Demystifying eIDAS

V4

Digital Challenges

Fear

Uncertainty

Doubt

Digital Challenges

Fear of technology failure

Uncertainty over security

Doubt over commercial governance

Background

The Reality of the European Union

- The European Union is made up of 27+ Member States, each with their own priorities, political drivers and cultural background. This extends to their views on privacy, data protection and the relationship between citizens and State
- Each Member State has its own types of eIDs, citizenship registry records, etc
- Contrary to public perception, there are only a few issues where the European Union can legislate directly for actions in Member States

EU Drivers and the Digital Economy

The Private Sector

By having a single European market, the EU becomes a single trading geography with all the benefits of scale – 700 million citizens

As a Digital Economy, businesses can interact electronically with customers anywhere in the EU boosting trade and demonstrating considerable improvements in efficiency and productivity

Citizens are able to move and work freely within the EU

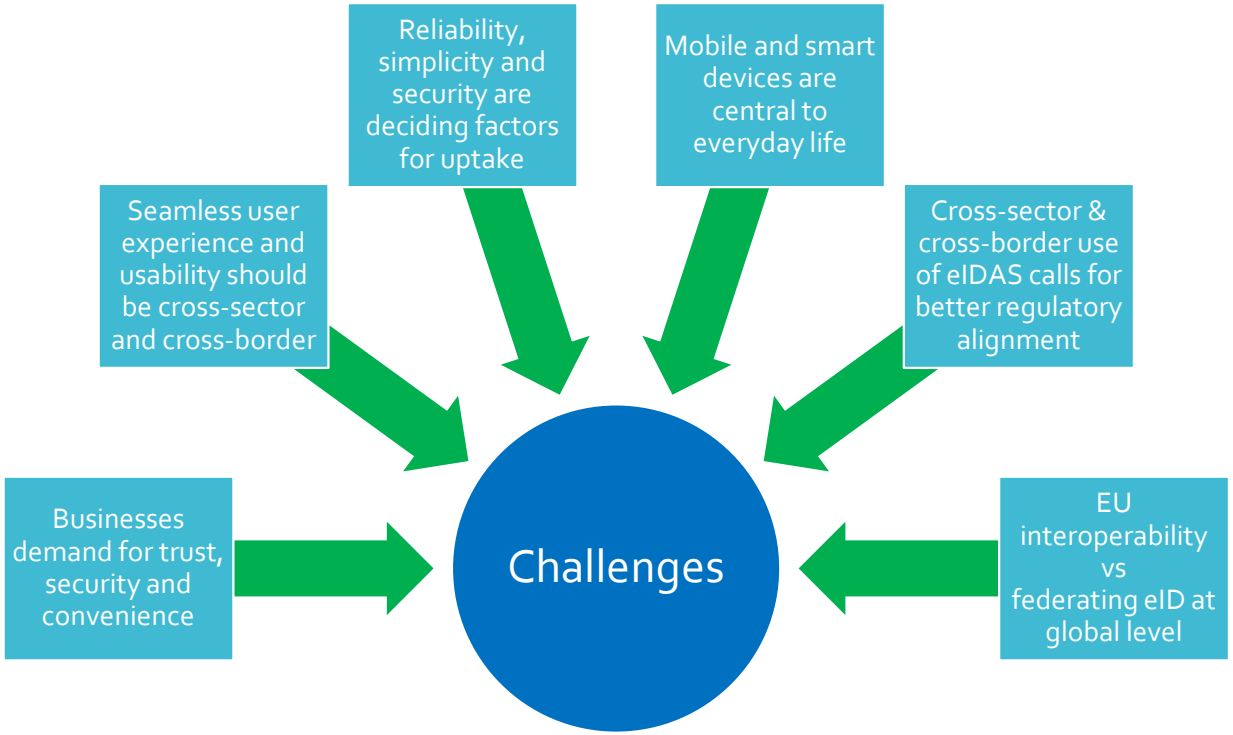
The Public Sector

Digital Government, where many services are available on-line, can make massive savings in terms of effort, and increase speed and impartiality of decision making

