Ministry
of Digital Affairs

Expert Group Meeting
on
THE BEST PRACTICES IN IMPLEMENTATION OF MOBILE IDENTIFICATION (mID)

18-19 October 2016
Warsaw, Poland
Ministry of Digital Affairs

Ministry
of Digital Affairs

PRESENTATION GUIDELINES:

- Each expert is asked to prepare ONE presentation (PowerPoint) comprising information on all 6 sessions.
- Each expert is given 10 minutes in a given session to present questions related to each sessions. After, presentation in each session will be followed by a discussion among all invitees.
- Keeping the above in mind, the experts can put more emphasis on sessions and topics they are more familiar with during the panels.
- In order to facilitate the discussion and to make it easier for experts to prepare, the next slides include guiding comments/questions.
- The moderator will use the guideline questions during the discussion.
- Each session lasts 2 hours.

Ministry
of Digital Affairs

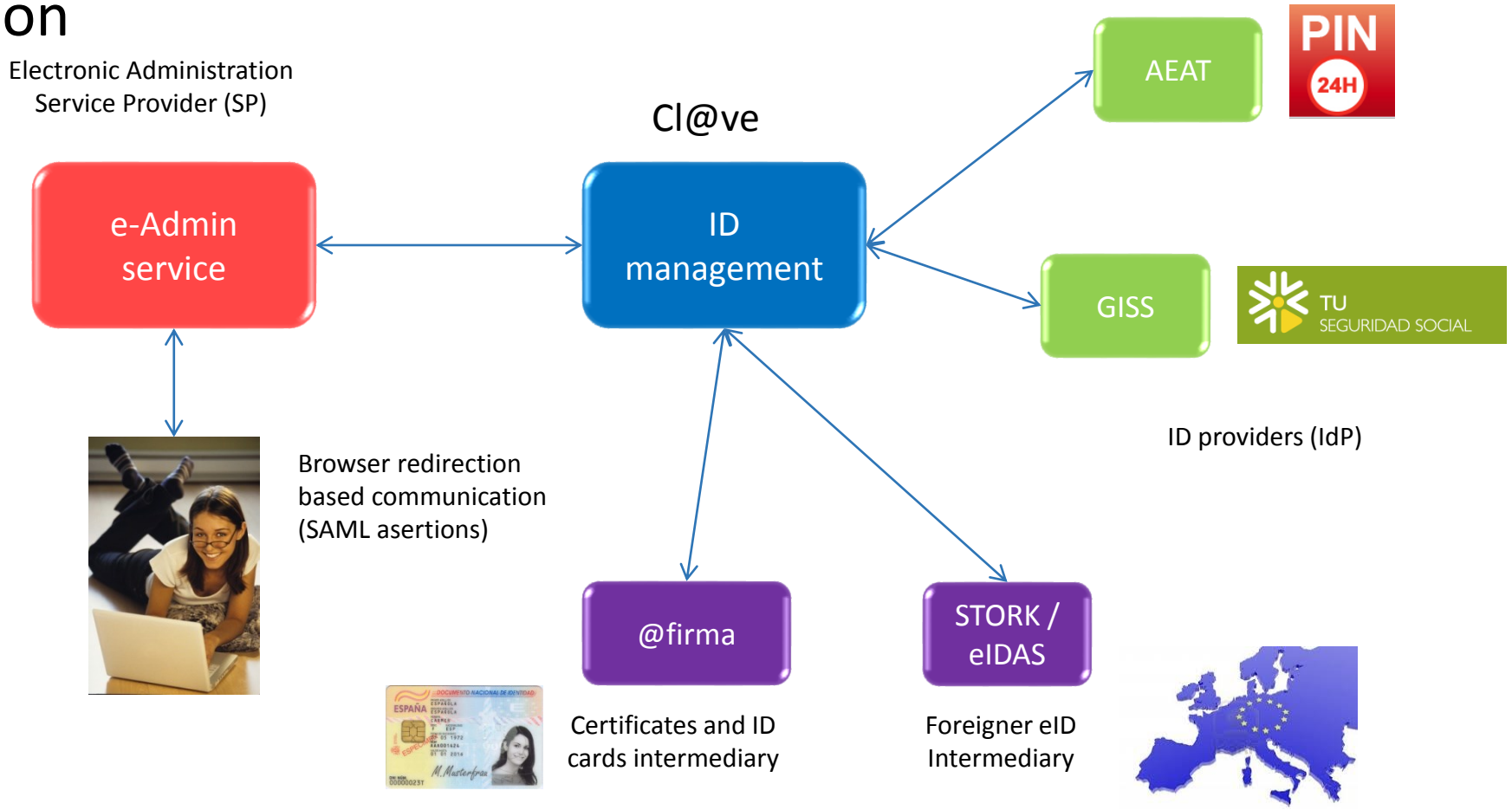
Session 1: Introduction on mID: Trends, Challenges and Opportunities (10 minutes)

