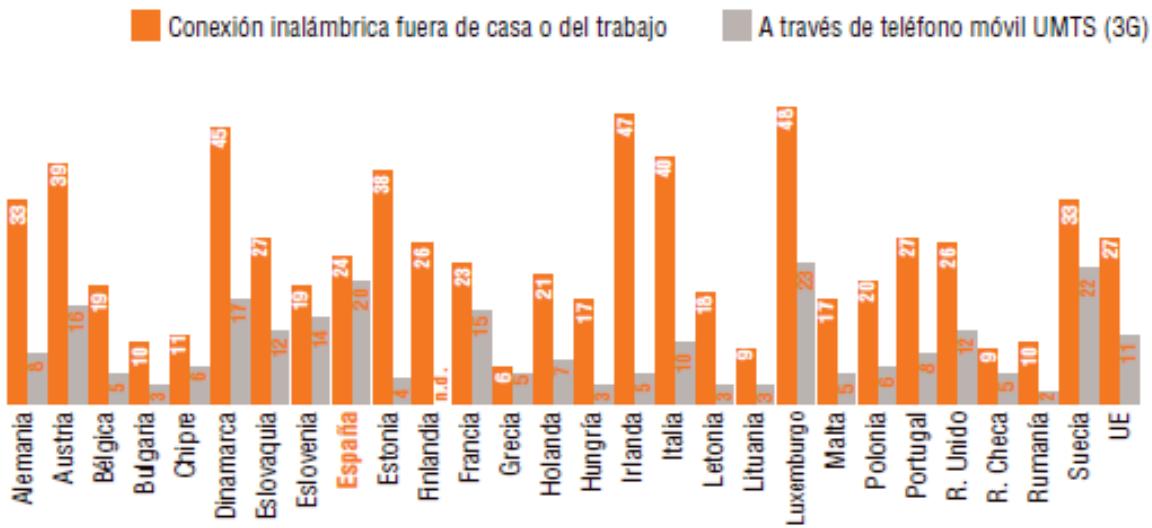


Mobile devices for interacting with Public Administrations

Spanish eID initiatives

Reykjavik May 2013

Why thinking of mobile devices?



Luxembourg, Sweden and Spain are the EU countries with the highest rate of 3G access to Internet

(Eurostat, 2010)

65% of mobile Internet users in Spain access to it by means of apps

(AMETIC-Accenture, 2011)



SERVE THE CITIZEN



¿Why thinking of mobile devices?

- Rights recognised by 11/2007 Law (Citizens' electronic access to public services)

"ensuring in particular universal accessibility, designed for all media, channels and environments with the objective that all members of the public shall be able to exercise their rights under equal conditions "



- Complete accessibility to all services
- Equal treatment
- Freedom to choose the technology and therefore the applications to interact with Public Administrations
- Obtaining the electronic identification means required for making use of the services

LEGAL FRAMEWORK



@firma mobile client

Access and Procedures processing by means of mobile devices

eGovernment services require electronic signature

@firma is the certificates validation platform for the Spanish National Administration
It manages +100 electronic certificates from 22 certification authorities

@firma client is an electronic signature tool that functions as a Java applet embedded in a web page using JavaScript

Mobile client @firma is a new initiative for developing APPs for using electronic certificates in mobile devices, under the following principles

- Collaboration among different Administrations
- Reusing efforts
- Low impact adaptation of current applications



Cliente móvil @firma

Client e

Bienvenido a Cliente @firma Android 0.2 Beta. Esta aplicación permite realizar firmas electrónicas en las páginas de los proveedores de servicios que lo soporten. Para funcionar correctamente debe tener un certificado electrónico y su clave privada instalados en su dispositivo, consulte la documentación de su sistema Android y con su proveedor de servicios de certificación.

