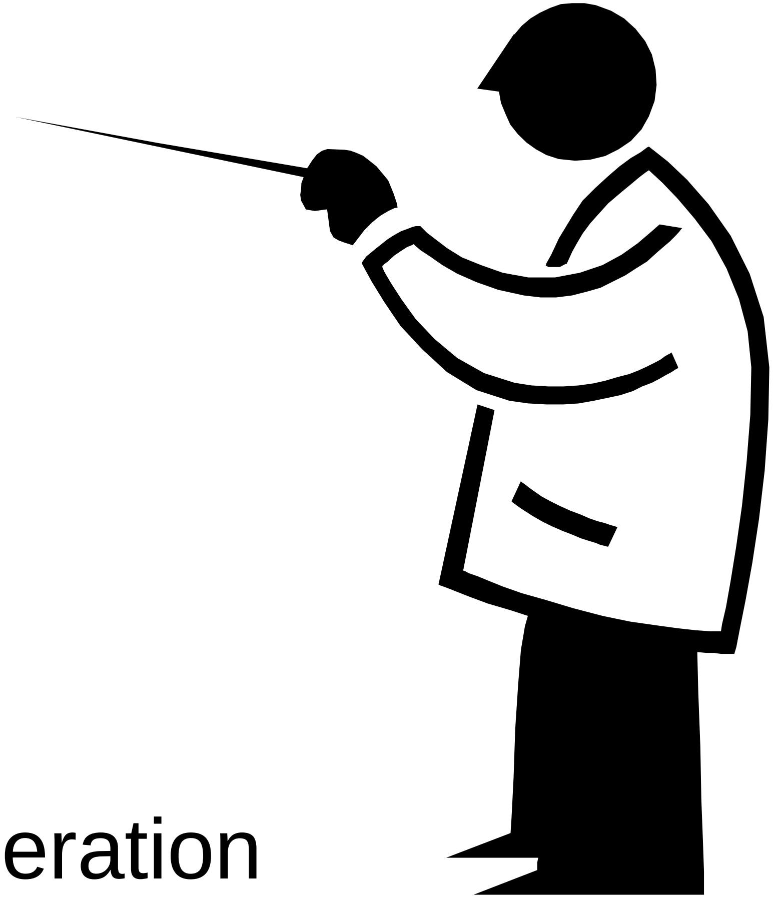
ENHANCEMENT OF THE BUSINESS ENVIRONMENT IN THE SOUTHERN MEDITERRANEAN

Best practice EU
Herbert Leitold, A-SIT
Jersualem, Dec. 5th, 2016

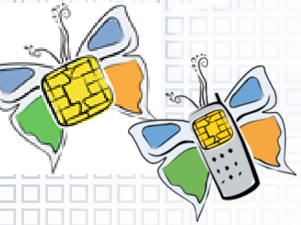
Contents

- The past: EU eID history
- The presence: Some MS eID
- The recent past: STORK
- The future: EU eIDAS eID federation



EU States’ eID projects

Early birds started late 1990’s early 2000



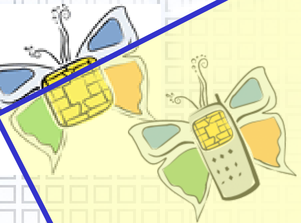
– Finish eID card:	December 1999
– Estonian eID card:	from January 2002
– Austrian citizen card:	from 2003, mass-rollouts 2005
– Italian CIE / CNS:	test phase 2003 (CIE)
– Belgian eID card:	from 2nd half 2003

EU States' eID projects

Early birds started late 1990's early 2000

- Finish eID card: December 1999

- Estonian eID card: from January 2002



- Austrian citizen card: from 2003, mass-rollouts 2005

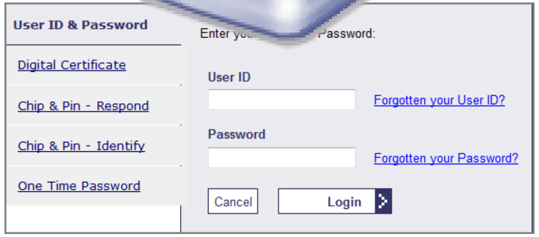
- Italian CIE / CNS: test phase 2003 (CIE)

- Belgian eID card: from 2nd half 2003

Evolved as national islands

Starting Point: National eIDs

- Heterogeneous in various dimensions
  - Technology
    - o Smartcards: AT, BE, DE, EE, ES, FI, IT, PT, SE, …..
    - o Mobile eID: AT, EE, FI, LU, NL, NO, …
    - o Soft certif.: ES, SE, SI, …
    - o usern./pass.: NL, UK, …
    - … STORK operated on some 100+ tokens
  - Operational
    - o Issued by public sector, private sector, combined
    - o Issued at federal, local, regional level
    - o Use of identifiers
  - Legal
    - o (limited) use of identifiers; flat, sectoral, combined
    - o (lacking) mutual recognition



User ID & Password

Digital Certificate

Chip & Pin - Respond

Chip & Pin - Identify

One Time Password

Enter yo… Password:

User ID

Forgotten your User ID?

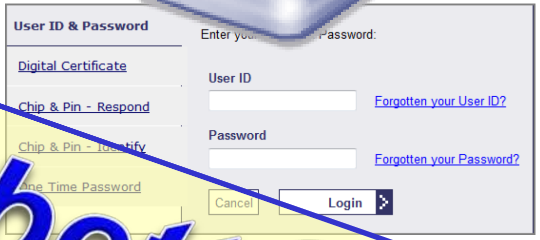
Password

Forgotten your Password?

Cancel Login

Starting Point: National eIDs

- Heterogeneous in various dimensions
  - Technology
    - o Smartcards: AT, BE, DE, EE, ES, FI, IT, PT, SE, …..
    - o Mobile eID: AT, EE, FI, LU, NL, NO, …
    - o Soft certif.: ES, SE, SI, …
    - o usern./pass.: NL, UK, …
    - … STORK operated on some 100+ tokens
  - Operational
    - o Issued by public sector, private sector, combined
    - o Issued at federal, local, regional level
    - o Use of identifiers
  - Legal
    - o (limited) use of identifiers, sectoral, combined
    - o (lacking) mutual recognition


User ID & Password

Digital Certificate

Chip & Pin - Respond

Chip & Pin - Identify

One Time Password

Enter your … Password:

User ID

Forgotten your User ID?

Password

Forgotten your Password?

