



GOBIERNO
DE ESPAÑA

MINISTERIO
DE POLÍTICA TERRITORIAL
Y FUNCIÓN PÚBLICA



Sharing & Reuse Conference

11 June 2019 - Bucharest, Romania



e-Certificate and e-Signature Validation Platform

Simplifying the implementation of e-Services



Santiago Graña Domínguez
General Secretariat of Digital Administration



The origins...

- The electronic certificates based on **public key infrastructure** are the most used mechanism in Spain for the identification and electronic signature in the **Public Administrations**, way ahead of the use of concerted keys with upfront registration.
- **Very dynamic market of Certificate Authorities:** 29 CAs published by the Ministry of Industry that issue Qualified Certificates according to eIDAS Regulation.
- Since 2006, the **National Identity Card (DNle)**. Currently **+30 million cards**) has been issued.
- The number of electronic certificates issued by national CAs is very high (+ than 100 types).





The origins...

CAs: A mature and complex scenario

- Existence of public and private CAs.
- Issuance of certificates in software support or in smart-card (that produce both non qualified or qualified signature).
- Types of certificates: individual, legal entity representative, electronic stamp, time stamp, website identification, ...
- Some certificates are issued to professional members (notaries, lawyers ...)



The origins...

Public CA

- **FNMT**: 2M+ certificates issued
- **DGP**: DNle: 30M+ cards issued and in a few years will cover 100% of the elderly
- **CAs of Regional Governments**: Catalonia (Catcert), Basque Country (Izenpe) and Valencia (GVA) Types of certificates: individual, legal entity representative, electronic stamp, time stamp, website identification, ...

Private CA

- Mainly oriented to Professional Collectives: Lawyers, Chambers of Commerce, Notaries ...





The origins... Regulation

Article 21.3 of Law 11/2007, of June 22, on electronic access of citizens to Public Services.

- 3. The General State Administration will have, at least, a platform to verify the status of revocation of all certificates admitted in the field of Public Administrations that will be freely accessible by all the Departments and Administrations.



What is your solution about?

@firma provides the following services:

1. Electronic Certificate Validation

- **26** Spanish Trust Service Providers
- **169** Trust Service Providers in rest of Europe, via Trust Service List (TSL) validation



2. Electronic Signature Validation

- European approved standards and formats



3. Electronic Signature Upgrades

- Upgrades to Long Term Validation formats



4. Electronic Signature Creation





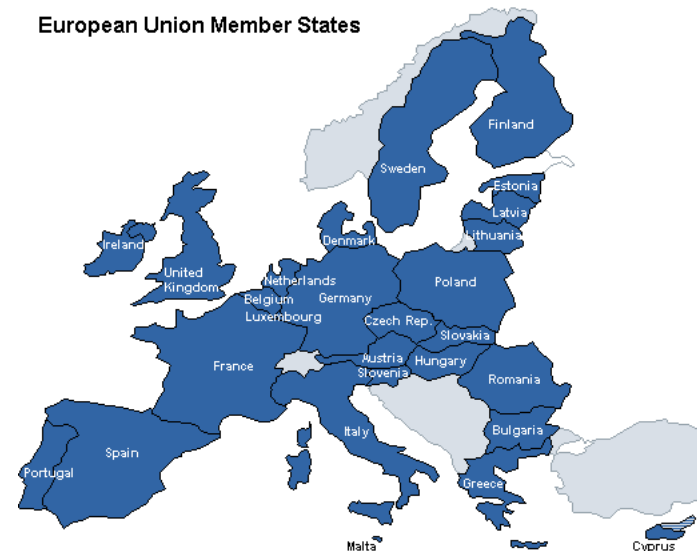
Current Regulation

REGULATION (EU) 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [eIDAS].

