A Security-Evaluation Framework for Mobile Cross-Border e-Government Solutions

THOMAS ZEFFERER, A-SIT Plus GmbH, Austria

BERND PRÜNSTER, A-SIT Plus GmbH, Austria

CHRISTIAN KOLLMANN, A-SIT Plus GmbH, Austria

ANDREEA ANCUTA CORICI, Fraunhofer FOKUS Institute, Germany

LUKAS ALBER, Institute of Applied Information Processing and Communications (IAIK), Graz University of Technology and Secure Information Technology Center Austria (A-SIT), Austria

ROLAND CZERNY, Institute of Applied Information Processing and Communications (IAIK), Graz University of Technology and Secure Information Technology Center Austria (A-SIT), Austria

BLAŽ PODGORELEC, Institute of Applied Information Processing and Communications (IAIK), Graz University of Technology and Secure Information Technology Center Austria (A-SIT), Austria

Security evaluation is crucial for any security-critical system. In this context, a system can mean technical systems, organizations, or any other entity with certain security requirements. The major challenge in doing risk analysis is the trade-off between completeness and complexity. When done on a more abstract level, certain risks are potentially overlooked. When done on a very detailed level, risk analyses quickly become complex and exceed available resources. To tackle this challenge, various norms and standards propose different security evaluation methodologies. These methodologies vary depending on their target scope. Also, these standards typically remain on a rather abstract level to ensure broad applicability to different systems. In practice, this often complicates the application of these standards to concrete technical systems. In this paper, we tackle this issue by proposing a customized security-evaluation framework tailored to the special characteristics of cross-border e-government services. The proposed framework does not re-invent the wheel but combines aspects and approaches of established norms and standards to cherry-pick from each standard those aspects most beneficial for the given context. We evaluated the proposed framework by applying it to a set of software building blocks, which have been developed in the Horizon-2020 project mGov4EU and leverage mobile cross-border e-government services in Europe. The conducted evaluation shows that the proposed framework facilitates the practical application of security evaluations in the targeted domain and supports evaluators in handling the trade-off between completeness and complexity.

CCS Concepts: • **Security and privacy → Domain-specific security and privacy architectures**; • **Information systems → Information systems applications**.

Additional Key Words and Phrases: Security evaluation, Risk analysis, Risk evaluation, Security, e-Government

ACM Reference Format:

Thomas Zefferer, Bernd Prünster, Christian Kollmann, Andreea Ancuta Corici, Lukas Alber, Roland Czerny, and Blaž Podgorelec. 2023. A Security-Evaluation Framework for Mobile Cross-Border e-Government Solutions. In . ACM, New York, NY, USA, 13 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

E-government services are a crucial backbone for today's interaction with public administration. Citizens and businesses use these services to complete necessary procedures in a secure and convenient manner. E-government services are gradually being further developed and extended to improve offered services and keep up with technological progress, changing policy environments, and new user habits [35]. Current trends in the e-government domain include a growing relevance of cross-border services within Europe and a shift towards mobile technologies and end-user devices [6]. The former is supported by EU policy frameworks such as the eIDAS Regulation ((Regulation (EU) No. 910/2014) on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market) [31] or the SDG Regulation (Regulation (EU) 2018/1724), which establishes a single digital gateway to provide access to information, procedures, and assistance and problem-solving services [33]. These frameworks leverage cross-border authentication and data retrieval within the European Union, thereby focusing on two of the main building blocks of cross-border e-government services. The latter trend is also driven by the current proposal for a new eIDAS Regulation (amending Regulation (EU) No 910/2014) which will have a strong focus on mobile wallet technology and aims to further improve the end-users' control of their data [34].

Security is a key requirement for e-government services, particularly for cross-border e-government services and their key building blocks cross-border user authentication and cross-border data retrieval. Ensuring security becomes increasingly difficult as complexity increases and new attack vectors appear frequently. The shift towards mobile end-user devices raises new challenges and threat potentials that need to be addressed [10]. Security can no longer be achieved by simply implementing standard security features. Instead, security must be considered a key requirement from the beginning and closely integrated into the entire software lifecycle of e-government solutions. This can be achieved through systematic security evaluations that accompany the design, implementation, and operation of e-government solutions.

Completeness is a key challenge in conducting systematic security evaluations. Completeness means that conducted evaluations must reliably reveal all relevant threats and related risks. In practice, this is non-trivial as relevant threats depend on various factors, such as involved assets, the characteristics of the system under evaluation, or the system's application context. To support the execution of security evaluations, several norms and standards exist that define methodological approaches and best practices. Most of these norms and standards intentionally remain on a more abstract and generic level to ensure broad applicability [2]. Consequently, they typically lack detailed and practical instructions for carrying out security evaluations for a specific use case. For instance, no norm or standard exists that takes into account the application context and the special characteristics of mobile cross-border e-government services, including eIDAS and SDG related features and building blocks.

To bridge this gap, we propose a customized security-evaluation framework for the given use case, i.e., for cross-border e-government services tailored to mobile end-user devices and relying on cross-border user authentication and data retrieval. To base our proposal on a solid foundation, we start with a survey and analysis of relevant norms and standards. We then combine useful aspects of the surveyed standards to come up with our own customized evaluation framework that meets the specific requirements of the given use case. We evaluate the applicability and usefulness of the proposed method by applying it to several software building blocks that have been designed and implemented in the Horizon-2020 research project mGov4EU and leverage mobile cross-border e-government services.

The contribution of the work presented in this paper is twofold. Firstly, it evaluates in detail the security of software building blocks developed in the research project mGov4EU. This directly enhances the security of the project's pilot applications that use these building blocks. Secondly, and even more importantly, the paper provides a tailored security-evaluation framework specifically designed for the use case of mobile cross-border e-government services. This framework can be used in future evaluations to evaluate and ensure the security of similar services.

