EUROPEAN
COMMISSION

Brussels, 3.6.2021
COM(2021) 290 final

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)

{SEC(2021) 229 final} - {SWD(2021) 130 final}

1. INTRODUCTION

This report outlines the results of the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market ('the eIDAS Regulation')[1]. Article 49 of the Regulation requires the Commission to review the application of this Regulation and to evaluate in particular whether it is appropriate to modify its scope or its specific provisions taking into account the experience gained in its application, as well as technological, market and legal developments[2], and where appropriate, the report should be accompanied by legislative proposals.

The accompanying staff working document contains more detailed evidence and analysis supporting these findings.

1.1. The eIDAS framework

With the eIDAS Regulation adopted in 2014 the EU broke new ground by introducing a first cross-border framework for trusted digital identities and trust services, now recognised and respected globally. The aim of the eIDAS regulation was to allow all EU citizens access to public services across the EU using means of electronic identification (eID) issued in their home country. It sought to enhance trust in electronic transactions in the internal market by providing a common foundation for secure and seamless electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the EU. It repealed Directive 1999/93/EC on a Community framework for electronic signatures that essentially covered electronic signatures only.

As implied by the legal base of the Regulation, Article 114 TFEU, it intended to remove existing barriers to the functioning of the internal market by promoting approximation of Member States legislation, in particular mutual recognition and acceptance of eID, authentication, signatures and related trust services across borders when needed for the access and completion of electronic procedures or transactions.

Before the Regulation entered into force there was no comprehensive EU cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions that encompassed electronic identification, authentication and trust services. The Commission proposal (COM(2012) 238 final) of 4 June 2012 accompanied by the Impact Assessment (SWD(2012) 135 final) identified the following four general objectives:

- ensuring the development of a digital single market;
- promoting the development of key cross-border public services;

---

[1] 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, *OJ L 257*, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN.

[2] "The Commission shall review the application of this Regulation and shall report to the European Parliament and to the Council no later than 1 July 2020. The Commission shall evaluate in particular whether it is appropriate to modify the scope of this Regulation or its specific provisions, including Article 6, point (f) of Article 7 and Articles 34, 43, 44 and 45, taking into account the experience gained in the application of this Regulation, as well as technological, market and legal developments."

- stimulating and strengthening competition in the single market;
- enhancing user-friendliness (citizens and businesses).

Despite the fact that the Regulation is delivering on many of its goals and has become a fundamental element to facilitate the single market in a number of sectors (e.g. for financial services and enabling access and reuse of data in administrative procedures), it carries a number of limitations: lack of obligation to notify national eID schemes, limited attributes (elements of personal information) that can be reliably disclosed to third parties, the act's focus on the public sector and the absence of clear incentives for private parties to use national eIDs. In addition, the European electronic identity ecosystem is distributed across different national regulatory environments, levels of digital governance, culture, and varying levels of trust in public institutions.

1.2. Context

Provision of digital identity is undergoing fundamental changes. Entities such as banks, providers of electronic communications services or utility companies, some of which are required by law to collect identity attributes, are leveraging their procedures to act as verified identity providers. Internet intermediaries, including major social media platforms and internet browsers[3], act as de facto digital identity gatekeepers and offer BYOI (bring your own identity) solutions that allow their users to authenticate on third-party websites and services by using their user profiles. This convenience comes at the cost of loss of control over disclosed personal data while these eID means are disconnected from a verified physical identity, which makes fraud and cybersecurity threats more difficult to mitigate. A large majority of EU citizens would like to have access to a secure digital identity that they could use to access online services.[4] Finally, although there are many different views on the future of digital identity, the key role of the national governments in the development of any far-reaching digital ID eco-system needs to be duly considered.

Users today expect seamless online journeys, mobile applications and single-sign-on solutions that can be used for online services in the public and private sector, covering all use cases for identification ranging from pseudonymous log-on to an online platform to secure identification for e-health or e-banking. Secure online identification and the exchange of attribute credentials is becoming more important as the number of identity-sensitive and personalised services increases. The ability to identify digitally will become an important factor of social inclusion and the provision of digital identity a strategic asset.