Ensure that individuals and companies can use their national and international signatures and identities across borders to access at least public services in other EU countries



European Union Member States





Identification and signature regulations applicable in Spain

EUROPEAN REGULATION AND STANDARDS

- Regulation 910/2014. eIDAS
- eIDAS Nodes.
- IMPLEMENTING DECISION (EU) 2015/1506. Signature formats.
- IMPLEMENTING DECISION (EU) 2015/1505. TSL

SPANISH REGULATION

- Law 39/2015 of Administrative Procedure
- Law 40/2015 of the Legal Regime
- Royal Decree 4/2010 of the National Interoperability Scheme.
- NTI of Signing Policy
- Draft Law Regulating Electronic Services Trust
- Draft Royal Decree by which Law 39/2015 is developed, and Law 40/2015



eIDAS Regulation

Types of signatures:

- Signature - of natural persons.
- Seal - of legal entities. To guarantee the origin and integrity of the data.



Levels (TSL):

- With non qualified certificates.
- With certified certificates.
- With qualified certificates and in a secure device.



Electronic certificates do not have to carry full identification data.



Cross-border recognition of signatures

Advanced signature required. It must be admitted:

Advanced
Signature

Advanced
Signature with
qualified
certificate

Qualified
Signature

Advanced signature with qualified certificate
required. It must be admitted: :

Advanced
Signature with
qualified
certificate

Qualified
Signature

Qualified Signature required (max). It
must be admitted:

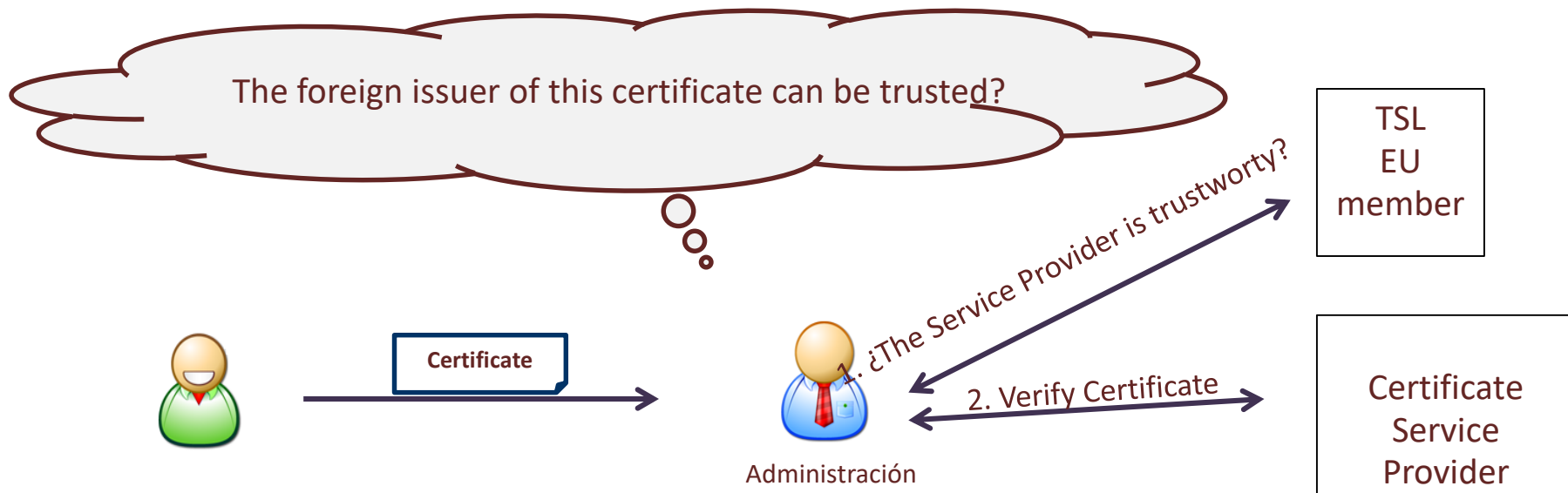
Qualified Signature



Trust Service Lists

Ministry of Industry as supervisor

- Information relating to qualified trust service providers
- <https://www.mincotur.gob.es/telecomunicaciones/es-es/Servicios/FirmaElectronica/Paginas/Prestadores.aspx>

