eIDAS Regulation (EU) 910/2014

"Website authentication services under eIDAS Regulation"

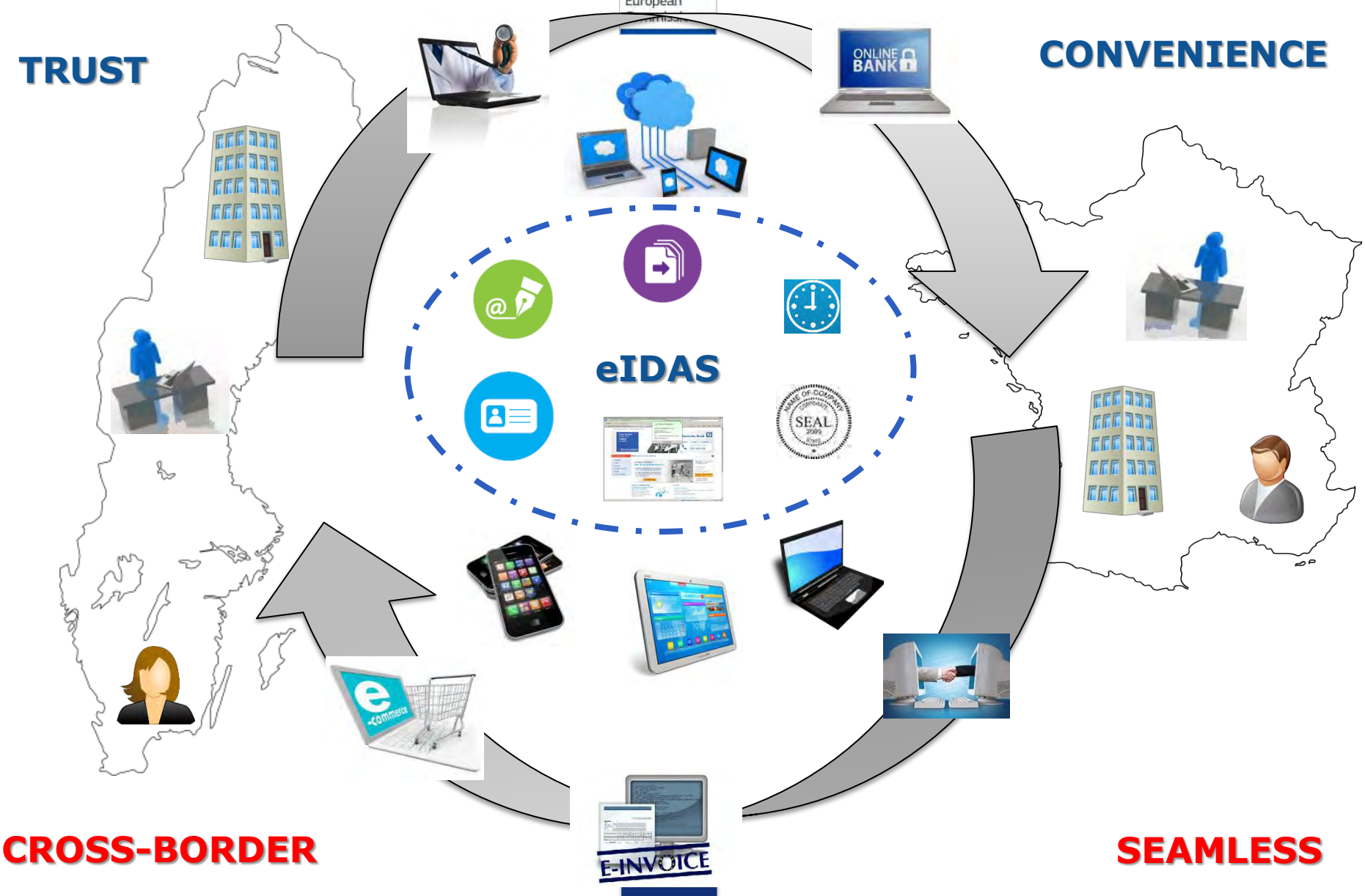
CA/Browser Forum

Istanbul 07 October 2015

Andrea SERVIDA
DG CONNECT, European Commission
Head of eIDAS Task Force
andrea.servida@ec.europa.eu

eIDAS: What is it about?