Cancel

Login

Claim: None is the “better” system, they’re just different, each made to fit the national situation

Early signs of cross-EU eID

Manchester Ministerial Declaration *(Nov. 2005)*

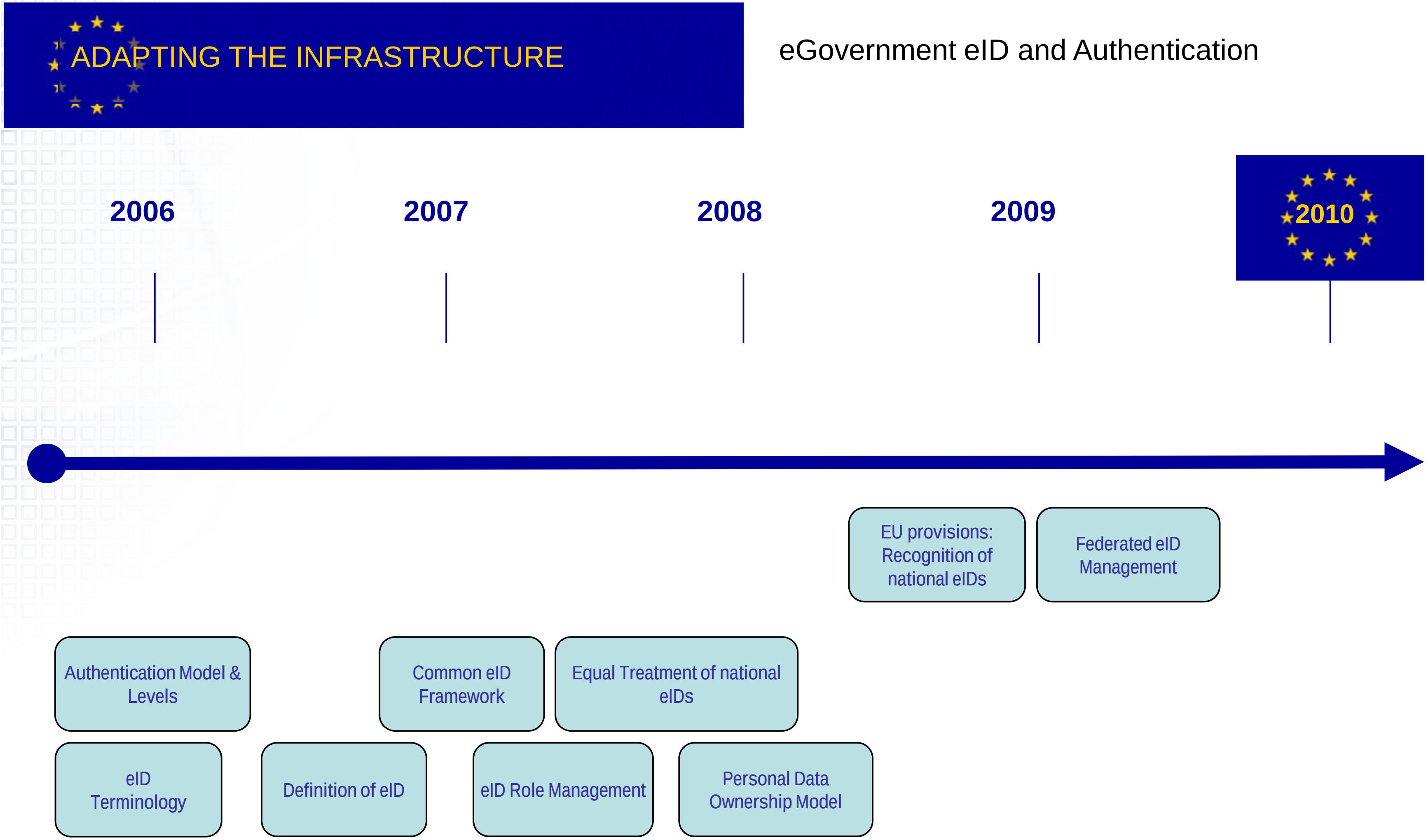
By 2010 European citizens and businesses shall be able to benefit from secure means of electronic identification that maximise user convenience while respecting data protection regulations.

Such means shall be made available under the responsibility of the Member States but recognised across the EU

History: eID ad-hoc group

(2004-2005)

… developed signposts with a roadmap



ADAPTING THE INFRASTRUCTURE

eGovernment eID and Authentication

2006

2007

2008

2009

2010

EU provisions: Recognition of national eIDs

Federated eID Management

Authentication Model & Levels

Common eID Framework

Equal Treatment of national eIDs

eID Terminology

Definition of eID

eID Role Management

Personal Data Ownership Model

SECTION 2: SOME MS EID

Major differences

- Member State core infrastructure differs
  - Conventional ID cards
    - Some MS have them, others don’t
    - Mandatory in several MS, voluntary in others
  - Persistent citizen identification numbers
    - Several MS have them, others don’t
  - Population registers
    - Several MS have them, others don’t
- Such aspects determine national eID choices
  - what token: amend ID card or use other means?
  - Issuer: public sector vs. private sector

Traditional identification

Existence and penetration of conventional ID often influenced choice of eID token

Determines backend processes (recognition, reconciliation)

Country	ID card (physical)	National identifier
Austria	non-compulsory	
Belgium	compulsory	
Estonia	compulsory	
Germany	compulsory	
Norway	non-compulsory	
United Kingdom	none	

eID Overview

Existence and penetration of conventional ID often influenced choice of eID token

Determines backend processes (recognition, reconciliation)

Country	ID card (physical)	National identifier	eID means
Austria	non-compulsory	Yes – sector-specific	Several *(voluntary)*
Belgium	compulsory	Yes – register number used across sectors	eID card (*obligatory*)
Estonia	compulsory	Yes – across sectors	eID card (*obligatory*) mobiil ID (*voluntary*)
Germany	compulsory	No – unconstitutional	nPA (*eID function voluntary*)
Norway	non-compulsory	Yes – across sectors	ID-porten – federation
United Kingdom	none	No	GOV.UK Verify – federation

