yubico

Feedback on the eIDAS inception impact assessment

Yubico's response to the EU Commission

 © 2020 Yubico. All rights reserved.

yubico

Contents

 © 2020 Yubico. All rights reserved.

yubico

Executive summary

Yubico's feedback to the eIDAS inception impact assessment document is summarized below.

As regards to Option 1, the reinforced baseline scenario, Yubico recommends the following improvements of the eIDAS EU regulation 910/2014 [5] with respect to eID schemes:

- The eIDAS regulation should specify well-defined rules for remote identity proofing
- The eIDAS regulation should be harmonized with the eID scheme requirements in the EU Cybersecurity Act, EU regulation 2019/881 [8]
- The Commission Implementing Regulation EU 2015/1501 [6] should require credential phishing resistance at Level of Assurance (LoA) High
- A framework for re-using pre-approved eID products could simplify the approval and notification processes of eID schemes
- Backup eID schemes with simplified processes for distribution and remote identity proofing could be allowed during emergency situations such as pandemics; such eID schemes may therefore go beyond traditional X.509 PKI smart cards
- LoA High should be mandatory for secure access to QTSPs with remote signing services in order to cater for sole control of remote creation of Qualified Electronic Signatures

When it comes to Option 2, the extended scope of eID regulation under eIDAS to the private sector, Yubico has the following comments:

- In general, it would be beneficial to extend the scope of eID regulation under eIDAS to the private sector; this would increase the use of eID schemes across the EU
- Existing large scale identity providers, such as technology companies, identity providers, banks and telecom providers with billions of users, could get their high-end authentication solutions notified as eID schemes
- The current eID approval process, which is based on national agencies' approvals, would have to be adopted for private identity providers, which may require new or complementary procedures in addition to the national approval procedures
- The architecture of national eIDAS-Nodes may have to be adjusted for private identity providers; in particular OpenID Connect [11] may be allowed as an alternative to SAML v2 for eIDAS-Nodes
- If banks in the EU would create approved eID schemes, they can be aligned with the PSD2 EU directive 2015/2366 [10] for meeting the requirements on Strong Customer Authentication and Dynamic Linking for authentication of financial transactions

Finally, with respect to the European Digital Identity scheme (EUid) in Option 3, Yubico would like to make the following comments:

- A European Digital Identity scheme (EUid) is not preferred in our view
- There are existing systems in various EU member states that may not be compatible with an EUid
- A pan-European EUid may be viewed as too regulated in various EU member states

 © 2020 Yubico. All rights reserved.

- Technical innovations, in particular in the private sector, could be suppressed or mitigated by an EUid
- Local support can be problematic with an EUid, with respect to physical identification, helpdesk support in local languages, and distribution of eID tokens
- Instead of an EUid, federated solutions could be considered instead; such federations will allow for better international interoperability, higher scalability, and be based on modern technology

Introduction

Background

The EU Commission has committed to revise the eIDAS Regulation [2] to improve its effectiveness, extend its application to the private sector and promote trusted digital identities for all Europeans.

The baseline is that the eIDAS regulation should remain unchanged. In order to improve the regulation further, the EU Commission has proposed three new options (that may be combined) for the revised eIDAS regulation:

- **Option 1** (reinforced baseline scenario) would revise and complement the existing eIDAS framework as necessary to improve coherence, consistency and interoperability.

- **Option 2** consists of a more ambitious legislative intervention and would extend the scope of eID regulation under eIDAS to the private sector, notably introducing new trust services for identification, authentication and for the provision of attributes, credentials and attestations and allowing the provision of identification for devices.

- **Option 3** would introduce a European Digital Identity scheme (EUid) complementary with eIDAS for citizens to access online public and private services, when identification is necessary.

Scope of this document

The scope of this document is Yubico's feedback to the EU Commission's inception impact assessment [9] regarding the revision of the eIDAS regulation [5]. In particular, the three different options have been commented on.

Audience

This document is a public document. The intended audience is the responsible DG CNECT H4 team and the eIDAS legislators in the EU Commission.