Import
Certificate

Importar certificado

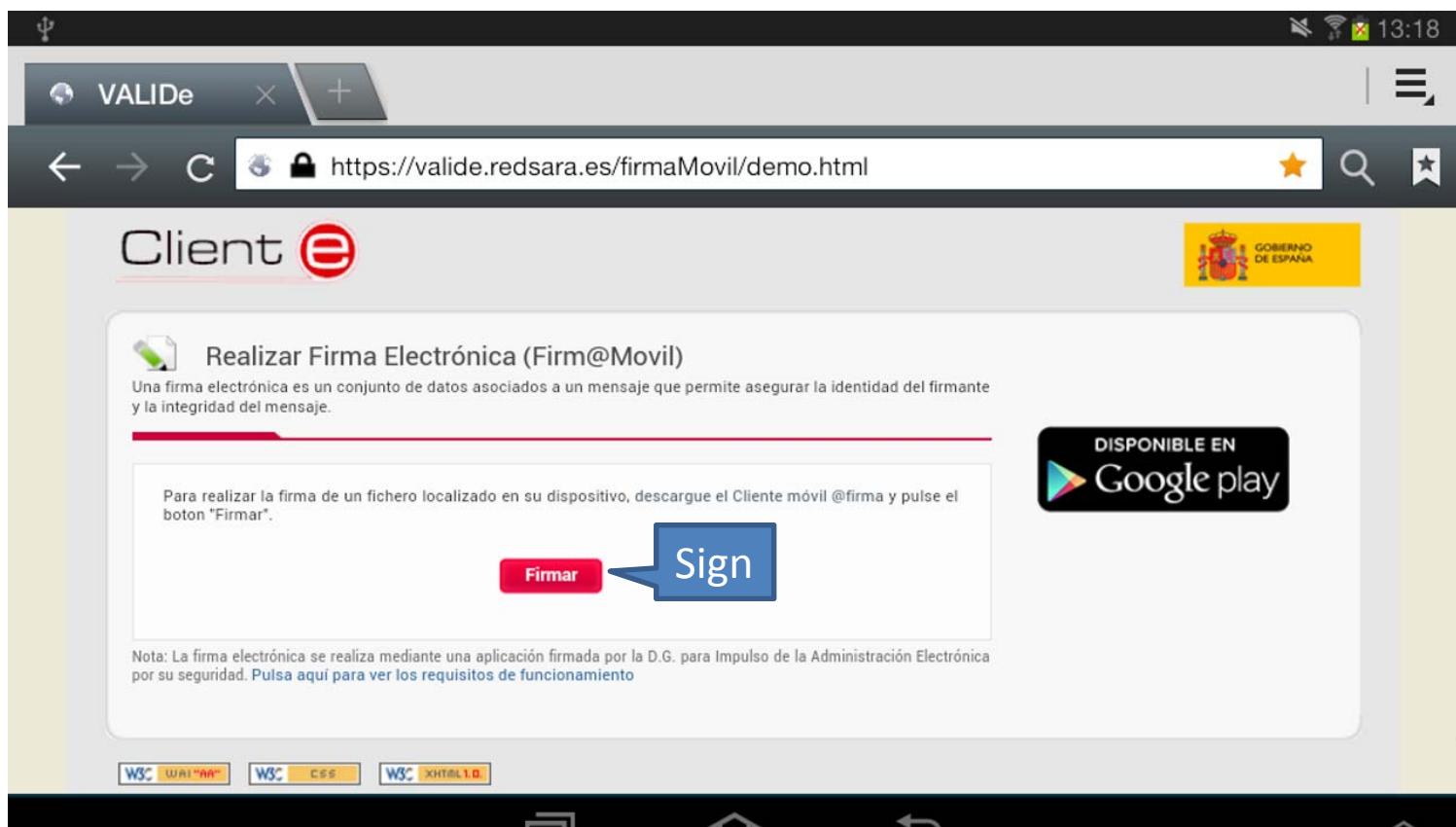
Request
Certificate

Solicitar certificado

With mobile @firma, certificates are also in the mobile device

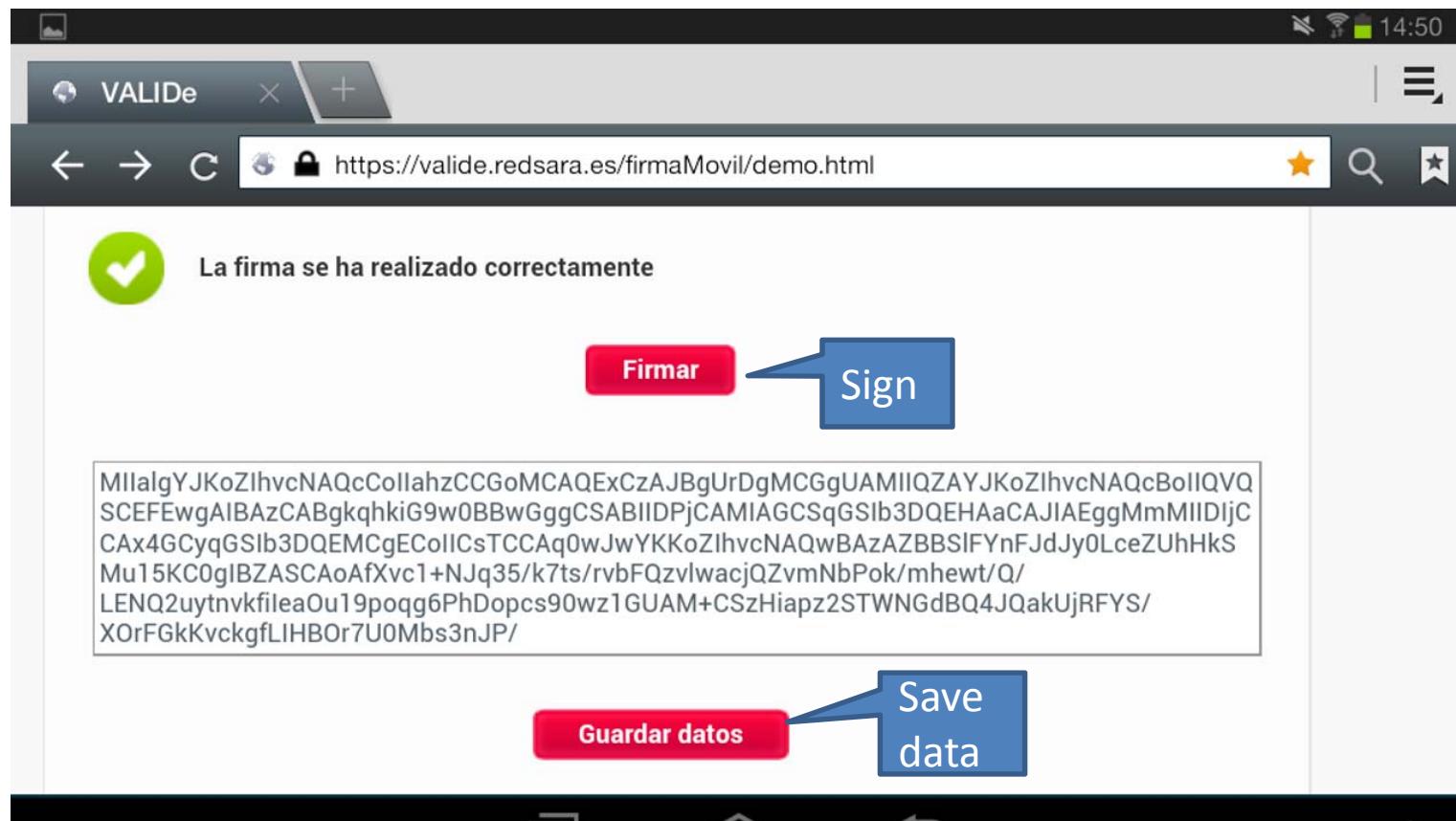
With @firma mobile client, by detecting the citizen's mobile device platform, and with a user-friendly experience, complete administrative procedures can be performed using electronic signature

