The final version is published in: M. Leitner et al., "A Versatile, Secure and Privacy-Aware Tool for Online Participation," 2016 IEEE 20th International Enterprise Distributed Object Computing Workshop (EDOCW), Vienna, 2016, pp. 1-4. doi: 10.1109/EDOCW.2016.7584342
URL: https://doi.org/10.1109/EDOCW.2016.7584342

A versatile, secure and privacy-aware tool for online participation

Maria Leitner*, Arndt Bonitz*, Bernd Herzog†, Walter Hötzendorfer‡, Christian Kenngott†, Thomas Kuhta†, Oliver Terbu§, Stefan Vogl§ and Sebastian Zehetbauer§
*AIT Austrian Institute for Technology GmbH
Digital Safety and Security Department
firstname.lastname@ait.ac.at
†rubicon IT GmbH
firstname.lastname@rubicon.eu
‡University of Vienna, Centre for Computers and Law
walter.hoetzendorfer@univie.ac.at
§Österreichische Staatsdruckerei
lastname@staatsdruckerei.at

***Abstract*—Online participations are gaining more momentum in recent years. Different tools for participation exist; however, often they support only one level of participation such as information, consultation or cooperation. What is missing so far is a secure and flexible tool that can be used for multiple purposes. In this paper, we propose an application that supports multiple levels of participation for participation procedures. Furthermore, privacy and security by design were incorporated into the software engineering process in order to make security and privacy top priorities from the beginning. In particular, the authentication of participants was a core concern in the implementation. In order to enable a low threshold for participation, we decided to offer the use of various electronic identities (eIDs) to the participants (e.g., by social eIDs or state-based eIDs). With this tool, we expect to increase the trust between operators and participants in online participations.**

1. Introduction

Electronic, participatory processes are ICT-supported participation procedures (notably in political decision-making processes) within society. The underlying ICT is important for the acceptance and participation in electronic processes [1], [2]. Hence, the decisions for information system design (e.g., architecture, software engineering tools and methods) and furthermore the concrete information system implementation (e.g., choosing data formats and protocols) have critical impact on the resulting e-participation solutions.

Furthermore, the technology has an impact on the participation procedures itself and the participants. Trust can play a significant role for (electronic) participation initiatives (e.g., [3], [4]). For example in [5], a security analysis is performed to identify potential risks and shortcomings that could affect the trust of people towards e-participation initiatives. In fact, the authors define security requirements and preventive measures to minimize the risk of exposure and to enable "trust by design".

Our approach aligns with these considerations. In this paper, we aim to address these security and privacy challenges in order to establish a secure and privacy-aware tool for e-participation. In particular, we describe and analyze requirements and design considerations for secure online participation. Furthermore, we will elaborate on privacy and security by design for e-participation. Based on these findings, we designed and developed a secure and privacy-aware architecture that is demonstrated with a proof-of-concept prototype. With the implementation, we aim to increase trust between operators and participants and to provide a secure infrastructure participatory processes. Furthermore, maintaining a privacy-aware and secure platform will minimize threats and risks of attacks or misuse and increase the trust in technology and the e-participation ecosystem.

The rest of this paper is structured as follows. Section 2 describes the main requirements and design considerations for secure online participation such as how security and privacy by design principles where established. Section 3 provides an overview of the architecture and the proof-of-concept prototype. Section 4 concludes the paper.

2. Design Considerations for secure Participation

Secure information system design is a key factor for establishing trust between operators and participants in e-participation[5]. In this section, we will elaborate on our design for secure participation.

2.1. Requirements

With our design, we aim to address the following requirements that were derived in the project consortium based on business needs, experience and expertise within the consortium:

TABLE 1: Levels of Participation (based on [6])

No.	Participation level	Examples
1	Information	Provision of information
2	Consultation	One- or two-way communication and ratings (e.g., liking or disliking)
3a	Co-operation	Collaborative preparation of results
3b	Co-decision	Vote on results or implementations (not legally binding)
4	Decision*	Legally binding decision

* Note that we do not support participation level decision in our tool.

I **Provide multiple levels of participation:** The first requirement is the support of various levels of participation such as shown in Table 1. Operators of participatory processes should be able to specify phases within one participation procedure. These phases have one level of participation such as consultation or cooperation. Furthermore, a period of time should be defined for each phase.

