Security Challenges in e-Assessment and Technical Solutions

Christophe Kiennert[1], Pierre-Olivier Rocher[1], Malinka Ivanova[2],
Anna Rozeva[2], Mariana Durcheva[2], Joaquin Garcia-Alfaro[1]

[1] SAMOVAR, Institut Mines-Telecom, CNRS, Université Paris-Saclay, France
[2] Department of Informatics, Technical University of Sofia, Bulgaria
{joaquin.garcia_alfaro@telecom-sudparis.eu, m_ivanova@tu-sofia.bg}

Abstract

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. The issue concerning security is challenging from both educational and technical point of views. Such issues are discussed under the scope of the TeSLA project. Educational challenging problems at e-assessment are analyzed and technical architectural recommendations for securing the e-assessment system according to the General Data Protection Regulation are provided.

Keywords — **e-assessment, security, TeSLA, PKI, identity management, data protection, GDPR**.

1. Introduction

The term e-assessment explains the role of technology in support of the assessment process. Technology could be used at a single or at all stages of the assessment process during its life cycle [1]. Where and when the technology is to be utilized depends on the existing institutional infrastructure and educational strategy. Part of the training institutions and universities use stand-alone e-assessment tools for the management of the assessment tasks [2], [3]. The educational practice shows that the more preferred approach for performing e-assessment is the integration of assessment in a Learning Management System (LMS) [4], [5] because of several reasons [6], [7]:

(1) It is an effective way for the organization of the student's learning in online environment where e-assessment activities are provided with the learning materials and assignments as well as an important stage in the earning process,

(2) It enables the straightforward assessment of students' knowledge achievements with the aim of improving it and increasing the motivation for learning,

(3) Online assessment contributes to the improvement of learning performance, because the student has a freedom to choose the time and location for performing assessment activities according to learning goals, style, preferences, etc.

(4) It supports the educator, responsible for the design of assessment activities, to monitor the students' progress and to evaluate intermediate and final results,

(5) It improves the communication between students and educators in different assessment activities, because it is performed in an integrated learning environment where several communication channels exist.

In spite of the existence of a wide variety of e-assessment tools and systems in educational practice, there is still a need for new e-assessment solutions, proposing innovative forms for student identification and authorship verification as well as ensuring an e-assessment process in a secure environment.

The TeSLA system (www.tesla-project.eu) aims at providing learners with an innovative environment that allows them to take assessments remotely, thus avoiding mandatory attendance constraints. TeSLA is designed as a complex architecture in which traditional LMSs and Virtual Learning Environments (VLEs) are the entry points. Integrating a relevant and secure identity management framework for TeSLA is part of the technical challenges that arise at an early stage of the development process, in order to design a robust architecture in which security issues are addressed beforehand.

Such integrated and web-based approach in the realization of e-assessment is exposed to a wide variety of threats and attacks [8], [9]. It requires appropriate measures to secure information authentication, transaction and storage. Security issues have to be considered from both educational and technical point of views. They are discussed in the scope of the TeSLA project and pose challenges for further investigations concerning the issues related to information disclosure and alteration as well as authentication flaws.

The aim of this paper is to analyze and discuss problems and issues related to the TeSLA e-assessment system from the following two perspectives: 1) educational – treating problems concerning learners' and

educators' behavior at the e-assessment process in case of different learning scenarios and the corresponding security problems; and 2) technical architectural recommendations for securing the assessment system according to the General Data Protection Regulation (GDPR) [16].

The remainder sections of the paper are organized as follows. A set of challenging security issues to be addressed during the e-assessment process, described from the educational perspective, is provided in Section 2. Technical aspects meant for securing the architecture are provided in Sections 3, 4 and 5. Section 6 closes the paper with some conclusions.