In her State of the Union speech on 16 September 2020, the President of the European Commission announced the Commission's ambition to deliver a secure and trusted digital identity to all EU citizens: *"We want a set of rules that puts people at the centre. (...) This includes control over our personal data, which we still have far too rarely today. Every time an app or website asks us to create a new digital identity or to easily log on via a big platform, we have no idea what happens to our data in reality. That is why the Commission will soon propose a secure European e-identity. One that we trust and that any citizen can use anywhere in Europe to do anything from paying your taxes to renting a bicycle. A technology where we can control ourselves what data and how data is used".*

---

[3] For example, Facebook or Google users can use their accounts to log into Booking.com or connect to EU Login:https://developers.facebook.com/docs/facebook-login/overview https://developers.google.com/identity/

[4] Eurobarometer 503, Attitudes towards the impact of digitalisation on daily lives, December 2019, see : https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2228

The European Council seconded the Commission's ambition and, in the Council Conclusions of 1-2 October 2020, called on the Commission to come forward with a proposal for a European digital identity framework initiative by mid-2021:

The European Council Conclusions call for *"The development of an EU-wide framework for secure public electronic identification (eID), including interoperable digital signatures, to provide people with control over their online identity and data as well as to enable access to public, private and cross-border digital services". The Council invites the Commission to come forward with a proposal for a European digital identity framework initiative by mid-2021."*

Electronic identification allows citizens and businesses to prove who they are when accessing services online. Trust services, such as electronic signatures, make online transactions more secure, convenient and efficient. The eIDAS Regulation is the only cross-border framework for trusted eID of natural and legal persons, and trust services. eIDAS enables the cross-border recognition of government eIDs for access to public services, under the condition the eID has been notified under eIDAS. eIDAS also establishes an EU market for trust services recognised across borders with the same legal status as their traditional equivalent paper-based processes.

2. MAIN FINDINGS OF THE EVALUATION

The main findings of the evaluation, according to the evaluation criteria, can be summarised under the following headings.

2.1. Effectiveness

The provisions on electronic identity have led to the creation of the eIDAS network, which seeks to enable holders of a notified eID scheme to access online public services across borders. The interoperability of only a limited number of eID schemes has been achieved at EU level.[5] The eIDAS Regulation has successfully established legal certainty on liability, burden of proof, legal effect and international aspects of trust services, but some issues remain. Availability and take-up of trust services in the EU have increased since the introduction of the eIDAS Regulation, however, there are differences among Member States and among different trust services

Despite some achievements, the regulation has not achieved its potential in terms of effectiveness. Only a limited amount of eIDs have been notified, limiting the coverage of EU citizens with a notified eID scheme (59% of the population). The acceptance of notified eIDs is limited, as not all eIDAS nodes are up and running, a limited number of public services offer the eIDAS notification or are connected to the infrastructure, and technical errors prevent users from effectively authenticating.

On the trust services side, the objective of the Regulation to remain technology neutral has led to a diversity of interpretation of the requirements between Member States also due to the lack of adoption of additional implementing acts. It cannot be concluded that a level playing field has been fully achieved at EU level. However, the eIDAS Regulation has set-up a strong

[5] Since the entering into force of the eID part of the Regulation in September 2017, 14 Member States have notified at least one eID scheme and four Member States have already notified multiple schemes. In total, 19 eID schemes have been notified so far: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+overview

framework that can be complemented with the necessary standards and requirements to reduce the current fragmentation of the market and divergences of interpretation by supervisory bodies and conformity assessment bodies and strengthened cooperation between the supervisory bodies.

2.2. Efficiency

The baseline assessment indicates that quantifiable costs have been so far higher than benefits. In the area of eID this is the result of a low uptake where benefits did not materialise.

The key stakeholder groups for which the eID part of the eIDAS Regulation has generated costs and benefits are national authorities, eIDAS node operators, eID providers and service providers. For the trust services the key stakeholder groups, which faced the main costs and benefits are accreditation, conformity assessment, and supervisory bodies and qualified and non-qualified trust service providers.

For individual stakeholders, a considerable part are expected benefits (discounted as future benefits) and therefore hardly quantifiable. Recurring costs for governance in the area of trust services are limited and mainly linked to ensuring compliance. For individual stakeholders, a considerable part of the benefits is only hypothetical at this stage (discounted as future benefits) and hardly quantifiable. Trust Service Providers register benefits in the form of revenue due to the provision of trust services in other EU countries and an extension of market base.