- Overview about eGovernment platforms – one / two slides (eg. is there one public services portal, open data portal, emergency notification server, identity services, e-signatures services, mobile signatures, interoperability platform, payment services)
- Overview of legal framework
- Overview of portfolio of ID solutions used by Citizens (like PKI, mID, Token/OTP, Smart Cards etc)
- Short history of identity development – key dates (eg. started in 2009)
- mID in numbers – statistics about uptake, popularity, transaction per day, avg transactions per citizen, popular transation
- What were the key success factor for successful mID implementation? (eg. easiness of use, use of current well-known mechanism from citizen point of view)

Ministry of Digital Affairs

Overview about eGovernment platforms

- mID on production



Ministry
of Digital Affairs

Overview about eGovernment platforms

- Electronic invoice (including local and regional admin.): FACe
- Public service portal (central administration): http://administracion.gob.es/
  - Specific for digital administration solutions: http://administracionelectronica.gob.es/pae_Home
- Open data portal: http://datos.gob.es/
- Transparency portal: http://transparencia.gob.es/
- Official notifications to citizens (not emergency): Notifica
- Interoperability solution: intermediation platform
- Digital signature and ID: @firma suite

Ministry of Digital Affairs

Overview of legal framework

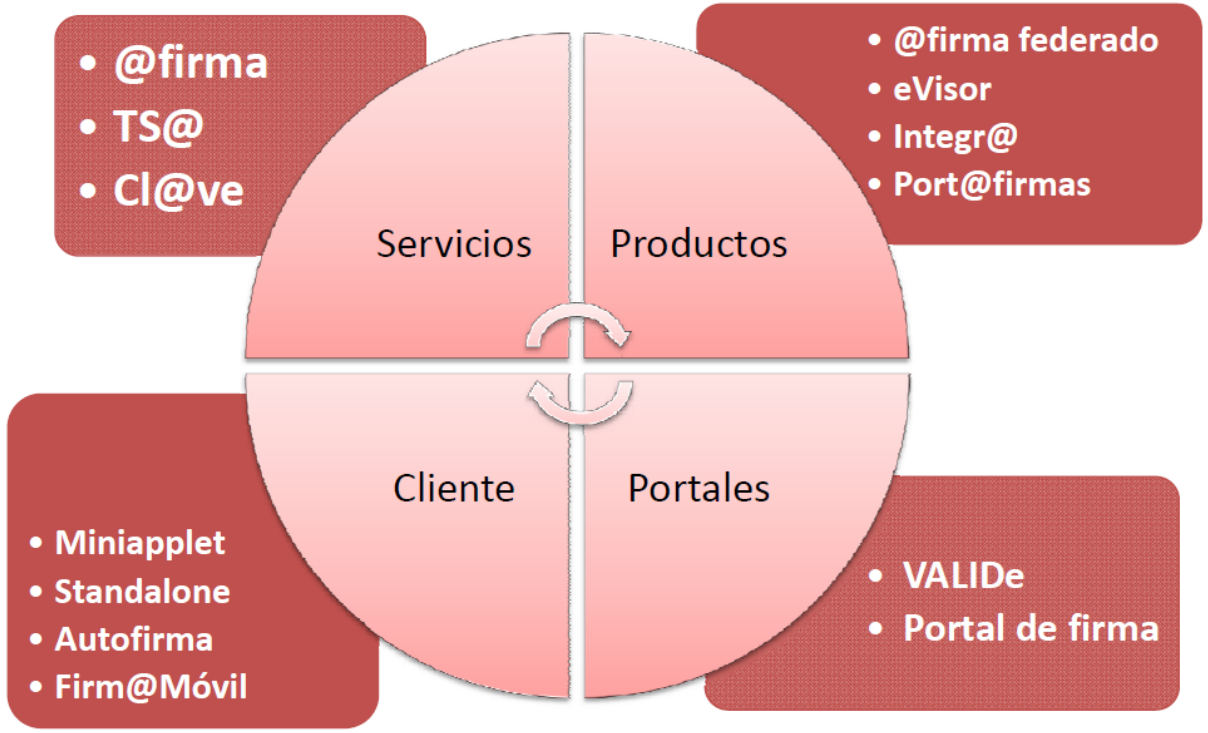
- The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (**eIDAS** Regulation)
- COMMISSION IMPLEMENTING DECISION (EU) 2015/1506: laying down specifications relating to **formats of advanced electronic signatures** and advanced seals to be recognized by public sector bodies
- - Low 40/2015 de Public Sector Judicial Regime: each administration (central/regional/local) can decide the eSignature system the staff will use. Such system can identify the staff by a code (pseudonym).
  - - Decrete 668/2015: enable these pseudonym-eSignature system for central administration.