The remainder of this paper is structured as follows. Section 2 surveys and analyses related work with a focus on proposed approaches and techniques for security analyses and evaluations. To dig more into the details, Section 3 then surveys norms and standards proposing security-evaluation methodologies. Based on the results of the conducted survey of related work, a customized security-evaluation framework for mobile cross-border e-government services is proposed and introduced in Section 4. The proposed framework is evaluated in Section 5 by applying it to a set of software building blocks that leverage mobile cross-border e-government services in Europe. Final conclusions are drawn and an outlook to future work is provided in Section 6.

2 RELATED WORK

This section presents comparable, i.e., related work on security analyses and evaluations recognized from surveyed scientific articles. Works are described and the main distinction points from the security-evaluation framework proposed in this paper are determined.

The Open Web Application Security Project (OWASP) has introduced a Threat Modelling Process as a systematic approach for identifying and analyzing potential threats to software systems [23]. The process proposed by OWASP involves decomposing the analyzed system and representing it with diagrams that depict its architecture and components, which are then used to identify threats. The STRIDE model (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege), introduced by Microsoft Corporation is adopted for categorizing the threats [16]. Additionally, the DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability) risk assessment model is applied to assess the identified threats [16]. Finally, countermeasures and mitigation strategies are identified, which complement the code-review processes and enhance the understanding of the system under evaluation. Our own security-evaluation framework introduced in this paper differs from the OWASP Threat Modelling technique in terms of the specific methods involved in each step. The core of the proposed evaluation framework draws inspiration from well-established norms. Especially relevant are related standards for threat identification published by ISO/IEC and the respective BSI Standard family, including steps such as creating a threat matrix table and threat evaluation. The goal of the proposed framework is to provide concrete technical recommendations for architects and developers, which is beyond the explicit scope of the OWASP Threat Modelling technique.

The AAFS architectural analysis method proposed by Ryoo et al. [30] is another method that can be regarded as related work to our own proposal. This method comprises three analyses.

- Vulnerability-oriented Architectural Analysis (VoAA): This analysis utilizes different lists of known vulnerabilities provided as Common Vulnerabilities and Exposures (CVE), Open Web Application Security Project (OWASP), and Common Weakness Enumeration (CWE).
- Pattern-oriented Architectural Analysis (PoAA): This analysis utilizes the architectural patterns and class- or code-level repositories.
- Tactic-oriented Architectural Analysis (ToAA): This analysis comprises tactics such as detecting attacks, resisting attacks, reacting to attacks, and recovering from attacks are considered.

According to this method, security vulnerabilities are first identified using ToAA. Subsequently, outcomes are related to patterns by means of PoAA. Finally, results of PoAA are related to vulnerabilities via VoAA. The analysis process is completed by examining source code based on VoAA results and verifying code-analysis results using testing results and incident reports. Compared to our own evaluation framework proposed in this paper and described below, the AAFS architectural analysis method is mainly applicable after the software-implementation phase, i.e., when source code is already available. In contrast, our proposed security-evaluation framework is already applicable at the architectural level of the system under evaluation.

Another security evaluation method related to our own proposal is the so-called Architecture Tradeoff Analysis Method (ATAM). According to Kazman et al. [15] and Putrama et al. [26], ATAM's goal is to extract and refine the architecture's quality attributes, indicating whether the architectural design decisions have addressed the quality attribute requirements. The ATAM method is not focused solely on security attributes but covers other attributes such as reusability, modifiability, availability, performance, maintainability, and testability. The method consists of several steps, including the preparation stage, where stakeholders are identified and their quality attribute requirements are collected. The preparation stage is followed by the assessment stage, where experts evaluate the architecture to determine its alignment with the quality attribute requirements. In the final stage, the assessment results are presented and discussed with the previously identified stakeholders, and recommendations for improvement are provided if necessary. In contrast to the security-evaluation framework proposed in this paper, which focuses solely on security analysis and provides concrete technical recommendations for architects and developers, ATAM considers a much broader range of quality attributes that are not tailored to mobile cross-border e-government services.

Overall, it can be concluded that several security-evaluation methods have already been proposed and introduced in related work. However, all these methods differ in several aspects from the security-evaluation framework proposed in this paper. Accordingly, the proposed framework closes a yet unaddressed gap.

3 SURVEY ON RELEVANT NORMS AND STANDARDS

In this paper, we propose a security-evaluation framework for mobile cross-border e-government services. The proposed framework, presented in the next section, aims to overcome limitations of established risk analysis methodologies especially regarding the given technical system context, i.e., cross-border e-government services. To prevent reinventing the wheel, development of the proposed security-evaluation framework has been based on the results of a survey on relevant norms and standards. Results of the conducted survey, which have served as input for the propose security-evaluation framework, are summarized in this section.

In general, the following norms and standards have been identified to be most relevant and to hence form the backbone of the security-evaluation framework proposed in this paper: ISO/IEC 15408 [13], ISO/IEC 27005 [14], ISO 31000 [12] and BSI standard family (200-1 [3], 200-2 [4], and 200-3 [5]). An overview of these norms and standards is provided in the following paragraphs.

