Received : January 2018; | Revised : March 2018; | Accepted —

DOI: xxx/xxxx

LETTER

Integration of an Adaptive Trust-based E-Assessment System into Virtual Learning Environments — The TeSLA Project Experience

UOC (Baró, Guerrero, Prieto)[1] | TUS (Rozeva, Marinov)[2] | IMT (Kiennert, Rocher, Garcia-Alfaro)[3]

[1]UOC, Universitat Oberta de Catalunya, Barcelona, Spain
[2]TUS, Technical University of Sofia, Department of Informatics, Bulgaria
[3]IMT, Institut Mines-Telecom, Université Paris-Saclay, France

Correspondence
*Joaquin Garcia-Alfaro, IMT & Université Paris-Saclay, France. Email: jgalfaro@ieee.org

Funding Information
This research was supported by the H2020-ICT-2015,
project no. 688520 (TeSLA Project)

Abstract

E-assessment is a novel form to evaluate learners' knowledge and skills in online education. Issues concerning security and privacy of learners' data must be guaranteed. Such issues are discussed under the scope of the TeSLA project, a EU-funded project that aims at providing learners with an innovative environment that allows them to take assessments remotely, thus avoiding mandatory attendance constraints. In this letter, we outline the main concepts underlying TeSLA in terms of security and privacy of learners' data. We also report some technical hands-on experience conducted by members of the consortium during the pilot phases of the project.

KEYWORDS:
E-assessments, Online Education, Authentication, Authorship, Security, Privacy.

1 | INTRODUCTION

The TeSLA project[1] is a EU-funded innovation action that addresses e-assessment challenges. E-assessments are at the center of novel online education sectors. The goal is to allow learners to take remote assessments, thus avoiding mandatory attendance constraints, while providing equivalent guarantees with respect to traditional examination scenarios. Solving physical attendance constraints paves the way for significant cost-effective learning and assessment approaches. The main achievement of the project to-date is of technological nature. TeSLA relies on a modular, secure and privacy-preserving design that integrates authentication and authorship verification of learners.

Related work in the literature reports existing models and platforms for electronic examination of learners. Services like Safe Exam Browser and Secure Exam may require the installation of dedicated software into learner's computers to conduct, e.g., final exams. The software controls the execution of unauthorized actions during the exam, such as executing multi-task applications, web connections, etc. From a pedagogical standpoint, this type of solutions has negative effects on the learners, provoking stress and affecting the results of the examination[2].

An alternative approach is the use of Proctor-based assessments. Human proctors are selected by the learners, whose main responsibilities rely on a face-to-face monitoring of learners, combined by some technological solutions, such as web cameras and voice services, during the execution of special examinations. Online services such as Kryterion, ProctorU and Pearson VUE use this type of approaches, being their main limitations technical scalability and lack of authorship guarantees[3].

Limitations of the aforementioned approaches also include the lack of a continuous process using technological solutions addressing identification, authentication and authorship as a whole. This is the main achievement of the TeSLA framework, which aims at covering those requirements by combining technologies such as biometrics, digital certificates and trusted time stamping[4]. Identification and authentication in TeSLA includes, but is not limited to, keystroke detection[5,6], face recognition[7] and voice recognition[8]. Authorship and cheating is addressed by using solutions such as plagiarism detection[9,10]. The combination of all such techniques is the proposed method of TeSLA to derive trust evidences associated to the learners.

The remainder sections of this letter are structured as follows. Section 2 presents generic background on the TeSLA architecture and a quick overview to the technological building blocks concerning security and privacy of learners. Section 3 reports a technical hands-on experience conducted by the consortium partners during the evaluation pilots of the project. Section 4 closes the letter with some conclusions about the ongoing results of the project.

2 | BACKGROUND

Figure 1 depicts the TeSLA architecture, which is comprised of several components that belong to two different domains: (i) educational components (hereinafter denoted as university domain); and (ii) e-assessment components (i.e., the TeSLA domain). Components that belong to the university domain must be present in the network of each university willing to make use of the TeSLA e-assessment framework, while components that belong to the TeSLA domain are completely independent of the university network. The two domains do not share data unless explicitly stated. The TeSLA domain contains the following components: (1) The TeSLA E-assessment Portal (TEP), which acts as a service broker that gathers and forwards requests to the TeSLA components; (2) the TeSLA Portal, that aims at gathering statistics regarding the e-assessment activities; and (3) Instruments, that analyze authorship and authentication properties (e.g., biometric samples) and send some analysis results back to the client side.

