Electronic Government and Electronic Participation
H.J. Scholl et al. (Eds.)

doi:10.3233/978-1-61499-670-5-51

Inclusion and Privacy in E-Participation Platform Design

Judith Schossböck[a1], Oliver Terbu[b], Michael Sachs[a], Maria Leitner[c], Vinzenz Heussler[d], Gregor Wenda[e], Arndt Bonitz[c], Walter Hötzendorfer[d], Peter Parycek[a], Stefan Vogl[b], Sebastian Zehetbauer[b]

[a]Danube University Krems, 3500 Krems, Dr. Karl Dorrek-Straße 30,
{peter.parycek|michael.sachs|judith.schossboeck}@donau-uni.ac.at
[b]Österreichische Staatsdruckerei, Tenschertstraße 7, 1239, Vienna, Austria,
{terbu|vogl}@staatsdruckerei.at
[c]AIT Austrian Institute for Technology GmbH, Digital Safety and Security Department, Information Management, Donau-City-Straße 1, 1220, Vienna, Austria,
{arndt.bonitz|maria.leitner}@ait.ac.at
[d]University of Vienna, Centre for Computers and Law, 1010 Vienna, Austria,
Schottenbastei 10-16/2/5,
{vinzenz.klaus.h eussler|walter.hoetzendorfer}@univie.ac.at
[e]Federal Ministry of the Interior (BMI), Herrengasse 7, 1010 Vienna, Austria,
Gregor.Wenda@bmi.gv.at

Abstract. Austria has seen some efforts in e-participation initiatives during the last years. However, a single platform comprising many e-participation levels and activities for a broader target group is so far missing. In the project *ePartizipation* researchers and practitioners worked on a platform demonstrator that integrates multiple online identification methods and offers activities on different levels of e-participation. This paper describes the conceptualisation of the platform and the inherent design principles, the first project results, in particular related to strategies aiming at enhancing inclusion and privacy, and the experiences from the project team.

Keywords. E-participation, identification, accessibility, Privacy by Design

Acknowledgement. The project *ePartizipation* is funded by the Austrian security research programme KIRAS of the Federal Ministry for Transport, Innovation and Technology (bmvit).

Introduction

E-participation is often seen as a means to increase engagement in political processes. There are many measures to be taken if platforms are meant to be hosted by public authorities, and if they are to attract a variety of citizens and not only tech-savvy users. Not only strategies to foster digital inclusion need to be considered [9, 6, 4] but also regarding privacy and data handling processes of the system [5]. Within regulations

[1] Corresponding author

and declarations of the European Union, e-participation and e-accessibility are seen as a measure towards social justice[2]. E-inclusion can be defined as a means to meet the goals of inclusion [11, 12, 7]. Recent research emphasizes foremost a capabilities approach [10]. As privacy is a key aspect in e-participation platform design, it is necessary to identify how Privacy by Design (PbD) can be included in the design of an e-participation platform. This paper presents the development of such a platform with consideration of the above mentioned design principles. The paper combines the insights of several publications that relate to the project *ePartizipation* and are listed in the bibliography.

1. Project Description and Methodology

The core goal of the project *ePartizipation* is to design a platform demonstrator that can be used as a single site for multiple e-participation purposes on different levels of participation. One of the sub-goals of the project was to map different methods of online identification and authentication with activities of e-participation. The methodology for the theoretical framework of the platform concept integrated desk research, the input from a focus group with interested citizens, qualitative expert interviews, and an internal focus group [14]. Within the scope of this paper, the authors will only focus on aspects of inclusion and privacy.

Latest data regulations were analysed on national and on EU-level. Legal advisers within the consortium constantly provided feedback to the developers during the implementation phase. At the time of finalising this paper, the platform is in the final development phase. While usability tests were integrated in the entire implementation phase, user acceptance tests are about to take place.

2. Project Results

2.1. Platform Demonstrator: Features and Design Principles

The concept of the tool allows high flexibility in the usage of the tool. On the one hand side, providers of e-participation processes can design their processes according to their needs. This means that a discussion activity can be followed by co-decision activity, which can be the end of a process or again be followed by a discussion. The platform allows the integration of multiple e-IDs for authentication. The host of e-participation processes can choose the e-IDs for each individual participation activity. This means that multiple e-IDs can be allowed in one participation process. While the activity of stating ideas could be open for social IDs, the process of co-deciding could be only allowed to users that login with a unique ID implemented by the state (e.g. in Austria: citizen card). The following design principles are reflected in the demonstrator:

- Integration of multiple online identification methods (e-IDs)
- Aspects of e-inclusion (Design for All)

[2] Europäische Kommission, KOM (2007) 332, 14.06.2007, Altern in der Informationsgesellschaft, http://eurlex.europa.eu/legal-content/DE/TXT/?uri=URISERV%3Al24292 (aufgerufen am 6. Januar 2016).

