H. Roßnagel, C. H. Schunck, S. Mödersheim (Hrsg.): Open Identity Summit 2021,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2021 223

"When need becomes necessity" - The Single Digital Gateway Regulation and the Once-Only Principle from a European Point of View

Carsten Schmidt[1], Robert Krimmer[2] and Thomas J. Lampoltshammer[3]

Abstract:
The Single Digital Gateway Regulation (SDGR) and the underlying Once-Only Principle (OOP) outlining that businesses and citizens in contact with public administrations have to provide data only once. Until now many MS and associated countries have started to implement the OOP at national level, but the cross-border implementation is still work in progress. The SDGR as one of the cornerstones of the Digital Single Market for the EU will bust this development. The authors of this paper present the development related to the SDGR and OOP in Europe. They will also show the interconnections and interdependencies between the OOP and electronic identities (eID). The paper gives an overview based on the findings of the EU-funded "The Once-Only Principle Project (TOOP)" and mobile Cross-Border Government Services for Europe (mGov4EU).

Keywords:
Once-Only Principle, Single Digital Gateway, SDGR, DSM, mGov4EU, TOOP, eID, eIDAS;

1 Introduction

Digitalization is key and the topic of our age. Politics, business, and society have recognised digitalization as one of the central tasks for Europe. This includes the transformation of all related services. Especially the COVID-19 pandemic is seen as an additional and major driver for digital transformation of our society. The transformation includes both the transition of currently paper-based services in "e-services", as well as the related business processes. The latter usually presents the greater challenge. The legal framework for this is the SDGR. It will have a decisive influence on the information exchange of the several hundred administrative services covered by it. The SDGR is intended to pave the way for comprehensive information, online administrative procedures, and services. A key point here is also the "once-only principle" (OOP). The OOP requires a technical system for cross-border automated exchange of evidence and application (Art. 14 SDGR). The implementation of the SDGR entails great demands and challenges, as well as opportunities.

This paper sheds light on distinct examples within the current landscape of activities, in

[1] Tallinn University of Technology (TalTech), Ragnar Nurkse Department of Innovation and Governance, Akadeemia tee 3, 12618 Tallinn, Estonia, carsten.schmidt@taltech.ee, https://orcid.org/0000-0001-8435-4313
[2] University of Tartu, ERA-Chair, Johan Skytte Institute for Political Studies Center for IT Impact Studies, Lossi 36, 51003 Tartu, Estonia, robert.krimmer@ut.ee, https://orcid.org/0000-0002-0873-539X
[3] Danube University Krems, Department for E-Governance and Administration, Dr.-Karl-Dorrek-Straße 30, 3500 Krems, Österreich, thomas.lampoltshammer@donau-uni.ac.at, https://orcid.org/0000-0002-1122-6908

particular towards SDGR and OOP, with a special focus on eID and its role in establishing a European, cross-border public service infrastructure, i.e., the Digital Single Market (DSM). The remainder of this paper is structured as follows: in Section 2, we provide a background overview of SDGR, OOP, as well as two associated project initiatives for their realisation. In Section 3, we discuss challenges concerning eIDAS/eIDAS II, technical interoperability, as well as the impact of mobile approaches to the domain of eID. In Section 4, we close the paper with our conclusions and final remarks.

2 Background

2.1 SDGR

The origin of the proposal for a single digital gateway (SDG) is based on the urgent need for a more coherent, streamlined approach in Europe. This was flagged by several business organisations, the European Parliament, 17 Member States (MS) and via the platform of the regulatory fitness and performance programme (REFIT) of the EC. Besides that, by public consultation on EU citizenship, 80 % of the citizens stated out that the repetition of provision of personal data on the one side and the unavailability of them on the other side is the biggest hurdle in cross-border cases [EC17].

For a presentation to the European Parliament, the EC has investigated the gaps in digitisation of 13 key procedures (see Fig. 1) [EP17]. These key procedures are related to different areas like, e.g., working or studying abroad and setting up a business in another MS or associated country [EC17]. The purpose of the SDG is to offer EU citizens and businesses easy and non-discriminatory online access to information about EU and national rules, national procedures for compliance with these rules and EU and national assistance services, in order to help them in exercising their rights of the DSM.

2.2 TOOP

"The Once-Only Principle project" (TOOP)[4] is the first large-scale pilot (LSP) project under the Horizon 2020 Framework Programme of the EU. The TOOP project was launched on 1 Jan 2017 as an initiative of mor than 50 organisations from 20 EU MS and associated countries. The main objective of TOOP is to explore and demonstrate the once-only principle across borders, to support the SDGR transition, focusing on data from businesses via three distinct pilots [LHP19], updating business register data in a cross-border context; cross-border e-services, in particular tenders; online ship and crew certificates, to enable better exchange of business-related data or documents with and between public administrations and reduce administrative burden for both businesses and public administrations. It identified various barriers (such as data protection and data-sharing requirements, implementation costs, public sector silo issues, and especially legal barriers and/or gaps) that could hinder the implementation [K17].