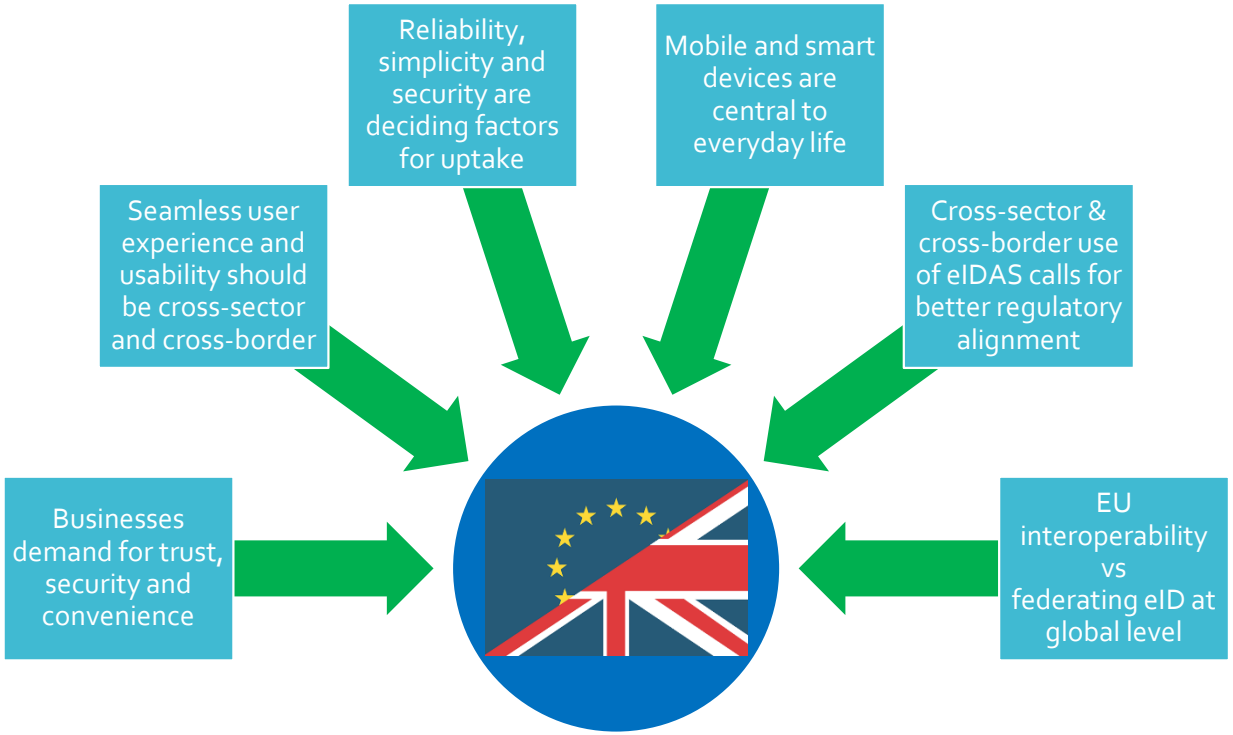
The Goal of Inter-Operability

- For the European Single Digital Economy to truly function, trust in the identity of the citizen or company, originating anywhere in the EU, is essential
- However the citizen or company must be confident that it is protected no matter wherever it happens to be, and it is able to interact locally and anywhere in the EU with equal safety
- Consequently a number of initiatives have been established to drive interoperability and ensure that no matter what Member State you are from, you can demonstrate your identity to obtain services and interact digitally with confidence and trust