II **Support authentication with various eIDs:** The platform should support various eIDs that citizens could use to get involved; the identity has to be suitable to the level of participation while preserving a low participation threshold and maintaining security and privacy requirements. For example, the levels information and consultation might require no authentication (no eID) or authentication by social eIDs [6]. However, other levels such as co-decision might require an eID with a higher assurance level (such as state-based eIDs).

III **Maintain security and privacy by design:** In particular, ensuring the identification and authentication of participants is important to establish reliability and trustworthiness between operators and participants.

IV **Ensure interoperability to existing identity solutions:** It is further important to ensure interoperability with already existing eIDs and services in order to facilitate reuse and enable citizens to use eIDs they already have. This can further enable a low threshold for participation.

V **Adhere to legal regulations:** In particular the e-participation system has to comply with data protection law and fulfil the legal requirements for the intended e-participation, if such requirements exist.

2.2. Administrative and Participant Perspective

Furthermore, two perspectives should be supported by the tool for online participation:

- The *participant perspective* provides features for the participatory processes and providing multiple levels of participation such as information, consultation, coordination and co-decision. Participants can get involved in participatory processes. In order to access certain processes, participants may or may not have to authenticate themselves with an eID. This is specified in the participatory process.
- The *administrative perspective* enables the organizers of the participatory processes to design and specify the planned participatory processes. Each participatory process can contain several phases (e.g., information, consultation). For each phase, admins can specify parameters such as start and end date, description, and level of assurance.

2.3. Use Cases

The proposed tool is designed to support different participation procedures throughout various levels of participation. However, to demonstrate our approach, we specify two concrete scenarios that the tool supports:

1) **Design of a square**: Citizens are informed (information) and can suggest ideas how a town square should be refurbished. After an idea phase (consultation), local citizens my vote for their favorite decision (co-decision).
2) **Establishment of a pedestrian area**: Citizens can inform themselves (information) and comment and discuss the transformation of a street into a pedestrian area (consultation) and can later vote for or against it (co-decision).
3) **Co-creation of house rules**: Tenants of a house can cooperatively create (co-operation) and discuss (consultation) a list of house rules.
4) **Works council election**: Employees of an enterprise can elect a works council.

However, these two scenarios are not the only ones that our tool supports. In particular, the flexible and general approach may support much more diverse scenarios.

2.4. Privacy and Security by Design

In order to adhere to legal regulation but also beyond that requirement the system is designed along the principles of security and privacy by design. This means to address security, privacy and data protection already during the design and software development phase as a whole rather than to build necessary measures on top of a ready-made system [7]. For this purpose a SCRUM-based privacy and security by design software engineering process was developed, which is described in [8].

3. Implementation

The aforementioned requirements and design principles directly influenced the design and implementation of the e-participation platform. In particular, we designed several components that will establish the privacy by design principles. The first component checks and verifies the identities used within the participation platform. The second component provides all functionality necessary for online participations. The advantages are that data is only requested according to the level of assurance (LoA). The LoA refers to the required quality of user identification. LoA 4 is the

highest level and guarantees an identity verified by the state, LoA 1 includes social IDs (e.g. Facebook), LoA 2 applies to reputation based IDs, LoA 3 refers to application specific user management (e.g. Microsoft Active Directory) and LoA 0 indicates no identification is required.

3.1. Architecture

The architecture contains two components as shown in Figure 1:

- The e-participation component provides all functionality for online participation. Four levels of participation (i.e. information, consultation, cooperation and co-decision) are supported. In case of information (and consultation) no authentication is required. However, for all other levels authentication can be mandatory. In this case, the e-participation component makes a specific authentication request with a specific LoA.
- The identity component verifies the identity of the participant and returns an anonymized ID specific for participation.

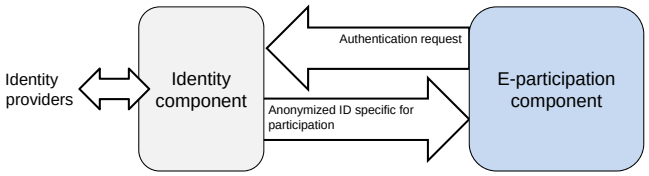

Figure 1: Architecture

Figure 2 displays the authentication procedure in more detail. It can be seen that (1) the participant wants to take part in an online participation. If authentication is required, (2) the e-participation component checks the required LoA and (3) requests an ID from the identity component. The identity component (4) suggests authentication methods to the user. The user selects a method and (5) authenticates. The authentication procedure itself (5a) is performed at an identity provider (such as Facebook, Twitter and others) and a confirmation is returned (5b). If the authentication was successful, the identity component (6) provides an anonymized ID to the e-participation component. Finally, (7) the user can participate (e.g., write a comment or rate a comment).