The ISO/IEC 15408 standard is typically applied when evaluating concrete security-critical products, such as smart-cards or hardware-based security tokens. Nevertheless, the purpose of our proposed security-evaluation framework is to enable risk analysis also on the architectural level of a technical system. For this purpose, the methodology introduced by ISO/IEC 15408 to systematically identify relevant security requirements is generic and can be valuable for the systematic identification of assets, threats, and countermeasures. Another standard, that the conducted survey has revealed as potentially useful, is ISO/IEC 27005, which is part of the ISO/IEC 27000 standard family. The main purpose of ISO/IEC 27005 is to guide managing information security risks. Therefore, parts related to security risk assessment, including the risk identification process description and characterization of relevant security properties to be analyzed, appear suitable for the security-evaluation framework proposed in this paper. Finally, the standard ISO/IEC

31000 has also been identified as helpful for risk identification for the security-evaluation framework proposed in this paper. The BSI standard family 200 (200-1, 200-2, 200-3) itself is largely based on the previously mentioned standards. Nevertheless, the conducted survey has identified BSI Standard 200-3 on risk evaluation as a good match for inclusion into the proposed security-evaluation framework.

While the four standards described above has been identified to form the backbone of our proposed security-evaluation framework, also other standards and norms can be useful and support the execution of practical security evaluations for cross-border e-government solutions. ETSI EN 319 401 [28] and ETSI EN 319 411 [29] have been identified as relevant standards for cross-border e-government solutions when analyzing risks associated with Trust Service Provider (TSP) systems, which often act as central trust establishers in cross-border e-government solutions. FIPS Publication 140-3 [17] has been identified as a suitable standard when analyzing risks related to cryptographic modules, such as encryption devices, secure communication protocols, and secure key storage. Two parts of NIST SP 800-57 Part 1 have been identified as relevant to be considered when analyzing the risks of a technical system related to managing cryptographic material, including the state-of-the-art algorithms currently used (Part 1 - General Description [21]), and Part 2 – Best Practices for Key Management Organizations [22] to be helpful when analyzing implemented key-management procedures. Further, two additional specifications, i.e., NIST SP 800-133 [19] and NIST SP 800-131A [18], have been identified to be relevant when analyzing risks related to implemented cryptographic key-generation mechanisms, cryptographic algorithms, and cryptographic key lengths utilized by the technical system examined. From the aspect of the mobile apps risk analysis, NIST SP 800-163 [20] and OWASP Mobile Application Security Verification Standard [25] have been identified as relevant. From the broad context of technical system software implementations and architecture, requirements defined in OWASP Application Security Verification Standard [24] have been identified to be relevant. To cover the most common security vulnerabilities within risk-analysis, the OWASP Top Ten [1] catalogue has been identified as crucial. This catalogue also provides examples and explains how to mitigate identified risks. Last but not least, General Data Protection Regulation (GDPR) [32] has been identified as relevant when analyzing personal data-related risks.

Summarizing, the conducted survey has revealed standards that show the potential to serve as a backbone for the security-evaluation framework proposed in this paper, as well as a set of additional standards, which at least contain some relevant parts and aspects that are worth to be considered. The security-evaluation framework proposed and introduced in the next section cherrypicks and combines from all these norms and standards those aspects most suitable for the framework's intended scope. Details of the proposed security-evaluation framework are provided in the following section.

4 PROPOSED SECURITY-EVALUATION FRAMEWORK

Based on the survey findings, this section describes the risk-analysis method to conduct the required security analysis of cross-border e-government solutions on architectural level. The proposed framework itself consists of the following steps:

(1) Collect technical specifications

As a first step, all the available specifications, especially those related to architecture and interfaces of the software building blocks of the technical system in the focus of analysis, are collected. Accordingly, these specifications serve as input and starting point for the proposed evaluation framework. For this initial step, parts of ISO/IEC27005 [14] (Section 6) and ISO 31000 [12] (Section 5.3) related to risk-analysis context establishment and defining the scope, context and criteria are relevant to be considered. BSI standard 200-1 (primarily Section 4 and Section 7) [3] related to communication and knowledge and security process planning are considered relevant as well. Moreover, parts of BSI standard 200-2 [4] (especially Section 3, Section 5 and Section 7) about processes, applications and IT systems acquisition, information flows, documentation and scope specifications can also be useful.

(2) Derive technical process flows

The next step in the proposed security-evaluation framework involves deriving technical process flows from the collected technical system specifications. This step is informed by BSI standard 200-2 [4], particularly Section 5, which covers technical documentation, work process documentation, and information flow reporting routes. Cross-border e-government services often consist of multiple independent building blocks. By putting the technical flows related to these software building blocks on the same technical denominator, the proposed evaluation framework supports achieving a common understanding and comprehensive documentation of the technical flows within the evaluated technical system. To achieve this, we suggest the use of sequence diagrams, as these have been shown to be effective in several scientific publications and reports for risk analysis purposes [8, 9, 11, 27]. All relevant, i.e., evaluated technical system software building blocks should have their technical flows derived and documented in this manner, including any specifications collected in the previous step. Documenting the technical flows provides a solid foundation for the ongoing security evaluation process and helps ensure that necessary information is readily available when needed.

(3) Identify assets

Based on the technical process flow description, relevant primary assets are identified for each software building block. This step marks the beginning of the risk identification process. ISO/IEC 15408 and ISO/IEC 27005 both describe assets as pieces of information or resources that require protection and have value to the organization holding the assets. A comparable principle is followed in the BSI standard family, where assets are called "Crown Jewels" and denote processes and pieces of information that are most important for the further existence of the organization. In all the considered standards, an asset could be anything. However, in ISO 27005, there is a clear distinction between primary and supporting (also called secondary) assets. Our framework follows this description, and therefore within this step, business processes and information are being identified. To sum up, identifying primary assets recognizes the value that requires protection. Moreover, as part of this step, for each identified asset, its relevant security properties [7] - sometimes called also security targets or categories of protection [13] or basic values [3] (i.e., confidentiality, integrity, availability, authenticity, and/or non-repudiation) should be reported. This is done using keywords "must", "must not", and "should", which state whether providing the respective security property is to be considered mandatory or not. Once all primary asset are identified, relevant secondary assets are derived. Secondary assets comprise software components or hardware components, whose security has a direct or indirect impact of the security of primary assets. As for primary assets, also secondary assets should be assigned security properties.