Factors driving Trust Services



Factors driving Trust Services



Examples of 'Large Scale Pilots' and Projects

LIGHTest

epsos
EUROPEAN PATIENTS SMART OPEN SERVICES

SENS moving services forward.eu

FutureTrust

e-CODEX making justice faster.eu

FutureID

STORK2.0
SECURE IDENTITY ACROSS BORDERS LINKED 2.0

ABC4TRUST

DE4A
Digital Europe For All

TOOP providing data once-only.eu

A Series of Regulations and directives for the Digital Single Market

eIDAS

Trust Services Regulations

eIDAS Trust Services

Areas Covered

- Mutual recognition of Electronic Identities
- Electronic signatures, including validation and preservation services
- Electronic seals, including validation and preservation services
- Time-Stamping
- Electronic registered delivery service
- Website Authentication

eIDAS
Key Principal

The Regulation does not impose the use of eID and trust services

eIDAS Key Principal on eID

- Sovereignty of Member State (MS) to use or introduce means for electronic identification
- Mandatory cross-border recognition only to access public services
- Full autonomy for private sector
- Principle of reciprocity relying on defined levels of assurance
- Interoperability framework
- Cooperation between Member States

eIDAS Key Principal on Trust Services

- Non-discrimination in Courts of electronic trust services vis-à-vis their paper equivalent
- Specific legal effects associated to qualified trust
- services
- Non-mandatory technical standards ensuring presumption of compliance
  - Leads to technological neutrality

Risk Management

- 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 Delegated Act and 28 Implementing Acts)

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 Principals

- Liability
- Supervision
- International aspects
- Security requirements
- Data protection
- Qualified services
- Prior authorisation
- Trusted lists
- EU trust mark

Implementation

3 eID Implementing Acts plus the draft on notification

Cooperation

- Member States have the obligation to cooperate
- Cooperation main focus is on achieving
  - Interoperability
  - Security
- Common language

Commission Implementing Decision On Cooperation - (Eu) 2015/296

Elements of the Cooperation (1)

- Points of single contact – exchange of information
- Peer review
  - Voluntary participation
  - Each Member State will bear its own costs
  - Confidentiality of information obtained
  - Avoiding conflict of interest
- Exchange of information, experience and good practices
- Request of information on interoperability and security

Elements of the Cooperation (2)

- Cooperation Network
  - MS are members
  - Meetings will be chaired by the Commission
- Tasks of the Cooperation Network – some examples
  - adopt guidance on the scope of peer review and its arrangements
  - adopt opinions on developments relating to the interoperability framework
  - examine relevant developments in the eID sector

Levels of Assurance (eIDAS Art 8)

"

- The assurance levels low, substantial and high shall meet respectively the following criteria:
  - assurance level "low" ……., the purpose of which is to decrease the risk of misuse or alteration of the identity;
  - assurance level "substantial" ….., the purpose of which is to decrease substantially the risk of misuse or alteration of the identity;
  - assurance level "high" ……, the purpose of which is to prevent misuse or alteration of the identity.

"

Elements of Levels of Assurance

- Enrolment (application, registration, identity proofing)
- eID means management (design, issuance, suspension, renewal etc)
- Authentication
- Management, organisation (ISM, record keeping, facilities and staff, controls, compliance etc)

An example of differences between LoAs: identity proofing

- Level “high”: “substantial” plus
  - physical appearance at registration (or at earlier stage) is required
  - verified possession of valid identity evidence (like photo/bio)
- Level “substantial”: “low” plus
  - physical appearance at registration not required
  - Based on recognised evidence checked to be genuine
- Level “low”:
  - physical appearance at registration not required
  - No direct verification of identity evidence assumed to be genuine

Principles of Notification

- eID scheme is either
  - Issued by the notifying Member State
  - Issued Under a mandate from notifying Member State
  - Recognised by the notifying Member State
- eID means used to access at least one public service
- eID scheme meets requirements at least of one of the assurance levels

Notification Template

- One common template used by all Member States for the notification
- Contains information on all the elements of notification
- Common language – English
- Submitted electronically
- Commission may request additional information if the form is not complete
- Possibility to add relevant supporting documents
- The template is to be used also for "pre-notification"

Summary of Trust Services Implementing acts

EU Trust Mark for Qualified Trust Services

"EU Safe"

The EU Trust Mark for Qualified Trust Services - (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.