- Privacy and Security by Design

In the following, we will describe those features and their application.

2.2. Integration of Multiple Online Identification Methods

One aspect of e-inclusion and low participation threshold is already reflected in the flexibility of being able to choose between different e-IDs as described above. E-participation providers are advised to implement a multiple identity management system that allows users to participate in some processes completely without registration (e.g. commenting). An e-ID management system allows the hosts of platforms guidance in selecting appropriate e-IDs. This allows both users and hosts some flexibility in selecting e-participation processes and their preferred ID method.

2.3. Inclusion of Target Groups: E-Inclusion and Design for All

The use of information and communication technology (ICT) in web-based participation-models creates the risk of excluding some target groups. These comprise people with disabilities such as visual, auditory, physical, cognitive, learning and neurological disabilities, as well as non-native speakers and elderly people. Each of these target groups imposes different requirements with view to accessible online content[3]. A comprehensive description of the different needs as well as a wide range of recommendations for making web content more accessible can be found in the Web Content Accessibility Guidelines (WCAG) 2.0[4]. Some of the layers of guidance[5] were accepted by the International Organization for Standardization as an ISO International Standard (ISO/IEC 40500:2012) in October 2012. [6] Additionally, pure online participation-models exclude people with no access to ICT as well as people who deliberately refuse to make use of ICT [13], which is why these people must be considered as target groups that can only be reached through offline activities (while this is not reflected in the demonstrator, future usage scenarios of it should take this into account). People with difficulties to make proper use of ICT, like elderly people, non-native speakers or people with disabilities, can also be helped or encouraged by capacity building. Summarizing, some people can be helped with (1) measures enhancing e-accessibility, some with (2) capacity building, some with (3) both, and some require (4) other support, like legal regulations or offline measures.

2.3.1. Measures Towards Inclusion: Design for All and E-Accessibility

Public authorities have to design accessible platforms. Private providers have to do this according to their resources. Independent from this prerequisite, which needs to be considered if the demonstrator is used in the field, there are simple features enhancing

[3] Wagner-Leimbach, H. (2010). Gestaltung barrierefreier Internetangebote, WEBACC 2.1.1 vom 30. August 2010, pp. 7–9; reference.e-government.gv.at/fileadmin/_migrated/content_uploads/webacc-2-1-1_2010-0830.pdf (accessed January 2nd, 2016).

[4] https://www.w3.org/TR/WCAG20/ (accessed 21st March 2016). The WCAG 2.0 is an international, legally non-binding standard that defines how to make web content more accessible to people with disabilities.

[5] Specifically the overall principles, general guidelines and testable success criteria

[6] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=58625 (accessed 21st March 2016).

inclusivity and accessibility which are reflected already in the demonstrator. The concept Design for All is based on the idea of accessibility. As design for "[…] social inclusion and equality"[7] it avoids the need for a specialised design or different viewing versions in order to not stigmatize some users. The demonstrator software is fully functional on a PC or mobile devices like tablets. Measures like mobile accessibility and operability via keyboard only can be done even by providers who are otherwise short on resources.[8] In line with the Design for All principle, one viewing version is recommended. Providers should seek to offer application specific user integration and many different e-IDs to attract different target groups. Even though some groups can nowadays be reached easily by mere online measures, it is still advised to offer online options in combination with offline participation or to make specific exceptions for certain target groups. Another measure is to stick to simple language and to offer content in other languages [4]. The target group should be crucial in defining processes and e-ID methods, and active exclusion of offline procedures or a specific group should only be made on the basis of a factual reason (f.i. youth participation projects with a target group that is 100 % on specific media channels).[9][10]