Austria: Technologies

Smartcard

Bank cards

from 2005; ceased

Health insurance card

since 2005

Profession cards, service cards, …

e.g. notaries, lawyers, ministries, …

Mobile *(server-signature)*

A1 signature

service by a MNO

from 2005; ceased in 2008

limited success

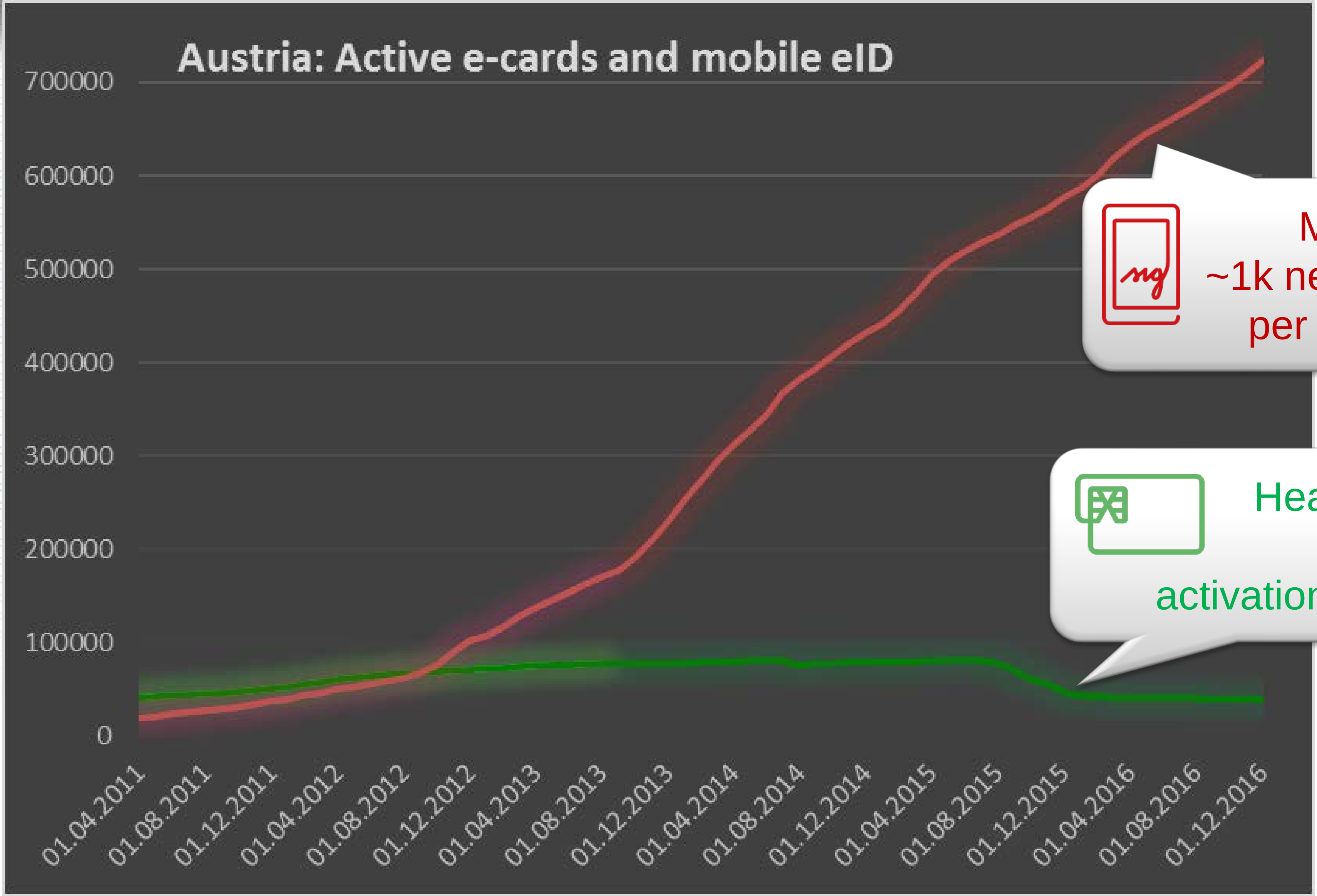
Mobile phone signature

Launched end 2009 through the LSP STORK

Contracted by gvmnt. to a private sector CSP

Success? Well, let's see ...