The university domain contains the following components: (a) A Virtual Learning Environment (VLE), which can be provided by a classic Learning Management System (LMS) such as Moodle[11]; (b) A plugin integrated to the VLE that acts as a client side interface with the TeSLA components; (c) Various tools integrated to the VLE that send requests and data to the TeSLA components through the plugin. There are three categories of tools: the learner tool, the instructor tool, and external tools. The learner tool and instructor tool are respectively designed to take or setup an e-assessment. External tools are in charge of sampling the learner's biometric data and sending them to TeSLA instruments for evaluation, as part of the anti-cheating countermeasures; and (d) the TeSLA Identity Provider (TIP), which is in charge of generating pseudonymous for the learners, called TeSLA ID, to be used in the communication with the TeSLA components.

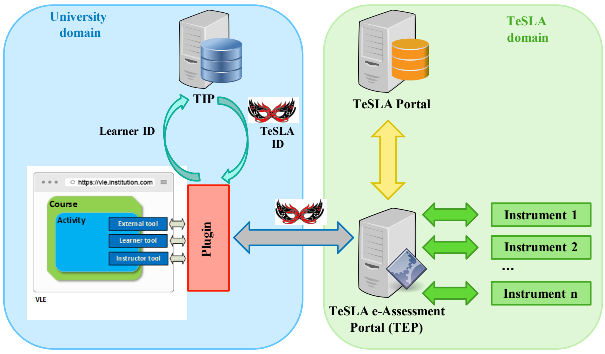


FIGURE 1 Representation of the TeSLA framework.

2.1 | Security and privacy features in the TeSLA framework

The security of the architectural components, as well as the intellectual property rights (IPR) of TeSLA via software licenses, is ensured by using standard technologies like PKI (Public Key Infrastructure) and X509 certificates[12]. The communication exchanges between all the components of the architecture use the TLS (Transport Layer Security) protocol[13]. Mutual authentication is enforced over the whole architecture, hence ensuring confidentiality and integrity of every data exchange. The underlying PKI infrastructure allows TLS deployment and management of certificates and authorities (cf.[14] and citations thereof, for further details about the TeSLA PKI infrastructure).

Taking an e-assignment in this architecture first requires to log in on the VLE (Virtual Learning Environment) that contains the client-side plugin. The learner can require the e-assignment using the learner tool available on the VLE as a third-party tool. The learner tool sends a request through the plugin to the TEP. The incoming request does not contain the name of the learner, but only the TeSLA ID, that the plugin requests from the TIP. Then, the TEP fetches the e-assignment in its database and sends it back to the VLE, where the learner will take the assignment while external tools and sample biometric data that will be regularly sent to instruments, e.g., for anti-cheating analysis.

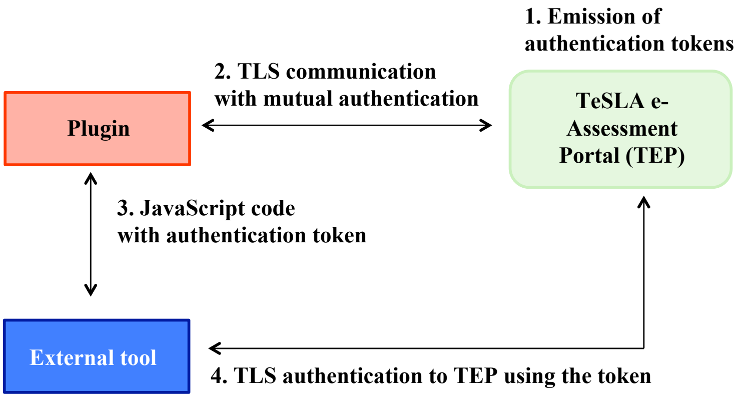

1. Emission of authentication tokens
2. TLS communication with mutual authentication
Plugin
TeSLA e-Assessment Portal (TEP)
3. JavaScript code with authentication token
External tool
4. TLS authentication to TEP using the token

FIGURE 2 Authentication of external tools.