eIDAS Trusted Lists Key Principals

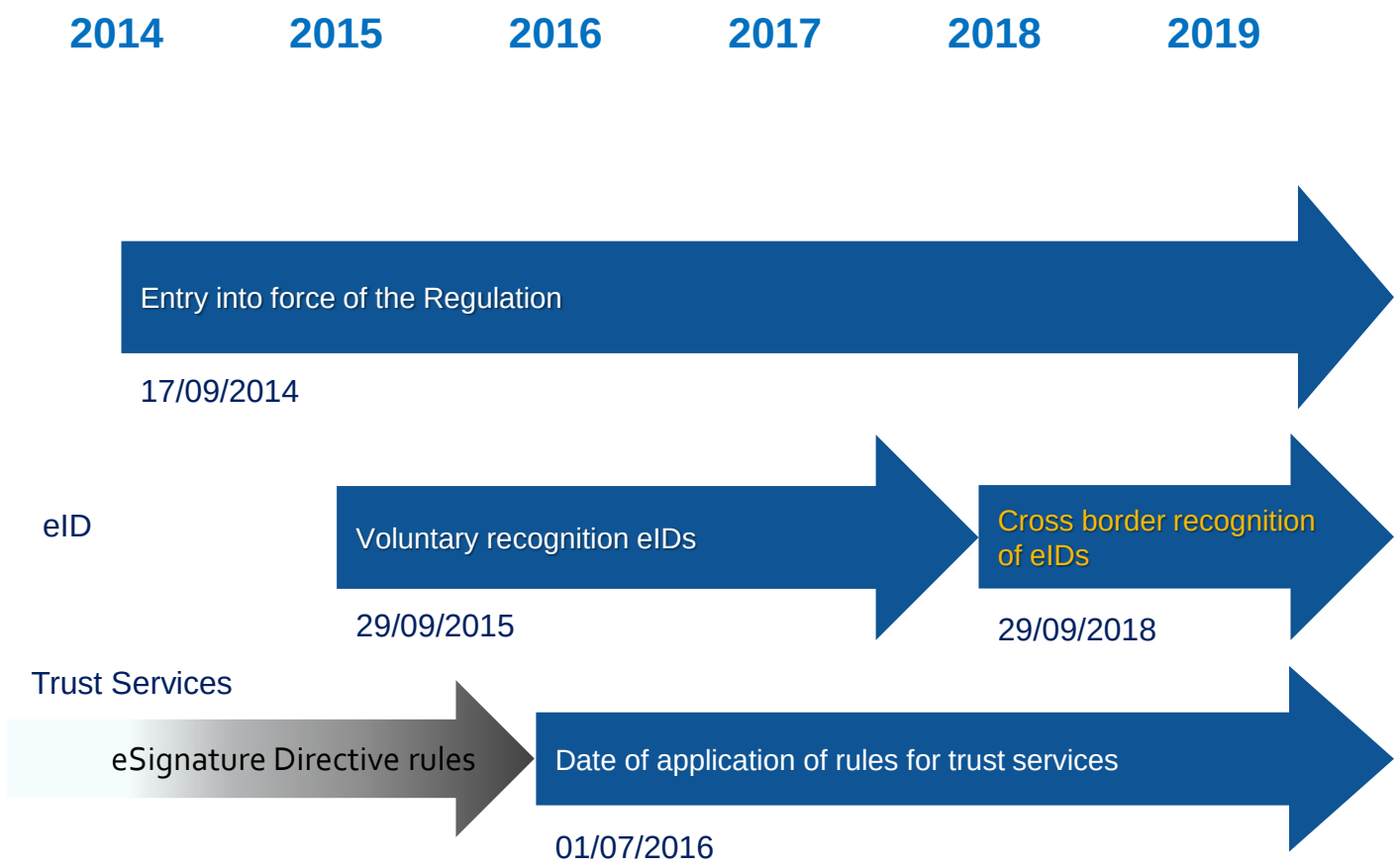
- Ensure continuity with the existing TLs established under the Service Directive.
- Ensure legal certainty.
- Foster interoperability of qualified trust services by facilitating the validation of e-signatures and e-seals.
- Allow citizens, businesses and public administrations to easily get the status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

eSignatures and eSeals Key Principals

- Ensure continuity with the principles adopted under the Service Directive.
- Facilitates cross-border transactions / applications with public sector bodies in a different MS (such as e-procurement).
- Ensure technological neutrality by setting a method for the use of non-standardised formats.