2. Challenging Security Problems in e-Assessment Processes

E-Assessment is an important part of eLearning, which involves either a set of specific tools/systems that utilize the functionality of a LMS or a solution that integrates an e-assessment tool in a LMS. Security of eLearning treats general security issues of a LMS or VLE. As discussed in several works, e-assessment with its purpose, characteristics and way of implementation poses specific challenges to security solutions [10], [11]. Similar challenges have been identified by the authors during their activities in piloting the TeSLA system. They provoked the following main question: "How can students and educators be confident that the e-assessment system can be trusted so that it can detect cheating attempts?" The answer to this question requires understanding how an e-assessment system can be misused. From an educational point of view, several security problems are challenging in this aspect.

The first one is related to the recognition of the student's identity in case of being used by someone else, rather than the real student to be assessed. This is referred to as identity misuse. Concerning this hypothesis, the following use cases are defined:

- 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 students and he/she does not recognize their faces. Then, additionally the educator must check the students' ID to be sure of their identity.
- It is possible the e-assessment to be performed in uncontrolled environment outside the university building where the educator does not have any control on students' identity, and this is the typical situation for online learning environments. Then, the educator must be sure that the assessed student is the same as the one from the declared personal data.

In these two cases, the fair e-assessment process can be compromised because of the possibility that the provided student's identity is changed. The emerging challenging problem concerns the proper identity authentication at e-assessment. When applying a suitable authentication mechanism, the educator will be sure of the identity of the assessed student no matter where the assessment is located and he does not need to check it, as this can be time consuming.

Secondly, during the e-assessment process, private and sensitive data are transmitted, and another challenging problem arises: it is related to the disclosure of information to unauthorized parties. Regarding this issue, the following use cases are defined:

- During the e-assessment, students share more data that 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 students 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, it has not to include problems for discussion by students that will reveal more private or sensitive data. The collection of any additional data will facilitate possibilities for information disclosure.
- Students' or educator's information can be stolen in result of the internal or external intervention of an intruder and the e-assessment might be compromised. The loss of information of students' achievements in this case will not allow the educator to form the final students' marks. As a result, students 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 for students and educators. Of course, students' data can be potentially stolen in traditional assessment environment, but in online assessment the information is much more vulnerable.

The two use cases described above make the possibility for information disclosure very high, when it is transmitted from one system component to another, which can cause difficulties and confusions in e-assessment. The described challenging problem concerns data confidentiality and requires data prevention and data security to avoid its disclosure to unauthorized parties.

Thirdly, e-assessment data are stored in records and databases, which might be exposed to fraudulent alteration. Their modification could lead to serious e-assessment problems for students and educators. The following use cases are identified:

- An intruder (student, staff, etc.) gains unauthorized access to educational records or databases and modifies private or sensitive information, for example the current quiz results of one, several or all students. It leads to a confusing situation and unclear picture for the educator.
- An intruder has unauthorized access to assessment tasks before they are assigned to students. In this case, the intruder could modify them or distribute

the assessment tasks to students. Therefore, the e-assessment loses its meaning which is to evaluate and measure the real students' knowledge and skills.

- Also, it is possible for the intruder to corrupt or delete a part or the whole assessment information that will create difficulties for the students and the educator.

In these cases, the challenging problem concerns data integrity that must be secured in case of fraudulent data alteration.

3. Securing the TeSLA Architecture

The TeSLA architecture is comprised of several entities, some of them located on the institution side, establishing communications with the LMS/VLE or with external tools embedded into the learners browsers; others belong to a separate domain independent of the institution. Securing such an architecture is a difficult task, and consists in expressing the security needs regarding sensitive and personal data on one hand, and analyzing threats both on hosts and network on the other hand. The choices made on security measures must follow the two main requirements of the GDPR [16]: (1) ability to ensure the confidentiality and integrity of system communications and related services; (2) ability to guarantee a proper pseudonymization process of all the user identities, as well as appropriate protection of all the personal data stored or processed by the system.