TOOP is using a federated IT architecture on a cross-border, pan-European scale. The

[4] https://toop.eu/

architecture is not built from scratch but re-uses and enhances already available building blocks in order to seamlessly preserve interoperability and to comply with regulations and existing technical standards (i.e., ISA²) [T20], [KS19]. If possible, the technical building blocks provided by the Connecting Europe Facility (CEF) (e.g., e-Delivery) are reused, amendments and additional technical solutions developed by TOOP complying with international standards set by standardisation organisations like, e.g., ETSI[5] or OASIS[6].

2.3 mGov4EU

The mobile Cross-Border Government Services for Europe (mGov4EU) began on 1 Jan 2021. Starting from the foundation of SDGR, mGov4EU provides new ways of cross-border service provision correlated and interlinked with eIDAS Regulation on cross-border identification and authentication. mGov4EU leverages for the first time both together, SDGR and eIDAS for mobile-device usage.

The project builds upon the existing eIDAS-Layer and combines it with user-centric mobile-based authentication, including a Single Sign-On (SSO) approach. At the same time, a privacy-preserving identity and consent management is established for the provision of cross-border application scenarios concerning E-Government processes and services. In addition, mGov4EU embraces the SDG-Layer, striving for a collaborative engagement with provisioning platforms concerning the delivery and re-use of digital services throughout Europe, while holding up the key elements of trust and accessibility. The therefore developed technical infrastructure will be piloted in three domains, i.e., electronic voting, smart mobility, and mobile signature.

3 Discussion

The before-mentioned development concerning SDGR, the DSM, as well as the two example initiatives (TOOP, mGov4EU) have clearly demonstrated that interoperability is key for a beneficial data exchange across borders. Interoperability has to be seen from different points of view. Within this section, we focus mainly on organisational, legal, and technical interoperability based on the outcomes of the ISA² Program of the EC. In addition, we also provide an outlook towards a key challenge, namely, the paradigm shifts of mobile-first approaches within the eID context.

3.1 eIDAS / eIDAS II – Organisational and Legal Issues

First, we are looking to the eIDAS regulation. The setup of the regulation was a big step forward on the way to create a common legal basis for the EU. But since the entry into force of the eIDAS in 2018, the implementation of digital identity is recognised as not harmonized across the MS. This is mainly caused by different interpretations of the regulation. Even Trust Services Providers, who are eIDAS compliant, have the procedures and requirements defined in different ways. The result is that the eIDAS

[5] European Telecommunications Standards Institute (ETSI)
[6] Organization for the Advancement of Structured Information Standards (OASIS)

certificates are not compatible across different MS. In order to change this fragmented state, there are mainly two options; a change of mindset and / or a change of technical implementation to accept all eIDAS qualified tools (e.g., certificates, signatures etc.)

Furthermore, as cross-border transactions and the digital economy continue to grow, and economic crimes and fraud become more sophisticated, the importance of accurately identifying and verifying counterparties - including business partners - is becoming more evident. Policies and procedures to prevent money-laundering and terrorist financing, as dictated by EU so-called Anti Money-Laundering (AML) Directives entails credit and financial institutions and other "obliged entities" to determine the true identity of a customer and the type of activity that is "normal and expected" (Know Your Customer).

3.2 Technical Interoperability Issues

The databases used by the different administrations in the MS are mostly designed for specific cases or services. The underlying structure of the register quite often are set up before generic rules to exchange eIDs like in the eIDAS regulation were established. The data schemes are strongly related to the provided services. This causes a gap of attributes that allows an automated exchange of and mapping of identities (identity matching issue).

Identification in Europe happens via eIDs notified under eIDAS. In this case, there is a record matching issue depending on MS infrastructure. While using notified eIDs under the eIDAS Regulation for the most part will allow data providers to match an identity with a record (evidence requested) using the attributes of the natural person provided by the eIDAS minimum data set, in some cases additional attributes are needed to ensure a match. This is based on a lack of interoperability and the credentials defined in the eID schemes of the MS (record matching issue).

The lack of a match with the regulated electronic identity circuits falls under the national sovereignty, and the consequent lack of a sound legal basis. The EC, the MS and associated countries have picked up this via the SDGR Coordination Group.