Commission Implementing Decision On Esign/Eseals Formats - (Eu) 2015/1506

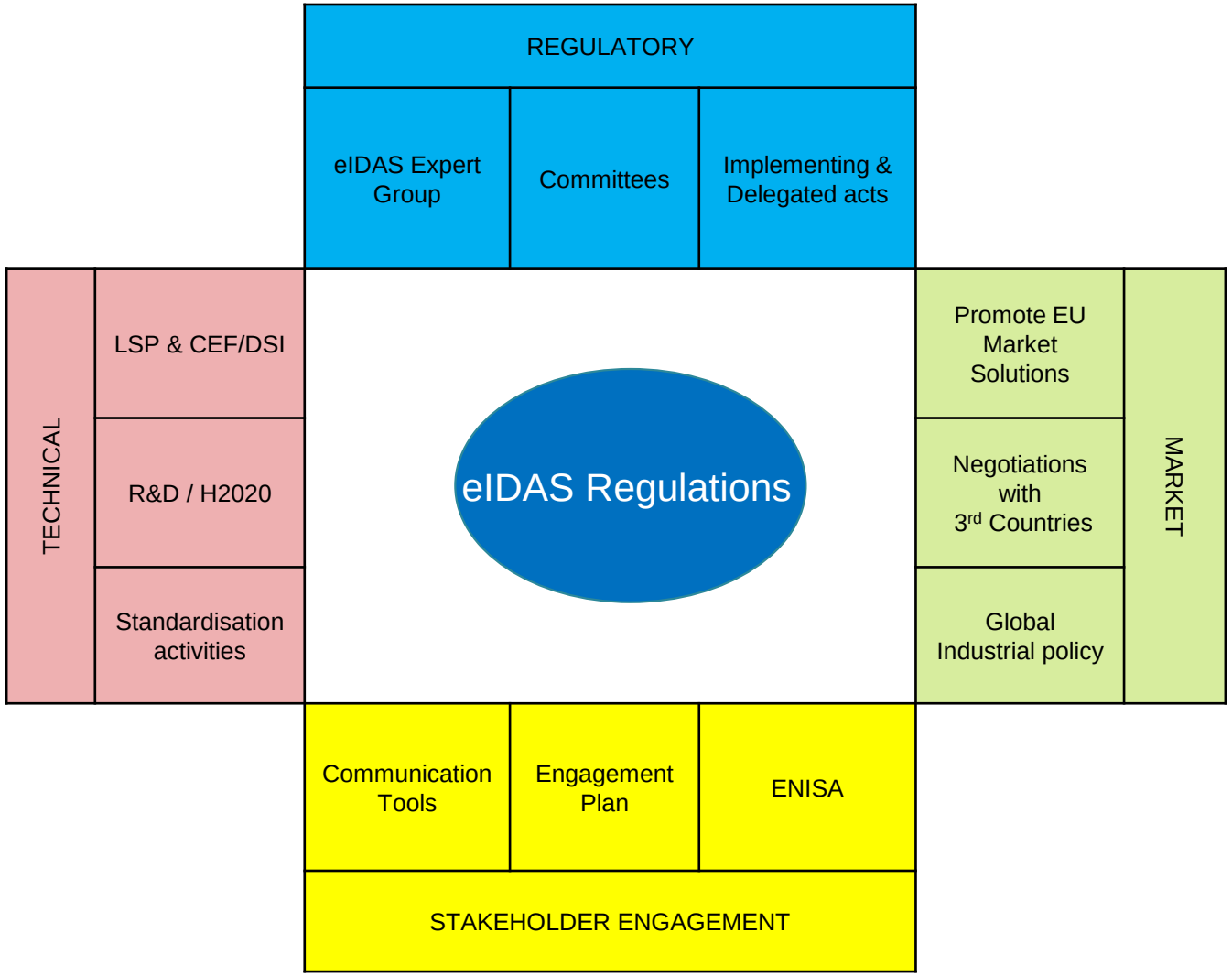
Timelines


2014
2015
2016
2017
2018
2019
Entry into force of the Regulation
17/09/2014
eID
Voluntary recognition eIDs
29/09/2015
Cross border recognition of eIDs
29/09/2018
Trust Services
eSignature Directive rules
Date of application of rules for trust services
01/07/2016