(4) Identify threat agents

Inspired by ISO/IEC 15408 [13] and ISO/IEC 27005 [14], relevant threat agents, also known as threat sources, are identified for the system under evaluation. A threat agent is an entity that aims to compromise the assets of the system under evaluation. This step results in a list of relevant threat agents for the system, considering both internal and external threat agents. Internal threat agents typically have privileges within the system, while external ones do not.

(5) Derive threats

With consideration of all identified threat agents and software components, relevant threats are derived for all identified assets. The goal of threat derivation is to be systematic. To support this goal, the proposed security evaluation framework applies a risk matrix inspired by the BSI standard 200-3 [5]. The framework foresees the following process for systematic threat derivation:

As a first phase in the threat derivation process, a table is created for each relevant security property (security target) for each system under evaluation. The assets that require protection are specified in the table rows, while the columns list the identified threat agents. This results in the creation of a threat matrix table. In the next phase, the table cells are populated to provide a comprehensive overview of all potential threat scenarios. These cells identify the vulnerable software component or communication channel and the threat agents that could threaten the asset. At this step, the proposed framework relies on standards and norms surveyed above.

(6) Identify threat potential

The use of the risk matrix allows for the identification of threat potential. To accomplish this, the framework employs a risk assessment and evaluation technique from the BSI standard 200-3 [5]. The focus at this stage is to estimate the impact factor, which represents the extent of damage that would result from successful threat exploitation, and the probability factor, which represents the likelihood of the threat being exploited. Based on the calculated impact and probability, the risk potential, or risk category, is determined by mapping the two factors onto a four-stage colour scheme. This colour scheme reflects the level of threat potential, with each stage indicating an increasing level of risk.

(7) Identify countermeasures

After determining the threat potential for each relevant threat, it is necessary to implement appropriate technical and/or organizational measures to mitigate these threats and reduce the risk of exploitation. For this, the identification of countermeasures is a crucial and logical follow-up to the risk-analysis process, as recognized in the ISO/IEC 15408 [13] and BSI standard 200-3 [5].

(8) Derive recommendations

The final step of the proposed security-evaluation framework is to provide concrete technical recommendations for the architects and developers of the technical system. These recommendations are based on the identified countermeasures that were previously suggested to mitigate threats and minimize risk. These recommendations aim to support the design and development of a secure technical system. Recommendations can contain specific technical measures or organizational processes to ensure the security of the assets and the technical system.

The steps of the proposed security-evaluation framework described above are illustrated in Figure 1, which shows the progression from technical system specifications to risk identification, threat identification, countermeasures and recommendations. The figure illustrates the relationship between each step in the evaluation process and the ultimate goal of implementing a secure technical system. We have evaluated the proposed security-evaluation framework by applying it to concrete software building blocks for mobile cross-border e-government services. Details on the conducted evaluation are provided in the next section.

5 EVALUATION

In this section we report on the practical application of the security-evaluation framework proposed in Section 4. By applying the framework to a set of concrete software building blocks, the applicability and usefulness of the framework has been evaluated. The Horizon-2020 mGov4EU project and the various software building blocks developed therein