2.3.2. Legal Framework for Inclusion and E-Accessibility

On an international level, the probably most prominent legal basis in this context is the United Nations Convention on the Rights of Persons with Disabilities[11] (Article 1). One of its principles is the full and effective participation and inclusion in society (Article 3 (c)). In the European Union, the Proposal for a Directive on the accessibility of public sector bodies' websites[12] aims to approximate the laws and regulations of the Member States on the accessibility of websites of public sector bodies to all users, including people with functional limitations (Article 1 paragraph 1).[13] The Federal Constitutional Law of Austria (original version Federal Law Gazette No. 1/1930, as amended by Federal Law Gazette I No. 102/2014) states (Article 7) that no one shall be discriminated against because of disability. Furthermore, the Republic commits itself to ensure the equal treatment of disabled and non-disabled persons in all spheres of everyday life. More specifically, Section 1 paragraph 3 of the Federal Act on Provisions Facilitating Electronic Communications with Public Bodies (E-Government Act – E-GovG; original version Federal Law Gazette I No. 10/2004, as amended by Federal Law Gazette I No. 83/2013) stipulates that measures shall be taken to ensure that official Internet sites which provide information or support are structured in such a

[7] EIDD Stockholm Declaration, 2004. http://dfaeurope.eu/what-is-dfa/dfa-documents/ (accessed March 15th, 2016).

[8] The question whether e-participation websites fall under the service category according to ordinance on barrier-free information technology (as it would be the case according to e-government law) is not relevant on the demonstrator design level, however, later the provider of such a platform becomes crucial, as with private providers the question of reasonableness has to be asked. To shorten this discussion, it is recommended to stick to simple design measures.

[9] DIVSI (2014), Kinder, Jugendliche und junge Erwachsene in der digitalen Welt, Hamburg, Februar 2014. https://www.divsi.de/publikationen/studien/divsi-u25-studie-kinder-jugendliche-und-junge-erwachsene-in-der-digitalen-welt/1-einfuehrung-3/ (accessed 6th January, 2016).

[10] Online only options could be used for processes that are done more frequently though.

[11] http://www.un.org/disabilities/convention/conventionfull.shtml (accessed 21st March 2016).

[12] Proposal for a Directive of the European Parliament and of the Council on the accessibility of public sector bodies' websites COM/2012/0721 final, adopted by the European Parliament legislative resolution of 26 February 2014, 2012/0340 (COD).

[13] The proposal is still in negotiation.

way as to comply with international standards for access, including unhindered access for disabled people. Accordingly, platforms provided by Austrian public authorities have to ensure accessibility. For private entities, the Austrian Federal Act on the Equalization of Persons with Disabilities (original version Federal Law Gazette I No. 82/2005, as amended by Federal Law Gazette I No. 138/2013) seeks to avert the discrimination of people with disabilities (Section 1), including discrimination by not accessible websites (Section 6 paragraph 5). Although the law is fully applicable for the federal administration (Section 2), private providers only fall under the obligation to ensure reasonable accessibility (Section 6).

2.3.3. Scenario Works Council Election

The demonstrator software also offers the option of co-decision or decision processes, for which the scenario of works council election was implemented. Arguments often used against online voting are the general principle of the personal right vote and the exclusion of people without access to ICT or of people with lacking IT-skills. However, in Austria the Regulations on Works Council Election 1974 (original version Federal Law Gazette No. 319/1974, as amended by Federal Law Gazette II No. 195/2012) makes an exception from the general principle of the personal right vote by providing the possibility for postal voting. PCs also allow for authentication. Consequently, online voting would be feasible for works council elections from the perspective of inclusion as it is at least equal to the already existing postal voting.[14]

3. Privacy by Design

PbD implies addressing privacy and data protection during the entire technology lifecycle (van Rest et al. 2014), integrating privacy and data protection into the system during the software development process as a whole. In the future General Data Protection Regulation (GDPR) of the European Union “data protection by design” will become a fundamental principle. Papers dealing with PbD in practice [16, 3, 18, 8] have some principles in common, most importantly data minimization. This (MINIMISE) is the first of eight privacy design strategies listed by Hoepman [5]. Other data-oriented strategies are to hide personal data (HIDE), to hold them separated and to process them in a distributed way (SEPARATE) on the highest level of aggregation that is still useful (AGGREGATE). The four process-oriented privacy design strategies are to inform data subjects about the data processing (INFORM), to provide them agency over it (CONTROL), to put in place and enforce a privacy policy compatible with legal requirements (ENFORCE) and to be able to demonstrate compliance with the privacy policy and legal requirements (DEMONSTRATE).

3.1. PbD in Software Engineering

PbD as a concept has been existing for quite some time, but was hardly relevant for software development. For this reason, we propose extensions of the Scrum framework to ensure privacy and data protection. Agile development processes are based on the

[14] However, risks of abuse and lacking traceability must not be neglected.