 © 2020 Yubico. All rights reserved.

About Yubico

Yubico has in the capacity of a privately held company submitted this feedback to the eIDAS inception impact assessment. This section gives an introduction to Yubico as a company.

Yubico is an IT-security company that sets new global standards for simple and secure access to computers, mobile devices, servers, and internet accounts. The company's core invention, the YubiKey, delivers strong hardware protection, across any number of IT systems and online services. The YubiHSM, Yubico's hardware security module, protects sensitive data stored in servers.

Yubico is a leading contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor open authentication standards, and the company's technology is deployed by nine of the top ten internet brands and by millions of users in 160 countries.

Founded in 2007, Yubico is privately held, with offices in Sweden, UK, Germany, USA, Australia, and Singapore. For more information see www.yubico.com.

Revision history

Revision	Author	Description	Date
1.0	Sebastian Elfors	First draft	2020-08-11
1.1	Sebastian Elfors	Updated based on review by John Bradley, Jerrod Chong, John Fontana, David Treece and Luke Walker	2020-08-13
1.2	Sebastian Elfors	Final version	2020-08-17

Comments on Option 1

General

Yubico proposes that the eIDAS regulation is improved as follows with respect to Option 1, which is the reinforced baseline scenario.

Allow for remote identity proofing

The eIDAS regulation, implementing acts and technical ETSI/CEN standards should be clarified and improved to allow for remote identification of individuals and organizations across the EU. Such remote identification systems should in the best case scenario cater for identification according to

 © 2020 Yubico. All rights reserved.

LoA High regarding eID schemes, and for QTSP certification authorities to issue Qualified Certificates.

At the moment, there are specific EU member states that may grant selected QTSPs the possibility to identify individuals remotely, but this should be harmonized for the rest of the EU in the eIDAS regulation.

It is also important that a strong binding is established between the issued eID and the individual during a remote identification process.

Remote identification of individuals has also proven to be relevant and useful during the COVID-19 epidemic. Furthermore, travelling costs and carbon dioxide emissions will be reduced if the individuals can be identified remotely instead of travelling to physical identification meetings.

The potential eIDAS legislation for remote identification should also be streamlined with ETSI TC ESI Specialist Task Force 588 on Identity Proofing, which has two deliverables:

- ETSI TR 119 460 Electronic Signature and Infrastructures (ESI); Survey of technologies and regulatory requirements for identity proofing for trust service subjects, due December 2020.

- ETSI TS 119 461 Electronic Signature and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects, due July 2021.

Harmonize eIDAS with the EU Cybersecurity Act

The EU Cybersecurity Act, regulation (EU) 2019/881 [8], defines requirements and processes for Information and Communications Technology (ICT) products and services that are used for eID schemes according to LoA Low, Substantial and High. The revised eIDAS regulation should be harmonized with the EU Cybersecurity Act.

Require credential phishing resistance at LoA High

The Commission Implementing Regulation EU 2015/1501 [6] on the interoperability framework should require credential phishing resistance at LoA High; solutions unable to provide that protection should be relegated to LoA Substantial or Low.

Framework for pre-approved eID products

If a product has been approved for use with an eID scheme in one EU member state, it would be beneficial with an eIDAS framework that could allow for the same product to be re-approved for other eID schemes. That could simplify the approval processes for eID schemes, which in turn could increase the rollout pace and adoption of eID schemes in the EU.

 © 2020 Yubico. All rights reserved.

Backup eID schemes during emergency situations

During emergency situations, such as pandemics, the eIDAS regulation may allow for backup eID schemes to be used as temporary alternatives to the default eID schemes. For example, in the USA during the COVID-19 pandemic, the White House Office of Management and Budget (OMB) released a directive that allows for alternative security solutions that are more appropriate for remote identification and authentication during the lockdown.

Hence, it is important that backup eID schemes allow for remote identification proofing and for an effective distribution model of eID devices. The temporary eID devices should be targeting an efficient deployment of a solution for electronic identification, and may not be equipped with visual photos and biometric information.