Both files located in the mobile device and online forms are signed, using the certificates installed in the citizen's device



With mobile @firma, certificates are also in the mobile device

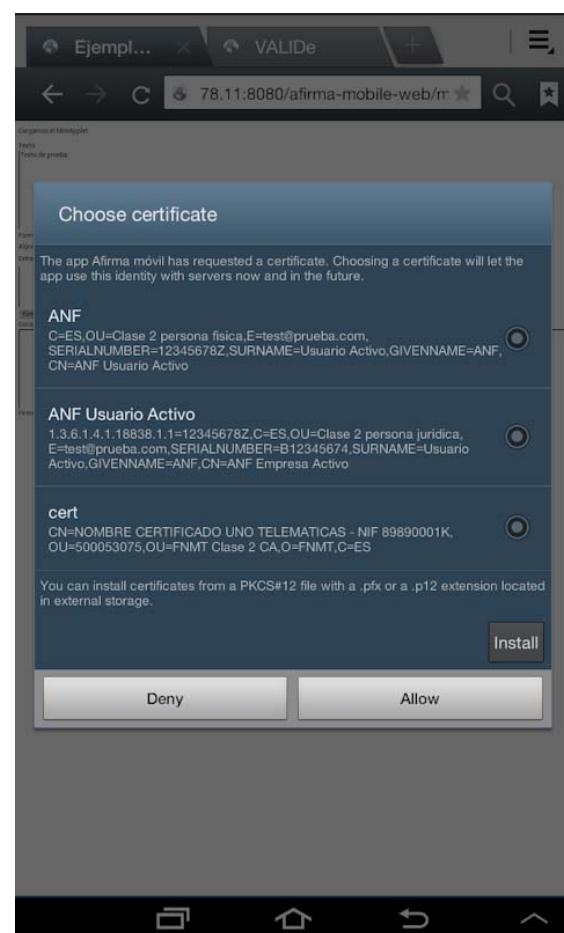
Data are sent without interruptions, avoiding problems with user experience. Currently, CADES signature available, but shortly it will also available for PADES