Ministry of Digital Affairs

Overview of portfolio of ID solutions used by Citizens

2- Suite @firma

Middle



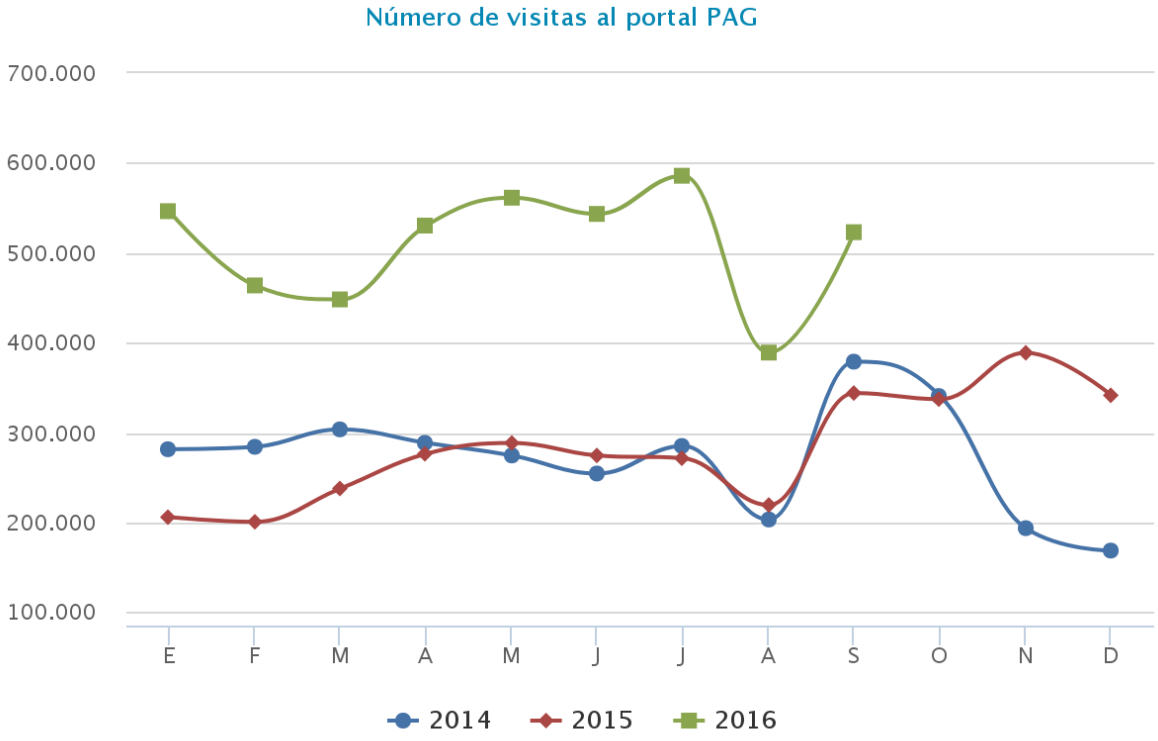
Ministry of Digital Affairs

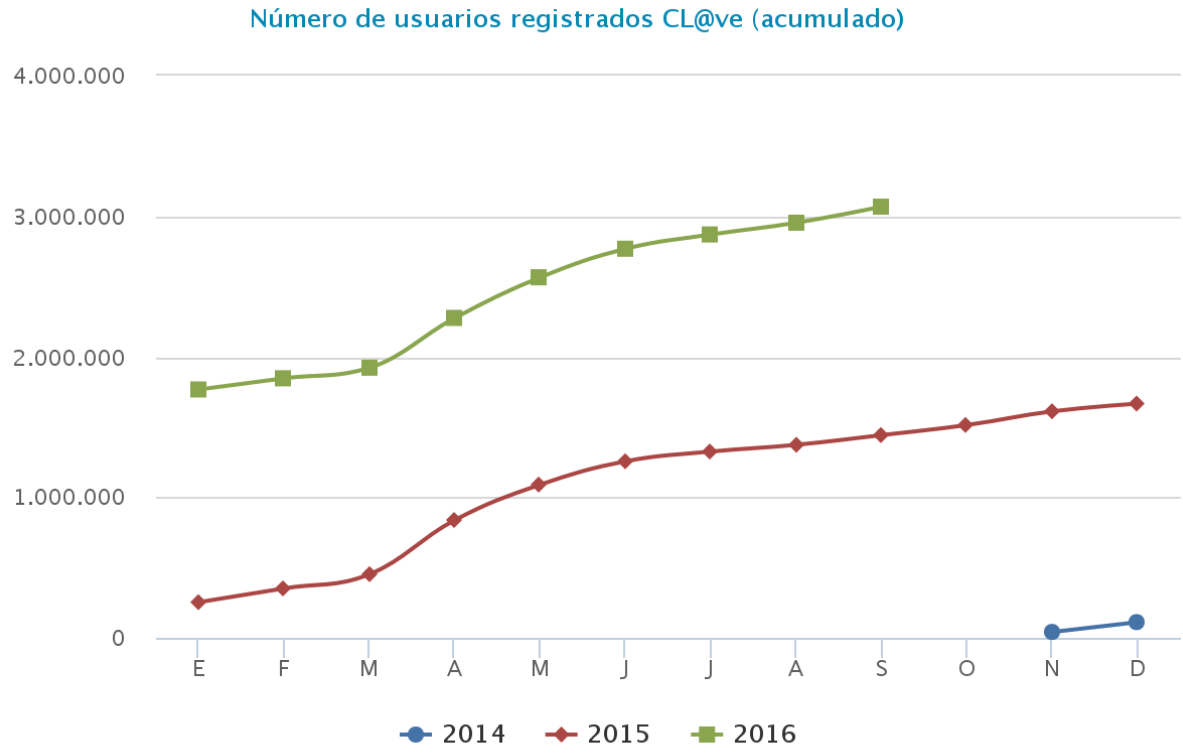
Short history of identity development

- 1999: CERES project. PKI-FNMT made possible to hand in annual tax declaration online with an Electronic Certificate.
- 1999: Directive 1999/93/EC Electronic Signature
- 2003: Electronic Signature Law and Certification Services Provider market regulation
- Before 2006: independent applications and user registries.
- 2006:
  - Signing tokens and validating the certificate in the token
  - @firma: platform for validating Electronic Certificate
  - DNI-e → 2016: v3.0 NFC ID and signature
- 2007: Law 11/2007. Citizens have the right to Electronic Administration
- 2008: Stork for some projects
- 2014: eIDAS regulation.
- Mid 2014: Cl@ve Platform
- Central federated platform using authentication keys (password, sms codes, etc) with a single user database and available for all administrations.
- Support for Single Sign On
- Goal: reduce the need for digital certificates and related technologies
- 2016: Cl@ve firma: digital signature on the cloud (next year)

Ministry of Digital Affairs

mID in numbers – services' demand and use of mID





- Transitions can be found at PAG

Ministry of Digital Affairs

What were the key success factor for successful mID implementation?

- The Cl@ve project has allowed to have an authentication mechanism adapted for mobile devices and mobile identification. It allows to get rid of technologies associated to digital certificates like java in the browser, smart card readers, etc. which allows easiness of use by using simpler tools like passwords and keys.
- Registration 100% online
- Use of Digital Certificates on Smartphones is also possible.

Ministry
of Digital Affairs

Session 2: Business Models of mID Finance Accord and Public-Private Exchange (10 minutes)

- Who pays for what – to whom and etc?
- What are the fees in system?
- Is the system private-based or public-based?
- Is there a central hub for eID exchange?

Who pays for what – to whom and etc?

- Electronic Certificate validation broker (@firma) is provided to all public sector by Finance Ministry (DTIC): SaaS
  - If heavy use is demanded: single installation needed (@firma_federado).
- Central administration pays SW development and maintenance: **Cl@ve** (next slide)
- Traditional Certification Authorities (CA):
  - Public or private
  - Cost for buying an Electronic Certificate
  - Cost for checking an Electronic Certificate
  - **Public CA doesn't charge to citizens** (receive money from government)