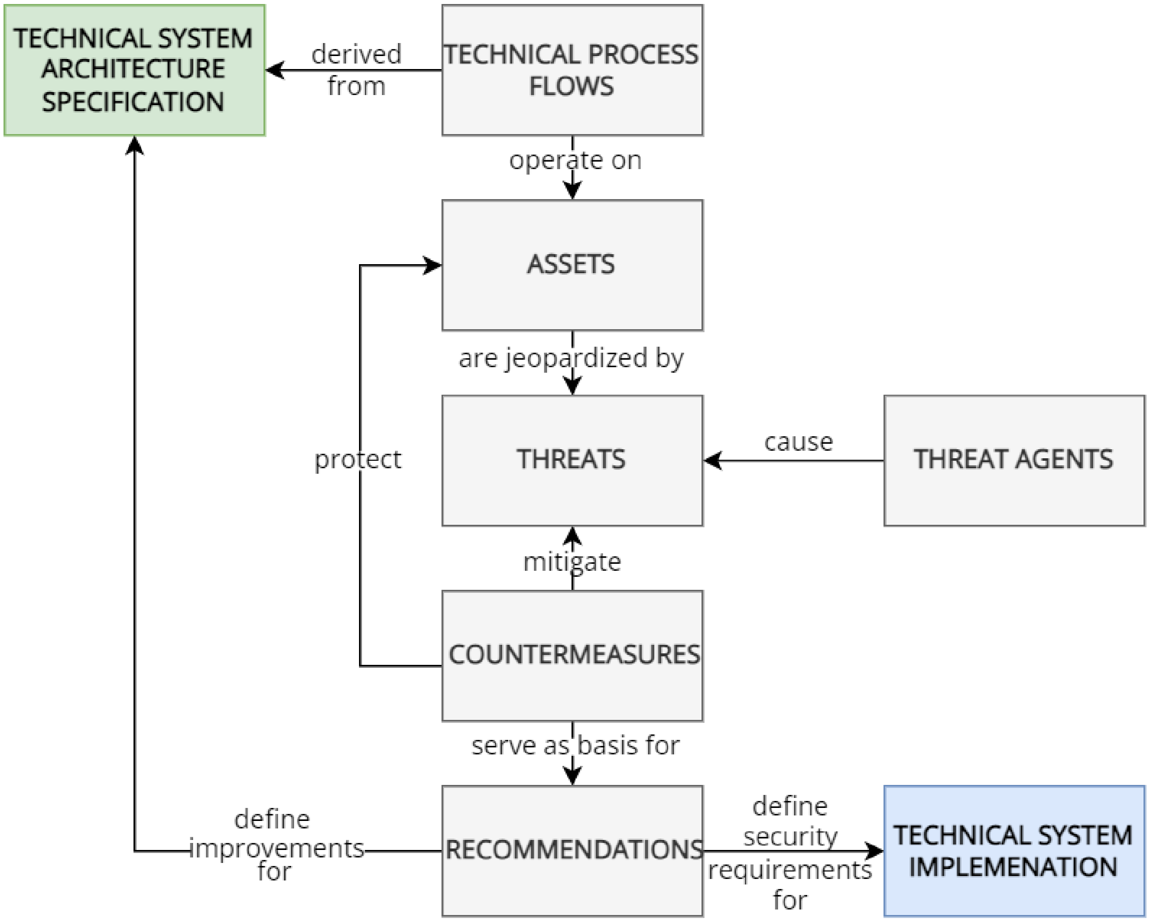


Fig. 1. Outline of proposed Security-Evaluation Framework.

have served as basis for the conduced evaluation. This section first gives an overview of the evaluated software building blocks, introduces the evaluation method applied, illustrates the application of that method by means of a case study, and summarizes the evaluation results obtained.

5.1 Evaluation Target

The proposed security-evaluation framework has been applied to four software building blocks. Each of these software building blocks has been developed by the Horizon-2020 project mGov4EU and represents a relevant building block of mobile cross-border e-government services. Concretely, evaluated mGov4EU software building blocks implement and provide features related to secure cross-border user authentication, signature creation, cross-border data retrieval, and mobile wallets. Each software building block consists of one or more software components (mobile apps, backend services, etc.) that together form the respective software building block. Technical specifications of all software building blocks have served as starting point and input for the conducted security evaluations.

5.2 Evaluation Method

The four software building blocks developed by the mGov4EU project have been evaluated using the security-evaluation framework proposed in Section 4. As the description of the framework in Section 4 is rather generic, this subsection describes the applied evaluation method in more detail.

The security-evaluation framework proposed in Section 4 defines six steps to be carried out in total. These six steps have been carried out in the following way during evaluation:

(1) **Technical Process Flows:** The technical system specifications produced in mGov4EU have served as starting point for the conducted evaluations. According to the proposed evaluation framework, technical architectures and process flows have been derived from these specifications in the form of C4 models[1] and sequence diagrams.

(2) **Assets:** From the derived technical architectures and process flows relevant assets have been identified in the next step. Focus has been put on primary assets, i.e., on security-critical data being processed by the respective software building block under evaluation. For each asset identified, relevant security targets (confidentiality, integrity, availability, etc.) have been identified and summarized in a table. As an example, Figure 2 shows the respective table for the asset 'Verifiable Credential', which is related to the mGov4EU software building block 'Mobile Wallet'. Similar tables have been created for all assets of all evaluated software building blocks. In total, more than 20 assets have been identified.

(3) **Threat Agents:** In the third step, relevant threat agents have been identified for the software building block under evaluation. Both internal and external attackers have been considered. Motives and assumed capabilities for each threat agent have been described.

(4) **Threats:** In this step, relevant threats have been derived systematically from identified assets and threat agents. This is the most complex step in the evaluation process. To follow a systematic approach, threats have been identified by carrying out the following steps:

  (a) A table has been created for each relevant security target identified during the identification of relevant assets. Accordingly, for each evaluated software building block, separate tables have been created for the security targets confidentiality, integrity, availability, authenticity, and non-repudiation. As an example, Figure 3 shows for the 'Mobile Wallet' software building block a section of the table related to the security target 'Confidentiality'.

  (b) In each table, a row has been added for each asset, for which the security target represented by that table is relevant. In addition, a table row has been added for each threat agent. As a result, table cells have represented a unique combination of a certain asset and a certain threat agent (for the security target covered by that table). The example table shown in Figure 3 contains the three threat agents identified for the 'Mobile Wallet' software building block and a list of assets like 'Identity Assertion', 'Attribute Selection', 'VC Request', etc.

  (c) In the next step, table cells have been filled. In each table cell, a list of software components and communication channels between software components has been entered. The list illustrates, at which components (and communication channels) the respective asset (related to that table cell) can be attacked by the respective threat agent (related to that table cell). For instance, Figure 3 shows that e.g. the asset 'Identity Assertion' can be attacked by the threat agent 'External Attacker' at the components 'PF' ('Provisioning Service Frontend') and 'PB' ('Provisioning Service Backend'), as well as on communication channels between components 'ES'