The learner's identity verification performed in the TeSLA e-assessment system relies on specific data of the learners (such as the biometric samples), collected from their environment via some external tools embedded in the VLE. The communications between the institution and the TeSLA components rely on exchanges between the VLE and the TEP. On the VLE side, an embedded plugin is in charge of establishing the authenticated connection with the TEP. Since the external tools, written in JavaScript, are also embedded in the VLE, they must be able to establish secure connections with the TEP in order to transmit sensitive data. Security risks associated to the JavaScript code of the external tools is handled using authentication tokens[19]. Since the JavaScript code is always available on the client side, this may allow learners to obtain control elements used by the external tool to authenticate to the TEP. The plugin retrieves the token from the TEP and transmits it to the external tool. When the plugin has successfully authenticated to the TEP, the latter generates and signs a token that will be transmitted by the plugin to the external tool, which will only have to send the token back to the TEP for validity checking. The corresponding architecture is displayed in Figure 2.

In terms of privacy, the constraints associated to the collection of learners' data makes possible the use of pseudonymity with regard to the components located in the TeSLA domain. Since it is mandatory to store the association between learners identifiers and their real identity, only partial anonymity, i.e. pseudonymity, can be provided to learners during exchanges with the TeSLA components. In this regard, pseudonymity is ensured with the randomized TeSLA identifier (i.e., the aforementioned TeSLA ID), which becomes the learner's identity within the TeSLA domain. This way, no TeSLA component shall ever access to the learner's true identity. The TeSLA ID is generated by the TIP component as a random number computed according to version 4 of the UUID standard[16]. The matching between the learner's identity and the TeSLA ID is stored in the TIP database. The TIP database is placed at the university side and is not accessible from TeSLA. The TIP database shall be shared with all the VLEs (Virtual Learning Environments). All the interactions between the university domain and the TeSLA domain will involve the plugin on one hand, and the TEP on the other hand. This is sufficient to make sure that any request sent to the TEP through the plugin is first redirected to the TIP to retrieve the learner's TeSLA ID and use it in place of the learner's identity.

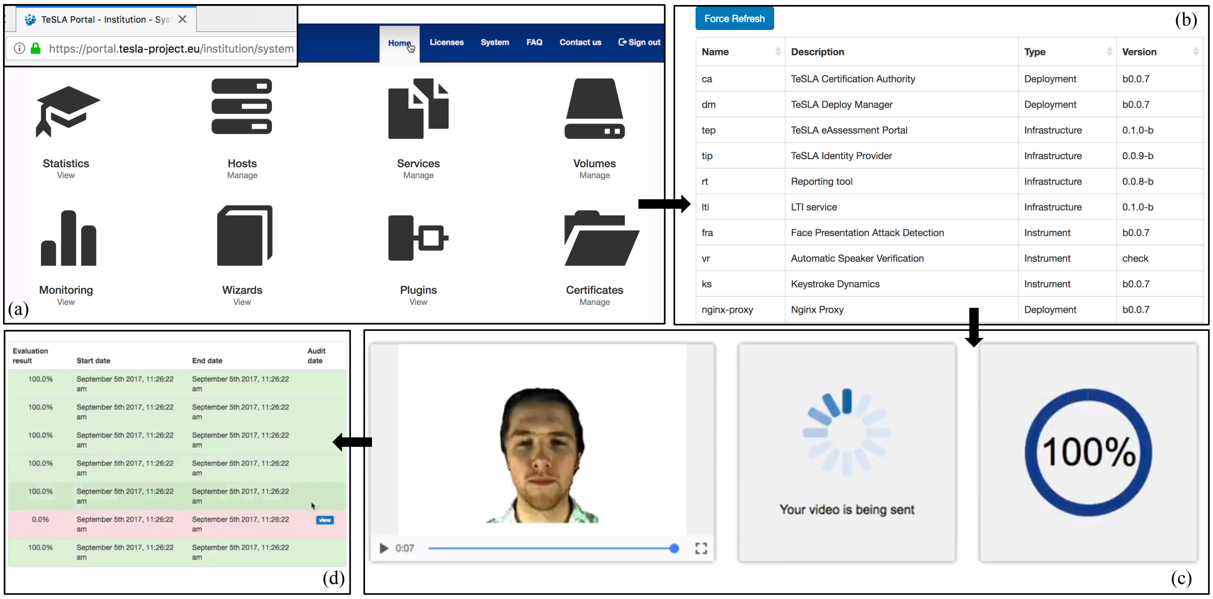
An additional enhancement of the TeSLA architecture towards improved privacy features, relies on the use of anonymous certification. As described in[17,18], anonymous certification allows to perform a privacy-friendly access control, in order to certify that users are allowed to access a resource because they own some attributes required by the verifier. Anonymous certification can be naturally integrated to the VLE (Virtual Learning Environment). Indeed, one of the functions of the VLE is to let the learners access material for courses they registered at. To ensure this function, the VLE does not need to identify the learner, but only requires the proof that the learner is authorized. Such authorization can be performed by defining the following attributes: (i) the university where the learner is enrolled; and (ii) the courses at which the learner registered. These attributes are sufficient to let the learners access to the VLE pages they are entitled to visit without relying on authentication (even using a pseudonym or an anonymized identifier), hence enhancing the learners' privacy. Indeed, the system is unable to profile the learners and keep track of meta information such as at which hours the learners are awake, or at what time and at which frequency they accessed the course material. It is also possible to enhance the privacy of e-assignments' post processing. When an e-assignment is completed by a learner, it must first be sent to a number of external anti-cheating instruments, that perform a number of verifications, such as whether the assignment contains plagiarism. To ensure the authenticity of these requests, one solution would be to transmit the e-assessment along with the learner's TeSLA ID. The requests can be anonymized and authorized using anonymous certification, without any need for identification, with the same set of attributes previously described. The unlinkability properties of the approach guarantee that two different instruments will not be able to deduce that the request was emitted from the same learner. This greatly limits the possibility for the instruments to correlate data, hence a significant improvement to the learners' privacy.