Agile Manifesto [1][15]. Scrum is the most popular way of establishing an agile process by providing a lightweight framework to optimize predictability and control risk [15]. PbD has to be treated individually for every project by implementing strategies, design patterns and technologies according to the required purpose. This procedure can be called privacy engineering and demands dedicated experts or privacy engineers. Usually the Product Owner (PO) is responsible for managing the requirements but often does not have the abilities of privacy engineers. Privacy experts are also not found in a typical Development Team (DT) that help in analysis, planning, implementation and validation of appropriate measures to protect individuals. For this purpose, a dedicated privacy team consisting of privacy experts assists the Scrum Team (ST) in accomplishing privacy related tasks. This team is represented by one Privacy Representative (PR) which has a holistic view on development, infrastructure, privacy and data protection. The PR is then an additional PO and is allowed to create, modify and prioritize privacy related US and acceptance criteria in consultation with the traditional PO. The privacy team is coordinated and represented by the PR in all Scrum meetings.

Privacy related requirements are normally non-functional requirements, making privacy invisible in standard Scrum. The following measures were taken in order to model PbD during development, make privacy more visible, explicit and sustainable:

- Adding privacy requirements to Product Backlog (PB) as User Stories (US), technical US, acceptance criteria or definition of done.
- Adding US from the perspective of a potential attacker that wants to abuse the system which are also referred as evil user stories or abuse stories.
- Integrating static code analysis based on custom code annotations to enforce encryption when accessing personal data.
- Executing automated privacy related tests.
- Performing incremental reviews of all artifacts through privacy glasses.

3.2. Implementation and Practice of PbD for E-Participation Platforms

Privacy-relevant US are added in the PB. Their effort is estimated within the Sprint Planning just like regular US. Our experience with this has been very positive. However, as this is the first time we apply the process, we believe that there are further software engineering cycles necessary to determine efficiency and usability of this method. Plus, in this project we find highly motivated developers who are interested in privacy, which lead to some lessons learned. The aforementioned design principles directly influenced the implementation of the platform. In particular, we designed several components that will establish the PbD principles [17]. 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 (f.i. 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

[15] This Manifesto is a collection of basic values which specifically weights “individuals and interactions”, “working software”, “customer collaboration” and “responding to change” more than classic models.

identification. Furthermore, no personal data is stored in the 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 participation, but also enables the participant to identify which data is requested for which process. F.i., if the platform requires further data such as age or location, the participant will receive a notification during identity check and verification.

4. Summary

Even though focusing on the technical solutions in e-participation is important, factors like technical skills and perceived privacy can only partly explain participation numbers and citizens' motivation, and strategies of inclusion only offer some chance to enhance participation. But if such measures are not undertaken, projects run the risk to exclude people from important processes or to violate human rights [7]. Furthermore, e-inclusion should always be seen in relation to social inclusion, for which other differences (f.i. education) might need to be addressed first. However, e-participation could offer, particularly if based on institutional resources, the chance to support principles that are otherwise given less priority in the hype around mainstream or economically orientated technology innovations. Additionally, research focusing on aspects of capabilities should be supported. While some of our recommendations focus on technical accessibility, measures of inclusion should not be limited to it [2, 10]. This could mean putting more emphasis on user capabilities with regard to privacy and personal data. On the project level, this could be done by video messages or a specific F.A.Q. On the broader level, capabilities and participation could be seen as two complementary subjects finding their way into educational curricula. An evaluation of the platform demonstrator with user acceptance tests is planned in June 2016. This should shed further light on citizen's motivation to use the platform.

References

1. Beck, K., Beedle, M., Van Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., Grenning, J., Highsmith, J., Hunt, A., Jeffries, R., Kern, J., Marick, B., Martin ,R. C., Mallor, S., Shwaber, K., Sutherland, J. (2001). The Agile Manifesto, http://www.agilemanifesto.org (accessed 21th March, 2016).
2. Garnham, N. (2000). Amartya Sen's 'Capabilities' Approach to the evaluation of welfare: Its application to communications, in: Cammaerts, B., Burgelman, J. (Hg.) Beyond Competition: Broadening the Scope of Telecommunications Policy, Brussels: VUB University Press, pp. 25-36.
3. Gürses, S., Troncoso, C., Diaz, C. (2011). Engineering Privacy by Design, Computers, Privacy & Data Protection (CPDP 2011).
4. Heussler, V., Schossböck, J., Böszörmenyi, J. (2016). Aspekte der Inklusion aus Sicht der E-Partizipation. In: Schweighofer, Kummer, Hötzendorfer, Borges, Tagungsband des 19. Internationalen Rechtsinformatik Symposions, Jusletter IT, Salzburg. http://jusletter-it.weblaw.ch/issues/2016/IRIS.html (accessed 30th January, 2016).
5. Hoepman, J. H. (2014). Privacy Design Stretegies, ICT Systems Security and Privacy Protection, IFIP Advances in Information and Communication Technology 428, 2014, p. 446-459.