2.3. Relevance

The eID ecosystem has profoundly changed since the introduction of the eIDAS Regulation with an increasing footprint of private identity providers. Taking into account the increase in digital transactions, all EU citizens should have access to a secure and interoperable digital identity, which is not the case today. The objectives of the eIDAS legal framework remain relevant to address the initially identified issues, notably the need to ensure the reduction of market fragmentation by ensuring cross-border and cross sector interoperability of trust services via the adoption of common standards. The current scope and focus of the eIDAS Regulation on eID schemes notified by EU Member States and on enabling access to online public services seems too limited.

Some key barriers to uptake by users and private sector service providers have prevented the regulatory framework to reach its full potential. Despite introducing references to eIDAS solutions in a number of sectoral EU legislation, the eIDAS Regulation has not yet replied to the needs of specific sectors (e.g. education, banking, travel, aviation). One of the limitation factors of the current framework with respect to these sectoral needs is the lack of specific attributes by domains.

The key tension is the ability of eIDAS to stay in line with the latest developments of technology in the domain of trust services. The extension of the trust services list, notably through the introduction of a trust service for eArchiving, a trust service supporting portable identity credentials and a trust service for electronic ledgers would address a number of use cases and provide citizens and businesses with the possibility to prove digitally who they are or to prove their attributes/characteristics, without needing physical documents.

2.4. Coherence

The evaluation shows that the eID part of the Regulation is supported by a generally coherent system for mutual recognition of eIDs based on notification and peer review. The trust services framework provides for a coherent supervisory system for trust services. However, certain issues have been identified impacting the internal coherence of the Regulation.

For eIDs, the notification and peer review system set out in the eIDAS framework intended to deliver a common understanding of the level of assurance (LoA) provided by an eID scheme but assessment of practical implementation shows that this is not always the case. Although it encourages flexibility and technological neutrality, a common understanding of what constitutes a substantial and high LoA is still missing. The focus on the public services contrasts with the possibility for the user to limit the transmitted data to the minimum necessary for the authentication to a specific service as the minimum data set is always transmitted to allow the identification of a person. The implementation of the current eIDAS system does not allow the user to facilitate the enforcement of the GDPR principles of data minimisation and privacy by default by controlling which data to share and with whom.

The rules on the assessment of the trust service providers against the functional requirements of the Regulation to obtain the qualified status shows some weaknesses as the role of conformity assessment bodies lacks sufficient detail on their obligations, liability or level of competence. Some provisions leave it up to the Member States to recognise certain identification methods (such as biometric verification) at national level, which hamper regulatory level playing field and creates uncertainty.

2.5. EU added value

The eIDAS Regulation created incentives for Member States to deploy national eID solutions but the added value of the eID framework has shown strong limitations due to its low coverage, uptake and usage. For trust services the Regulation has provided a common legal framework for their use, reducing market fragmentation and increasing their uptake. With the help of trust services, public administrations are able to modernise and digitalise services and issue evidence digitally thereby reducing administrative burden.

On the eID part the originally identified needs for the adoption of the Regulation remain still relevant and repealing the Regulation would lead to fragmentation and negative consequences to other legislative areas that rely on eIDAS. Some adaptations to the regulatory framework could increase its EU added value (such as facilitating the use of trusted government eIDs by the private sector and defining a framework for the exchange of specific attributes and credentials provided by the public and private sector). For trust services, some barriers resulting from national interpretation and/or conflicting national law still remain and limit the uptake of trust services

3. REVISION OF THE EIDAS FRAMEWORK

The eIDAS Regulation is a fundamental element to facilitate the single market in a number of sectors (e.g. in the banking sector to supply some of the required identity data to facilitate compliance with Anti-Money Laundering rules[6], the Payment Services Directive (PSD2)[7]

[6] 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

builds on eIDAS trust services, such as eSeals and Qualified Website Authentication Certificates (QWACs) to identify the authenticity of websites by third-party payment providers, eIDAS based eIDs are a requirement for the exchange of administrative certificates across borders, and is essential for the successful implementation and functioning of the Once-only principle (OOP) as of 2023[8]). The trust services framework is recognised internationally, and forms the basis for a draft provision[9], expected to become a UN model law on trust services in electronic commerce in 2021, as well as for the ongoing electronic trade negotiations within the WTO[10].

