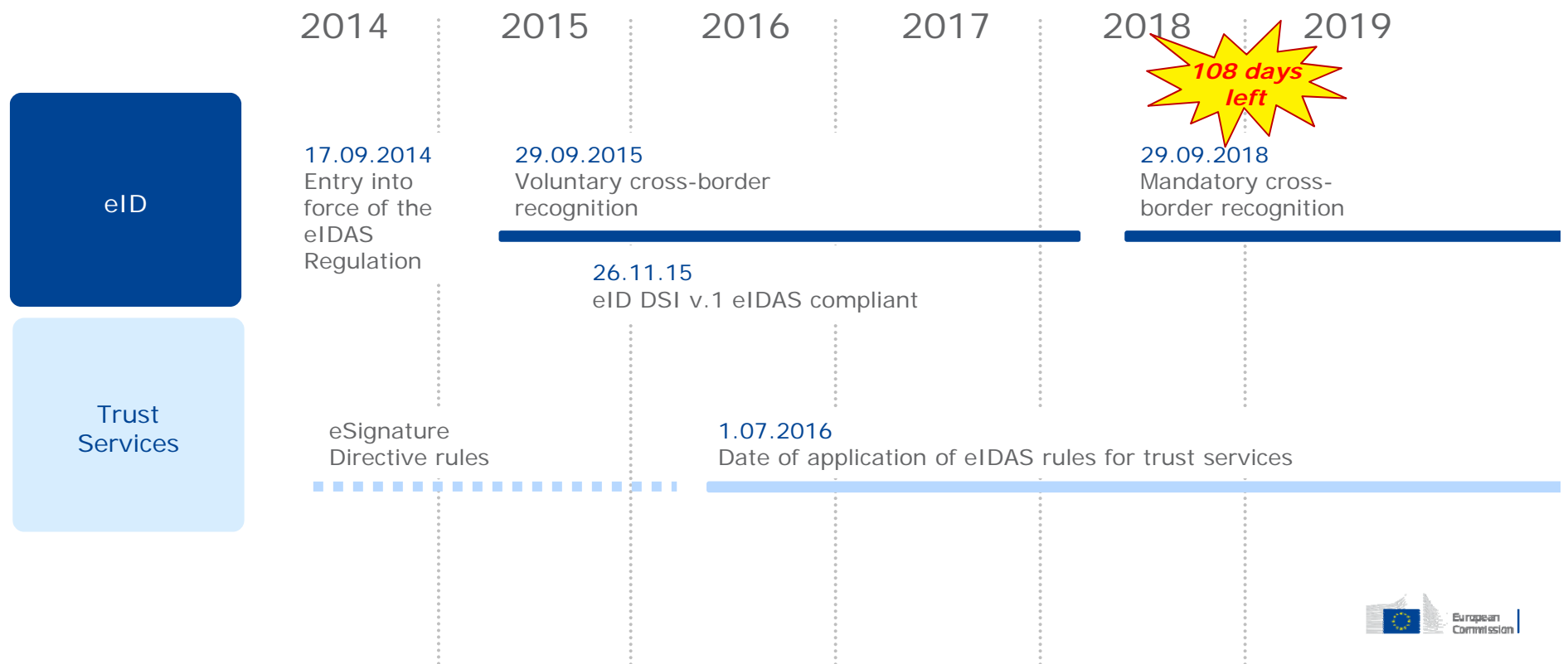




Update on the eIDAS Regulation

DG CONNECT, European Commission
Unit "eGovernment & Trust"

Timeline



Where eIDAS plays a role

PSD2

RTS on SCA: Commission Delegated Regulation (EU) 2018/389

AMLD5

Finally adopted on 14/05/2018

Digital on-boarding and portability of KYC

EC Expert Group on eID and remote KYC (1st meeting held in April)

Company law

Proposal to amend the Directive (EU) 2017/1132 adopted by EC on 25/04/2018

Fighting Fake News

COM(2018) 236 final adopted on 26/04/2018)

Once-Only Principle cross-border

EU Regulation on Single Digital Gateway agreed on 24/05/2018

GDPR compliance

Data minimisation; use of trusted attributes, credentials and entitlements (such as age verification, proof of residence, etc.)