3 | DEPLOYMENT USE CASE DURING THE PILOTS OF THE PROJECT

As a EU-funded innovation action, the TeSLA project is a conducting large-scale pilots to evaluate the technological building blocks presented in the previous section. The evaluations are being performed taking into account quality assurance in education, privacy and ethical issues, as well as educational and technological requirements throughout Europe. The pilots are used formatively to evaluate e-assessment scenarios among the institutional partners of the project. The pilots are conducted in order to asses constructed response tests, e-Portfolios, and peer review collaborative learning[20]. The response to an activity can be of various kinds (i.e., the learner has to select, create or perform the activity) but they all comprise technological actions such as text typing or code programming. The assessor (i.e., a university teacher) uses the identification, authentication and authorship mechanism of TeSLA as a posteriori auditing tool, during the validation of results.

Most of the pilots assume the following scenarios. Learners and assessors use a VLE (Virtual Learning Environment) based on, e.g., Moodle[11]. The piloting activity uses the TeSLA plugin to access the TeSLA domain (cf. Section 2 and on-line video-captures at the website of TeSLA for further details[1]). The TeSLA Identity Provider (TIP) converts the identities of the learners into the pseudonyms when learners start working on their assessments upon TeSLA-enabled VLEs. The data of the learners is captured during the execution of the activities, and redirected to the TeSLA instruments through the TeSLA E-assessment Portal (TEP). The TEP may also interrogate the related instruments to analyze and process learners' data (e.g., their biometric models) while verifying their identities. Finally, the TEP may also receive requests from, e.g., the auditing tools executed by the assessors, to verify that learners did not cheat during the execution of their activities.

Figure 3 shows a practical hands-on deployment and testing of the TeSLA system at the Technical University of Sofia. The Technical University of Sofia (TUS for short) is a face-to-face university providing blended education supported by electronic platforms for distant learning. The virtual learning environment of TUS is based on Moodle[11]. The deployment decision for the TeSLA system in the institutional VLE was presupposed by the existing infrastructure of their electronic platforms. VLEs in TUS are distributed between separate faculty servers. The installation of the TeSLA system was performed on top of the Moodle services of TUS. The deployment of TeSLA is conducted using the Docker containers[21] provided by the TeSLA Technical Consortium. The remainder elements of the infrastructure and instruments are obtained and installed via the TeSLA framework by web-based wizards (see Figure 3(a) and available media at the project websites[1], for on-line video-captures). The TeSLA framework offers a web portal for the monitoring and automation of the installation processes and the provision of the TeSLA system as a series of cloud services. Locally, the network infrastructure of TUS for the evaluation of the TeSLA system involves 150 Mbit/s guaranteed connection. The amount used for the maintenance of students logged into the TeSLA system is 80 Mbit/s.