With mobile @firma, certificates are also in the mobile device

Already available on Android, available soon on iOS (Apple)

Also available for Windows 8, in a project led by the AEAT (tax agency) in CTT collaborative environment (e.g. collaboration between administrations and reuse efforts with free SW)



Bienvenidos

Escuchar Identificarse | Registrarse

Ejempl... VALIDE +

78.11.8080/afirma-mobile-web/mstar

Gobierno de España PAE portal administración electrónica

Actualidad Estrategias Soluciones - CTT Observatorio - OBSAE Documentación Organización

Estás en: Inicio > Soluciones - CTT > Cliente de firma electrónica de @firma

Soluciones - CTT

- ¿Qué es el CTT?
- Actualidad CTT
- Soluciones por área técnica
- Soluciones por área funcional
- Soluciones por área orgánica
- Buscador de Soluciones
- Forjas asociadas
- Forja CTT
- Comunidades CTT
- Registro nueva solución

Campaña>
-Actualízate tus datos- !

Centro de Transferencia de Tecnología CTT

Cliente de firma electrónica de @firma Client

General Info. Adicional Área Descargas

Descripción | Noticias

- Nombre Abreviado: cliente @firma
- Accesos Directos: FAQ, Forja-CTT
- Resumen: Con la Plataforma de servicios de validación y firma electrónica multi-PKI @firma, las Administraciones Públicas disponen de los instrumentos necesarios para implementar la autenticación y firma electrónica avanzada de una forma rápida y efectiva.

El Cliente de Firma es una herramienta de Firma Electrónica que



With mobile @firma, certificates are also in the mobile device

 Cliente móvil @firma

Client e

Bienvenido a Cliente @firma Android 0.2 Beta.
Esta aplicación permite realizar firmas electrónicas en las páginas de los proveedores de servicios que lo soporten. Para funcionar correctamente debe tener un certificado electrónico y su clave privada instalados en su dispositivo, consulte la documentación de su sistema Android y con su proveedor de servicios de certificación.

Listado de autoridades soportadas

Seleccione la autoridad de certificación a la que desee solicitar su certificado.



Certificados CERES
Solicitud de certificados CERES de la FNMT

List of supported certificates

Importar certificado

Solicitar certificado

2013 Gobierno de España

Mobile @firma app allows to access the certificates stored in the device

It also allows to link to the apps of the certification services providers that have these apps available

Currently, mobile @firma links to the app for using mobile certificates provided by the FNMT (National Mint)



Information available in the CTT (Technology Transfer Center)

CTT Technology Transfer Center is foreseen in 11/2007
 Law as a tool for sharing knowledge and reusing SW among Spanish Public Administrations

All the information, the source code and the forge are available to other Public Administrations in the CTT

The screenshot shows the official website of the CTT (Technology Transfer Center) of the Spanish Government. The header features the Spanish flag, the coat of arms, and the text "GOBIERNO DE ESPAÑA" and "MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS". The main navigation bar includes links for "Contactar", "Mapa del web", "El CTT", "Fuentes RSS", and "Forjas Asociadas". A search bar is also present. The left sidebar contains a "MENU" with various links, including "clientE @firma" which is currently selected. The main content area displays a news item titled "Últimas novedades" (Last news) by Jorge Martín del Álamo, dated 2013-02-21 18:55. The news article discusses the "Cliente@Firma Móvil" application for Android, its compatibility with various operating systems, and its availability on the CTT website.