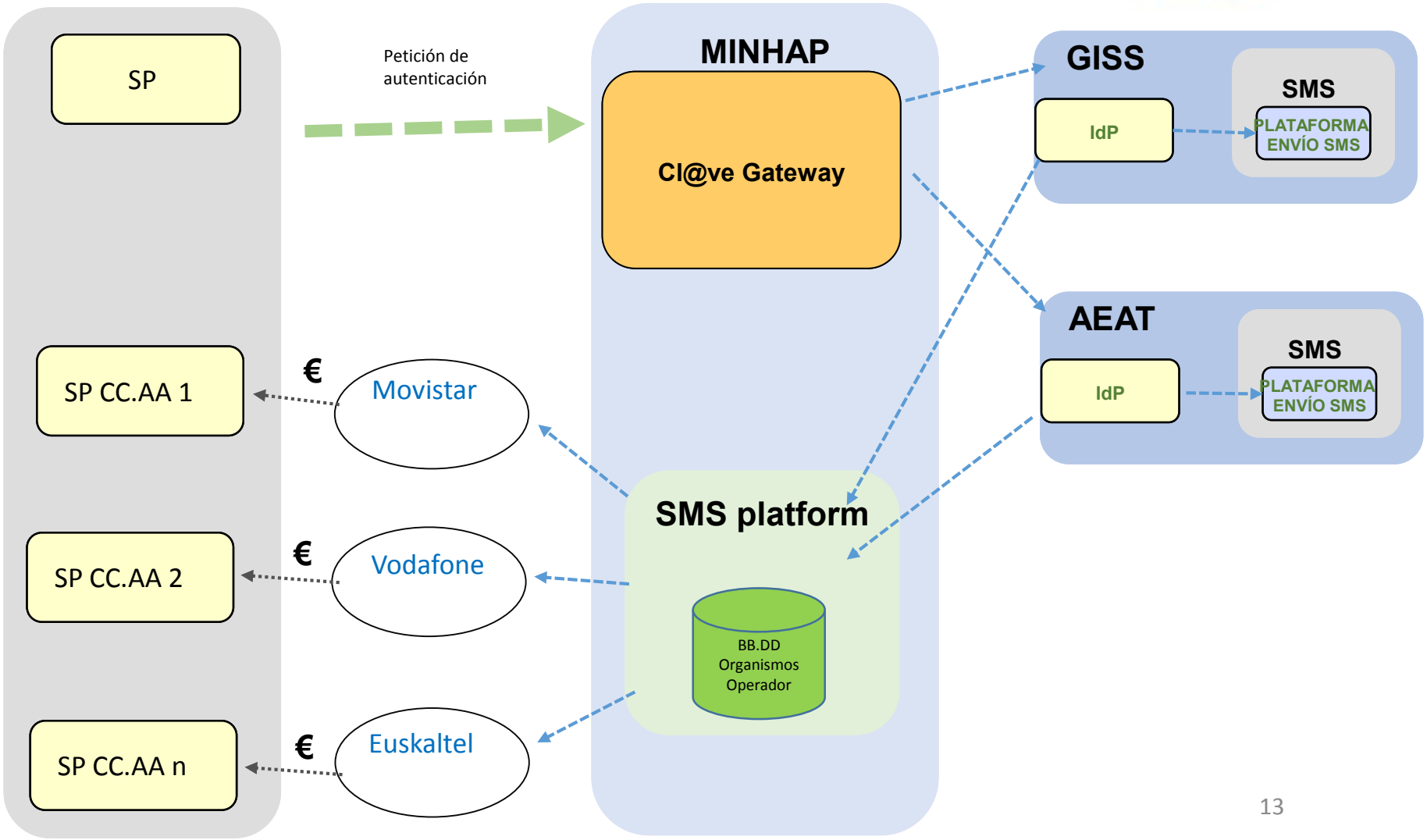
Ministry of Digital Affairs

Who pays for what – to whom and etc?

Cl@ve system internal SMS cost:

SaaS

Middle



Ministry of Digital Affairs

What are the fees in system?

- @firma and Cl@ve: developing cost 1.000.000€/year to hire (not considering internal staff)
  - Usage to public sector is for free
- Certification Authorities revenue ???

Ministry
of Digital Affairs

- Is the system private-based or public-based?
  - Mix
- Is there a central hub for eID exchange?
  - @firma: hub for validating EC
    - Connects to CAs
  - Cl@ve: hub for validating ID

Ministry
of Digital Affairs

Session 3: IT and Technical Achitecture: Solutions, Services and Advantages (10 minutes)

- What were the key technical questions that were answered during project?
- Was the identity solution implementation Client-side (on SIM/device) or server-side (eg. token generated via centralized system)
- Was the system build in house or bought from the market? Is the system open-sourced and current code could be reused by other countries?
- Does mID solution use biometrics? Which kind (iris, palm, fingers etc). What is the name of biometrics provider (vendor like Fujitsu)
- Does mID allow to use it in real, physical work or only digital?
- Is there any central system which logs every transactions?
- Is every transaction handled by central system? This means that country / system knows about every transactions (citizen could have problem with privacy)
- Does citizen has access to his transactions and logs (like where his mID was used?)
- How is mID verified? Are there any physical chips or scanners which are used by eg. Policeman in order to verify mID ?

Ministry
of Digital Affairs

What were the key technical questions that were answered during project?

- Simpler technologies help citizens to access electronic administration more easily.
- Federated authentication is the way to go in Spanish electronic administration.
- Different assurance levels are possible using passwords and authentication tokens without the need of digital certificates.
  - SMS PIN
  - SMS PIN + password

Ministry
of Digital Affairs

Client-side or server-side

- Client-side:
  - SW Electronic Certificate based authentication
    - Miniapplet
    - Autofirma
    - mID: @firma_mobile_client: run a daemon reached by web browser (afirma://)
  - HW Electronic Certificate based authentication: eDNI 3.0
    - mID: NFC
    - Connection for apps: *under development* for applications to be able to use it
- Server-side:
  - Cl@ve: user&pass with password holder certification
  - Cl@ve_signature: digital signature on the cloud (mid 2017).