Name	Description	Type	Version
ca	TeSLA Certification Authority	Deployment	b0.0.7
dm	TeSLA Deploy Manager	Deployment	b0.0.7
tep	TeSLA eAssessment Portal	Infrastructure	0.1.0-b
tip	TeSLA Identity Provider	Infrastructure	0.0.9-b
rt	Reporting tool	Infrastructure	0.0.8-b
lti	LTI service	Infrastructure	0.1.0-b
fra	Face Presentation Attack Detection	Instrument	b0.0.7
vr	Automatic Speaker Verification	Instrument	check
ks	Keystroke Dynamics	Instrument	b0.0.7
nginx-proxy	Nginx Proxy	Deployment	b0.0.7

Evaluation result	Start date	End date	Audit date
100.0%	September 5th 2017, 11:26:22 am	September 5th 2017, 11:26:22 am	
100.0%	September 5th 2017, 11:26:22 am	September 5th 2017, 11:26:22 am	
100.0%	September 5th 2017, 11:26:22 am	September 5th 2017, 11:26:22 am	
100.0%	September 5th 2017, 11:26:22 am	September 5th 2017, 11:26:22 am	
100.0%	September 5th 2017, 11:26:22 am	September 5th 2017, 11:26:22 am	
0.0%	September 5th 2017, 11:26:22 am	September 5th 2017, 11:26:22 am	view
100.0%	September 5th 2017, 11:26:22 am	September 5th 2017, 11:26:22 am	

FIGURE 3 Practical hands-on deployment (based on available on-line media). (a) TeSLA deployment portal. (b) System initialization. (c) Enrollment of learners. (d) Visualization of sample audit tool results.

By implementing compression of some activities, such as the enrollment activities (i.e., to build the biometric models of learners, as shown in Figure 3(c)) required about 8 Mbit/s per student. Pilots are being conducted by groups of ten students working in parallel, which required about 80 Mbit/s.

The deployment is performed over a series of virtual hosts running at the TeSLA server of TUS, using Docker Swarm[21]. The result of the infrastructure deployment is the initialization of all the TeSLA components discussed in Section 2, e.g., TEP and TIP components, together with their databases. The instrument deployment presents the biometric and authorship instruments for learner authentication. Some other modules, such as the `Certification Authority` (CA) associated to the PKI of the TeSLA framework, are initialized as well (cf. Figure3(b)). The cloud structure of the deployment consists of the TEP, TIP, CA and the biometric instruments. Both PKI and TeSLA ID deployments, based on[14,16,19], allow protecting learners' identity. Protection of the Docker containers and virtual Docker images follow well established recommendations[22]. Figure3(d) shows the visualization of sample audit tool results.

Data management is complemented with a series of remote database servers over on-demand cloud computing platforms for TeSLA at Amazon Web Services. Dedicated databases at TUS handle the anonymized learner data from all the assessment activities. The TeSLAplug-in has been tested over different operating systems including *Windows*-based operating systems (e.g., *Windows-7* and *Windows-10*, Professional, Home, Education editions) and GNU/Linux operating systems (e.g., *CentOS*). In terms of Web browsers, tests included browsers such as *Firefox*, *Chrome*, *Internet Explorer*, and *Edge*. Fault redundancy of the platform is ensured against physical (hardware, electrical supply failures, environmental factors) and virtual infrastructure (human and program errors) risks by: (a) Support of alternative servers at another location; (b) Server resources are enhanced with duplicate processor technologies, operating memory and RAID massive for enhancing the disk capacity; (c) Electric supply failure is mitigated with UPS devices of a market leader company; (d) External device backups of all virtual machines at periods of 72 hours in a month are maintained for eliminating human and program errors.

The system reached relatively stable exploitation status. It provided for monitoring and data gathering from enrollment and assessment activities from the pilots. TUS designed some testbed scenarios suiting their existing distributed platforms for on-line distance education. To avoid collisions and problems with their existing learning environments, TUS implemented a parallel replica. The data from the different faculty servers was duplicated, and the test infrastructure was connected to TUS e-learning framework to test connectivity and student data transfers. This was achieved by a server Linux based (KVM) virtualization. The results showed fault redundancy of educational process and compliance with the existing working infrastructure in TUS. Further formative evaluation results of the pilots at TUS are available on-line, at the website of TeSLA[1].

4 | CONCLUSION

In this letter we have presented TeSLA, an e-assessment system that provides to educational institutions an adaptive way for assuring on-line assessment. It supports both continuous and final evaluation in either full on-line or blended environments. The system has been implemented and deployed taking into account challenging issues such as security, trust and privacy of learners. We have reported how the TeSLA project consortium has handled the deployment of the TeSLA platform during the evaluation phases of the project. More precisely, we have reported some technical hands-on experience conducted by partners of the consortium, during the preparation of the pilots of the project, including close collaboration with technical leads from the involved institutions.