Require LoA High for access to QTSP

The Commission Implementing Decision (EU) 2016/650 [7] does not refer to any standards for signing devices operated by a trust service provider in a secure environment that could meet the requirements in the eIDAS Regulation (EU) 910/2014 Annex II [5] for qualified signature or seal creation devices.

Now, there are three CEN standards that define how to deploy a remote QSCD in conjunction with SAM-modules at a QTSP for remote creation of qualified signatures:

- CEN EN 419 221-5, Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services [1]
- CEN EN 419 241-1, Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements [2]
- CEN EN 419 241-2, Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing [3]

The revised Commission Implementing Decision (EU) 2016/650 should refer to these CEN-standards in order to provide solutions for creating remote qualified signatures under sole control.

Furthermore, ENISA has published a report that describes how the EU Commission Implementing Decision 2016/650 [7] may be updated to reference the CEN standards above to regulate the security and operations of a QSCD at a QTSP with the purpose of creating remote qualified electronic signatures.

This feedback has previously been reported by Yubico to the EU Commission as part of the eIDAS public consultation in October 2019.

 © 2020 Yubico. All rights reserved.

Comments on Option 2

General

Yubico promotes the initiative to extend the scope of eID regulation under eIDAS to the private sector, notably introducing new trust services for identification, authentication and for the provision of attributes, credentials and attestations and allowing the provision of identification for devices.

By allowing private eID schemes, large-scale identity providers, could certify their eID schemes to be used by EU citizens and organizations. This would open up for billions of citizens to use their existing credentials, certificates and electronic identities as approved eID schemes according to eIDAS.

Potential private identity providers

Private companies that could be potential candidates for identity providers to operate eIDAS-compliant eID schemes are for example: multinational technology companies (such as Microsoft, Google, Facebook and Amazon), identity providers (such as OKTA, PING and Duo), financial institutes, and telecom operators.

If such private companies were to create eIDAS-compliant eID schemes, the identification and authentication requirements should preferably meet the LoA according to High in order for the eID schemes to be fully notified on the EU level. If needed, separate tenants with specific identification and authentication solutions may be deployed to increase the security level as required to meet LoA High.

The private companies may take the legal responsibilities and liabilities for the eID schemes, equivalent to the supervising agencies in the EU.

Adopt the eID approval process for private IdP:s

If private identity providers will be allowed to get their eID schemes notified by the EU, a different approval process will be needed than the existing procedure with national eID schemes, which can be notified on the EU level. Several private identity providers may however be operated independently of the EU member states, so an agency such as ENISA on EU level may be needed for approving private companies eID schemes. (In some cases, the private companies may still get their eID schemes approved by the national agencies.)

Adopt the architecture of eIDAS-Nodes for private IdP:s

The concept of nationally operated eIDAS-Nodes may have to be revised if private identity providers would get their eID schemes approved. Either the private identity providers may connect to the national eIDAS-Nodes, or the identity providers may operate their own eIDAS-Nodes. The

 © 2020 Yubico. All rights reserved.

latter alternative will be easier to deploy and maintain for private identity providers, since large scale operators such as Microsoft, Google and Facebook already have federated Web-SSO protocol such as OpenID Connect [11] deployed and distributed. See the next section for more information on federated solutions based on OpenID Connect.

Allow OpenID Connect for private IdP:s

The Commission Implementing Regulation EU 2015/1501 [6] on the interoperability framework refers to technical specifications with SAML v2 as the federation protocol used for interaction between the eIDAS-Nodes. The scope could be broadened to include OpenID Connect [11], since that is a modernized version of federation protocols, which is deployed at several private and governmental systems. In particular, the European national governmental systems FranceConnect, CZ.NIC MojeID, and GOV.UK Verify already rely upon OpenID Connect.

OpenID Connect solutions can also be deployed and used independently of eIDAS-Nodes, which could allow for a more scalable federated system.

Alignment with PSD2

If banks in the EU would set up privately approved eID schemes, those authentication solutions could be aligned with the Payment Services (PSD2) Directive (EU) 2015/2366 [10], in order to meet the requirements on Strong Customer Authentication (SCA) and Dynamic Linking to authenticate a financial transaction.