Ministry
of Digital Affairs

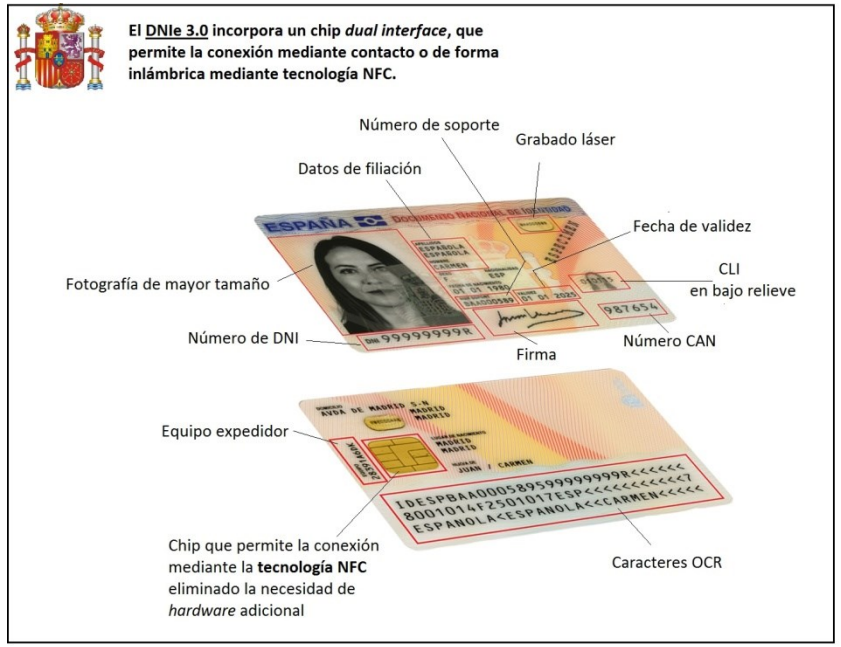
Was the system build in house
or bought from the market?
Open-source?

- System is build on the house
  - ACs can be public or private
- Client side components are open source now
- Server side
  - @firma hub is scheduled to be opened in November (version 6.3).
    - Library IAIK (newer versions) can be distributed in open source projects
    - Library BouncyCastle will be included instead of IAIK: it's open source
  - Cl@ve hub: open source

Ministry of Digital Affairs

Does mID solution use biometrics?
Which kind (iris, palm, fingers etc).
What is the name of biometrics provider (vendor like Fujitsu)

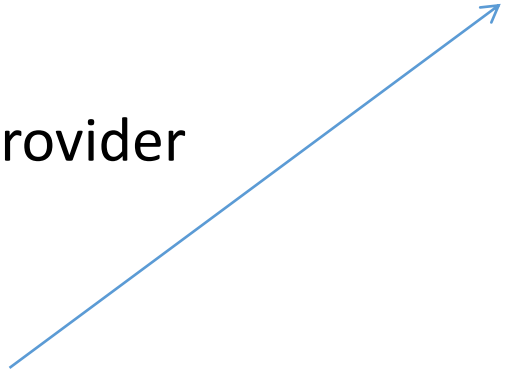
- Only higest security use biometrics: eDNI
  - If password is forgoten, citycens can use the finger to reactivate it.
  - Provided by the police
  - *Does mID allow to use it in real, physical work or only digital?*
    - This is the only allowed use for biometrics



Middle

3 main log systems

- @firma: logs every EC validating request. It's previously done before validating a digital signature (authentication) / content commitment
  - eIDAs: TSL (Trusted Service List) will be loged by @firma
- Cl@ve:
  - Password base: loged by ID provider
    - AEAT
    - SS
  - EC based: connets to @firma



Ministry
of Digital Affairs

Is every transaction handled by central system?
This means that country / system knows about
every transactions (citizen could have problem with privacy)

- Privacy:
  - Systems are 100% managed by Public Services
    - CAs can be private but Law is severe (3,000,000€ insurance policy)
  - Telephone company ID provider not allowed for the moment

Ministry of Digital Affairs

Does citizen has access to his transactions and logs (like where his mID was used?)

- No web portal is available for this use
- Info can be consulted in case of jurisdictional process
- Also if demanded through transparency portal

Ministry
of Digital Affairs

How is mID verified? Are there any physical chips or scanners which are used by eg.
Policeman in order to verify mID ?

- mID verification:
  - Cl@ve: password based
  - @firma: EC based
- 3 minutes example: eDNI 3.0 → NFC (Near Field Communication)

Ministry
of Digital Affairs

Session 4: Security and Privacy: Mechanism and Requirements (10 minutes)

- What are the security mechanism used eg. in order to assure integrity, authentication?
- Have the mID solution been ever hacked or did somebody tried to hack mID? What were the typical attacks?
- Is there a central certification body? Its is public or private?
- Was there any generated false mID on the market?
- What are the key security requirements for secured ID?
- How is the mID verified during registration (eg. at Police station, face-to-face)?
- If mID is an app then how is it certified and distributed?
- Is mID device paired with mID?

Ministry
of Digital Affairs

How is the mID verified during registration (eg. at Police station, face-to-face)?

- eDNI:
  - Police office (face2face), 2.5 years validation period
- Password based (cl@ve)
  - Annual tax declaration agency (AEAT): PIN24 responsible agency
    - Has information about every citizen
    - When cl@ve registration is demanded, a position of the last annual tax declaration is asked
    - Whole process is done online
  - Social Security: permanent password system responsible organism
    - Same idea.
- Traditional CA: EC based.

Ministry
of Digital Affairs

What are the security mechanism used
eg. in order to assure integrity, authentication?