3.3 eID and Mobile Usage

Research has shown that user acceptance can lead to a better technological development, as well as value creation within the domain of e-government services, especially considering mobile government (m-government) [HCK13]. In this context, the combination of mobile aspects and approaches, e.g., as suggested by the mGov4EU project, can boost the acceptance and thus the usage of critical components such as eID. Tesap et al., conducted a literature review concerning factors for public acceptance of eID [TPD19]. The identified 11 core categories and their associated impact (positive, negative, bilateral, or neutral). For the sake of discussion in this paper, we focus on the categories which have been found to have the most positive influence on the acceptance of eID and combine them with mobile aspects in table 1.

Category	Description	Mobile Aspect

Ease of use	Convenience/usability /comfort when using eID technology	Provision of eID functionality without the necessity of an additional artefact, e.g., an eID card
Functionality	Availability of services to be used with eID	Full eID integration with mobile e-government apps
Awareness	Understanding/knowing how to use of the provided eID solution	Know-how and experience concerning mobile phone handling is transferred to eID solutions
Trust	Institution-based trust/characteristics trust concerning the provision of eID solutions	Trust in other widely used mobile applications (e.g., banking apps) can be leveraged for eID solutions
Control and Empowerment	Control over eIdentity/Identity and empowerment of citizens	Mobile eID solutions can provide this control and empowerment anytime and everywhere

Tab. 1: Positive influential factors for eID acceptance, complemented with mobile aspects

When studying the above side-by-side comparison, it becomes obvious that eID solutions profit the most from spill-over effects of positive experience of citizens in their daily use of mobile phones. The better the eID solutions are integrated in day-to-day business and activities around the life-situations of the citizens, the higher are the changes that these provided solutions are accepted; and this is the key to a true cross-border, pan European public service provision.

4 Conclusions

To solve the issues related to the described problems of identity matching mostly on the data provider side and record matching mainly on the data consumer side a further alignment of the schemes and attributes in use are necessary. It is important to find solutions that covers the needs on national and international level at the same time. Therefore, a European initiative is the most valuable approach. The recommendation is to pick up the outcomes of the ongoing discussions around the implementation of the SDGR in the Members States, associated countries and the European level and feed them into the update of the eIDAS regulation. The preparation of the amendment of the eIDAS regulation is a great opportunity from a legal and technical point of view. Ideally this should be aligned with the initiative of the EC to implement a secure European electronic identity. The combination of all these activities would allow a new level of harmonisation in the field of e-Identity in Europe that can initiate a bust in using the eID on a daily basis as this can be recognised already in some of the Members States, as described before.

As solution could be the introduction of state-of-the-art mobile technologies that are supported by the implementation of sound mobile government solutions and a transition of regular (paper based) governmental services into smart government services.

5 Acknowledgement

This work received funding in the context of the EU H2020 projects eCEPS and mGov4EU under grant agreements 959072 & 857622.

Bibliography

[K17] Krimmer, R. et al.: Exploring and Demonstrating the Once-Only Principle. In (Hinnant, C. C.; Ojo, A. Eds.): Proceedings of the 18th Annual International DGO. ACM, New York, NY, USA, 06072017; pp. 546–551.

[T20] Tepandi, J. et al.: Towards a Cross-Border Reference Architecture for the Once-Only Principle in Europe: An Enterprise Modelling Approach. In (Gordijn, J.; Guédria, W.; Proper, H. A. Eds.): 12th ifip working conference, poem 2019. SPRINGER NATURE, 2020; pp. 103 – 117.

[KS19] Krimmer, R.; Schmidt, C.: Chancen und Anforderungen des Single Digital Gateways. In Innovative Verwaltung, 2019, 41; pp. 10–14.

[LHP19] Lampoltshammer, T. J., John, K., Helger, P., & Piswanger, C. M. (2019). Connectathons-A Sustainable Path Towards Development in European Large-Scale Pilots. EGOV-CeDEM-ePart 2019, 207.

[HCK13] Hung, S. Y., Chang, C. M., & Kuo, S. R. (2013). User acceptance of mobile e-government services: An empirical study. GIQ, 30(1), 33-44.

[TPD19] Tsap, V.; Pappel, I.; Draheim, D.: Factors Affecting e-ID Public Acceptance: A Literature Review. In (Kő, A. et al. Eds.): Electronic Government and the Information Systems Perspective. Springer, Cham, 2019; pp. 176–188.

[EC16] EC: EU eGovernment Action Plan 2016–2020 - Accelerating the Digital Transformation of Government. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 2016, no. 179, pp. 1–11, 2016.

[EP17] European Parliament: Commissioner Bieńkowska and MEPs debate the merits of the single digital gateway, 2017.

[EC17] European Commission: The Single Digital Gateway. A proposal for easy, online navigation of the Single Market for EU citizens and businesses. https://www.europarl.europa.eu/cmsdata/129820/PPT%20single%20digital%20gateway.pdf, accessed 1 Mar 2021.