Austria: Card vs mobile ID active users

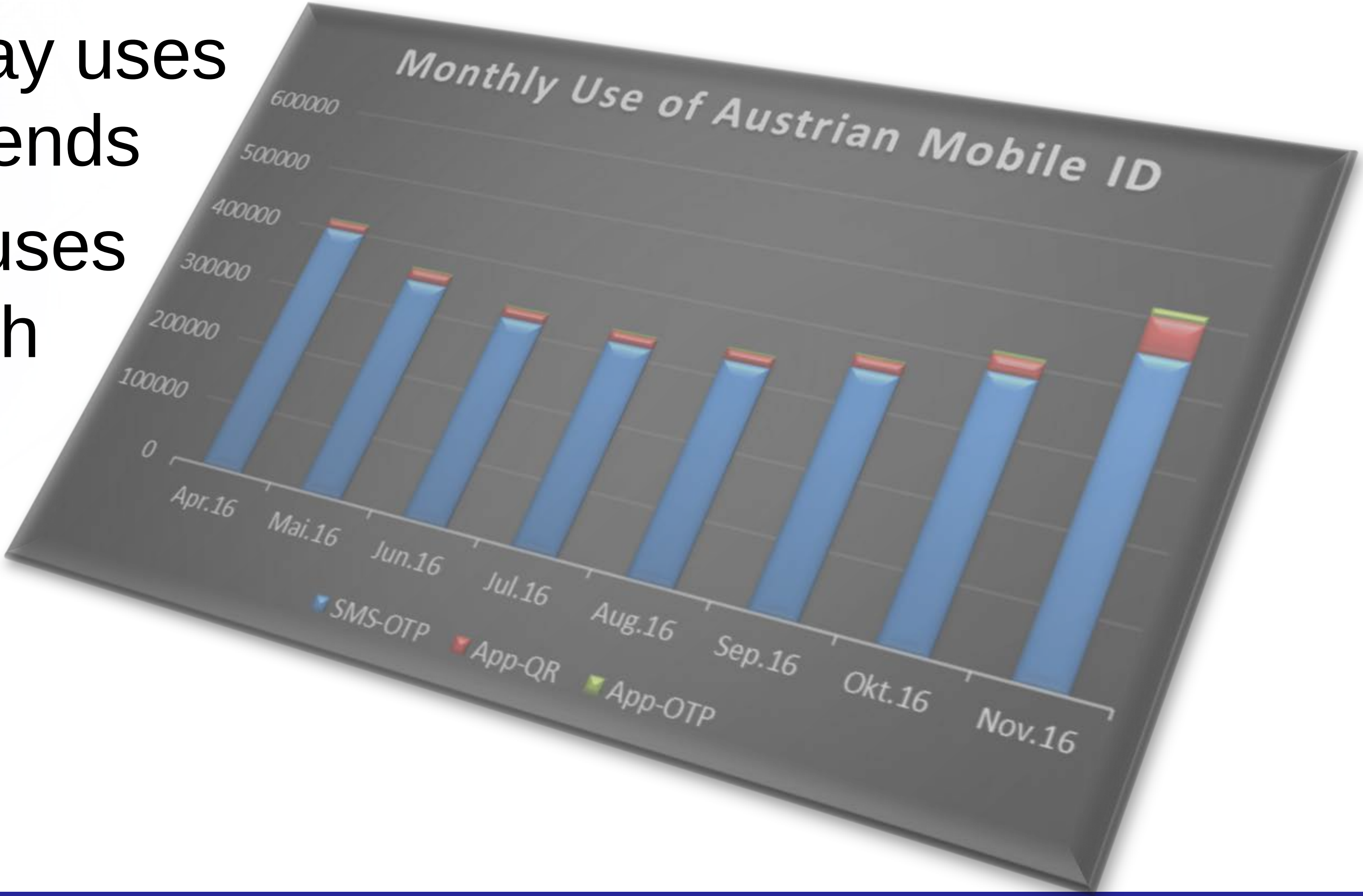


Mobile ID
~1k new users
per workday

Health card,
~1 k eID
activations/month

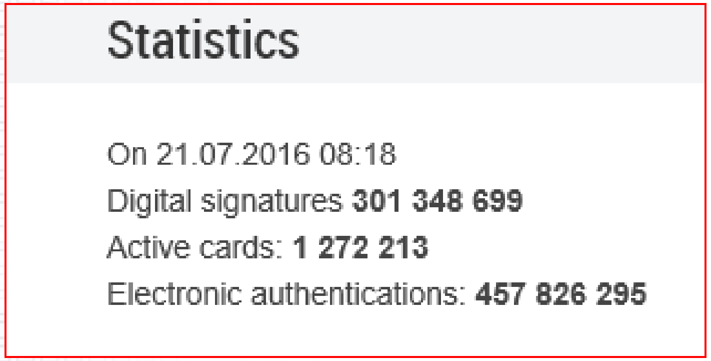
Austria: Actual usage … (mobile only)

- About 15-20 k/day uses on a typical working day
- ~4-6 k/day uses on weekends
- ~ 400 k uses per month
- 500 k in Nov.'16



Estonia

- Card eID introduced in 2002
  - 2015: ~100 mio. transactions



Statistics

On 21.07.2016 08:18

Digital signatures **301 348 699**

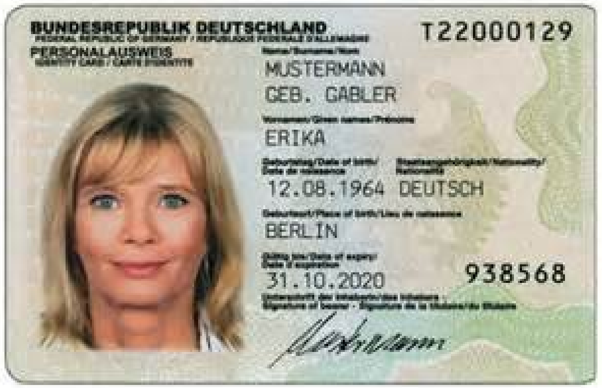
Active cards: **1 272 213**

Electronic authentications: **457 826 295**

- Mobile ID since 2007 (crypto-processor on SIM)
  - Less than 10 % of ID card owners (growing fast)
  - 2015: ~25 mio. transactions

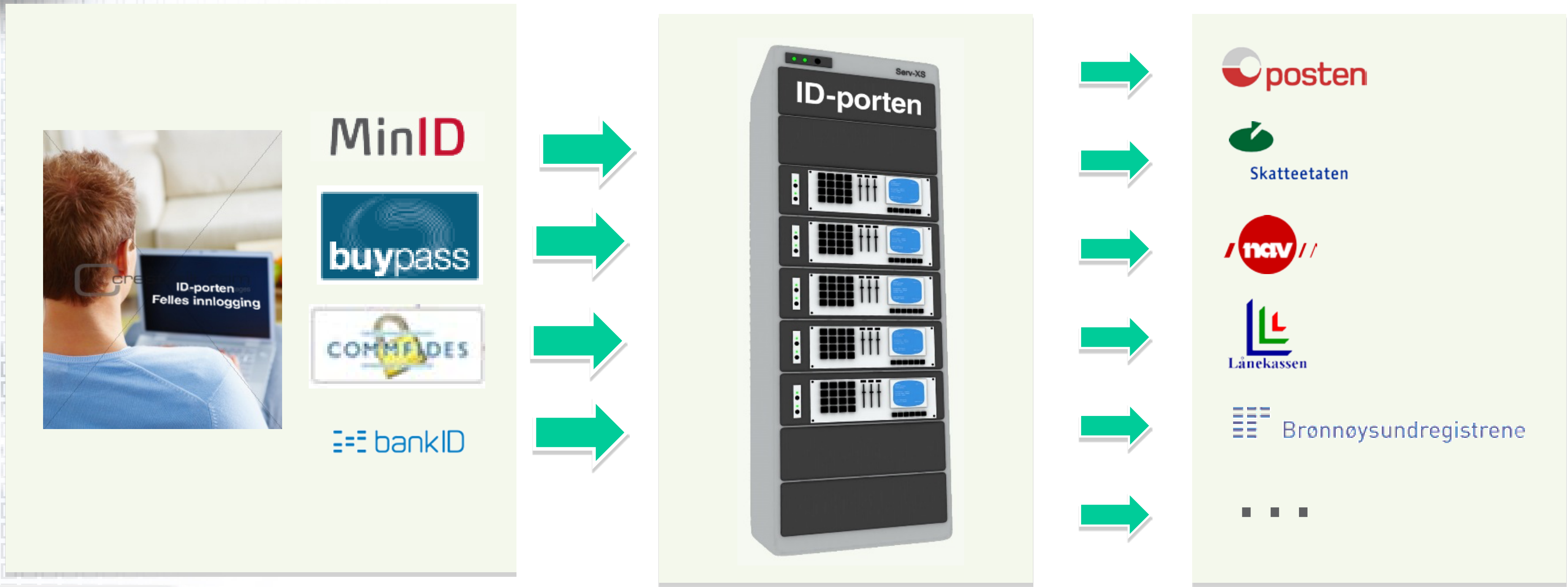
Germany

- nPA introduced in 2010
- All ID cards issued since can be enabled an "eID function" (voluntary)
  - About 1/3 of holders do so
- Some technical specifics
  - Contactless chip
  - Card-verified access certificate for relying parties
    - Minimum disclosure
    - Application specific identifiers; non-persistent (card-specific)



BUNDESREPUBLIK DEUTSCHLAND
T22000129
PERSONALAUSWEIS
MUSTERMANN
GEB. GABLER
ERIKA
12.08.1964 DEUTSCH
BERLIN
31.10.2020 938568