Supporting businesses!



eIDAS breaks new ground

Takes a risk management perspective, not based on normative rules but on principles:

- **Transparency and accountability: well-defined minimal obligations for TSPs and liability**
- **Trustworthiness of the services together with security requirements for TSPs**
- **Light-touch reactive monitoring for TSPs *vs.* full-fledged supervision for QTSPs**
- **Technological neutrality: avoiding requirements which could only be met by a specific technology**
- **Market rules and building on standardisation**

Provides one set of rules directly applicable across all EU MS

→ Regulation (plus 1 DA and 28 IA)

eIDAS – Mutual recognition of eIDs

Mandatory recognition of electronic identification

Voluntary notification of eID schemes

"Cooperation and interoperability" mechanism

Liability rules

Assurance Levels: "high" and "substantial" *(and "low")*

Interoperability framework

Access to authentication capabilities: free of charge for public sector bodies & according to national rules for private sector relying parties

eIDAS – Trust services

Horizontal principles: Liability; Supervision; International aspects; Security requirements; data protection; Qualified services; Prior authorisation; trusted lists; EU trust mark

- **Electronic signatures, including validation and preservation services**
- **Electronic seals, including validation and preservation services**
- **Time stamping**
- **Electronic registered delivery service**
- **Website authentication**

Website authentication – Recital (67) [1/2]

*"**Website authentication services** provide a means by which **a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website**. Those services **contribute to the building of trust and confidence** in conducting business online, as **users will have confidence in a website that has been authenticated**. The provision and the **use of website authentication services are entirely voluntary**. However, in order for website authentication to become a means to boosting trust, providing a better experience for the user and furthering growth in the internal market, **this Regulation should lay down minimal security and liability obligations for the providers and their services**…*

Website authentication – Recital (67) [2/2]

"… To that end, ***the results of existing industry-led initiatives, for example the Certification Authorities/Browsers Forum — CA/B Forum, have been taken into account****. In addition, this* ***Regulation should not impede the use of other means or methods to authenticate a website*** *not falling under this Regulation nor should it prevent third country providers of website authentication services from providing their services to customers in the Union. However, a* ***third country provider should only have its website authentication services recognised as qualified*** *in accordance with this Regulation, if an international agreement between the Union and the country of establishment of the provider has been concluded."*

eIDAS – Definition of Trust Services & electronic documents

- **Trust services – art. 3(16)**
  - ✓ '**trust service**' means an **electronic service normally provided for remuneration** which consists in:

    (a) the creation, verification, and validation of **electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services** and certificates related to these services or

    b) the creation, verification and validation of certificates for website authentication or

    (c) the preservation of electronic signatures, seals or certificates related to these services;

- **Electronic document - art. 3(35)**
  - ✓ '**electronic document**' means **any content stored in electronic form**, in particular text or sound, visual or audiovisual recording

eIDAS – General principles for trust services

- **Liability regime for Q & non-QTSPs (art.13)**
  - Liability for damages caused **intentionally or negligently**
  - **Reverse burden of the proof only for QTSPs**
  - Possible **limitations of liability** for the use of the service by the TSP subject to clear information to customers
  - **Applicability of national rules on liability**
- **Recognition of 3rd countries TSPs (art.14)**
  - Only through international agreements between the Commission and a third country or international organisation
  - **Principle of reciprocity**
- **Accessibility for persons with disabilities (art.15)**

eIDAS – Role of the Supervisory body

- **Light touch ex post reactive monitoring of non-qualified TSPs vs. Full-fledged ex ante and ex post supervision of qualified TSPs (art.17)**
- **Detailed tasks of the Supervisory body (art.17.4)**
  - **Analyse conformity assessment reports**
  - Report to the Commission about main activities
  - **Carry out audits / Request conformity assessments**
  - Inform **data protection authorities where appropriate**
  - Grant and withdraw qualified status
  - Inform national body responsible for trusted lists
  - **Require (Q)TSPs to remedy any failure to fulfil the requirements**
  - …

eIDAS – Obligations of TSPs

- **Minimum security requirements + notification of significant security breaches by all TSPs (art.19)**
- **Specific requirements to be met by QTSPs (art.24):**
  - staff,
  - **trustworthiness of their systems**,
  - **liability insurance scheme**,
  - identification of the certificate owner,…
- **Conformity assessment of QTSP (art. 20 & 21):**
  - **Ex ante (prior authorisation scheme** – art.21) ➔ SB may grant the qualified status in a given timeframe ➔ Inclusion in the Trusted Lists
  - **ex post (every 24 months & *ad hoc*** – art. 19) ➔ May withdraw the qualified status
  - building upon Regulation 765/2008 conformity assessment scheme

eIDAS – Supporting tools

- **Trusted lists for QTSPs and QTSs (art.22)**
  - ➢ **Implementing Decision adopted on 08/09/2015**