Últimas novedades

Enviado por: Jorge Martín del Álamo
Día: 2013-02-21 18:55
Resumen: Cliene @firma Móvil disponible para Android
Proyecto: clientE @firma

El Cliente@Firma Móvil permite incorporar la firma electrónica a los servicios de administración electrónica desde dispositivos móviles. La creciente tendencia a utilizar dispositivos móviles para conectarse a internet hace necesario adaptar el cliente @firma del entorno del ordenador de sobremesa al mundo móvil, ampliado la compatibilidad actual (Windows, Linux, MAC) a los sistemas operativos móviles más extendidos. De este modo se facilita la implantación de los servicios basados en firma electrónica, accesibles ahora también a través del canal móvil, manteniendo una experiencia de usuario homogénea y

Últimas novedades

Clinete @firma Móvil disponible para Android
 Jorge Martín del Álamo - 2013-02-21 18:55

Publicada la nueva versión v1.1 del MiniApplet
 Jorge Martín del Álamo - 2013-02-11 15:22

Compatibilidad con los últimos sistemas operativos
 Jorge Martín del Álamo -

Actualidad CTT

Soluciones destacadas - Primer trimestre 2013
 17/04/2013
 Conoce el "Top 10" de las soluciones disponibles en el CTT Top 10 - So...

Liberación del código fuente de datos.gob.es
 17/04/2013
 La iniciativa Datos.gob.es pone a disposición el código fu...

Lista de correo de novedades sobre política de firma electrónica
 15/04/2013
 Se ha creado una lista de