Norway



Nasjonalt ID-kort

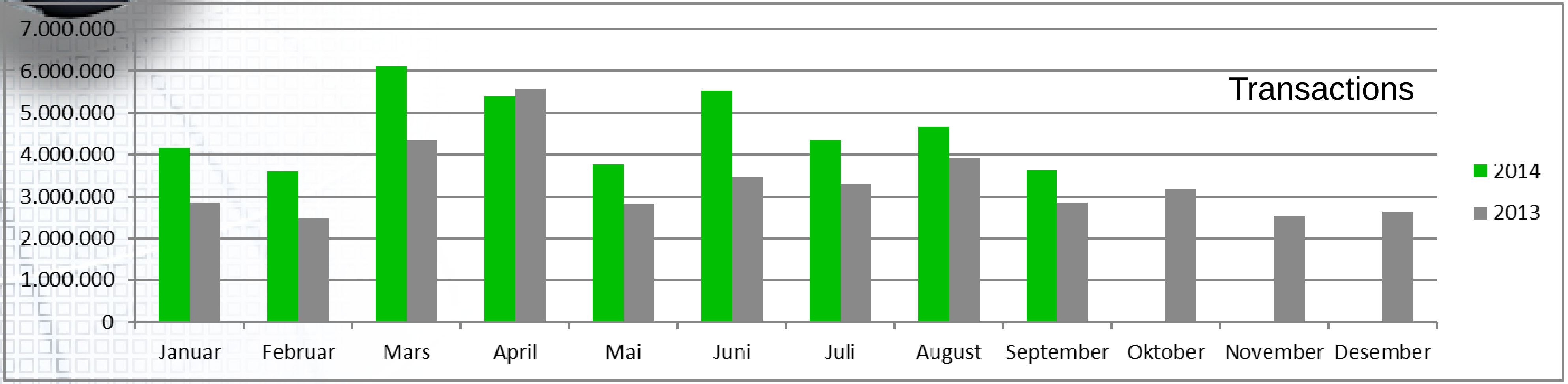
National ID-card with eID is planned for 2018

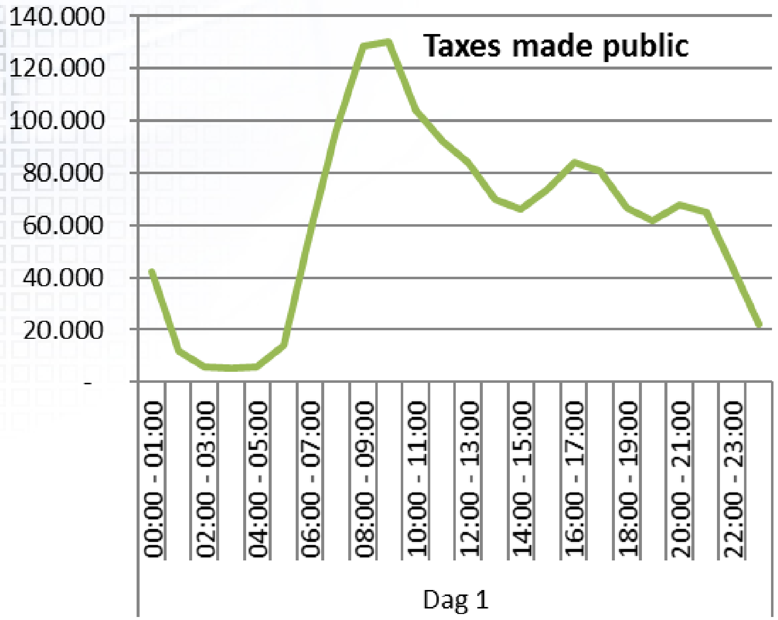
ID-porten authentication portal.
50 mill transactions in 2014

About 660 services from about 300 (?) public agencies

Source: Tor Alvik, Difi (Direktoratet for forvaltning og IKT)
see also https://www.youtube.com/watch?v=n3n4dqhIfEE

Norway: Facts and numbers

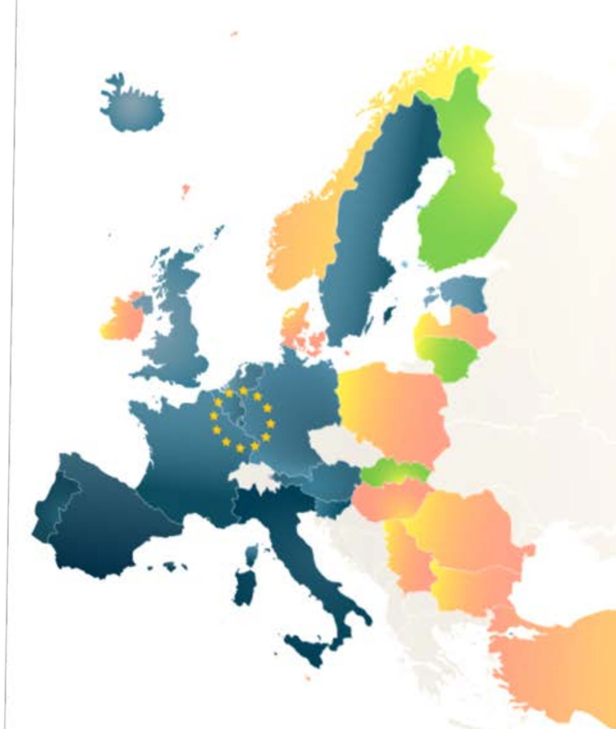




Source: Tor Alvik, Difi (Direktoratet for forvaltning og IKT)
see also https://www.youtube.com/watch?v=n3n4dqhIfEE