Comments on Option 3

General

Option 3, which would introduce a European Digital Identity scheme (EUid), is not preferred in our view. Instead of an EUid, federated solutions could be considered instead; such federations will allow for better international interoperability, higher scalability, and be based on modern technology. The arguments for this standpoint are elaborated in the sub-sections below.

Existing systems in various EU member states

Several EU member states have already designed, approved and implemented national eID schemes that have been approved by the relevant agency and been notified on EU level. The national eID schemes are to a large extent designed for the member states' identity providers and governmental portals. In certain cases, the eID schemes are based on legacy authentication solutions that have been in production for two decades. The technology, eID devices and protocols differ from member state to member state. Replacing those authentication systems with a pan-European EUid will be a very costly process for several EU member states.

 © 2020 Yubico. All rights reserved.

Regulatory challenges

A pan-European EUid may be viewed as too regulated in various EU member states, which could result in objections from member states that prefer local solutions.

Mitigation of technical innovations

Technical innovations, in particular in the private sector, could be mitigated by an EUid. The competition on the authentication market in the EU may also be suppressed by an EUid. Therefore, it is important to allow for private companies to invent, implement and deploy identity and authentication solutions across the EU market.

Local support needed

Local support will always be needed for authentication solutions. This is relevant for the identification process (which in many cases requires a physical meeting), helpdesk staff that speak the local language, distribution of eID tokens, etc.

Rely upon federated solutions

As an alternative to meet the objectives in Option 3, federated authentication solutions based on modern technology such as OpenID Connect [11] could be considered. Such federated solutions could provide scalable and standardized ways for cross-border authentication and Web-SSO. Furthermore, such EU federated solutions could be made interoperable with international authentication infrastructures in countries such as Australia and Canada.

Glossary of terms

Abbreviations

CEN	Committee European Normalization
EBSI	European Blockchain Service Infrastructure
eID	electronic IDentity
eIDAS	electronic IDentification Authentication and trust Services
EN	European Norm
ENISA	European Union Agency for Cybersecurity
ESI	Electronic Signature and Infrastructures
ESSIF	European Self-sovereign Identity Framework
ETSI	European Telecommunications Standards Institute
EU	European Union
EUid	European Digital Identity
FIDO	Fast Identity Online
ICT	Information and Communications Technology

 © 2020 Yubico. All rights reserved.

IdP	Identity Provider
LoA	Level of Assurance
OMB	Office of Management and Budget
PSD2	Payment Services Directive
QSCD	Qualified Signature Creation Device
QTSP	Qualified Trust Service Provider
SAM	Signature Activation Module
SAML	Security Assertion Markup Language
SCA	Strong Customer Authentication
SSO	Single Sign On
TC	Technical Committee
TR	Technical Report
TS	Technical Standard

References

[1] CEN: EN 419 221-5, Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services, available at this link.

[2] CEN: EN 419 241-1, Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements, available at this link.

[3] CEN: EN 419 241-2, Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing, available at this link.

[4] ETSI: TC ESI on Identity Proofing, Specialist Task Force STF 588, available at this link.

[5] EU Commission: eIDAS (electronic IDentification Authentication and trust Services), Regulation EU 910/2014, available at this link.

[6] EU Commission: eIDAS Implementing Regulation EU 2015/1501, Commission Implementing Regulation EU 2015/1501 on the interoperability framework, available at this link.

[7] EU Commission: eIDAS Implementing Decision EU 2016/650, Commission Implementing Decision EU 2016/650 laying down standards for the security assessment of qualified signature and seal creation devices, available at this link.

[8] EU Commission: EU Cybersecurity Act, Regulation EU 2019/881, available at this link.

[9] EU Commission: Inception impact assessment - revision of the eIDAS Regulation, available at this link.

[10] EU Commission: Payment services (PSD2), Directive EU 2015/2366, available at this link.

[11] OpenID Foundation: OpenID Connect v1.0, available at this link.

 © 2020 Yubico. All rights reserved.