- **EU trust mark for qualified trust services (art.23)**
  - ✓ **Usage by QTSP after qualified status** has been indicated in the TLs
  - ✓ **Trustmark** indicates in a simple, recognisable, and clear manner the qualified status of a trust service
  - ✓ **Link to the relevant TL has to be ensured by the QTSP**
    - ➢ **Implementing Regulation adopted on 22/5/2015**

eIDAS – Website authentication: the legal provisions

- **Website authentication certificate (SSL, TSL, …) TSPs are subject to supervision (QTSPs) or monitoring (non-QTSPs) – (art 17)**
- **Website authentication certificate TSPs have to match minimum security requirements as well as to notify significant security breaches (art 19)**
- **QTSPs issuing Q-website authentication certificates have to match all reqs for QTSP set in the Regulation (in particular art 24)**
- **Website authentication certificate TSPs are subject to the liability regime (art 13)**
- **Requirements for Q-certificates for website authentication (art.45 + annex IV)**

Certificates for Website authentication – Key Elements (1)

- **Legal**: eIDAS Regulation applies to all TSPs established in a MS ➔ predominant wrt companies' policies.
- **Market**: Transparent services building upon clear requirements and transparent procedures (including for the identification of the owner of the QWACs) ➔ new market opportunities and new customers.
- **Technical**: eIDAS requirements build upon CAB Forum Recommendations
- **eIDAS reliable source** for qualified certificates for website authentication = National Trusted Lists and EU "List of the Lists"
- **Differences between the eIDAS TLs and the Service Directive TL**:
  - eIDAS: TLs are constitutive and QTSPs and QWACs are included in the eIDAS TLs following a strict EU harmonised procedure
  - Service Directive: TLs are informative and CSPs issuing QCs are included on the grounds of non-harmonised procedures.

Certificates for Website authentication – Key Elements (2)

- **Security**: eIDAS ensures
  - Transparency of, trustworthiness of and accountability for the qualified certificates for website authentication.
  - Strengthened supervision system + risk management obligations (both for Q and non-Q TSPs and services) ➔ providers liable for the services they provide + tools to SB in order to monitor the market ➔ prevent incidents like Diginotar
- **Procedure**
  - (1) TSP issuing (Q)WACs requires the supervisory body to become qualified,
  - (2) conformity is assessed by CAB (ETSI EN 319 403 V2.2.2).
  - List of CABs ➔ always informal: may be NABs or ACAB.
  - (3) SB assesses TSP + service and decides to grant Q-status ➔ SB is the only authoritative authority
  - (4) QTSP + QTS added to the TLs ➔ **YOU ARE QUALIFIED ONLY IF IN TL**

Certificates for Website authentication – Key Elements (3)

- **International:**
  - **Legal option:** Providers established in non-EU countries ➔ WA certificates = eIDAS QWACs if international agreement EU / country of establishment.
  - **Operational option:** set a legal entity in one of the Member States and to go through supervisory procedure describe above in order to be granted the qualified status.
  - **location of the technical infrastructures in a non-EU country**
    - **➔ impact operationally**
    - **➔ does not represent a legal impediment.**
- **Operational aspects:**
  - QWACs might be issued from new roots.
  - a root might issue both types of certificates provided that it meets the requirements for the higher level (qualified one).
  - QTSPs + QWACs will be included mandatorily by MS in the TL.
  - A new policy OID for QWACs is foreseen in draft ETSI TS 319-411
- **QWACs for Natural persons:**
  - only the fields related to the identification of the owner of the certificate will differ ➔ no impact in terms of audits or of validation of the certificate.

eIDAS – What does it means for website authentication

- **eIDAS Website authentication provides with:**
  - **clear requirements for website authentication certificates to be trustworthy**
  - **minimal obligations for providers of such certificates with regard to the security of their operations (art.19)**
  - **liability providers of such certificates (art 13)**
  - **(light-touch) supervision regime (art 17)**

➔ the Regulation will ensure:

- **transparency of service quality offered to users,**
- **accountability of providers with regard to security of their services,**
- **trustworthiness of the data associated to authenticated websites,**
- **technological neutrality of services and solutions.**

Trust Services - Adopted Implementing Acts:

- **Commission Implementing Regulation (EU) 2015/806 of 22.05.2015**
  - ✓ Form of the EU Trust Mark for Qualified Trust Services (art. 23.3)