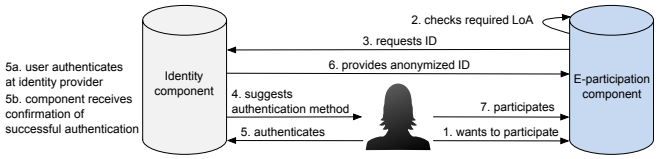

Figure 2: Authentication procedure

Furthermore, no personal data is stored in the e-participation platform. The identity is not known by the e-participation component and the specific participation activities are unknown to the identity component. This ensures not only privacy in online participations but also enables the participant to identify which data is requested in what participations. For example, if the e-participation platform requires further data such as age or location, the participant will receive a notification during the identity check and verification.

3.2. Proof-of-concept Prototype

A prototype has been implemented to proof feasibility of the concept introduced before. Both the e-participation component and the identity component have been implemented as two independently hosted web applications based on Microsoft's ASP.NET MVC framework with Bootstrap for CSS presentation and AngularJS for smooth user interaction. The identity component additionally makes use of the IdentityServer3 framework for the implementation of the OpenID Connect protocol and MOA-ID for the integration of the Austrian Citizen Card (Bürgerkarte).

Whereas the e-participation component provides the main user interface to interact with, the identity component will hardly be noticed by the user at all, as it only provides a selection of identification providers, redirects to the selected identity provider and then back to the e-participation component, where the user can participate in various levels of participations as described before (see Table 1).

An organizational administrator can create or modify online participation processes and their phases in the administration part of the e-participation component (see Figure 3) and assign an appropriate LoA. Whenever a user wants to participate, the LoA for that phase and higher are computed to offer the corresponding identity providers.

With the prototype, we demonstrate not only that we fulfilled all requirements (see Section 2.1):

I Our prototype supports the participation levels information, consultation, co-operation and co-decision. With this set of participation levels, a vast amount of diverse participation procedures can be supported and proves to be flexible.

II Administrators can predefine a set of eIDs that can be used not only within a participation procedure but also specifically for each phase (information, consultation, co-operation and co-decision).

III Security and privacy were a top priority from the beginning and we specifically used a software engineering process that included these aspects (see [8], [9]).

IV We provide interoperability to already existing eIDs. In particular, we provide access to state-based eIDs as well as social IDs (e.g., Facebook, Twitter).

V During the design as well as the engineering phase, legal guidance identified potential chances and pitfalls during the development in order to avoid legal complications. In addition, we analyzed current practice of data use in participation procedures [10].