Protection of minors online

Age verification and parental consent

Online banking
Union citizenship
Finance Mobile eHealth
eCommerce
Customs Transport Taxation
Social security
Sharing economy
eJustice
eProcurement

Background - TSPs and Qualified Trust Service Providers

- **Trust Service Providers**
 - Light touch approach pursuant to Article 19, ex-post
- **Qualified Trust Service Providers**
 - The granting of qualified status by the supervisory authority pursuant to Article 21
 - Comply with certain requirements pursuant to Article 24
 - Submitted to the supervision of the supervisory body pursuant to Article 20
- **Justification: different legal effects provided**
 - Article 25(2): A qualified electronic signature shall have the equivalent legal effect of handwritten signature,
 - Article 25(3) and qualified electronic signature based on a certificate issued in a Member State shall be recognised in all other Member States

Electronic signatures can be created remotely (eIDAS recital 52)

- *“The creation of remote electronic signatures, where the electronic signature creation environment is managed by a trust service provider on behalf of the signatory, is set to increase in the light of its multiple economic benefits.*
- *However, in order to ensure that such electronic signatures receive the same legal recognition as electronic signatures created in an entirely user-managed environment, remote electronic signature service providers should apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels, in order to guarantee that the electronic signature creation environment is reliable and is used under the sole control of the signatory”.*
- **These considerations apply equally to both qualified and non-qualified signatures**
- *“Where a qualified electronic signature has been created using a remote electronic signature creation device, the requirements applicable to qualified trust service providers set out in this Regulation should apply”.*

Electronic signatures can be created remotely involving third parties, requirements

- *Recital 51: "It should be possible for the signatory to entrust qualified electronic signature creation devices to the care of a third party, provided that appropriate mechanisms and procedures are implemented to ensure that the signatory has sole control over the use of his electronic signature creation data, and the qualified electronic signature requirements are met by the use of the device".*
- Article 29: Requirements for qualified electronic signature creation devices
- *"Qualified electronic creation devices shall meet the requirements laid down in Annex II*
 - *Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider (Annex II 3)"*
 - *Recital 56: "This Regulation should lay down requirements for qualified electronic signature creation devices to ensure the functionality of advanced electronic signatures. This Regulation should not cover the entire system environment in which such devices operate. Therefore, the scope of the certification of qualified signature creation devices should be limited to the hardware and system software used to manage and protect the signature creation data created, stored or processed in the signature creation device. As detailed in relevant standards, the scope of the certification obligation should exclude signature creation applications."*
- Article 30: Certification of qualified electronic signature creation devices.

Principles applicable to secondary acts

Adoption of secondary legislation for which no obligation for adoption is set in the eIDAS Regulation would take into account the following principles:

- **Framework consistency**
- **Stakeholders / market needs**
- **Favouring a non-regulatory / co-regulatory approach first**
- **Developments under other Regulatory frameworks**
- **Availability and adequacy of standards & technical specifications**

Conclusion(s)

- Nothing In the Regulation prevents a user from entrusting qualified electronic creation devices, which may be remote systems, to trust service providers **under the conditions** set out in the Regulation for the validity of each type of electronic signature
- **Only** qualified trust service providers that have been granted qualified status pursuant to Article 21 using trustworthy systems and products that meets the requirements of Article 24(2), in particular letter e) and f), may generate or manage electronic creation data on behalf of the signatory.

This requires a specific secure environment

- The question of implementing acts in relation to the eIDAS Regulation follows the principles that apply to the enacting of secondary acts in the EU

For further information and feedback

Web page on eIDAS

<http://ec.europa.eu/digital-agenda/en/trust-services-and-eid>

eIDAS Observatory

<https://ec.europa.eu/futurium/en/eidas-observatory>

Text of eIDAS Regulation in all languages

<http://europa.eu/lux73KG>

**Connecting Europe Facility –
Catalogue of Building Blocks**

<https://ec.europa.eu/cefdigital>

eIDAS twitter account

[@EU_eIDAS](https://twitter.com/EU_eIDAS)

Unit "e-Government and Trust"

CNECT-EGOVERNMENT-AND-TRUST@ec.europa.eu