

based, e.g., learners interacting with TeSLA through a series of plugins, the learner only needs to authenticate once. The certificate used for the authentication of each component is associated to learner's true identity. Then, when a request is sent to TeSLA, the system retrieves the TeSLA ID associated to learner's identity from the identity provider, and eventually communicates with other TeSLA components, while guaranteeing the pseudonymity of the learner.

Some external tools, embedded as JavaScript code within the learner's web browser, also need to communicate to the TeSLA system without revealing learner's true identity, nor retrieving the TeSLA ID either. A session token mechanism, based on JWT (JSON Web Tokens) (Jones, Bradley & Sakimura 2015), is used for this purpose. When a TeSLA plugin authenticates to the identity provider and retrieves the TeSLA ID, tokens are created and provided to the external tools, using public key cryptography to secure the signature of the tokens.

With respect to the protection of learners' data outside their respective institution data centers, no traceability features are implemented. Apart from the TeSLA ID association, stored at the identity provider (within the learner's institution domain), all the remainder personal data of learners, such as the IP address or similar data, which could be used to map different sessions of the same learner, are omitted. As a result, the architecture presented in Section 2 provides full pseudonymity for learners. Learner's identity remains only known within the institution, while never transmitted to other components.

4.2 Future Directions towards Extended Privacy Functionalities

As already stated in Sections 2 and 3, an e-assessment 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 might lead to disastrous consequences, such as data leakage or identity theft. In addition, and to meet the GDPR recommendations (EUR-Lex 2016), it is also necessary to ensure a reasonable level of security in the system (cf. Section 3).

Security and privacy are two 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, 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 user's identity, and to prevent any undesired traceability, which is often complex to achieve.

In the context of TeSLA, several privacy technological filters are already included in the underlying design of the architecture. The randomized TeSLA identifier

associated to each learner (cf. Section 4.1) is a proper example. This identifier is used each time the learner must access TeSLA, hence ensuring pseudonymous identification of learners – full anonymity not being an option in TeSLA for legal reasons. Yet, a randomized identifier alone cannot protect 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 to handle such issues, which is proposed as potential extension of the TeSLA PKI architecture (Kaaniche et al. 2017) and (Kiennert, Kaaniche et al. 2017),, 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", "studies at IMT", 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 a learning environment, it should be enough to prove that the learner comes from an allowed institution and is registered for this course. That way, it becomes impossible for the learning environment to follow the studying activity of each learner, while still letting learners access the course material. Similarly, when a learner has taken an assessment, the learner'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.

We argue that anonymous certification might prove to be a solid and innovative asset to enhance privacy in TeSLA, and to prevent traceability of learners whenever traceability is not required. Other approaches might also be added, following the same direction for privacy enhancement. One of them consists in mixing together the data stored in a database in order to make it impossible to associate the various attributes of a table entry, hence offering anonymous data storage. Should such a technique be integrated to TeSLA, it would guarantee that even a data leak from a sensitive database will not provide any certain information to anyone — as long as the leaked data do not contain secrets such as private keys or passwords.

In terms of trust, enhanced features beyond learners' privacy can also be added to future releases of the architecture. A system like TeSLA, where learners have to take e-assessments under strict anti-cheating countermeasures, requires a high degree of trust from learners in order to be widely deployed and accepted as a legitimate assessment tool. TeSLA should provide public guarantees that its claims regarding privacy and security are met, meaning that TeSLA is as transparent as possible with respect to personal data management processes. Though it is not directly related to security and privacy, TeSLA should also ensure transparency regarding the anti-cheating decision processes, and let learners know how these decisions are made

while informing them of possible resorts at their disposal in case of false positive detection.

Pushing the analysis further requires an overall look on the global architecture, and on the fundamental choices that led to its design. Among these choices, relying on biometry for learners' authentication there is one that particularly stands out in terms of privacy. Contrary to a password, which would authenticate learners using what they know, biometric samples authenticate them using what they are. The data transmitted over the network, from the learner's computer to the TeSLA instruments, are parts of learners' identity and as such, are much more sensitive than mere passwords, which can be changed at will. With encrypted data exchanges over the network, TeSLA ensures that these biometric samples cannot be retrieved by an attacker. The anonymous treatment of samples by the TeSLA instruments strongly limits the risks in terms of unwanted access and exploitation of personal data.