Consequently, the main security services that are to be provided by the TeSLA architecture for the purposes of e-assessment concern the enforcement of authentication and protection of both communications and data storage. Authentication aims at proving an entity's identity to another, leading to providing enough guarantees in terms of confidentiality and integrity. In turn, confidentiality consists in protecting data to prevent, e.g., 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 [17], which allows entities to authenticate to each other and creates a secure tunnel with data encryption and integrity checks.

Authentication in TLS does not rely on passwords, but on X.509 certificates. The certificates rely on 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) [20], 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 hand. This way, the communications between the various entities of the TeSLA architecture can be entirely secured.

As mentioned in the previous section, the identity of the learners should not be disclosed to TeSLA for privacy reasons. To provide partial anonymity to the learners, a randomized TeSLA ID is generated for each TeSLA user, and represents their identity within the TeSLA domain, where the full identity of the learner (and related data) remains unknown.

Finally, an in-depth security analysis must also be conducted on the host side of the architecture. Deploying the software components of TeSLA in Docker containers [27] provides a lighter and more flexible virtualization solution than relying on traditional virtual machines, but fails to provide isolation with the host operating system. Should the host system be compromised, every container running on it will also be compromised, which can turn into a major threat for TeSLA. This issue is merely one of the several challenges that have been addressed in order to succeed in securing the whole TeSLA architecture.

Most of the aforementioned challenges and issues are addressed in the following sections, where we summarize the main actions and guidelines followed during the design 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. We refer the reader to references [12, 13, 14, 15] and citations thereof, for further details.

4. TLS and PKI-based Communication

The TeSLA architecture needs to guarantee that traditional information security properties such as confidentiality, integrity and authentication are always respected. The main recommendations to fulfill the previous properties are the following: (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 TeSLA components.

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 [18]). 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 [19], 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