- Cl@ve (password based):
  - PIN24: something you have (SMS sent to citizen's cell)
  - Permanent password: something you have (cell) plus something you know (password)
- Cl@ve_firma (next year): digital signature on the cloud
  - Next year
  - No client side EC
  - HSM: private company provided
- Client side EC based (have + know)
  - SW EC: @firma_mobile_client: asymmetric cryptography
    - afirma:// protocol installed on device
  - HW EC: eNDI 3.0 NFC
    - @firma_mobile_client available next year for apps to use it

Ministry
of Digital Affairs

Have the mID solution been ever hacked or did somebody tried to hack mID? What were the typical attacks?

- There always are attacking attempts. Most common from China and Russia. No detected success

Is there a central certification body? Its is public or private?

- CCN (National Cryptologic Center): public institution dealing with SW security
  - Monitors SARA network with IDSs
  - Cl@ve: decentralized systems. Security lines are set by CCN
- @firma: emergency mode

Middle

Ministry
of Digital Affairs

Was there any generated false mID on the market?

- Not registered yet
- Client side exploit is possible on the mID EC based mode:
  - afirma:// protocol is installed on client device
    - Used for the web browser to access EC client vault
  - @firma_mobile_client is open source
  - If afirma:// protocol is spoofed (client side) there's no way to detect it
- Other studied options:
  - Store client EC on text files, accessible through JavaScript
  - Use native Apps
- Ideas?

Ministry
of Digital Affairs

What are the key security requirements for secured ID?

- EC based:
  - Client side security → if private device, dificult to control
- Password based (Cl@ve)
  - Client side:
    - Cell could be stolen: SMS could be received by other person.
      - There's still "something you know" factor (password)
- Key: clean client equipment

Ministry
of Digital Affairs

If mID is an app then how is it certified and distributed?

- @firma_mobile_client (EC based authentication): distributed through Play Store or AppleStore
- Cl@ve: no App client needed

Is mID device paired with mID?

- Yes (if password based (Cl@ve))
  - PIN24 and permanent password: SMS is sent

Ministry
of Digital Affairs

Session 5: mID use cases and processes: Is it a real usage? (10 minutes)

- Is mID used in real, physical world?
- Is mID used in electronic transactions?
- Whether mID is used in public or private sectors?
- What the the most popular services which use mID?
- Is mID offered to every citizen including child?
- What is mID used for?
- Please describe high-level processes for registration, first verification and revoking and re-registering for ID.
- Please describe high-level process for transaction.

Ministry
of Digital Affairs

Is mID used in real, physical world?

- Cl@ve (password based) is used in IPS, FACE, AEAT (annual tax declaration), Citizen shared folder, transparency… Aim: all services to be linked

Is mID used in electronic transactions? → imply money

- Annual tax declaration
- Social Security processes (unemployed allowance)
- eDNI bank access is possible

Ministry
of Digital Affairs

Whether mID is used in public or private sectors?

- Designed for public sector although open source
- Banks can use eDNI to ID and sign transactions
- *Public and private*

What the the most popular services which use mID?

- AEAT: annual tax declaration
  - Uses PIN24

Ministry
of Digital Affairs

Is mID offered to every citizen including child?

- Has to be face-to-face in the case of children
- Child needs valid DNI

What is mID used for?

- Identify citizen and make digital administration possible

Middle

Ministry
of Digital Affairs

High-level processes for registration, first verification and revoking and re-registering for ID.

- Cl@ve (password based mID):
  - Option 1: going to an office: all processes are possible
    - If cell is lost or password forgotten and no EC available: face to face is needed
  - Option 2: online registration
    1. URL: clave.gob.es (select register)
    2. Select verification by annual tax declaration agency or Social Security
    3. Answer last questions about last year annual tax declaration or Social Security documentation
    4. Link cell phone
- @firma (EC based):
  - Traditional Registry Authority process

Ministry
of Digital Affairs

Please describe high-level process for transaction.

- Cl@ve (password based mID):
  - Citizen connects to Public Sector web application
  - ID needed: citizen chooses ID method (Cl@ve password based)
  - Citizen receives a SMS with a code
  - Citizen types SMS_code + personal password
  - Authenticated