6. Horrigan, J. B. (2005). On Demand Citizens: E-Government at High Speed. Pew Internet & American Life Project, Washington DC, USA.
7. Kettemann, M. (2008). E-Inclusion as a Means to Bridge the Digital Divides. Conceptual Issues and International Approaches. In Benedek, W., Bauer, V., Kettemann, M. (Eds.) Internet Governance and the Information Society. Global Perspectives and European Dimensions. Portland: Eleven international publishing, pp. 51-62.
8. Kung, A. (2014). PEARs: Privacy Enhancing ARchitectures, Proceedings of the Second Annual Privacy Forum APF 2014, Lecture Notes in Computer Science, Springer, Berlin und Heidelberg 2014, pp.18–29.
9. Macintosh, A., Coleman, S., Schneeberger A. (2009). eParticipation: The Research Gaps. In: Macintosh, A. and Tambouris, E. (Eds.), Electronic Participation. First International Conference, ePart 2009 Linz, Austria, September 1–3, Proceedings, pp. 1–11.
10. Mansell, Robin (2002). From digital divides to digital entitlements in knowledge societies. Current sociology, 50 (3), pp. 407-426.
11. Marcantoni, F., Polzonetti, A. (2011). Digital Inclusion: A Target not Always Desirable. In: Klun, M., Decman, M., Jukic, T. (Hg.), The Proceedings of the European Conference on eGovernment, Ljubljana, 16-17 June 2011, pp. 369-376.
12. Millard, J. (2006). eGovernance and eParticipation: Lessons from Europe in promoting Inclusion and Empowerment. Paper presented to the UN Division for Public Administration and Development Management (DPADM), Workshop: E-Participation and E-Government: Understanding the Present and Creating the Future, 27-28 July 2006. http://unpan1.un.org/intradoc/groups/public/documents/un/unpan023684.pdf (accessed January 2nd, 2016).
13. Ringler, P.; Parycek, P.; Schossböck, J., Sturmberger, W.; Schönherr, D.; Oberhuber, F.; Aichberger, I.; Hacker, E. (2013). Internet und Demokratie in Österreich. Grundlagenstudie. SORA Forschungsbericht, SORA - Institut für Social Research and Consulting, Wien.
14. Sachs, M.; Schossböck, J. (2015). Perspectives on Electronic Identity Application in Online Engagement. In: Parycek, P.; Edelmann, N., CeDEM15 Proceedings of the International Conference for E-Democracy and Open Government, Edition Donau-Universität Krems, pp. 373-376.
15. Schwaber K., Sutherland J. (2013). The Scrum Guide, http://www.scrumguides.org/docs/scrumguide/v1/Scrum-Guide-US.pdf, (accessed 7th January, 2016).
16. Spiekermann, S., Cranor, L.F. (2009), Engineering Privacy, IEEE Transactions on Software Engineering 2009, pp. 67–82.
17. Terbu, O., Hötzendorfer, W., Leitner, M., Bonitz, A., Vogl, S. & Zehetbauer, S. (2016). Privacy and Security by Design im agilen Softwareentwicklungsprozess. In: Schweighofer, E., Kummer, F., Hötzendorfer, W. & Borges, G. (eds.), Netzwerke: Tagungsband des 19. Internationalen Rechtsinformatik Symposions IRIS 2016. Wien: Österreichische Computer Gesellschaft (OCG), pp. 457-464.
18. van Rest, J., Boonstra, D., Everts, M., van Rijn, M., van Paassen, R. (2014). Designing Privacy-by-Design, in Preneel, Bart/Ikonomou, Demosthenes (Hrsg.), Proceedings of the First Annual Privacy Forum, APF 2012, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg 2014, pp. 55–72.
19. Wu, L., Zhou, S., Zhou, Z., Hong, Z., Huang, K. (2015). A Reputation-based Identity Management Model for Cloud Computing. Mathematical Problems in Engineering, May 2015. http://www.hindawi.com/journals/mpe/ (accessed January 2nd, 2016).