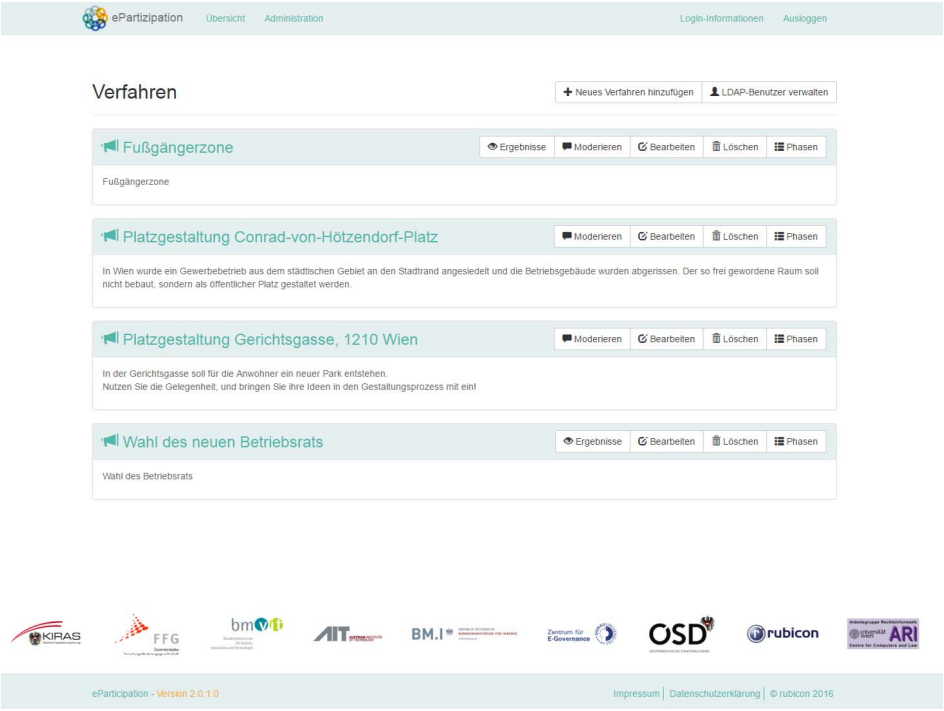

Figure 3: Screenshot of administration interface (April 2016)

4. Conclusion

This paper introduced and described the design and development of a comprehensive, secure and privacy-aware application for online participations. We analyzed and reviewed the main challenges and requirements for the design and development of an e-participation tool that provides flexibility while preserving fundamental security and privacy principles. Furthermore, we outlined the overall architecture and displayed how this has been adapted into a proof-of-concept prototype.

Acknowledgments

This work is part of the project ePartizipation that is funded by the Austrian security research programme KIRAS of the Federal Ministry for Transport, Innovation and Technology (bmvit).

References

[1] V. Peristeras, G. Mentzas, K. Tarabanis, and A. Abecker, "Transforming E-government and E-participation through IT," *IEEE Intelligent Systems*, vol. 24, no. 5, pp. 14–19, Sep. 2009.

[2] S. Scherer and M. A. Wimmer, "Analysis of Enterprise Architecture Frameworks in the Context of e-Participation," in *Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times*, ser. dg.o '11. New York, NY, USA: ACM, 2011, pp. 94–103.

[3] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, "Not So Different After All: A Cross-Discipline View Of Trust," *Academy of Management Review*, vol. 23, no. 3, pp. 393–404, Jan. 1998.

[4] S. Kim and J. Lee, "E-Participation, Transparency, and Trust in Local Government," *Public Administration Review*, vol. 72, no. 6, pp. 819–828, Nov. 2012.

[5] S. Scherer and M. A. Wimmer, "Vertrauensförderung in E-Partizipation," *Datenschutz und Datensicherheit - DuD*, vol. 39, no. 5, pp. 295–302, Apr. 2015.

[6] P. Parycek, J. Schossböck, and B. Rinnerbauer, "Identification in E-Participation: Between Quality of Identification Data and Participation Threshold," in *Electronic Participation*, ser. Lecture Notes in Computer Science. Springer International Publishing, Aug. 2015, no. 9249, pp. 108–119.

[7] J. v. Rest, D. Boonstra, M. Everts, M. v. Rijn, and R. v. Paassen, "Designing Privacy-by-Design," in *Privacy Technologies and Policy*, ser. Lecture Notes in Computer Science, B. Preneel and D. Ikonomou, Eds. Springer, Oct. 2012, no. 8319, pp. 55–72, dOI: 10.1007/978-3-642-54069-1_4.

[8] O. Terbu, W. Hötzendorfer, M. Leitner, A. Bonitz, S. Vogl, and S. Zehetbauer, "Privacy and security by Design im agilen Softwareprozess," in *Internationales Rechtsinformatik Symposion (IRIS)*, Salzburg, 2016.

[9] J. Schossböck, M. Sachs, and M. Leitner, "E-Participation Platform Features and Design Principles," in *CeDEM16 Proceedings of the International Conference for E-Democracy and Open Government 2016*, P. Parycek and N. Edelmann, Eds. Krems, Austria: Edition Donau-Universität Krems, 2016, pp. 69–74. [Online]. Available: http://www.donau-uni.ac.at/imperia/md/content/department/gpa/zeg/bilder/cedem/cedem16/cedem16_inhalt_160414.pdf

[10] I. Serov, M. Leitner, and S. Rinderle-Ma, "Current Practice and Challenges of Data Use and Web Analytics in Online Participations," in *15th IFIP Electronic Government (EGOV) and 8th Electronic Participation (ePart) Conference 2016*, 2016, (to appear).