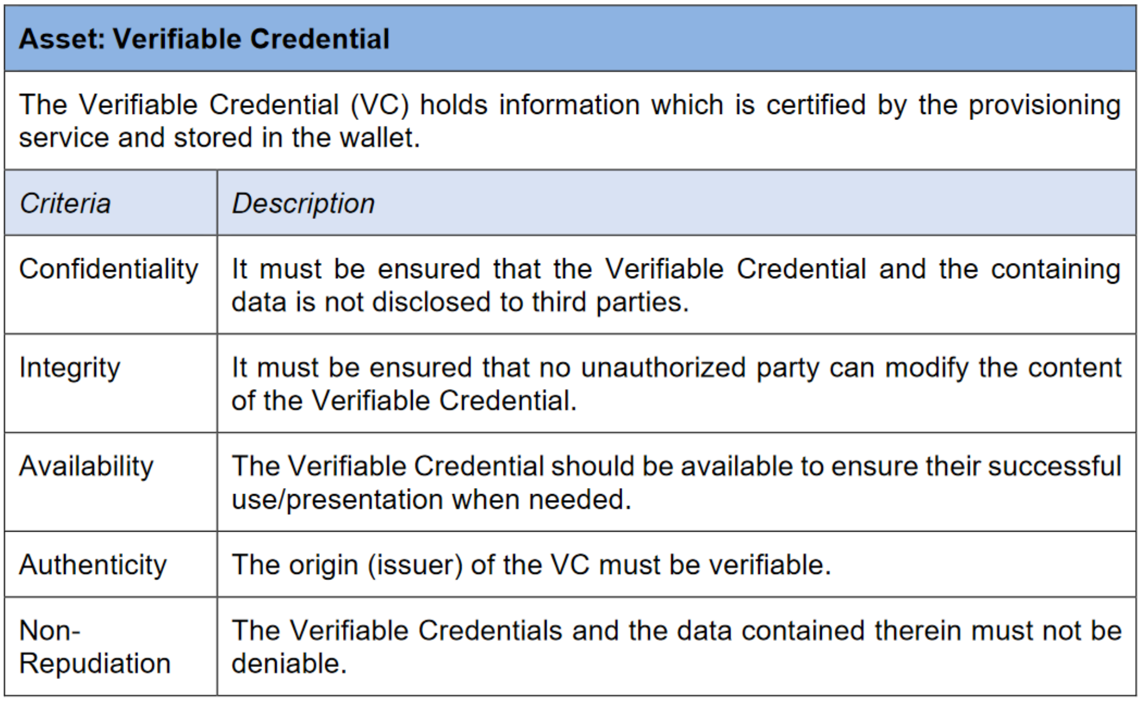
[1] https://c4model.com/

('External Data Source') and 'PF', and 'PF' and 'PB'. The applied tabular approach has enforced a strictly systematic procedure, which in turn ensures a complete coverage of all possible attack scenarios.

(d) Using a four-stage color scheme, each table-cell entry, i.e., each threat scenario, has been assigned a threat potential. This is also illustrated in the example table shown in Figure 3.

(5) **Countermeasures:** After identifying all possible threat scenarios using the tabular approach described above, necessary countermeasures have been derived and described in detail.

(6) **Recommendations:** In the last step, concrete recommendations have been derived from necessary countermeasures and their current state of implementation in the respective software building block under evaluation. Made recommendations have been fed back into the development processes of the respective software building blocks and have hence directly contributed to their increased security.