The choice of biometric-based authentication for learners who are taking e-assessments entails other issues. Firstly, the biometric samples are collected from the learner's computer, which by definition has no guarantee whatsoever regarding security. Even if the samples are not meant to be stored on the learner's computer, the risk of personal data theft at this point is independent from the TeSLA architecture, but is induced by the choice to rely on biometry. As such, it should be taken into account for further improvement of the TeSLA system. Secondly, even though the biometric samples are anonymized before they are sent to the TeSLA instruments, it may be better not to send such sensitive data to TeSLA at all, and decentralize Trusted Third Parties (TTPs) as much as possible. The role of TeSLA is to offer a specific service, namely the possibility to take e-assessments. It does not, and could not act as a TTP. In the current configuration, what happens to the biometric samples depends on how TeSLA is managed. With a TTP, which would have no specific connection to TeSLA or to the academic institutions, there would be a dedicated entity whose explicit role would be to guarantee the treatment of these sensitive data, independently of the current TeSLA policy. Notice that anonymous certification will benefit of such a TTP-decentralization, as well.

To sum up, we consider that improving the privacy in TeSLA requires further decentralization of its fundamental choices, in order to offer the best privacy guarantees. Even if the use of biometry is maintained as it is, extending current TTP elements, such as the TeSLA Public Key Infrastructure (PKI), and the underlying Certification Authorities (CAs), would be a significant step in this direction.

5 Conclusion

On top of addressing numerous challenges, we have seen in this chapter that the TeSLA architecture has been designed with security guarantees in terms of communication exchanges, as well as in terms of learners' data protection with respect to their privacy, in compliance with the GDPR requirements of the European Union. Ensuring privacy in TeSLA consists in minimizing the personal information retrieved by the system during its interactions with learners. While obviously securing

the access to databases, TeSLA makes sure to anonymize every sensitive data collected from the learner. This process applies to e-assessments, which are taken by learners with an anonymized identifier, but also to the biometric samples required to authenticate the user. These biometric samples are anonymized in the same way before reaching the TeSLA system, where they are dispatched to various instruments that will analyze them accordingly, and return the results to TeSLA.

In the first part of this chapter, we have addressed possible security risks in different learning scenarios implemented in an e-assessment process from learners' and educators' perspectives. It highlights the recognition and verification of learner's identity, the disclosure of information to unauthorized parties and the fraudulent data alteration as the most challenging ones. Technical solutions, guidance and actions implemented as security services in the architecture of the TeSLA e-assessment system, are outlined and discussed. The presented solution is mainly based on TLS protection via authorized certificates and public key infrastructures. Certificate management and security procedures to apply in case of private key disclosure were also explained. It has been shown that TeSLA guarantees the required security level concerning confidentiality and integrity of system communications of the e-assessment process in different learning scenarios, which respects the European regulations for the appropriate protection of all personal data referring to user identities.

In the second part, we have performed a methodological verification of the underlying services of TeSLA. The evaluation has been performed in the technical context of the TeSLA deployment at TUS (the Technical University of Sofia), as a representative member of the TeSLA consortium where the pilots of the TeSLA project were conducted. The evaluation concerned the deployment environment and experience gained by TUS during the execution of the three pilots of the project. The methodology used for the execution of our evaluation is based on the use of Fuzzy Set Theory and Multi-Criteria Decision Making Methodologies. Both disciplines have been applied to analyze the current security level of the TeSLA environment at TUS, in order to provide information to responsible professionals, interested bodies as well as to end users about the security level of the TeSLA deployment at TUS and suggest issues for its proper maintenance.

In the third part, we have presented the precise approach for pseudonymization of learners in TeSLA. We have also provided some ideas for future research directions, towards extended privacy functionalities. Among them, we have highlighted enhancements such as adding anonymous certification, and improving the level of transparency of the whole system. We have argued that the technical completion of the TeSLA platform, as well as its seamless integration to usual educational activities, are probably the two most obvious factors that one can name. TeSLA must succeed in convincing learners that they can trust the system as a legitimate examination module that is devoid of any serious risk for their personal data. Ensuring privacy and transparency not only allows TeSLA to meet the requirements of the GDPR; it will greatly help TeSLA to obtain learners' trust, even more than achieving legal and ethical considerations.

References

Ansari, S, Mittal, P & Chandna, R 2010, 'Multi-criteria decision making using fuzzy logic approach for evaluating the manufacturing flexibility', *Journal of Engineering and Technology Research*, vol. 2, no. 12, pp. 237-244..

