UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

Digital Identity and Trust: Response to the Open Public Consultation on the eIDAS Regulation.

Giannopoulou, A.

Publication date
2020

Document Version
Final published version

Link to publication

Citation for published version (APA):
Giannopoulou, A. (2020). *Digital Identity and Trust: Response to the Open Public Consultation on the eIDAS Regulation.*

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:23 Jan 2022

Feedback
with regard to the
Open Public Consultation
on the revision of the
rules on electronic identification and trust services
for electronic transactions
in the internal market,
the eIDAS Regulation

on behalf of

Blockchain and Society Policy Research Lab
Institute for information Law
University of Amsterdam

2 October 2020
Author: **Alexandra Giannopoulou**

The Lab has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme under grant agreement No 759681.

Table of contents

Decentralized identity development

Control over individual identity is substantial, if not synonymous, to the concept of self-determination, which is a precondition for a democratic society[1]. Identity is determined through external validation by state or third parties, and most importantly, it often hinges on them. Control over identity data and trusted identity management systems becomes fundamental.

In the last decades, power asymmetries between individual data subjects and the entities that produce, collect, and benefit from data have been flagrantly growing within a complex data ecosystem (Solove 2004) and thus, a considerable legal framework is being developed to address this in the European Union. Data operates and circulates in an environment surrounded by a multitude of -oft contradictory- interests between actors trying to simultaneously achieve different objectives (Daly 2016).

Data protection is the main battlefield over which individual control over data has been asserted. Historically, the EU Charter has given the right to protection of personal data a fundamental rights status, and has proclaimed it to be a freedom, devoid of the precondition of harm (González Fuster 2014). The essence of the right is rendered not simply defensive, but also proactive in its safeguard. In that regard, data subjects are empowered and can ensure that informational privacy, autonomy, and fundamental rights aspects are safeguarded. The creation of the European legal framework, governing the free flow and protection of personal data, aimed to create a trust relationship between all stakeholders involved in data processing, by the implementation of a data protection framework. The General Data Protection Regulation (GDPR) describes a network of enforcement measures, rights, obligations, and responsibilities involving data subjects, data controllers, processors, and supervisory authorities. The rationale behind this design, and the overall objective of the GDPR is to create **trustworthy processing of personal data**. This could be achieved through the accountability measures and responsibilities that the data controllers would have, but also through the individual rights empowering data subjects themselves.

However, **individual 'data empowerment', as described in the Charter and as designed within the GDPR, is becoming more challenging to ensure.** The use of appropriate technological tools becomes, thus, essential. In particular, privacy-enhancing technologies have been consistently evolving for many years. Significant progress has been made in encryption technologies, with privacy-enhancing technologies focusing on privacy-as-confidentiality. This means that the rationale of the development of various encryption methods was to prevent surveillance and control from diverse actors of the communicated information. Overall, the 'privacy-enhancing' vision is to design technological architectures that create a private, secure, and modular ecosystem at the centre of which sits an empowered individual (Giannopoulou 2020; Bodo 2020).

Empowerment of the individual over their data is intrinsically tied with control of one's identity. Creating the conditions for self-determination of the elements constituting one's identity, becomes a crucial part of data empowerment. Until recently, control of identity has come up under the guise of "unlawful use of identifying data from another person" (Koops & Leenes 2006). However, this aspect of control as preventing appropriation of identity data is mainly addressed through enforcement and legal processes. More broadly, the aspiration of self-determination of identity data transcends criminal enforcement processes and aims to place the individual in the centre of all decisions involving processing of data that can be linked to their identity. **In this**

[1] This is particularly highlighted in the recently announced European data strategy.

context, the trust framework described in the eIDAS Regulation is a fundamental enabler for digital identification and authentication.

Identity is a dynamic set of malleable data with significant value for an individual and for all actors that interact with them. Within this versatile field, taking control of one's personal digital identity is the objective of emerging techno-legal solutions (sector specific or broader). This objective is often described as **data sovereignty**, with sovereignty meaning to denote 'the receiving of a general recognition of exclusive domain and consequent possession of the capacity to establish rules of conduct within a particular field of action' (Manski & Manski 2018). **These techno-legal solutions share the hybrid objective of using a specific technological infrastructure to enable an identity that prioritizes security, privacy, and empowerment of individuals within its determining features. This infrastructure frequently includes a distributed ledger, and is for a large part relying on privacy enhancing technologies (PETs). Decentralized identity systems on distributed ledgers have been highlighted as 'particularly impactful'** (Verhulst & Young, 2019).