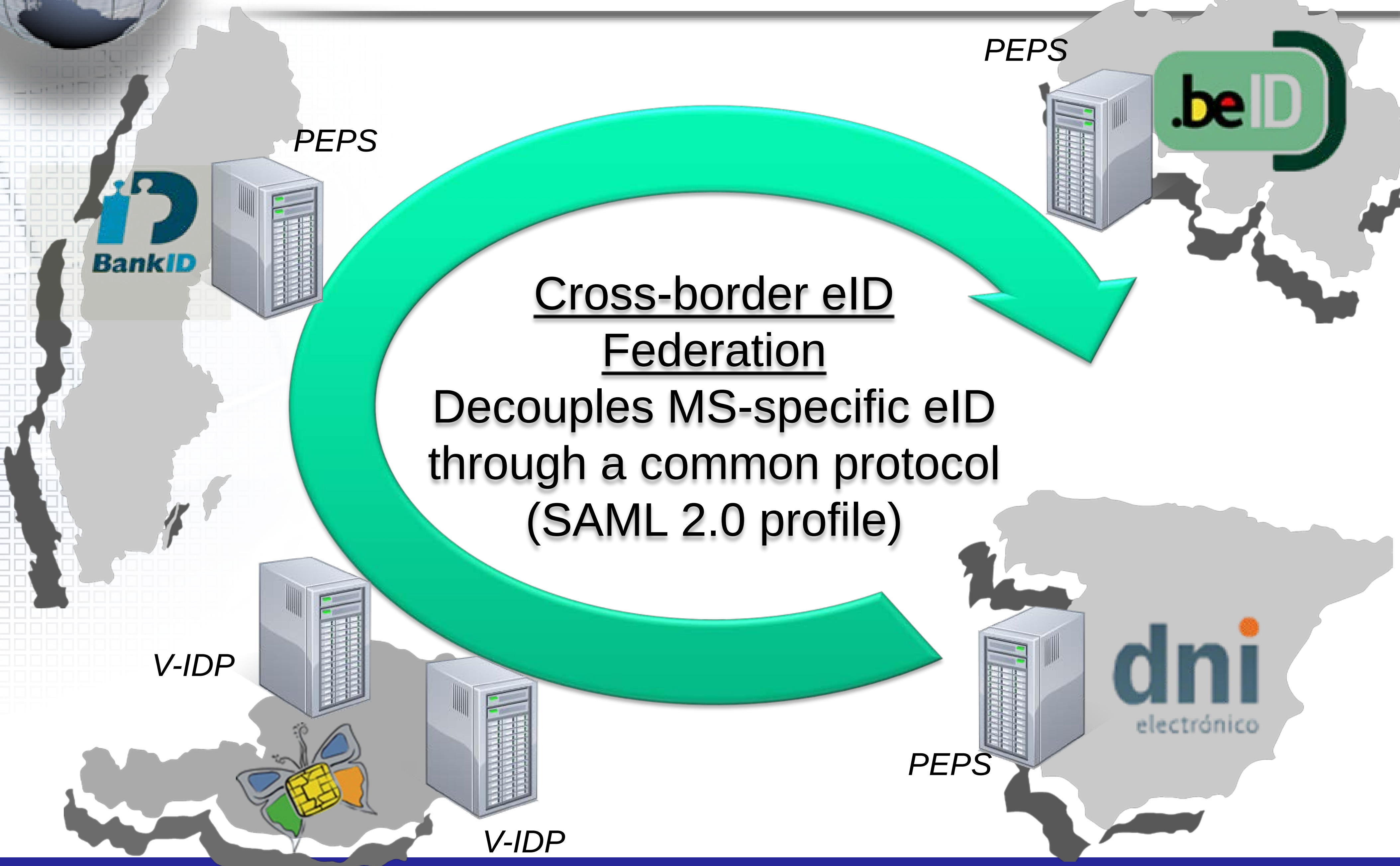
SECTION 3: STORK

STORK Key-facts



- Project than ran from 2008-2011
  - Successor STORK 2.0 until 2015
- National eID federation between
  - 18 MS
  - 100+ national eID token types
  - 6 pilots in production systems
- Resulted in
  - Open specifications (SAML 2 + QAA)
  - Open source reference implementations
  - Lessons learned as basis for EU legislation (eIDAS)

Architecture Overview



Cross-border eID Federation

Decouples MS-specific eID through a common protocol (SAML 2.0 profile)

STORK pilots

- Six pilots live as “pioneering applications”
  - Online authentication

    🇩🇪 🇦🇹 🇧🇪 🇪🇪 🇫🇮 🇮🇸 🇱🇹 🇵🇹 🇪🇸
  - Safer Chat

    🇮🇸 🇦🇹 🇸🇰
  - Student Mobility

    🇪🇸 🇦🇹 🇪🇪 🇮🇹 🇵🇹
  - eDelivery

    🇦🇹 🇪🇪 🇫🇮 🇱🇺 🇸🇮 🇩🇪 Affiliate
  - Change of Address

    🇵🇹 🇪🇪 🇮🇸 🇫🇮 🇪🇸 🇸🇮 🇸🇪
  - ECAS

    🇦🇹 🇧🇪 🇪🇪 🇩🇪 🇫🇷 🇮🇸 🇮🇹 🇱🇹 🇱🇺 🇵🇹 🇸🇮 🇪🇸 🇸🇪 🇬🇧

Lessons Learned

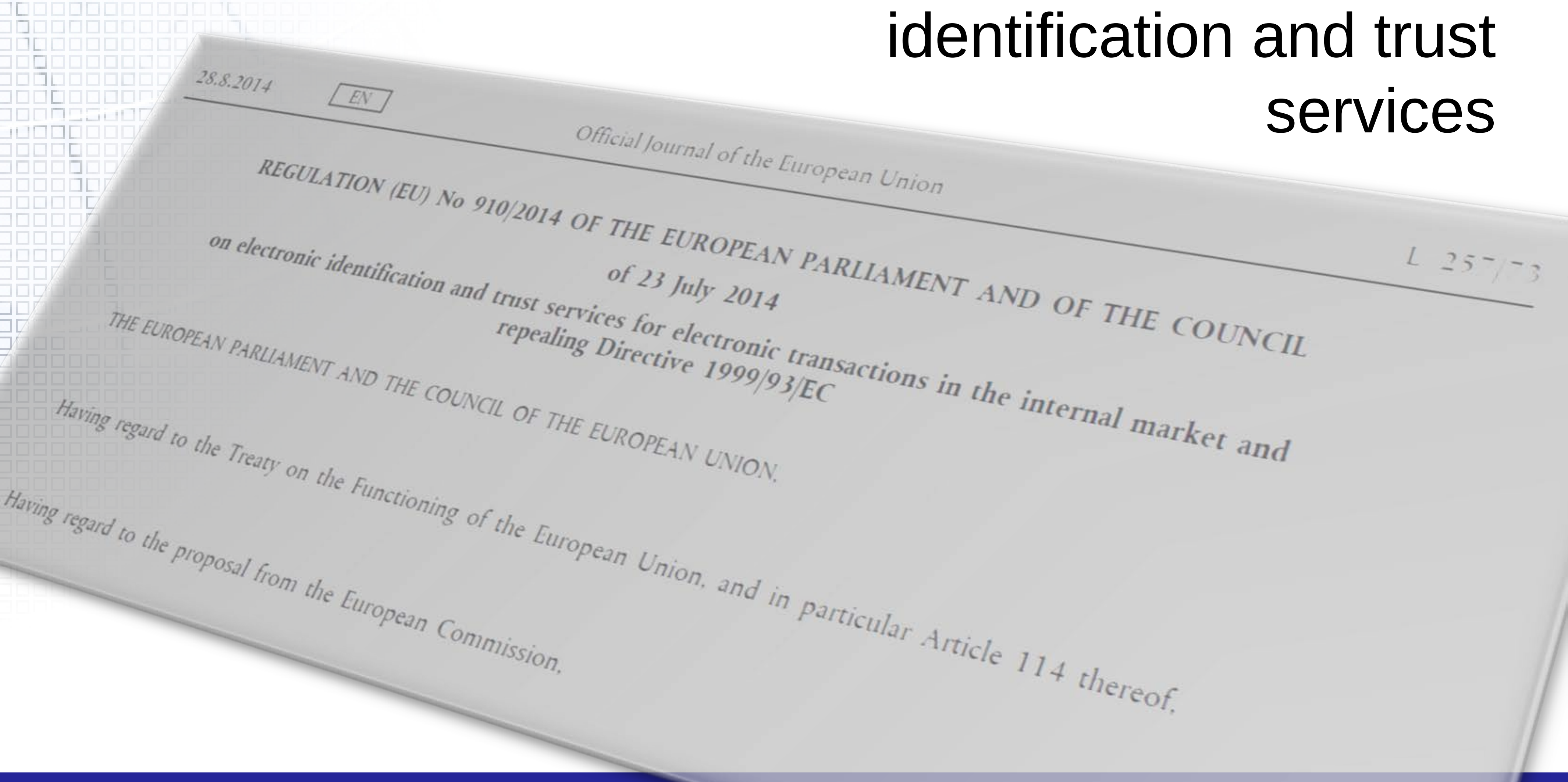
On cross-border eID federation we found …