Ministry
of Digital Affairs

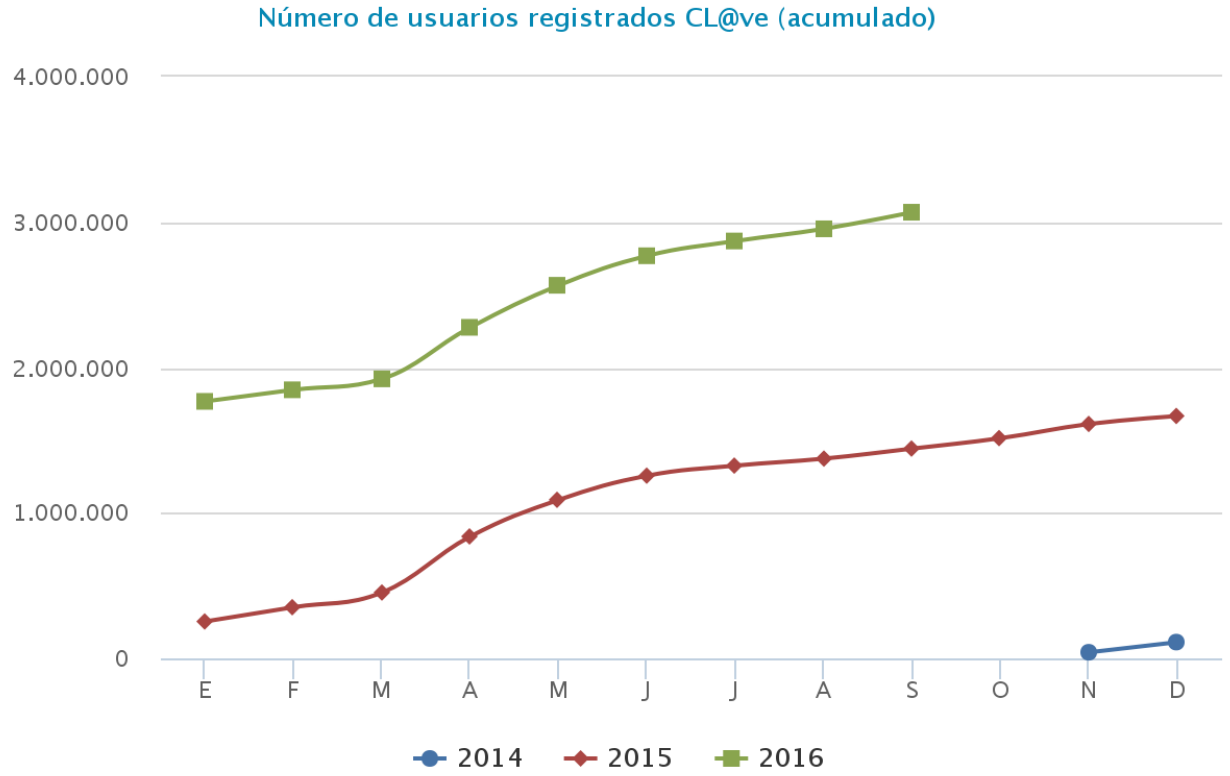
Session 6: Aspect of awareness raising and information campaign: Are we well aware of mID? (10 minutes)

- What is the rise of the awareness about mID?
- What were the main concerns with regards to mID (in society)?
- How were they addressed?
- What was the societies' response in each case?
- What stages were the campaigns composed of?
- What were the strengths and weaknesses of each component?

Ministry of Digital Affairs

What is the rise of the awareness about mID?

- Traditional EC based authentication is not widely welcome by society. Something simpler is demanded as shown below:



Ministry of Digital Affairs

What were the main concerns with regards to mID (in society)?

- Citizens were able to log in to Facebook or Google 100% online
- Why Public Services were not the same?

- Main concern: the use of Digital Public services was low although most of the citizens had a Smartphone

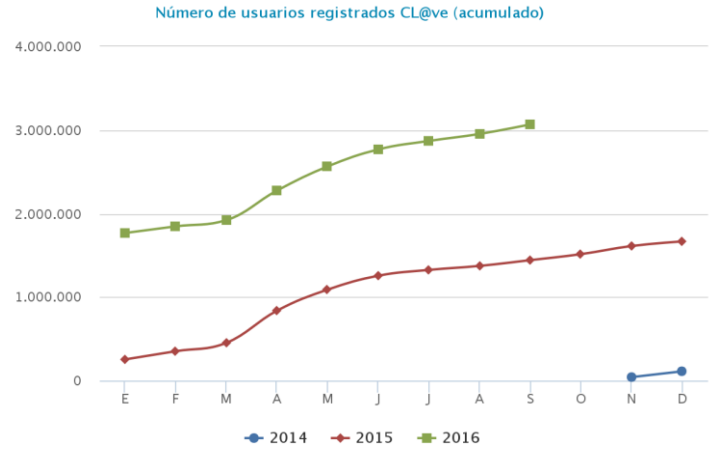
Middle

Ministry of Digital Affairs

How were they addressed?

- AEAT and SS had several systems for not to use EC
- Hub Cl@ve was developed to make possible other systems to use it

What was the societies' response in each case?



Ministry
of Digital Affairs

What stages were the campaigns composed of?

- Mainly during annual tax declaration: cl@ve was promoted
- Cl@ve portal

What were the strengths and weaknesses of each component?

- Strengths
  - Password based ID + double factor + register 100% online is possible
  - Traditional EC based ID is available for mobile devices too
- Weaknesses
  - Digital signature on the cloud and eDNI 3.0 NFC not finished yet
  - Technology changes too fast. Will Public Services be adapted on time?