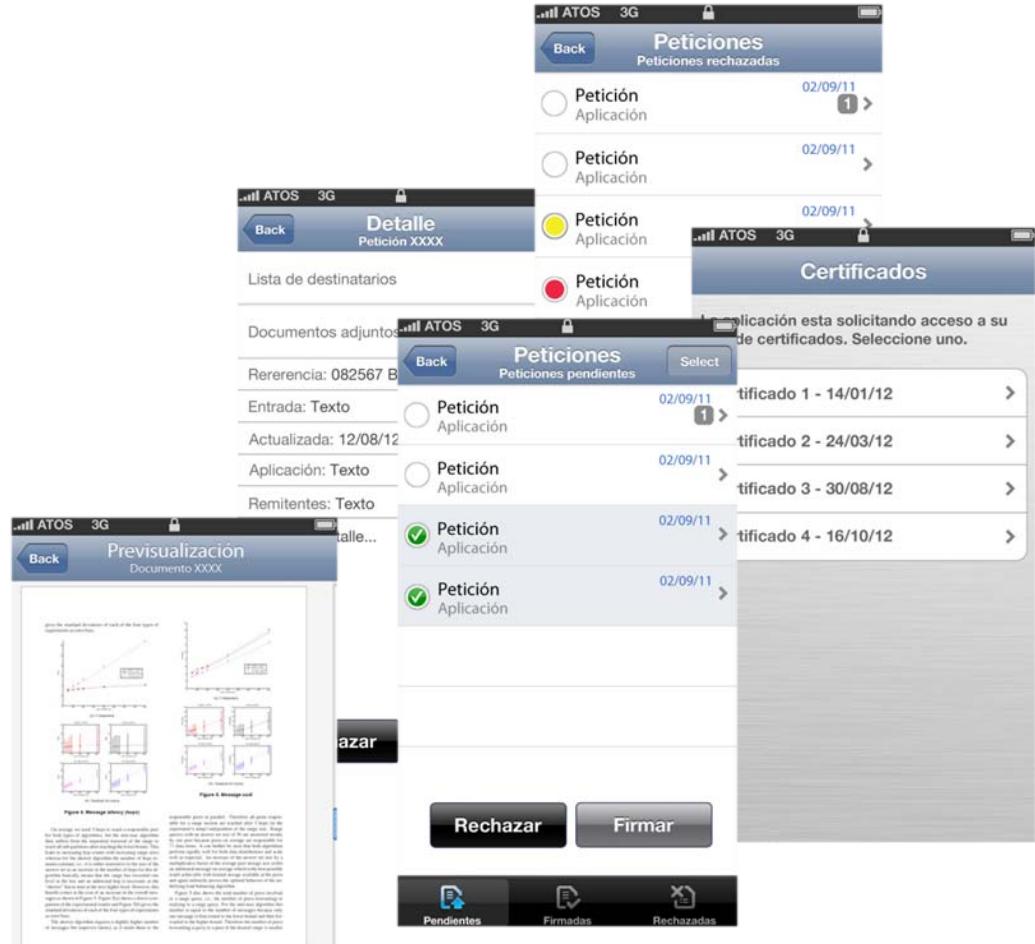
Mobile Port@firmas

**Services based on mobile electronic
signature**

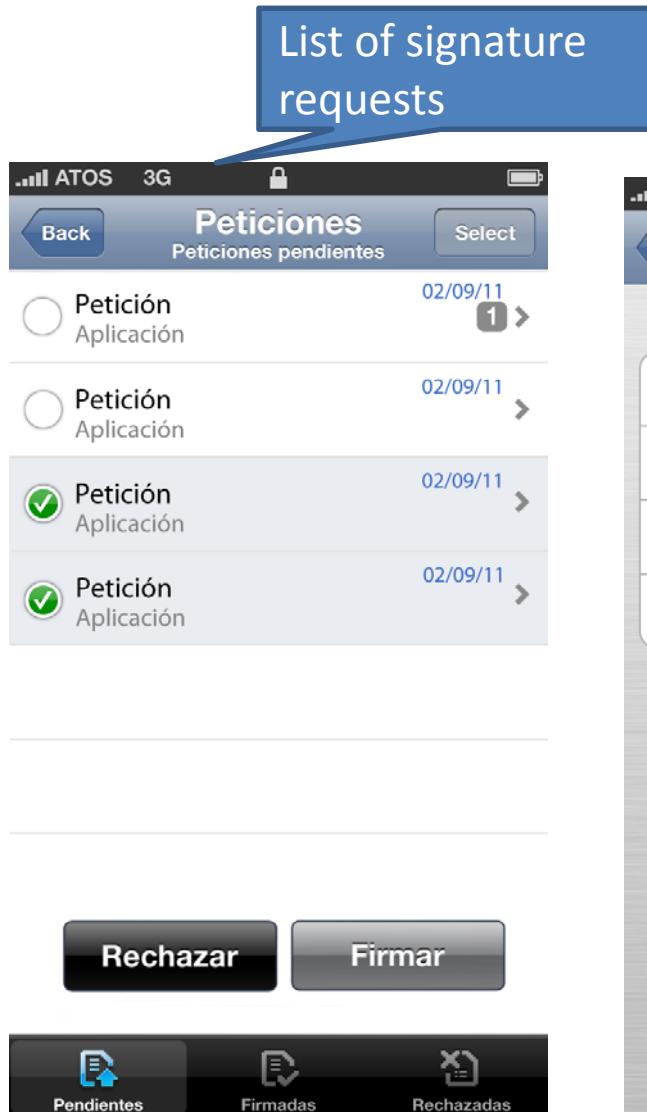
- ▶ Corporate solution for mobile signature
- ▶ Compatible with the existent signature application for PC
- ▶ Access from smartphones and tablets.
- ▶ Certificate authentication
- ▶ Review and signature of documents



- ▶ Certificate authentication
- ▶ List with the pending, signed and rejected signature requests
- ▶ Access to the request detail
- ▶ Mass signature requests
- ▶ Document viewing