Policy interest in digital identity

The management of identity is subject to national regulation, as an expression of state sovereignty. However, on a European level, several legislative initiatives have been launched with a focus on digital identity services. The recently announced European digital strategy, through the communication document entitled 'Shaping Europe's Digital Future'[2], includes an explicit reference to the role of identity: '**A universally accepted public electronic identity (eID) is necessary for consumers to have access to their data and securely use the products and services they want without having to use unrelated platforms to do so and unnecessarily sharing personal data with them**'.

According to the Commission, the promotion and regulation of digital identity is essential in maintaining an '**open, democratic, and sustainable society**', which is one of the main objectives of this data strategy. In that regard, trusted and secure interactions are key. The establishment of these interactions can be done through ensuring appropriate, and most importantly, interoperable, identification and authentication frameworks.

The management of identity and identity-related data is reflected in many legislative initiatives that interact with each other, aiming to give citizens more control and protection over their data. For instance, the **General Data Protection Regulation** (GDPR)[3], the **Payment Services Directive 2** (PSD 2)[4], the **Anti-Money Laundering Directive** (AML5)[5] to name a few, all aim to regulate identity data and identification processes. The latest Commission Communication entitled 'Digital

[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Shaping Europe's digital future, Brussels, 19.2.2020 COM(2020) 67 final.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[4] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

[5] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

Finance Strategy for the EU[6] refers to the importance of a digital identity framework rather often. According to the strategy, '**by 2024, the EU should implement a sound legal framework enabling the use of interoperable digital identity solutions**', which would bring technological standardisation, interoperability, and broader security in customer/user identification and authentication by financial institutions. Thus, it becomes apparent that the 'unnecessary' over-sharing of personal and identity data with different platforms is a transdisciplinary concern for the European legislator.

The eIDAS is a necessary step towards that direction. It incorporates these values by promoting interoperability standards with the public sector. However, **it is essential to consider the standards, values, and trust frameworks that will have to be implemented by some dominant players in the private sector**. For example, projects related to identity development in financial institutions (especially after the PSD2 opening of financial data towards stimulating FinTech innovation), relies upon trust services that guarantee the integrity of the identification and authentication transmitted.

This document aims to shed light into some of the necessary steps that would render the evolution of identity management systems compliant with eIDAS rules. It aims to clarify points of ambiguity in the current interpretation of the Regulation, with a particular focus on decentralised identity technological systems, and their surrounding governance rules.

Decentralized identity and eIDAS standards

Among the core principles of eIDAS is technological neutrality. According to **Recital 27**, 'this Regulation should be technology-neutral. The legal effects it grants should be achievable by any technical means provided that the requirements of this Regulation are met'. Furthermore, **Recital 16** points out that assurance levels describing the degree of confidence in a technological identity implementation should be 'technology-neutral. It should be possible to achieve the necessary security requirements through different technologies'. Most importantly, **Article 12(3)** specifies that the interoperability framework shall remain technology neutral without discriminating 'between any specific national technical solutions for electronic identification within a Member State'.

With the simultaneous rapid advancement of European decentralized[7] identity frameworks, it is fundamental to ensure that eIDAS standards can be applied in order to support and provide the appropriate level of confidence to these systems. Namely, we wish to point out two issues as examples of the particularities of decentralized identity systems within the current regulatory framework.

Firstly, and without entering into the fundamental components of decentralized identity technological architectures, the **processes that ensure secure authentication and identification, as well as storage of the individual elements constituting one's identity would benefit from standardisation.** For instance, the list of attributes included in the eIDAS **minimum data sets** are defined in the Annex of the interoperability framework implementing act. These minimum data sets would need to be inclusive of the decentralized identity prerequisites,

[6] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Digital Finance Strategy for the EU, Brussels, 24.9.2020 COM(2020) 591 final

[7] When assessing decentralization, it is essential to distinguish which aspects of the architecture are, in reality, decentralized (Bodo & Giannopoulou 2019).

according to established standards, such as those set out by the World Wide Web Consortium (W3C). In this way, the transmission of certificates, credentials, or parts of an individual identity, would be fulfilled only with the exposure of minimal data in a secure way.