- Technical issues are minor
  - e.g. integration with legacy systems
  - e.g. standardization / lacking standards
- Operational issues are **relevant**
  - needs governance
  - needs support and maintenance
  - needs getting the message to IdPs and SPs
- Legal issues are **key**
  - Data Protection
  - Liability
  - Mutual recognition

SECTION 4: EIDAS

Recent policy development

- eIDAS: Regulation on electronic identification and trust services



28.8.2014 EN Official Journal of the European Union L 257/73

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

Signature Directive vs. eIDAS Regulation

- The Signature Directive was enacted in 1999
  - Transposed to national laws (Austrian Signature Act)
- The eIDAS Regulation was enacted in July 2014
  - A Regulation applies directly (no national laws)
- Covers “eID” and “trust services” / “trust service providers”
  - mutual recognition of *notified* eID
  - electronic signatures
  - electronic seals
  - eDocument admissibility
  - Website authentication
  - electronic delivery

Two main parts of eIDAS

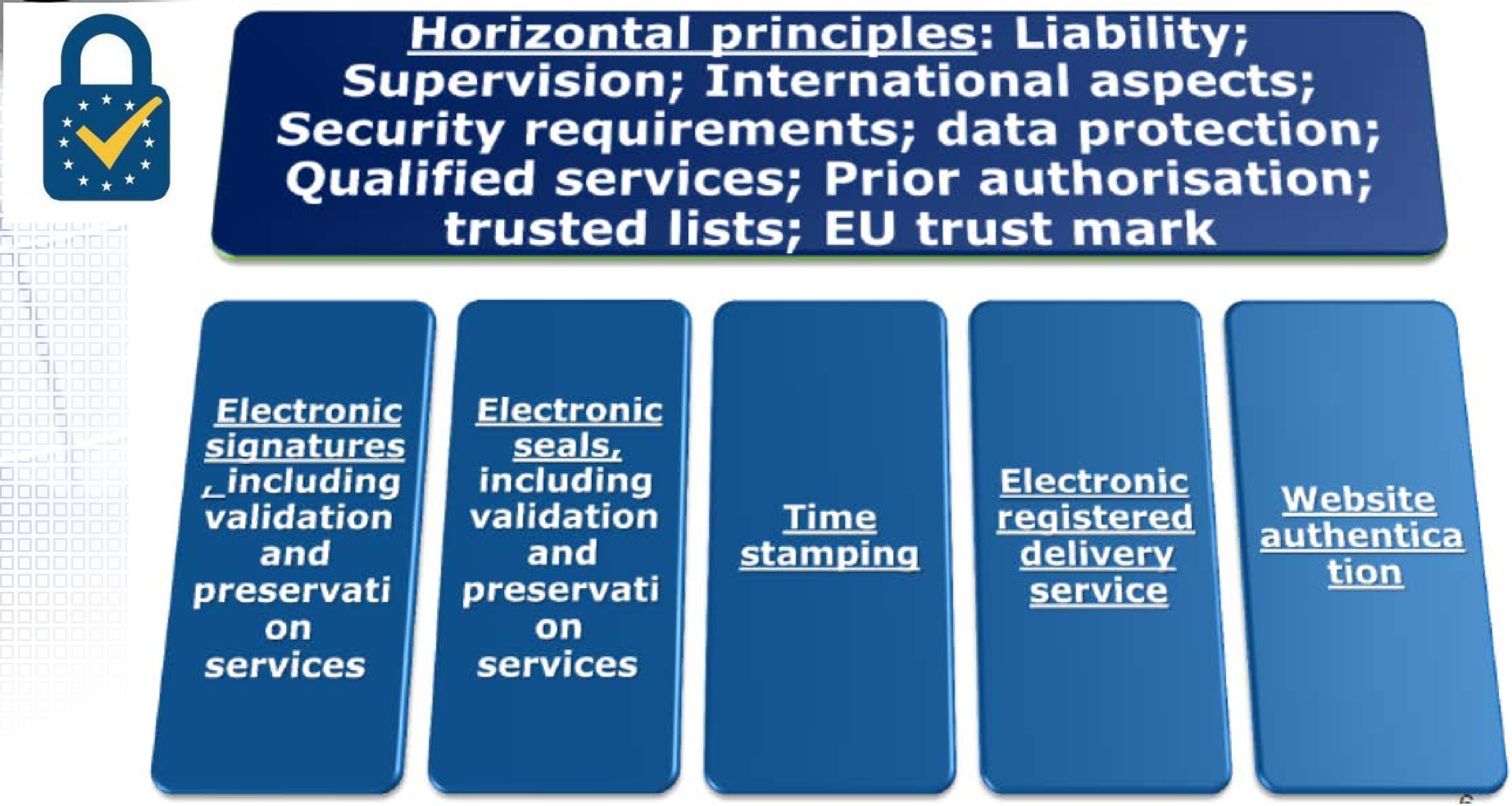
- eID
  - Notification, Recognition, Coordination

MS sovereignty, but recognition obligation
(Coordination on interoperability and security)

- Trust services
  - electronic signatures
  - electronic seals
  - validation, preservation
  - electronic timestamps
  - el. registered delivery
  - website authentication