List of signature requests



Peticiones
Peticiones pendientes

Back Select

02/09/11 1 >

Petición Aplicación

Petición Aplicación

Petición Aplicación

Petición Aplicación

Rechazar Firmar

Pendientes Firmadas Rechazadas

Enclosed documents



Back Doc. Adjunto Petición XXXX

Documentos adjuntos

Documento.pdf

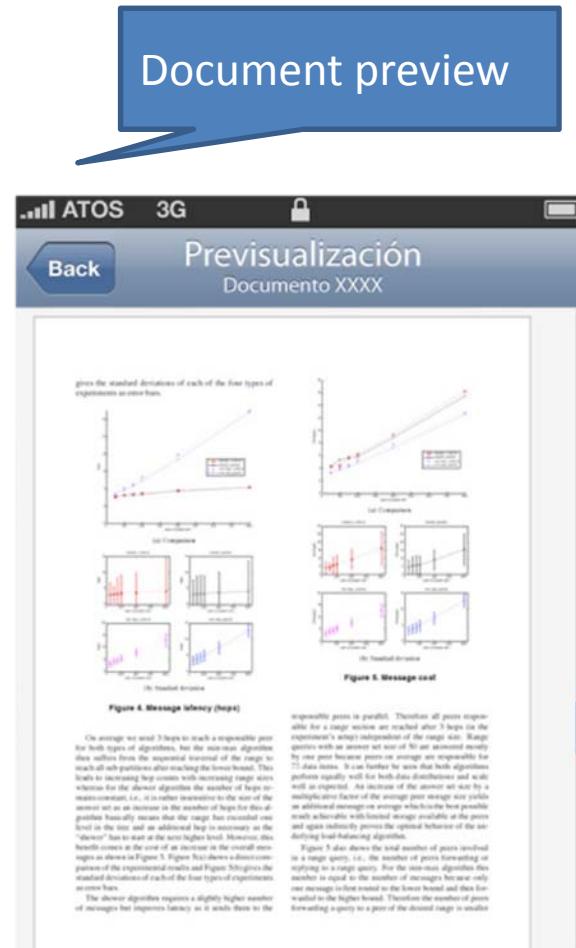
Documento.doc

Documento.pdf

Documento.docx

Back Previsualización Documento XXXX

Document preview



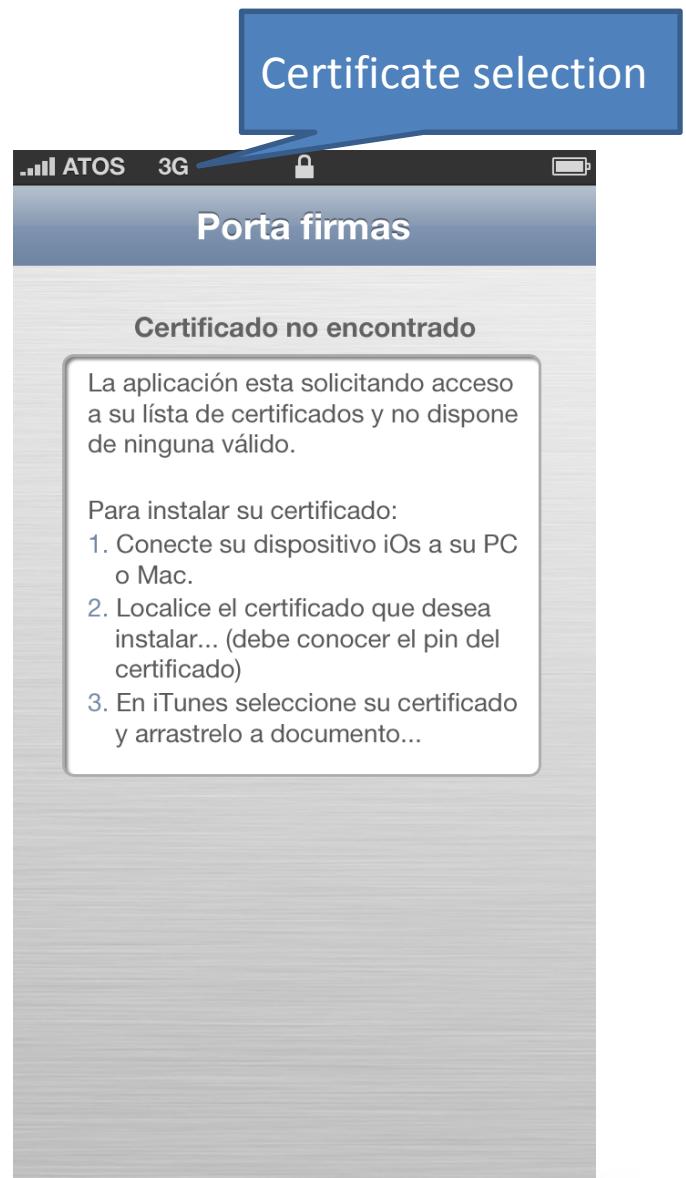
Previsualización Documento XXXX

Figure 4. Message latency (hepa)

On average we send 3 hops to reach a responsible peer for both types of algorithms, but the min-max algorithm still suffers from the sequential traversal of the range to start its process. In fact, searching the lower bound is likely to increase hop count than searching range size, whereas for the shower algorithm the number of hops remains constant, i.e., it is rather insensitive to the size of the answer set. This is due to the fact that the shower algorithm basically means that the range has exceeded one level in the tree and additional hops is necessary as the 'shower' continues. The main disadvantage of this benefit comes at the cost of an increase in the overall message size. Figure 4 shows the average message size per query for a range selection as a function of the size of the range queries with an answer set size of 30 are answered mostly by one peer because peers on average are responsible for less than 10% of the total storage. The shower algorithm performs slightly better for both data distributions and scale well as expected. An increase of the answer set size by a multiplicative factor of the average peer storage size yields an increase in the average message size. However, this leads achievable with limited storage available at the peers and again indirectly proves the optimal behavior of the shower algorithm.