ANSSI 2016, Best Practices, Available from: , https://www.ssi.gouv.fr/administration/bonnes-pratiques/. [20.10.2016]

Apampa, KM,Wills, G & Argles, D 2009, 'Towards Security Goals in Summative E-Assessment Security', *2009 International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 1-5, Available from IEEE Xplore Digital Library. [29 January 2010]

Baró-Solé, X, Guerrero-Roldan, AE, Prieto-Blázquez, J, Rozeva, A, Marinov, O, Kiennert, C, Rocher, PO & Garcia-Alfaro, J 2018, 'Integration of an Adaptive Trust-based E-Assessment System into Virtual Learning Environments - The TeSLA Project Experience'. *Internet Technology Letters*, Available from: https://doi.org/10.1002/itl2.56 [09 June 2018].

Durand, G & Downes, S 2009, 'Toward simple learning design 2.0', *2009 4th International Conference on Computer Science & Education*, ,pp. 894-897, Available from IEEE Xplore Digital Library. [01 September 2009]..

EUR-Lex 2016, *Regulation (Eu) 2016/679 Of The European Parliament And Of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, 2016, Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj. [27 April 2016]

IEEE Standards 2018**,** *29148 – 2018 - ISO/IEC/IEEE International Standard – Systems and software engineering – Life cycle processes -Requirements engineering*, Available from: https://ieeexplore.ieee.org/document/8559686. [30 November 2018].

ITU 2016, *X.509: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*, Available from: https://www.itu.int/rec/T-REC-X.509-201610-P/en. [14 October 2016]

ISO 2013, ISO/IEC 27001:2013 – Information technology – Security techniques - Information security management systems- Requirements, Available from: https://www.iso.org/standard/54534.html . [1 October 2013]

Ivanova, M & Rozeva, A 2017, 'Methodology for Realization of Secure Web Services', *Proceedings of Academics World International Conference*, Edinburgh, UK,, pp.16-21.

Kiennert, C, Rocher, PO, Ivanova, M, Rozeva, A, Durcheva, M & Garcia-Alfaro, J 2017, 'Security Challenges in e-Assessment and Technical Solutions', *8th International workshop on Interactive Environments and Emerging Technologies for eLearning, 21st International Conference on Information Visualization*, London, UK, pp. 366-371. Available from IEEE Xplore Digital Library. [16 November 2017]..

Kiennert, C, Kaaniche, N, Laurent, M, Rocher, PO & Garcia-Alfaro, J 2017, 'Anonymous Certification for an e-Assessment Framework', *Proceedings of 22nd Nordic Conference on Secure IT Systems (NordSec 2017)*, Tartu, Estonia, pp. 70-85.,.

Kaaniche, N, Laurent, M, Rocher, PO, Kiennert, C & Garcia-Alfaro, J 2017, 'PCS, a privacy-preserving certification scheme', *12th International Workshop on Data Privacy Management (DPM 2017), 22nd ESORICS symposium*, Oslo, Norway, pp.239-256.

Kumar, S & Dutta, K 2011, 'Investigation on security in LMS MOODLE', *International Journal of Information Technology and Knowledge Management*, vol. 4, no. 1, pp. 233-238.

Laurent, M & Bouzefrane, S (eds) 2015, *Digital Identity Management*., ISTE, London...

Leiba. B 2012, OAuth web authorization protocol, *IEEE Internet Computing*, vol. 16, no, 1, pp.74-77, Available from. https://www.computer.org/csdl/magazine/ic/2012/01/mic2012010074/13rRUxjyX0o. [20 February 2012],.

Menezes, AJ, van Oorschot, PC & Vanstone, SA 2011, *Handbook of Applied Cryptography*,,CRC Press, US

Barker, E 2016,.*Recommendation for Key Management,Part I: General*, Available from: https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-4/final . [12 February 2019]

OWASP 2013, OWASP Top 10 Most Critical Web Application Security Risks... Available from: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project. [1 November 2016]

Porebski S & Straszecka, E 2016, 'Membership functions for fuzzy focal elements', *Archives of Control Sciences*, vol. 26,, no. 3, pp. 395–427.

Leach, P, Mealling, M & Salz. R 2005, *A Universally Unique IDentifier (UUID) URN Namespace*, Available from:, https://tools.ietf.org/html/rfc4122.