Regulation of the storage of these identity datasets in technological 'wallets' would need to be harmonised on a European level, in order to ensure the security of citizen data. This regulation could fall under the 'Trust service providers' framework, with appropriate delimitation of the minimum criteria that would need to be fulfilled for these operations.

Secondly, the decentralized architecture of any identity system necessitates the intervention of a **framework of nodes**. Although not essential in producing the identity itself, they ensure the anchoring of the information. Thus, these nodes, distributed among Member States, are fundamental in ensuring the integrity of the information transmitted. In that sense, they could be subject to eIDAS norm setting so that liability and standardisation obligations would be a priori formalised for the whole network with appropriate agreements towards maintaining the integrity of the services provided.

eIDAS and GDPR compliance for decentralized identity

The eIDAS Regulation necessarily interacts and aligns itself with data protection rules. Thus, it would need to be in compliance with the GDPR framework of rules and techno-legal standards. Trusted service providers are especially required to comply with data protection obligations, and to report breaches of security or loss of integrity of the data they hold (**Articles 17-19 eIDAS**).

Taking into consideration that all identity data would be qualified as personal data (even if pseudonymised), the technological standards that would apply to the secure transmission and storage of private keys, verifiable credentials, and attestations, will be also subject to the data protection by design and by default rules (**Article 25 GDPR**).

For instance, private key management would need to comply with the GDPR since private keys are considered to be personal data[8]. In that regard, a number of 'privacy enhancing technologies' could be examined from a policy perspective, in order to permit the standardisation of practices. This standardisation appears to be essential in ensuring the empowerment of data subjects in light of the European data sovereignty strategy. Namely, data minimisation is a fundamental principle of the GDPR. The integration of this principle in the technological standard of identification would permit the disclosure of essential only information and enhance the trustworthiness of the overall framework. It would also elevate the responsibility of trusted data service providers, in simultaneously providing data security and data protection through accepted 'minimum technical requirements, standards and procedures' (**Recital 16 eIDAS**).

Similarly, data subjects' rights would need to be taken into consideration. For instance, the fundamental right to data portability stands at the centre of any decentralized identity solution. The creation of interoperable identity frameworks through the eIDAS requires similar levels of attention towards this right.

[8] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014, 0829/14/EN WP216

Finally, the coexistence of accountable actors according to the GDPR with the trusted service providers according to the eIDAS, implies ensuring that no conflicts will arise between the two - oft coinciding- roles and responsibilities.

Bibliography

Bodo B (2020), Mediated Trust – A Theoretical Framework to Address the Trustworthiness of Technological Trust Mediators, New Media and Society, doi:10.1177/1461444820939922

Bodó B & Giannopoulou A (2019), The Logics of Technology Decentralization: the Case of Distributed Ledger Technologies. In M. Ragnedda, & G. Destefanis (Eds.), Blockchain and Web 3.0: Social, Economic, and Technological Challenges Routledge

Giannopoulou A (2020), Putting privacy by design on the blockchain, forthcoming.

González Fuster G (2014), *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer.

Koops B-J & Leenes R (2006), ID Theft, ID Fraud and/or ID-Related Crime - Definitions Matter, Datenschutz und Datensicherheit, 30(9):553-556

Manski S & Manski B (2018), 'No Gods, No Masters, No Coders? The Future of Sovereignty in a Blockchain World, Law Critique 29:151–162

Verhulst S G & Young A, (2018). Field Report - On the Emergent Use of Distributed Ledger Technologies for Identity Management. *GovTech report*. Available online at: https://blockchan.ge/blockchange-fieldreport.pdf (accessed August 7, 2019).

Solove D (2004), *The Digital Person: Technology and Privacy in the Information Age,* New York University Press

Wagner K, Némethi B, Renieris E, Lang P, Brunet E, & Holst, E. (2018). *'Self-sovereign identity' Position Paper*. Blockchain Bundesverband. Available online at: https://www.bundesblock.de/wp-content/uploads/2018/10/ssi-paper.pdf (accessed August 7, 2019).

Wang F & De Filippi P (2020), Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion, Frontiers in Blockchain,