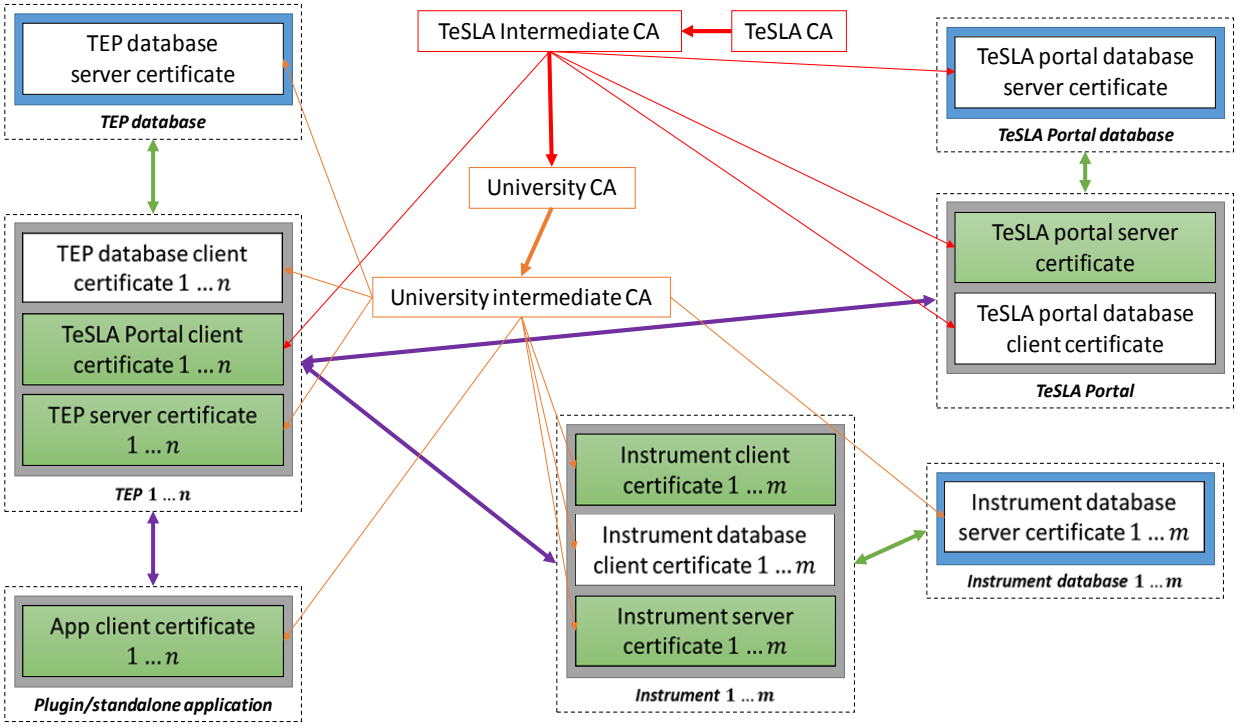

Figure 1. Public Key Infrastructure (PKI) of TeSLA.

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.

A simplified version of the PKI model proposed for the TeSLA architecture is presented in Figure 1. TEP stands for TeSLA E-Assessment Portal, a service broker that forwards requests from the LMS/VLE plug-ins to TeSLA. Instruments refer to the TeSLA components in charge of evaluating data to assess learner's identity and authorship (cf. Section 2, second use case: "*the educator must be sure that the assessed student is the same as the one from the declared personal data*"). In a nutshell, the PKI contains the following elements: (a) TeSLA components (depicted as gray boxes); (b) their respective databases (one per component, depicted as blue boxes); (c) the certificate chain (orange and red boxes/arrows); (d) secured network connections between components (purple arrows); (e) secure connections between components and databases (green arrows); and (f) X.509 certificates for each component. More information about the use of certificate is provided next.

4.1 Certificate Management

With regard to the PKI certificate chain management, Figure 1 identifies some representative certificate authorities: (i) TeSLA CA; (ii) TeSLA intermediate CA; (iii) University CA; and (iv) University Intermediate CA.

First of all, 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 [12, 17]. Then, the TeSLA intermediate CA is the certificate authority. It will sign the University CAs (one for each university) and deliver client/server certificates for the TeSLA Portal. The University CA is the top certificate authority regarding the university based TeSLA components. Basically, this certificate is used only once, to sign University the intermediate CA signature request. As for the TeSLA CA, it is also recommended to use this certificate as scarcely as possible. Finally, the University Intermediate CA will be used to deliver client/server certificates of the architecture components (e.g., backend components of TeSLA and databases).

4.2 Revocation Lists

The TeSLA PKI shall maintain, update and provide a secure access to two main revocation lists [21]: (i) the revocation list associated to the TeSLA CA; and (ii) the revocation list associated to the TeSLA intermediate CA. Each university using its corresponding CAs has to manage, update and provide a secure access to two revocation lists: the revocation list associated to the University CA, and the revocation list associated to the University intermediate CA.

With respect to the secure connections between the TeSLA components, the certificate validity must be checked with respect to their respective revocation lists. A certificate may indeed be valid (i.e., not expired and with a correct signature), but marked as revoked.

4.3 Security Procedures

This section indicates security procedures to apply when a private key is disclosed, as suggested in [22, 14]. Possible incidents are classified in terms of levels – zero being the most critical one.

- **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 University CA private key has been compromised, then the TeSLA Intermediate CA has to revoke this certificate. All the certificates that were signed by the University CA have also to be revoked.
- **Level 3 -** If a University Intermediate CA private key has been compromised, then the TeSLA University CA has to revoke this certificate. All the certificates that were signed by the University Intermediate CA have also to be revoked. Likewise, if a client/server private key associated to a certificate signed by the University Intermediate CA has been compromised, then the University Intermediate CA has to revoke this certificate.

Finally, CA certificates must use RSA keys with a modulus of at least 4096 bits [18, 14, 22]. The validity is fixed to ten years maximum (also limited by the TeSLA license validity period). Client/server certificates must use RSA keys with a modulus of at least 2048 bits [14, 22]. The validity is fixed to one year. Attention should be paid to certificate management in order to avoid malfunctions in the architecture. In particular, a new certificate has to be emitted to the client/server before its actual certificate becomes expired.