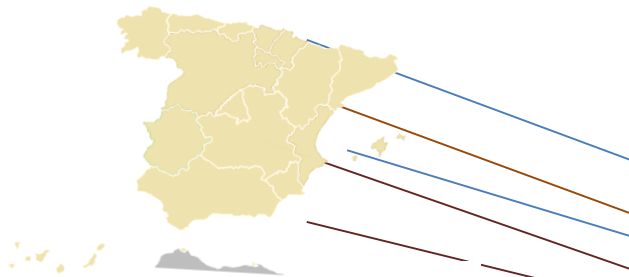




Which issue does your solution address?

Simplifies the validation of digital certificates and signatures, hiding the connection to an array of Trust Service Providers, speeding up the provision of electronic Services by Public Admins

26 National TSP's



+ 169 European TSP's



No coding required
(parameterized based configuration)

Public Administrations

17 x
National Ministries

1.000 x
Public Entities

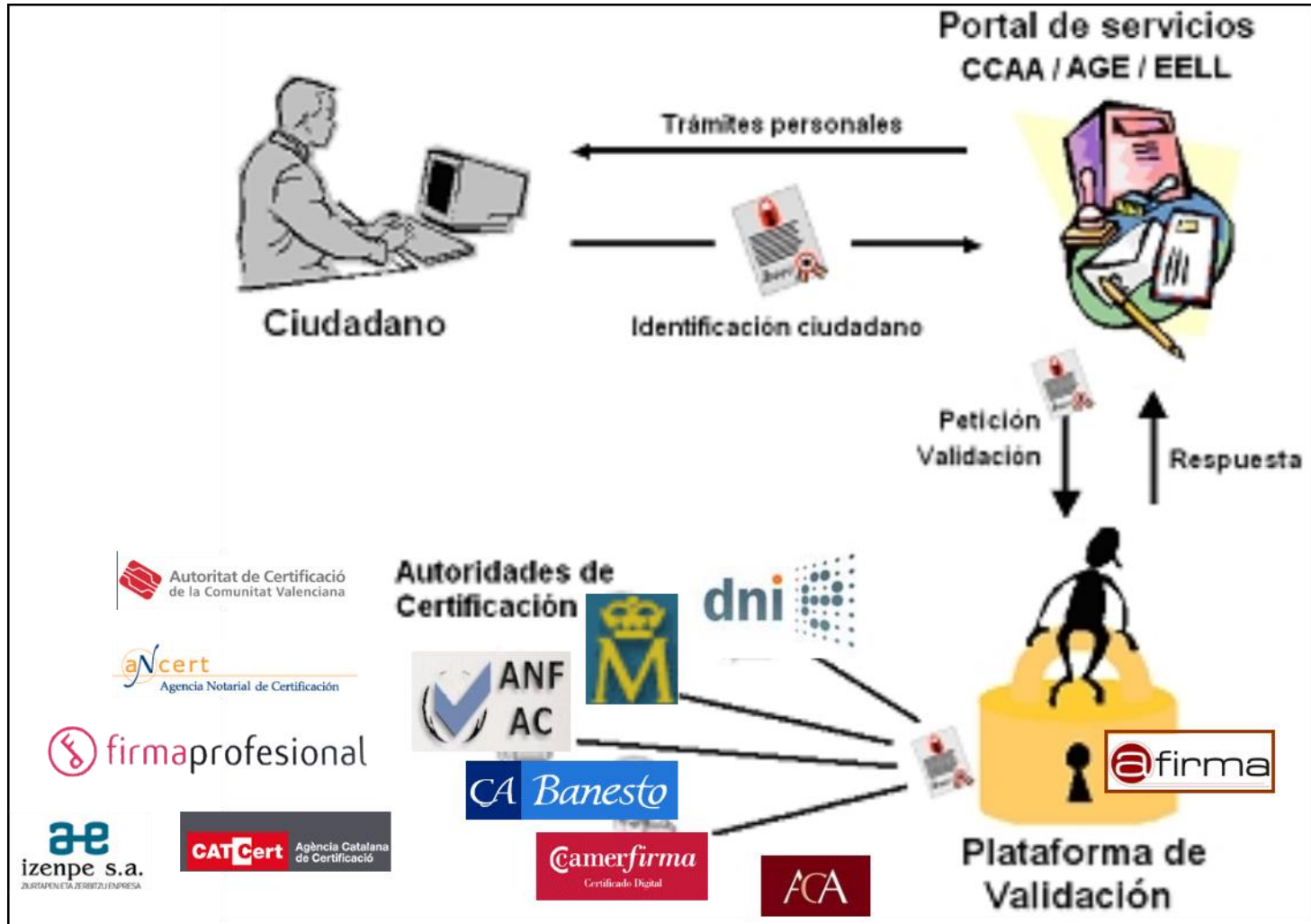
100 x
Public Agencies

17x Regional Administrations

8.100 x
Municipalities



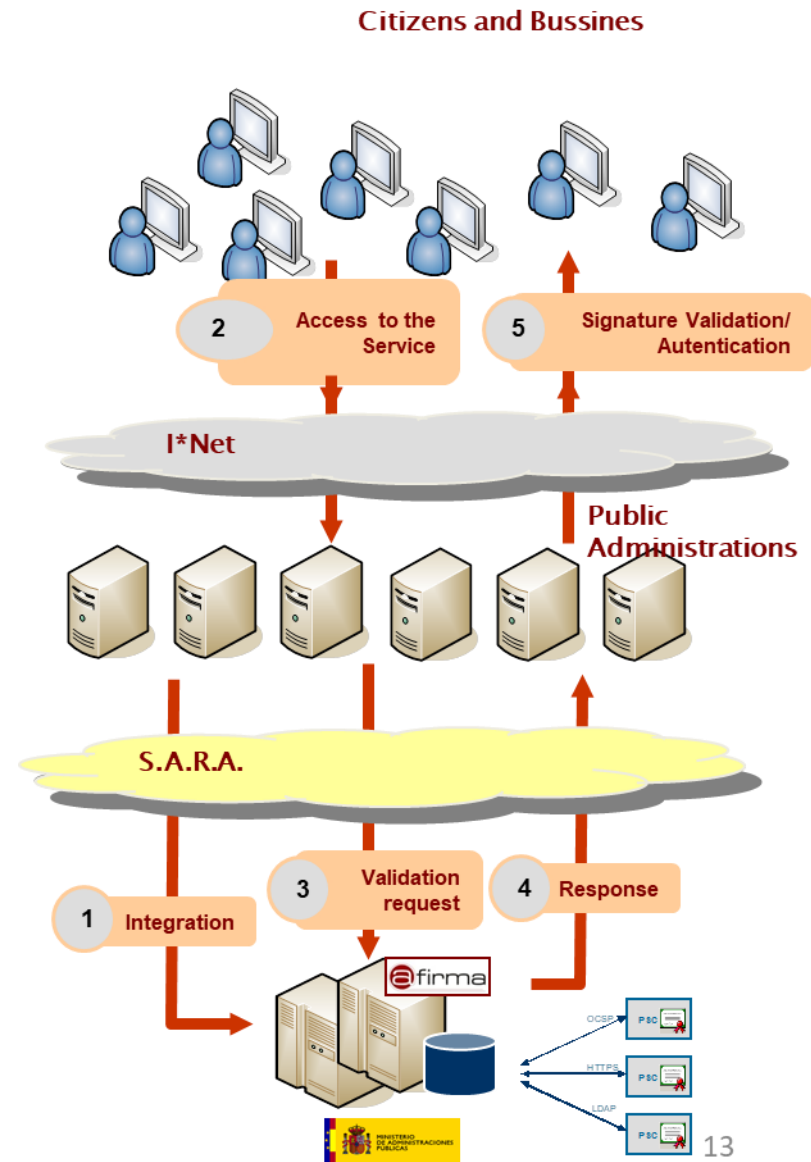
How validation services are used





Service model

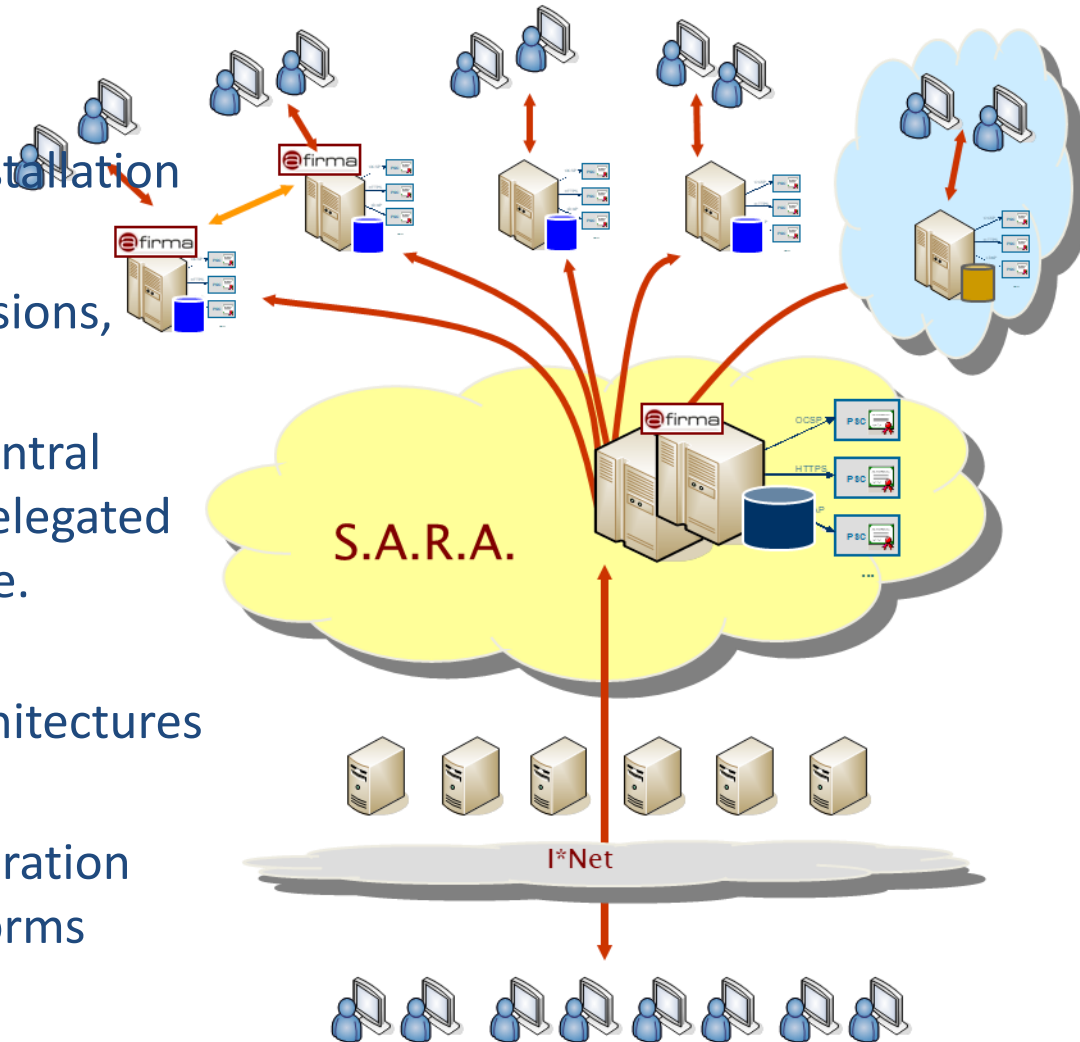
- Access to services through S.A.R.A.
- CAU available to support integration and testing.
- Advantages:
 - Reduction of costs and investments: development, support, infrastructure, ...
 - Complexity reduction:
 - Independence from certification service providers (OCSP, HTTP, LDAP).
 - Independence from electronic signature complexity: XAdES, CAdES, PAdES ...
 - Fast implementation of changes and new services
 - Interoperability