Cooper, M, Dzambasow, Y, Hesse, P, Joseph, S & Nicholas, R 2005, *Internet X.509 Public Key Infrastructure. Certification Path Building.* Available from: https://tools.ietf.org/html/rfc4158. [11 November 2018]

Dierks, T, & Rescorla, E 2008, *The Transport Layer Security (TLS) Protocol*. Available from: https://tools.ietf.org/html/rfc5246. [11 November 2018]

Cooper, D, Santesson, S, Farrell, S, Boeyen, S, Housley, R & Polk, W 2008, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile*, Available from: , https://tools.ietf.org/html/rfc5280. [11 November 2018]

Santesson, S, Myers, M, Ankney, R, Malpani, A & Adams, C 2013, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*. Available from: http://www.rfc-editor.org/info/rfc6960. [11 November 2018]

Jones, M, Bradley, J & Sakimura, N 2015, *JSON Web Token (JWT)*, Available from: http://www.rfc-editor.org/info/rfc7519. [19 January 2019]

Thamadharan, K & Maarop, N 2015, 'The Acceptance of E-Assessment Considering Security Perspective: Work in Progress', *World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering*, vol. 9, no. 3, pp.874-879..

TeSLA 2016, *TeSLA Home Page*, Anonymous Certification in TeSLA. Available from:. https://tesla-project.eu/anonymous-certification-tesla/. [20 July 2017]

Zadeh, L 1965, 'Fuzzy sets', *Information and Control*, vol. 8, pp. 338-353.

List of acronyms

GDPR	General Data Protection Regulation
TLS protocol	Transport Layer Security protocol
PKI	Public Key Infrastructure
LMS	Learning Management System
VLE	Virtual Learning Environment
CA	Certification Authority
TTP	Trusted Third Party
RSA	A public-key cryptosystem
OCSP	Online Certificate Status Protocol
TUS	Technical University of Sofia
LTI	Learning Tools Interoperability
SAML	Security Assertion Markup Language
UUID	Universally Unique Identifier
JWT	JSON Web Token

Glossary of terms

Anonymity Privacy filter to assure that an identity is not identifiable within a given set.

Authentication Verifying the validity of at least one form of identification.

Authorship Proving the identity of the creator of a piece of work.

Certification Authority , In charge of delivering certificates (i.e., the association between a public key and an identity, w.r.t. asymmetric cryptography).

Confidentiality Adding restrictions on certain types of data and services, to prevent information disclosure to unauthorized parties.

Fuzzy Set Uncertain sets in fuzzy logic, whose elements have degrees of membership.

General Data Protection Regulation A regulation in European Union (EU) law on data protection and privacy for all individuals within EU.

Integrity Preventing fraudulent data alteration.

Learning Management System , Educational courses (e.g., administration, documentation, reporting and delivery).

Public Key Infrastructure Infrastructure, in which specific trusted entities, called Certification Authorities (CA), are in charge of delivering certificates (i.e., the association between a public key and an identity, within the context of asymmetric cryptography).

Pseudonymity Within the context of an online activity, e.g., web surfing, use of a pseudo-identifier to allow communication without linking real identities, while allowing some monitoring tasks such as authentication and authorship.

RSA public-key cryptosystem Created by Rivest, Shamir and Adleman, and based on the mathematical difficulty of factoring very large numbers.

Transport Layer Security protocol Protocol, which evolved from Netscape's Secure Sockets Layer (SSL) protocol, and nowadays regulated by IETF's RFC5246 (Dierks & Rescorla 2008).

Trusted Third Party An intermediary entity which facilitates interactions between two parties who both trust the third party.

Virtual Learning Environment Similar to a Learning Management System (LMS), with collaborative and training features for educational goals.

X.509 A standard defining the format of public key certificates.

Index of terms

Anonymity 17, 18
Authentication 1, 2, 3, 4, 5, 6, 16, 17, 18, 19
Authorship 1, 6
CA 5, 6, 7, 8, 18, 19, 20
Confidentiality 1, 2, 4, 5, 6, 18, 20
Fuzzy Set 8, 9, 10, 11, 12, 13, 21
GDPR 4, 18, 20
Integrity 1, 2, 4, 5, 6, 18, 20
LMS 1, 4
PKI 2, 5, 6, 7, 18, 20

Pseudonymity 2, 4, 16, 17, 18, 21
RSA 8
TLS 2, 5, 6, 17, 20
TTP 6, 19, 20
VLE 1, 4, 9, 10, 15
X.509 2, 5, 6, 7