5. Identity Management and Data Protection

For the purpose of e-assessment, the TeSLA system must provide pseudonymity to its users [24, 16]. As such, it must not be able to identify an end-user (e.g., the learners), regardless of whether the TeSLA system is standalone or linked to a LMS/VLE as a third party system, e.g., using standard specifications such as Learning Tools Interoperability (LTI) [23]. The user must be authenticated and authorized in TeSLA without allowing TeSLA to know the real user's identity. Hence, anonymity can only be partial in this context, since links between the TeSLA ID and the user name remain available to the university. The suggested approach to manage such requirements follows.

Let the university manage user partial anonymity, the university will generate a randomized UUID [25] (version 4 of the standard) for each user, for instance, learners. As such, the university will be the only entity able to make the link between a UUID and a learner record. Using public information, such as the students e-mail address to generate a UUID using version 3 or version 5 of the UUID standard should be avoided, as it would allow an attacker to compute all the possible TeSLA IDs from the students directory, and deduce the link between the students' names and the TeSLA IDs.

The UUIDs should be stored in a database shared between all LMS/VLEs. A dedicated component, i.e., an identity provider, will be attached to this database in order to receive requests from the TeSLA system, issued with a learner's true identity, and reply with the corresponding UUID. The communication between TeSLA plugins and the identity provider will be mutually authenticated with TLS. In case learners' authentication is certificate-based, since the learner only interacts with TeSLA through a series of plugins, the learner only needs to authenticate to the LMS/VLE. Therefore, the certificate used for authentication to the LMS/VLE will be associated to the learner's true identity. Then, when a request is sent to TeSLA, it shall first retrieve the TeSLA ID associated to the learner's identity from the identity provider, and eventually communicate with TeSLA, while guaranteeing the pseudonymity of the learner.

Some external tools, embedded as Javascript within the learner's web browser, need to communicate to the TeSLA system without revealing the learner's true identity, nor retrieving the TeSLA ID either. A session token mechanism, based on JWT (JSON Web Tokens) [26], is proposed. When the TeSLA plugin authenticates to the identity provider and retrieves the TeSLA ID, some JWT 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 learner ID – 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 TeSLA IDs, which could be used to map different sessions of the same user, are omitted. As a result, the proposed architecture presented in this paper, provides full pseudonymity for learners and provides

unlinkability over different sessions of the same learner. The learner's identity remains only known within the university, and is never transmitted to the TeSLA components. Finally, and in terms of learners' certification, the security framework presented in this paper has been designed to handle pseudonymous credentials [28], based on attribute-based signatures [29]. This will allow the TeSLA learners to authenticate with verifiers in a pseudonymous manner, providing only the minimum amount of information to service providers, and ensuring unlinkability between e-assessment sessions. The use of pseudonymous certification and attribute-based signatures represents the main novelty of the proposed technical solutions presented in this paper, with regard to existing systems in the literature.

6. Conclusion

The paper investigates possible security risks in different learning scenarios implemented in an e-assessment process from students and educators perspectives. It highlights the recognition and verification of student'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 based on TLS protection via authorized certificates and public key infrastructures. Certificate management and security procedures to apply in case of private key disclosure are explained. The approach for pseudonymization applied for the identity management during an e-assessment process and data protection is also explained. It is shown that it will guarantee 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.

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.

References

[1] A. Chatzigavriil, T. Fernando and M. Werner. e-Assessment Practice at Russell Group Universities. The London School of Economics and Political Science. November 2015, url: http://eprints.lse.ac.uk/64328/

[2] S. Mettiäinen. Electronic Assessment and Feedback Tool in Supervision of Nursing Students During Clinical Training. Electronic Journal of e-Learning, 13(1):42-56, 2015.