Service model - distributed

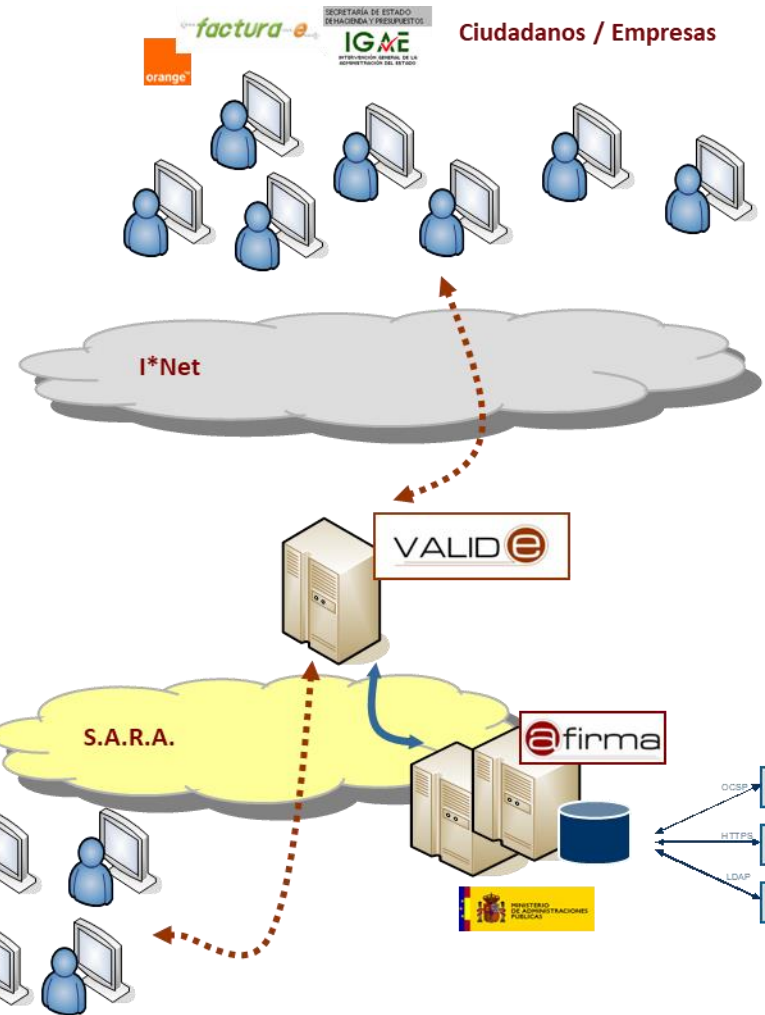
- @Firma is distributed for installation in public Administrations
- Free distribution of new versions, patches, etc.
- The configuration of the "Central Server" is exported to the delegated implementations. Coherence.
- Permits adaptation to the performance needs and architectures of each Organization.
- Possibility of backup configuration between the different Platforms





VALIDE

- Online service validation of signatures and certificates
- 18 national and 4 international providers
- Available services:
 - Validate certificate
 - Validate Electronic Office
 - Validate signature and view document
 - Signing





How is @firma used and reused?