Author contributions — All authors contributed equally to the manuscript.

Conflict of interest — The authors declare no potential conflict of interests.

ORCID — Contact Author: Joaquin Garcia-Alfaro http://orcid.org/0000-0002-7453-4393

References

1. TeSLA Consortium. Trust based Authentication & Authorship e-Assessment Analysis. Available on-line at http://tesla-project.eu/, 2016.

2. Ala-Mutka. A survey of automated assessment approaches for programming assignments. *Computer Science in Education*, 15(2):83–102, 2005.

3. Petri, Tuukka, Ville, Seppälä. Review of recent systems for automatic assessment of programming assignments. 10th international conference on computing education research, pp. 86–93, ACM, 2010.

4. Lu, Yang, Chang, Yang. The design and implementation of intelligent assessment management system. 2013 Global Engineering Education Conference (EDUCON), pp. 451–457, IEEE, 2013.

5. Peacock, Ke, Wilkerson. Typing patterns: A key to user identification. *IEEE Security & Privacy Magazine*, 2(5):40–47, 2004.

6. Choraś, Mroczkowski. Recognizing individual typing patterns. Iberian Conference on Pattern Recognition and Image Analysis, pp. 323–330, Springer, 2007.

7. Sinha, Balas, Ostrovsky, Russell. Face recognition by humans: Nineteen results all computer vision researchers should know about. *Proceedings of the IEEE*, 94(11):1948–1962, 2006.

8. Kinnunen, Karpov, Franti. Real-time speaker identification and verification. *IEEE Transactions on Audio, Speech, and Language Processing*, 14(1):277–288, 2006.

9. Graven, MacKinnon. A Consideration of the Use of Plagiarism Tools for Automated Student Assessment. *IEEE Transactions on Education*, 51(2):212–219, 2008.

10. Cook, Sheard, Carbone, Johnson. Academic integrity: differences between computing assessments and essays. 13th International Conference on Computing Education Research, pp. 23–32, ACM, 2013.

11. Dougiamas, Taylor. Moodle: Using learning communities to create an open source course management system, Available on-line at https://research.moodle.net/33/, 2003.

12. Cooper, Dzambasow, Hesse, Joseph, Nicholas. Internet X.509 Public Key Infrastructure: Certification Path Building, RFC 4158, https://tools.ietf.org/html/rfc4158, 2005.

13. Dierks, Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2, RFC 5246, https://tools.ietf.org/html/rfc5246, 2008.

14. Kiennert, Rocher, Ivanova, Rozeva, Durcheva, Garcia-Alfaro. 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, pp. 366–371, 2017.

15. Santesson, Myers, Ankney, Malpani, Galperin, Adams. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, RFC 6960, https://tools.ietf.org/html/rfc6960, 2013.

16. Leach, Mealling, Salz. A Universally Unique IDentifier (UUID) URN Namespace, RFC 4122, https://tools.ietf.org/html/rfc4122, 2005.

17. Kaaniche, Laurent, Rocher, Kiennert, Garcia-Alfaro. PCS, a privacy-preserving certification scheme. 12th International Data Privacy Management workshop, 22nd European Symposium on Research in Computer Security (ESORICS), pp. 239–256, Springer, 2017.

18. Kiennert, Kaaniche, Laurent, Rocher, Garcia-Alfaro. Anonymous Certification for an e-Assessment Framework. 22nd Nordic Conference on Secure IT Systems (NordSec 2017), pp. 70–85, Springer, 2017.

19. Jones, Bradley, Sakimura. JSON Web Tokens (JWT), RFC 7519, https://tools.ietf.org/html/rfc7519, 2015.

20. Mellar, TeSLA Consortium. D2.1 Report with the state of the art. Available on-line at http://tesla-project.eu/deliverable/deliberable-2/, 2016.

21. Merkel. Docker: lightweight Linux containers for consistent development and deployment, Linux Journal, 239(2), 2014.

22. Martin, Raponi, Combe, Di Pietro. Docker ecosystem – Vulnerability Analysis, Computer Communications, 122:30–43, 2018.

How to cite this article: Baró, Guerrero, Prieto, Rozeva, Marinov, Kiennert, Rocher, and Garcia-Alfaro (2018), TeSLA Project Experience, *Internet Technology Letters*, *2018;00:1–6*.