[3] E. Heinrich, J. Milne and M. Moore. An Investigation into E-Tool Use for Formative Assignment Assessment - Status and Recommendations. Educational Technology & Society, 12(4), 176–192, 2009, url: http://bit.ly/2s5IiOG

[4] S. Perry, I. Bulatov and E. Roberts. The Use of E-assessment in Chemical Engineering Education. url: http://bit.ly/2rbX0DR

[5] J. Moscinski. Example of LMS based assessment in engineering education, url: http://bit.ly/2s5OpTp

[6] N. A. Buzzetto-More and A. J. Alade. Best Practices in e-Assessment. Journal of Information Technology Education, 5:251-269, 2006.

[7] A. Oldfield, P. Broadfoot, R. Sutherland and S. Timmis. Assessment in a Digital Age: A research review, url: http://bit.ly/2reoieY

[8] M. Alabdulkareem, A. Aljuraid and H. Albahly. Security Assessment of Learning Management System, url: http://bit.ly/2rNodzH

[9] S. Kumar and K. Dutta. Investigation on security in LMS MOODLE. International Journal of Information Technology and Knowledge Management, 4(1):233-238, 2011.

[10] K. Thamadharan and N. Maarop. The Acceptance of E-Assessment Considering Security Perspective: Work in Progress. World Academy of Science, Engineering and Technology, International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering, 9(3):874-879, 2015.

[11] K. M. Apampa, G. Wills and D. Argles. Towards Security Goals in Summative E-Assessment Security, International Conference for Internet Technology and Secured Transactions, 2009, url: https://eprints.soton.ac.uk/268487/

[12] ISO. ISO/IEC 27001:2013 - Information security management.

[13] OWASP. The Open Web Application Security Project. OWASP Top 10 – 2013. The Ten Most Critical Web Application Security Risks. Jun 2013. url: https://www.owasp.org

[14] ANSSI. Best Practices, National Cybersecurity Agency of France. url: http://bit.ly/2r3tK3K

[15] IEEE. ISO/IEC/IEEE 29148 International Standard – Systems and software engineering – Life cycle processes – Requirements engineering. Dec 2011.

[16] General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council.

[17] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol. Aug 2008. url: https://tools.ietf.org/html/rfc5246

[18] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. Handbook of Applied Cryptography. ISBN: 0-8493-8523-7. Jul 2011, url: http://cacr.uwaterloo.ca/hac/

[19] ITU-T & ISO/IEC 9594-8:2014. Recommendation X.509. Information technology – Open Systems Interconnection – The Directory – Part 8: Public-key and attribute certificate frameworks, 2016, url: https://www.itu.int/rec/T-REC-X.509-201610-P/en

[20] M. Cooper, Y. Dzambasow, P. Hesse, S. Joseph, R. Nicholas. Internet X.509 Public Key Infrastructure. Certification Path Building. Sep 2005, url: https://tools.ietf.org/html/rfc4158

[21] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile. May 2008, url: https://tools.ietf.org/html/rfc5280

[22] NIST. Special Publication 800-57. Recommendation for Key Management, 2016, url: http://bit.ly/2rbDpnm

[23] IMS Global. Learning Tools Interoperability, url: http://www.imsglobal.org/activity/learning-tools-interoperability

[24] M. Laurent and S. Bouzefrane (Eds). Digital Identity Management. ISTE Press. ISBN 978-0-08-100591-0. Apr 2015.

[25] P. Leach, M. Mealling, and R. Salz. A Universally Unique IDentifier (UUID) URN Namespace, July 2005, url: https://tools.ietf.org/html/rfc4122

[26] M. Jones, J. Bradley, and N. Sakimura, JSON Web Token (JWT), May 2015, url: https://tools.ietf.org/html/rfc7519

[27] Dirk Merkel. 2014. Docker: lightweight Linux containers for consistent development and deployment. *Linux J.* 2014.

[28] J. Camenisch and A. Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2001), pp. 93-118, 2001.

[29] H. K. Maji, M. Prabhakaran, M. Rosulek. Attribute-based signatures. Cryptographers' Track at the RSA Conference, pp. 376-392, 2011.