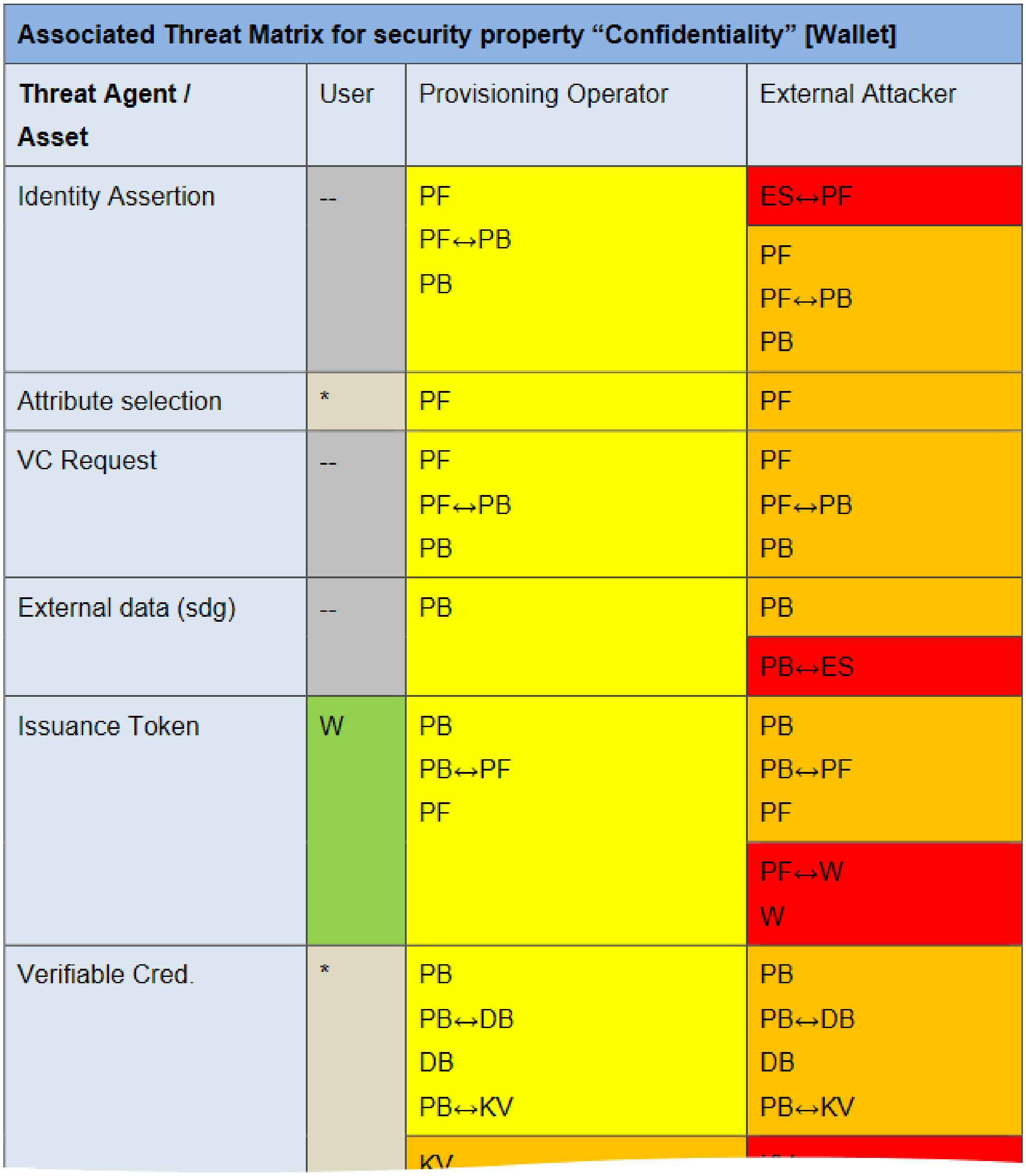


Asset: Verifiable Credential	
The Verifiable Credential (VC) holds information which is certified by the provisioning service and stored in the wallet.	
Criteria	*Description*
Confidentiality	It must be ensured that the Verifiable Credential and the containing data is not disclosed to third parties.
Integrity	It must be ensured that no unauthorized party can modify the content of the Verifiable Credential.
Availability	The Verifiable Credential should be available to ensure their successful use/presentation when needed.
Authenticity	The origin (issuer) of the VC must be verifiable.
Non-Repudiation	The Verifiable Credentials and the data contained therein must not be deniable.

Fig. 2. Mobile Wallet Software Building Block: Identification of relevant security targets for asset Verifiable Credential.

5.3 Evaluation Results

The evaluation method described above has been applied to all four software building blocks developed in the Horizon-2020 project mGov4EU. In total, the security of 23 assets has been analyzed by means of 20 threat tables similar to the one shown in Figure 3. From the evaluation results obtained, ten recommendations have been derived and classified into three categories. These recommendations have been considered by the mGov4EU project to further strengthen the robustness and security of developed software building blocks.



Associated Threat Matrix for security property "Confidentiality" [Wallet]			
Threat Agent / Asset	User	Provisioning Operator	External Attacker
Identity Assertion	--	PF PF↔PB PB	ES↔PF
			PF PF↔PB PB
Attribute selection	*	PF	PF
VC Request	--	PF PF↔PB PB	PF PF↔PB PB
External data (sdg)	--	PB	PB
			PB↔ES
Issuance Token	W	PB PB↔PF PF	PB PB↔PF PF
			PF↔W W
Verifiable Cred.	*	PB PB↔DB DB PB↔KV	PB PB↔DB DB PB↔KV
		KV	

Fig. 3. Mobile Wallet Software Building Block: Identification of relevant threat scenarios related to security target Confidentiality.

Overall, obtained evaluation results are twofold. First and foremost, the successful application of the security-evaluation framework proposed in Section 4 shows the framework's applicability to concrete software solutions in the domain of mobile cross-border e-government services. By applying it to different software components (i.e., mGov4EU softare building blocks), we have demonstrated that the proposed framework is generic enough to be applied to different software solutions yet detailed enough to yield meaningful results.

Second, the Horizon-2020 project mGov4EU and the software building blocks developed by this project have benefited directly from the conducted security evaluations. Potential weaknesses in the evaluated software building blocks have been identified early and constructive feedback in the form of 10 concrete recommendations has been provided, which has had an immediate positive impact on the overall level of security.

6 CONCLUSIONS

In this paper we have proposed a customized security-evaluation framework that is tailored to mobile cross-border e-government services. The proposed framework relies on established norms and standards by cherry picking from these norms and standards those elements and aspects most appropriate and useful for the given use-case.

The practical applicability of the proposed framework has been evaluated by means of four software building blocks developed by the Horizon-2020 project mGov4EU with the goal to leverage mobile cross-border e-government services in Europe. The evaluation of the four software building blocks using the proposed framework produced several recommendations for improving their security, demonstrating the framework's practical applicability and usefulness.

In future work, the proposed security-evaluation framework will be further developed to increase its range of applicability. So far, the framework has been applied to rather isolated software building blocks only. In a next step, we will apply the framework to real-world e-government applications that rely on and make use of the already evaluated software building blocks to provide end user comprehensive mobile cross-border e-government services.

ACKNOWLEDGMENTS

This paper is supported by European Union's Horizon 2020 research and innovation programme under grant agreement No 959072, project mGov4EU. The paper relies and is based on work conducted in this project and described in mGov4EU Deliverable 5.4.

REFERENCES

[1] 2021. OWASP Top Ten. "https://owasp.org/Top10/"

[2] Sultan AlGhamdi, Khin Than Win, and Elena Vlahu-Gjorgievska. 2020. Information security governance challenges and critical success factors: Systematic review. *Computers & security* 99 (2020), 102030.

[3] BSI Standard 200-1 2017. *BSI Standard 200-1, Information Security Management Systems (ISMS).* Standard. Federal Office for Information Security (BSI), Bonn, DE.

[4] BSI Standard 200-2 2017. *BSI Standard 200-2, IT-Grundschutz Methodology.* Standard. Federal Office for Information Security (BSI), Bonn, DE.

[5] BSI Standard 200-3 2017. *BSI Standard 200-3, Risk Analysis based on IT Grundschutz.* Standard. Federal Office for Information Security (BSI), Bonn, DE.

[6] Andreea Ancuta Corici, Blaz Podgorelec, Thomas Zefferer, Detlef Hühnlein, Jordi Cucurull, Hans Graux, Stefan Dedovic, Bogdan Romanov, Carsten Schmidt, and Robert Krimmer. 2022. Enhancing European Interoperability Frameworks to Leverage Mobile Cross-Border Services in Europe. In *DG. O 2022: The 23rd Annual International Conference on Digital Government Research.* 41–53.