1. Common Service (as of 2018)

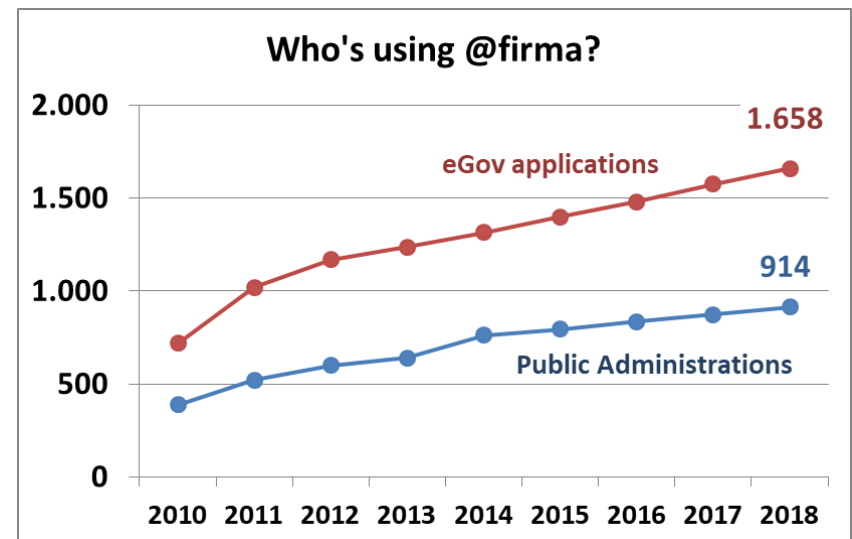
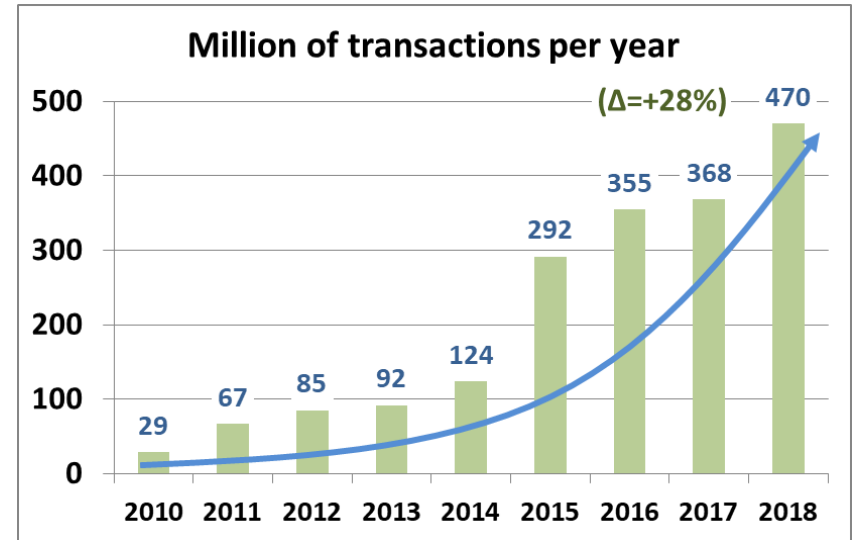
- 470M+ transactions
- 1.600+ eGov applications

2. Dedicated instances (reutilization)

- 25+ deployments across Spanish Administrations
- Increases performance for high demanding Organisations

3. Open source (since feb'19)

- Published under EUPL





Next steps...

Mature solution, focused on high availability / high performance

- Expected to **increase usage 4-fold** in 3 years
- Continue implementing and adopting **European Standards for eCertificates and eSignatures**





GOBIERNO
DE ESPAÑA

MINISTERIO
DE POLÍTICA TERRITORIAL
Y FUNCIÓN PÚBLICA



Sharing & Reuse Conference

11 June 2019 - Bucharest, Romania



Thank you

santiago.grana@correo.gob.es

General Secretariat of Digital Administration

Spanish e-Government Strategy Information Website

<http://administracionelectronica.gob.es>