



GOBIERNO
DE ESPAÑA

MINISTERIO
DE INDUSTRIA, ENERGÍA
Y TURISMO

eIDAS implementation, 6 months later. Vision of the Spanish SB

19/12/2016

Rafael Pérez Galindo
rperezga@minetad.es

S.G. de Servicios de la Sociedad de la Información
Secretaría de Estado para la Sociedad de la Información y la Agenda Digital

Competences

- 1. eID and TS regulation**
- 2. TSP supervision**
- 3. TSL building**

Actions regarding eIDAS application

1. **TSP supervision:** prior authorisation for QTSP but light touch approach to non-Q (art. 17)
2. **Guide on initiation** (art. 21) including structure and minimum information required in the **CAR**:
<http://www.minetad.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Documents/GuiaNotificacion.pdf>
3. **TSL** (art. 22) adaptation to CID 2015/1505
4. **Web info** service adaptation to eIDAS services
5. **Communication** to COM: SB, TSLO, eID PoSC, certification body.
6. Forthcoming **notification** of Spanish national **eID scheme** (DNle)
7. **New Law on electronic services**

Transitional issues (I)

1. **Qualified eSeal certificates** available in Spain for Public Administration since 2007 ➡ turned to *non-Q* as of 1 July 2016 until Q status granted in the TL.
2. **Qualified Legal person certificates** available in Spain since 2003 ➡ turned to *non-Q* as of 1 July 2016.
3. **Transitional measure** art. 51.3 applies **only** to former CSP issuing Qc for eSig ➡ Distinguish QTSP from QTS/non-QTS they provide.

Transitional issues (II)

4. **Lack of standards** for eDelivery misguided TSP into believing Q was not possible.
5. **Standards are not mandatory**, but only a presumption of compliance with the R.
6. Confusion about relationship between **eID** schemes and QTS.

Transitional issues (and III)

7. 9 and only 9 QTS are regulated in eIDAS:

- ❖ Qualified certificate for electronic signature (Art. 28)
- ❖ Qualified certificate for electronic seal (Art. 38)
- ❖ Qualified certificate for website authentication (Art. 45)
- ❖ Qualified validation service for qualified electronic signatures (Art. 33)
- ❖ Qualified validation service for qualified electronic seals (Art. 40)
- ❖ Qualified preservation service for qualified electronic signatures (Art. 34)
- ❖ Qualified preservation service for qualified electronic seals (Art. 40)
- ❖ Qualified electronic time stamps (Art. 42)
- ❖ Qualified electronic registered delivery services (Art. 44)

8. SS CD as QSCD □ What about server signing?

National Law adaptation to eIDAS

- As of 1 July 2016, any disposition laid down in Law 59/2003 opposing eIDAS renders **inapplicable**
- Preliminary assessment of impact and consultation underway
- A new “**Law on Electronic Trust Services**” is under development, repealing Law 59/2003 on electronic signatures
- Aspects that eIDAS leaves to **national legislation**, a.o.:
 - **Legal effects** of qualified trust services
 - **New QTS** defined at national level (recital 25)
 - **Penalties** (art. 16)
 - **Identity verification** (art. 24.1)
 - **Financial resources or liability insurances** (art. 24.2.c)
 - Certificate **suspension** (art. 28.5 and 38.5)
 - National rules on **liability** (art. 13.3)
- Dispositions to be ruled out, i.a. **eSig Qc for legal person**

Issues under discussion (I)

1. Art. **19.4** Security requirements applicable to all TSP: priority implementing act.

2. Art. **20.4** Rules applying to conformity assessment bodies accreditation and conformity assessment report, as well as auditing rules: priority implementing act.

3. Art. **24.1.d)**: other identification methods recognized at national level which provide equivalent assurance in terms of reliability to physical presence.

The equivalent assurance shall be confirmed by a CAB.
Under what rules or standards or procedures?

Issues under discussion (II)

4. Server signing: QSCD certification and sole control

- eIDAS recital 52): *“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.”*
- CID 2015/650 recital 6) delay in CEN standards: 419241-1 final version approved on 8th Dec 2016!
- Art. 30.3.a) and b): alternative procedure notified to COM
- eIDAS Art. 3(12): AdES + Qc + QSCD = QES \square guarantee of sole control required!
- Interpretation of art. 3(16): RAdESCaaS

Issues under discussion (and III)

5. **Secure cryptographic algorithms**

key lengths and hash functions applicable to trustworthy systems and products (art. 24.5 eIDAS/rec. 8 CID2015/650)

6. **Non-Q providers and services**

Legal regime: no prior authorization, only reactive supervision. Voluntary communication?

Listing in national information service and/or TL?

7. **TSP financial stability and insurance coverage:**

harmonized EU approach advisable. Differences among supervisory regimes at national level should be avoided.