[7] Gurpreet Dhillon and James Backhouse. 2000. Technical opinion: Information system security management in the new millennium. *Commun. ACM* 43, 7 (2000), 125–128.

[8] Gencer Erdogan, Atle Refsdal, and Ketil Stølen. 2014. A systematic method for risk-driven test case design using annotated sequence diagrams. In *Risk Assessment and Risk-Driven Testing: First International Workshop, RISK 2013, Held in Conjunction with ICTSS 2013, Istanbul, Turkey, November 12, 2013. Revised Selected Papers 1.* Springer, 93–108.

[9] Katerina Goseva-Popstojanova, Ahmed Hassan, Ajith Guedem, Walid Abdelmoez, Diaa Eldin M Nassar, Hany Ammar, and Ali Mili. 2003. Architectural-level risk analysis using UML. *IEEE transactions on software engineering* 29, 10 (2003), 946–960.

[10] Rasha G Hassan, Othman O Khalifa, et al. 2016. E-Government-an information security perspective. *International Journal of Computer Trends and Technology (IJCTT)* 36, 1 (2016), 1–9.

[11] Øystein Haugen, Knut Eilif Husa, Ragnhild Kobro Runde, and Ketil Stølen. 2005. STAIRS towards formal design with sequence diagrams. *Software & Systems Modeling* 4 (2005), 355–357.

[12] ISO 31000:2018(E) 2018. *Risk management — Guidelines*. Standard. International Organization for Standardization, Geneva, CH.

[13] ISO/IEC 15408:1999(E) 1999. *Information technology — Security techniques — Evaluation criteria for IT security*. Standard. International Organization for Standardization, Geneva, CH.

[14] ISO/IEC 27005:2018(E) 2018. *Information technology — Security techniques — Information security risk management*. Standard. International Organization for Standardization, Geneva, CH.

[15] Rick Kazman, Mark Klein, and Paul Clements. 2000. *ATAM: Method for architecture evaluation*. Technical Report. Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst.

[16] JD Meier. 2003. *Improving web application security: threats and countermeasures*. Microsoft press.

[17] NIST.FIPS.140-3 2019. *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION - SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES*. Standard. National Institute of Standards and Technology (NIST), Gaithersburg, Maryland, USA.

[18] NIST.SP.800-131Ar2 2019. *NIST Special Publication 800-131A Revision 2 - Transitioning the Use of Cryptographic Algorithms and Key Lengths*. Standard. National Institute of Standards and Technology (NIST), Gaithersburg, Maryland, USA.

[19] NIST.SP.800-133r2 2020. *NIST Special Publication 800-133 Revision 2 - Recommendation for Cryptographic Key Generation*. Standard. National Institute of Standards and Technology (NIST), Gaithersburg, Maryland, USA.

[20] NIST.SP.800-163r1 2019. *NIST Special Publication 800-163 Revision 1 - Vetting the Security of Mobile Applications*. Standard. National Institute of Standards and Technology (NIST), Gaithersburg, Maryland, USA.

[21] NIST.SP.800-57pt1r5 2020. *NIST Special Publication 800-57 Part 1 Revision 5 - Recommendation for Key Management: Part 1 - General*. Standard. National Institute of Standards and Technology (NIST), Gaithersburg, Maryland, USA.

[22] NIST.SP.800-57pt2r1 2019. *NIST Special Publication 800-57 Part 2 Revision 1 - Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations*. Standard. National Institute of Standards and Technology (NIST), Gaithersburg, Maryland, USA.

[23] Open Web Application Security Project (OWASP). 2021. OWASP Threat Modeling Process. https://owasp.org/www-project-threat-modeling/ Accessed on 2022-10-01.

[24] owasp.asvs 2021. *OWASP Application Security Verification Standard (ASVS) Project*. Standard. OWASP Foundation. "https://owasp.org/www-project-application-security-verification-standard/"

[25] owasp.masvs 2021. *OWASP MASVS (Mobile Application Security Verification Standard)*. Standard. OWASP Foundation. "https://mas.owasp.org/MASVS/"

[26] I Made Putrama, Kadek Teguh Dermawan, Gede Rasben Dantes, and Kadek Yota Ernanda Aryanto. 2017. Architectural evaluation of data center system using architecture tradeoff analysis method (ATAM): A case study. In *2017 International Conference on Advanced Informatics, Concepts, Theory, and Applications (ICAICTA)*. IEEE, 1–6.

[27] Atle Refsdal and Ketil Stølen. 2008. Extending UML sequence diagrams to model trust-dependent behavior with the aim to support risk analysis. *Electronic Notes in Theoretical Computer Science* 197, 2 (2008), 15–29.

[28] REN/ESI-0019401v231 2021. *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers* . Standard. European Telecommunications Standards Institute (ETSI), Valbonne, FR.

[29] REN/ESI-0019411-1v131 2021. *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates*. Standard. European Telecommunications Standards Institute (ETSI), Valbonne, FR.

[30] J. Ryoo, H. Lee, K. Kim, J. Lee, and S. Lee. 2017. AAFs architectural analysis method for secure software development. *Journal of Systems and Software* 126 (2017), 121–137.

[31] European Union. 2014. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN.

[32] European Union. 2016. General Data Protection Regulation (GDPR). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.

[33] European Union. 2018. Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R1724&from=EN.

[34] European Union. 2021. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0281&from=EN.

[35] David Valle-Cruz. 2019. Public value of e-government services through emerging technologies. *International Journal of Public Sector Management* (2019).