- **Commission Implementing Decision (EU) 2015/1505 of 8 September 2015**
  - ✓ technical specifications and formats relating to trusted lists (art. 22.5)

- **Commission Implementing Decision (EU) 2015/1506 of 8 September 2015**
  - ✓ specifications relating to formats of advanced electronic signatures and seals to be recognised by public sector bodies (art. 27.5 & 37.5)

The EU Trust Mark for Qualified Trust Services – *winner of "e-Mark U Trust" Competition* - (EU) 2015/806

EU Safe

COMMISSION IMPLEMENTING REGULATION ON EU TRUST MARK -(EU) 2015/806

Key principles of the EU Trust Mark for QTS:

- Can only be used by a qualified trust service provider
- Can only "label" its qualified trust services
- Can be used on any support (provided that the requirements of article 23 of the Regulation and of the implementing Regulation are met)
- The use of the EU trust mark is voluntary
- Foster transparency of the market
- Helps Customers distinguish between qualified trust services and non-qualified ones.

COMMISSION IMPLEMENTING DECISION ON TRUSTED LISTS - (EU) 2015/1505

Key principles

eIDAS Trusted Lists:

- Ensure continuity with the existing TLs established under the Service Directive.
- Ensure legal certainty.
- Foster interoperability of qualified trust services by facilitating a.o. the validation of e-signatures and e-seals.
- Allow citizens, businesses and public administrations to easily get the status of a trust service.

Timeline

2014 | 2015 | 2016 | 2017 | 2018 | 2019

17.09.2014 - Entry into force of the Regulation

29.09.2015
Voluntary recognition eIDs

1.07.2016
Date of application of rules for trust services

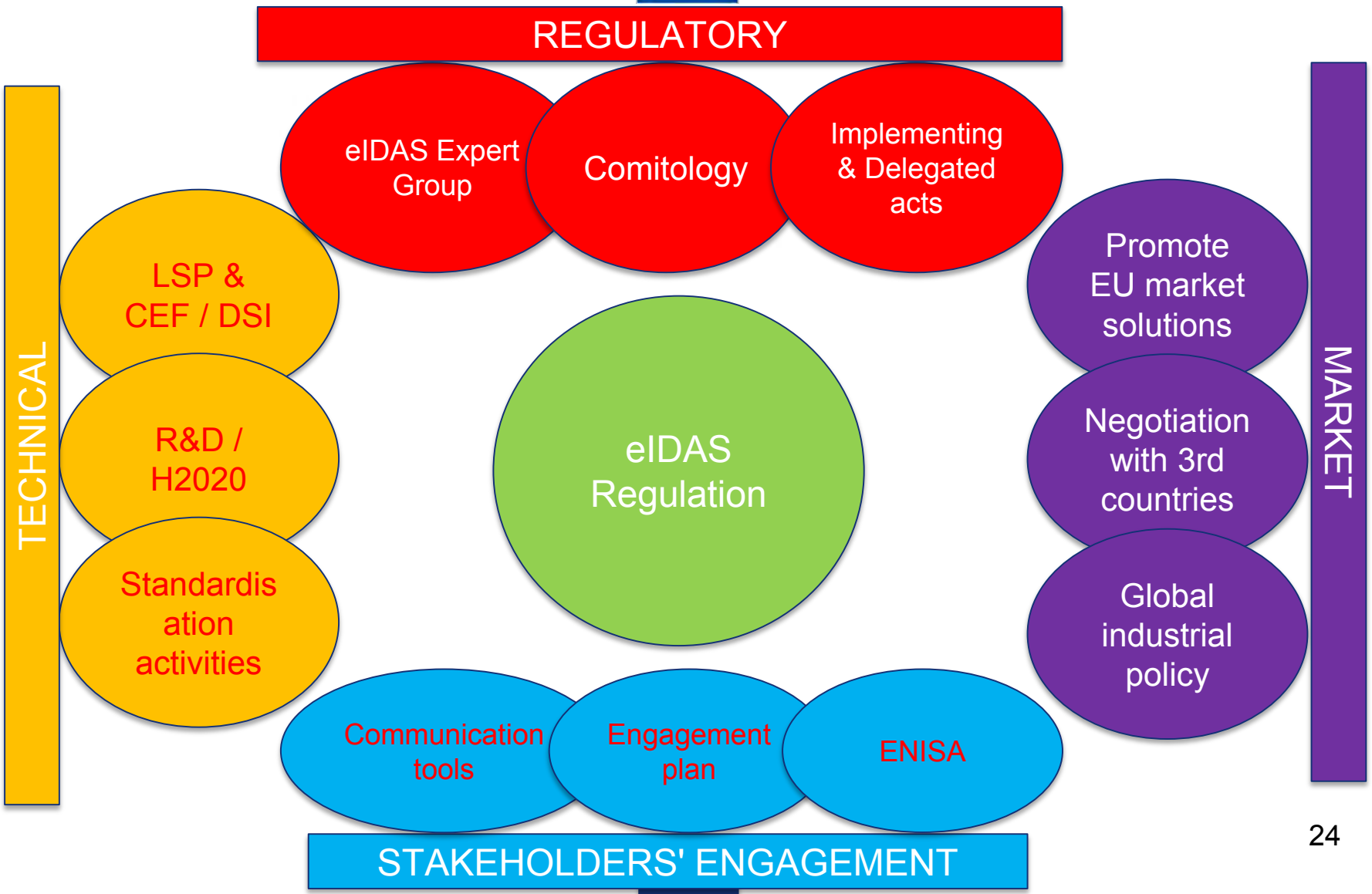
29.09.2018
Cross border recognition of eIDs