Opportunities for e-Services

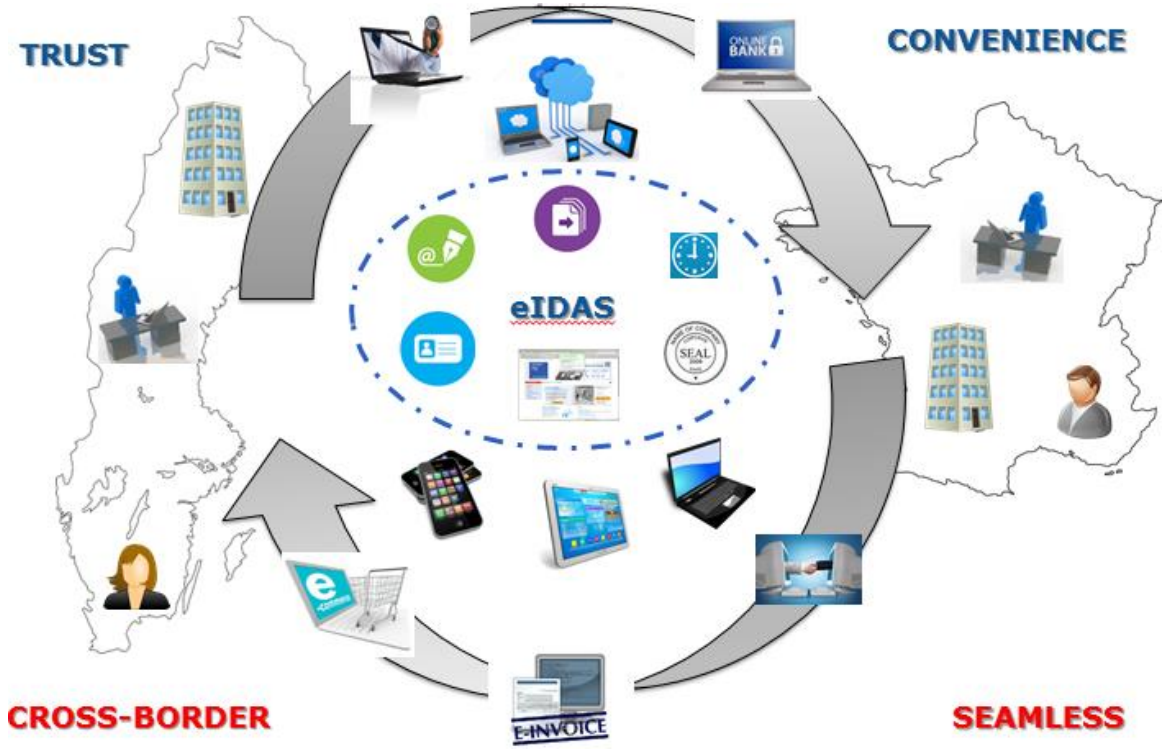
- Facilitate on-line seamless consumer experience without face-to-face verification
- Easier access to distance credit for consumers; EU cross-border market for banks
- Trusted credentials ease discharging regulatory requirements (e.g. Anti-Money Laundering, PSD2, etc.)
- Verified identities to check credit rating and contact with public administrations (tax agencies)
- Lower risk & more convenience by relying on e-ID, e-sign, e-seal, e-registered

eIDAS Ecosystem



eIDAS
Global dimension and opportunities

eIDAS is seen as a total package of activity



The EU is the first and only region in the world to have:

- Policy
- Technology
- Regulation
- Rules
- Interoperability

In Conclusion

Challenges

Fear of technology failure

Uncertainty over security

Doubt over commercial governance

Confidence building

Opportunities

Operational cohesion

Leadership

Opportunities

Jon Shamah

jshamah@ejconsultants.eu

+44 7813-111290