Harmonisation (Supervision, Liability, Recognition, Formats, Trust Lists, …)

eIDAS Trust Services

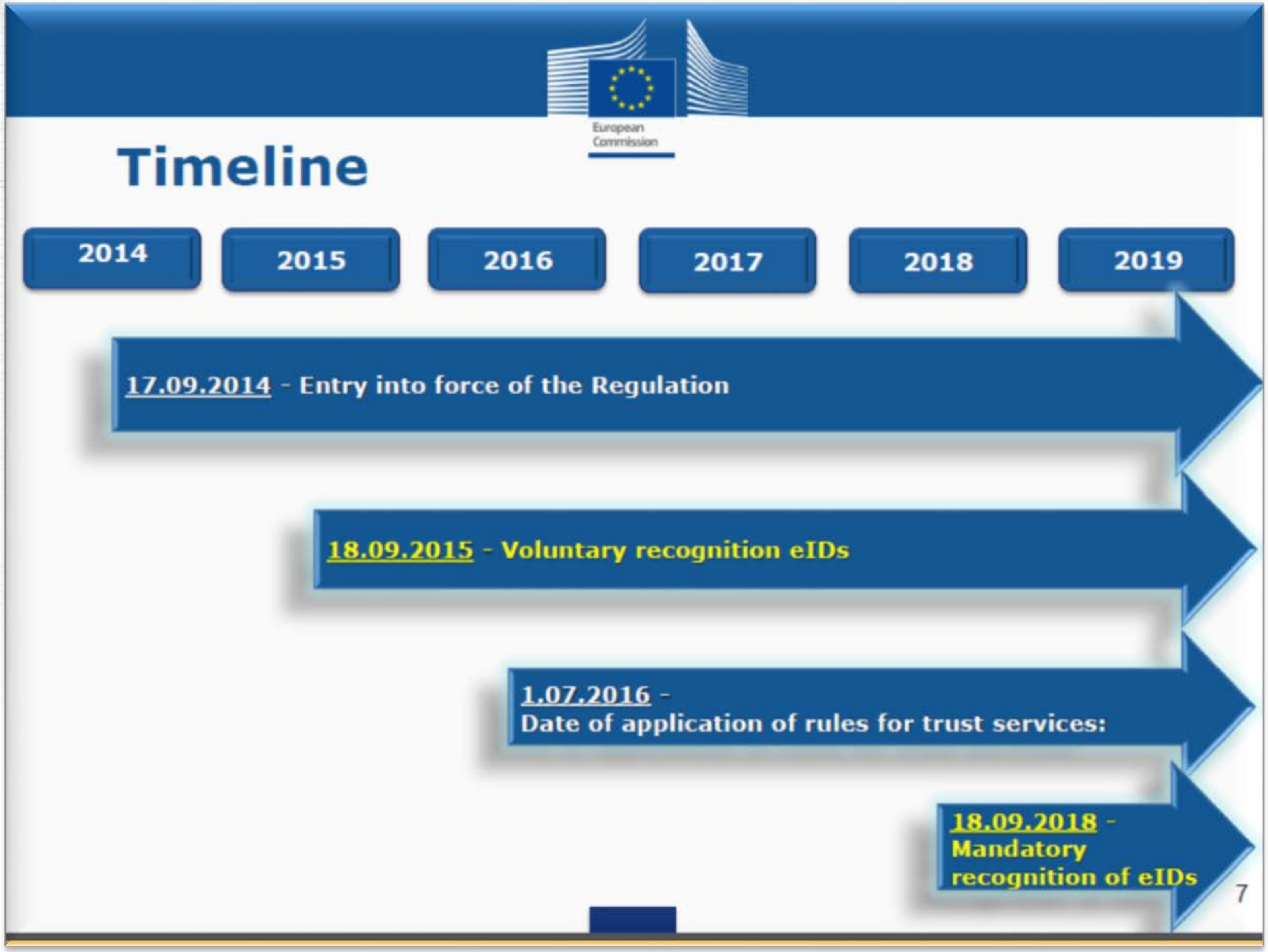


Horizontal principles: Liability; Supervision; International aspects; Security requirements; data protection; Qualified services; Prior authorisation; trusted lists; EU trust mark

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

Source: Andrea Servida (European Commission), Mobile eID Forum, 29 April 2015

eIDAS eID Timeline



European Commission

Timeline

2014 | 2015 | 2016 | 2017 | 2018 | 2019

17.09.2014 - Entry into force of the Regulation

18.09.2015 - Voluntary recognition eIDs

1.07.2016 -
Date of application of rules for trust services:

18.09.2018 -
Mandatory
recognition of eIDs

7

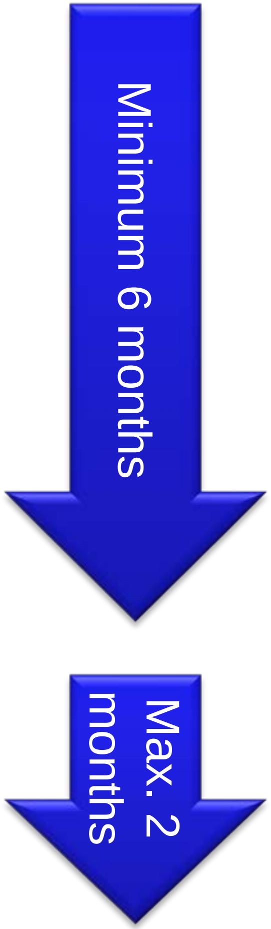
Source: Andrea Servida (European Commission), Mobile eID Forum, 29 April 2015

eIDAS eID Key Principles

- Based on “notified eID”
  - Member State decides, if/what eID scheme to notify
  - 3 Levels of Assurance (LoA) “high”, “substantial”, “low”
- Recognition of notified eID
  - Mandatory for public services LoA “high” & “substantial”
  - Voluntary for private services
- Interoperability and cooperation of MS
  - Based on STORK
- Implementing acts on …
  - LoA, Interoperability Framework, Cooperation, …

eIDAS eID Notification Process

1. MS pre-notification
   - MS describe eID scheme(s) and their LoA
   - Show how LoA requirements are met
2. Peer Review
   - Other MS assess the eID scheme(s)
   - Cooperation Network opinion (non-binding)
3. MS Notification
4. Publication by EC



Minimum 6 months

Max. 2 months

On Recognitions

- All MS have to recognise all notified eIDs at LoA substantial or high in all public services
  - If the service is eID enabled
  - even if the MS does not notify its own eID
- MS voluntarily can accept LoA low
- Authentication is free of charge for public services
- Private sector use is encouraged, but no obligation
- Notifying MS may set conditions for private sector use

Thank you for your attention

Contact:

Herbert Leitold

Phone: +43 316 8735521

Email: Herbert.Leitold@a-sit.at