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**

An eIDAS World



Stakeholder engagement activities (1)

- **eIDAS stakeholder engagement plan** -> an enabler of DSM
  - Key sectors: **Financial & Banking Services, Sharing economy, eCommerce**, Transport, **Mobile Operators**, Social Innovators
  - Setting-up of an **eIDAS European Observatory** on online trust, security and transparency
  - Online **eIDAS participatory platform** (in DIGITAL4EU)
  - Launching a series of **high-level roundtables** with private sector to define strategic recommendations to foster the use of eID and trust services as enablers of market digitisation (DSM)
  - Setting-up a **cross-DG eIDAS interest group** to discuss existing and planned legislative proposals to benefit from the transformative role of eID and trust services (under eIDAS)

ENISA Support for eIDAS

- **ENISA** (European Agency for Network and Information Security):
  - 2012 → **Report on the implementing eIDAS art. 15**
  - 2013 → **Guidelines for Trust Service Providers**
  - 2014
    - ✓ Common audit schemes for trust services providers in MS.
    - ✓ Technical guidelines for independent auditing bodies and supervisory authorities
  - 2015 focus on:
    - ✓ **Introduction of qualified website authentication certificates**
    - ✓ **ENISA Trust Service Forum (1st meeting 30/6/15)**
    - ✓ **Evaluation of standards**
    - ✓ **Technical guidelines for Implementation of Art 19**
    - ✓ **Awareness raising - European Cyber Security Month (Oct 2015)**

EUROPEAN CYBER SECURITY MONTH

ENISA activity in 2015: Introduction of qualified website authentication certificates

- **Objectives and process**
  - Analyse the characteristics of the current market situation of website authentication certificates;
  - Comparative analysis of the different available types of website authentication certificates + identify existing industry level initiatives;
  - Compare with requirements set in Regulation 910/2014, in terms of content and assurance level;
  - SWOT analysis of the usage of qualified website authentication certificates;
  - Make recommendations on strategies for the successful introduction in the European market of qualified website authentication certificates.
- **Modus operandi**
  - ENISA is working with an expert group
  - Collaborative work, in liaison with the eIDAS Informal Expert Group
  - **TIMING:** Draft under external review; final draft by December
  - **CONTACT @ENISA:** Clara GALAN (email: isdp@enisa.europa.eu)

ENISA activity in 2015 (2): Analysis of standards for TSPs

- **Objectives**
  - Input to implementing acts supporting eIDAS
  - Analysis of eIDAS requirements related to standards
  - Mapping between the standards and the provisions of the Regulation
  - Analysis of standards in the context of m460,
  - Analysis of existing (also non EU) standards
  - Identify and prioritize existing gaps
- **Modus operandi**
  - ENISA is working with an expert group
  - Collaborative work, in liaison with the eIDAS Informal Expert Group

Few questions

- **How to make QWACs an opportunity to improve transparency, accountability, security and trust in the web?**
- **What the obstacles to implement QWACs in web browsers roots?**
- **How to make visually different for users the authentication based on QWACs?**
- **How to cooperate closer with CA / Browser Forum and its constituency?**
- **…**

For further information and feedback

Web page on eIDAS

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

Impact assessment

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012SC0135

Text of eIDAS Regulation in all languages

http://europa.eu/!ux73KG

eIDAS functional mailbox

CNECT-TF-eIDAS-LT@ec.europa.eu

EU eIDAS