However, a lot has changed since the adoption of eIDAS in 2014. The framework is based on national eID systems following diverse standards and focuses on a relatively small segment of the electronic identifications needs of citizens and businesses: secure cross-border access to public services. The services targeted mainly concern the 3% of EU's population[11] residing in a Member State different from the one they were born in.

Since then, digitalisation of all functions of society has increased dramatically. Not least has the COVID-19 pandemic had a very strong effect on the speed of digitalisation. As a result, the provision of both public and private services is increasingly becoming digital. Citizens and businesses' expectations are to achieve high security and convenience for any online activity such as submitting tax declarations, enrolling in a foreign university, remotely opening a bank account or asking for a loan, renting a car, setting up a business in another Member State, authenticating for internet payments, bidding to an online call for tender, and more.

As a consequence, the demand for means to identify and authenticate online, as well as to digitally exchange information related identity, attributes or qualifications securely and with a high level of data protection, has increased radically[12]. This has triggered a paradigm shift, moving towards advanced and convenient solutions that are able to integrate different verifiable data and certificates of the user. Today, this demand cannot be fulfilled by the eID means and trust services as regulated by eIDAS, given its current limitations. As regards identification or authentication means, developed by the private sector outside the eIDAS framework they only partly answer to this challenge. While they offer user-friendly third-party authentication services (e.g. using a Facebook or Google account to log in to different services), they are common to access unregulated private online services that do not require a high level of security. They cannot offer the same level of legal certainty, data protection and privacy, mainly because they are self-asserted and cannot offer a link to trusted and secure government eID.

---

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

7 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

8 The Once Only Principle will, from 2023, allow public administrations to reuse and share data and documents that people have already supplied in a transparent and secure way. (Article 14 of 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. OJ L 295 of 21.11.2018).

9 https://undocs.org/en/A/CN.9/WG.IV/WP.167

10 See e.g. Session documents for UNCITRAL Working Group IV / Electronic Commerce, Session 6-9 April 2021: https://uncitral.un.org/en/working_groups/4/electronic_commerce

11. https://ec.europa.eu/eurostat/statistics-explained/index.php/EU_citizens_living_in_another_Member_State_-_statistical_overview

12 For instance, in Italy the number of users of SPID (launched in 2016) at the end of 2019 was ~5 million. Today, the active users are more than 18 million active (see https://avanzamentodigitale.italia.it/it/progetto/spid) with a steadily increase of ~1 million users per month. The use of SPID went from ~55 million for the entire year 2019 to ~32,4 in the sole month of February 2021

In February 2020, the Commission committed itself in its Strategy on Shaping Europe's Digital Future[13] to revise the eIDAS Regulation aiming to improve its effectiveness, extend its application to the private sector and promote trusted digital identities for all EU citizens and businesses. The urgency of this revision became clear with the outbreak of the COVID-19 pandemic. The disruptions to offline public and private services, and the sudden need for accessing and using all types of public and private services online, revealed the limitations of eIDAS in delivering the expected benefits to citizens, businesses and governments six years from its adoption. A revised and strengthened eIDAS Regulation would be able to answer to new market and societal demands by addressing the needs for trusted government eIDs linked solutions, but also for attributes and credentials provided by the public and private sector, all being fully managed by the user and recognised across the EU to access both public and private services. This would support a large number of existing or proposed regulatory frameworks strengthening the EU's Single Market.

4. CONCLUSIONS

Overall, the eIDAS Regulation has contributed to the further development of the Single Market. It has provided the foundations for the development of an identity and trust services market in the EU, supporting the ever-increasing need for secure digital transactions. However, in a future-looking perspective, which has evolved as regards objectives and user-expectations, the eIDAS Regulation needs to be improved in terms of effectiveness, efficiency, coherence and relevance to deliver on new policy objectives, user expectations and market demand also taking into account recent developments in digitalisation.

What is emerging in the market is a new environment where the focus has shifted from the provision and use or rigid digital identities to the provision and reliance on specific attributes related to those identities. There is an increased demand for electronic identity solutions that can deliver these capabilities providing efficiency gains and a high level of trust across the EU to services, both in the private and the public sector, relying on the need to identify and authenticate users with a high level of assurance.

The current eIDAS Regulation cannot address these new market demands given its inherent limitations to the public sector, the complexity for online private providers to connect to the system, its insufficient availability in all Member States and its lack of flexibility to support a variety of cases.

[13] European Commission. (2020). Strategy on Shaping Europe's Digital Future.