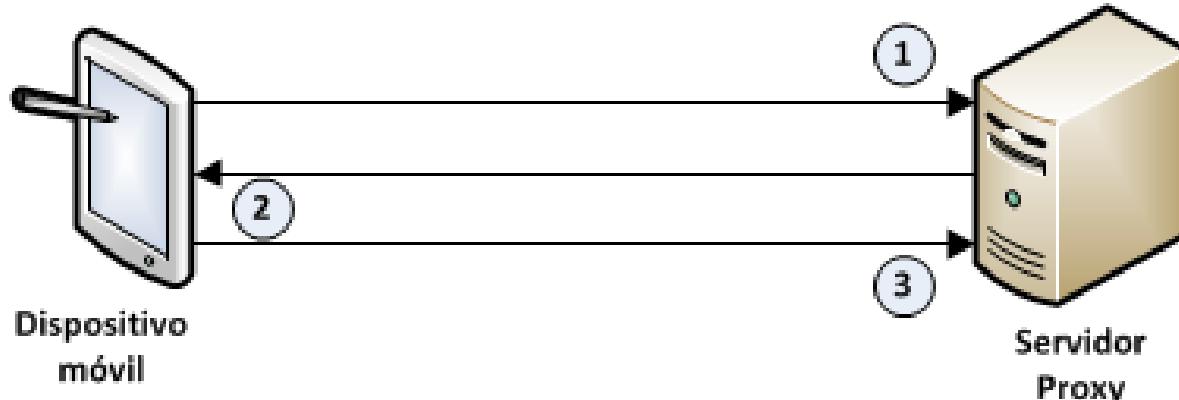
Figure 5 also shows the total number of peers involved in a range query, i.e., the number of peers forwarding or replying to a range query. For the min-max algorithm this number is constant, while for the shower algorithm it may one message is first routed to the lower bound and then forwarded to the higher bound. Therefore the number of peers forwarding a query to a peer of the desired range is smaller.

Figure 5. Message cost



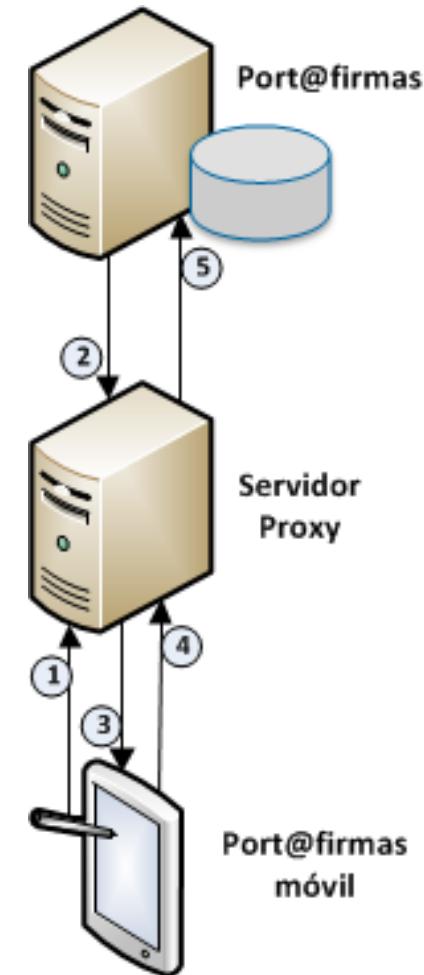
- App easy to use with the interface appropriate to each mobile platform (currently Android 4)
- Use of the Android 4 central store certificate
- Use of personal certificates for the authentication of users, against the Portafirmas, only for registered users
- Three phase system. Minimum transfers of data (request and documents to sign identifiers)
- Advance electronic signature in CAdES format, extensible to other formats

- 3phase signature for minimum transfer of data



1. Signature request and composition of the signature data in the server
The server composes the pre-signature according to the configuration established from the Client
2. Minimum information for the realization of the signature is sent to the device
Document hash, signature certificate, signature time...
3. Sending of the signature to the server for the composition of the electronic signature
The server composes the signature and sends it back to the port@firmas

- **Port@firmas**
 - Component for the integration of the signature process in the work flows
 - Currently used by the PC application
 - New services developed for specific use in mobile devices
- **Proxy component**
 - Web application for the connection between the mobile device and Port@firmas
 - 3 phase signature service
- **Mobile Port@firmas**
 - App for mobile devices



MiDNle

Using DNle in mobile devices



- **DNI – National document of Identity**
 - Mandatory as an identification means of nationals
 - DNI number associated (unique, persistent)
 - Used widely as identifier
- **DNIe**
 - New generation of DNI in a smart card
 - Usable in electronic environments
 - Authentication certificate
 - Signature certificate
 - Citizens' right to use it in their interactions with Public Administrations (Law 11/2007)
 - Obligation for the Public Administrations to accept it in their eGovernment applications

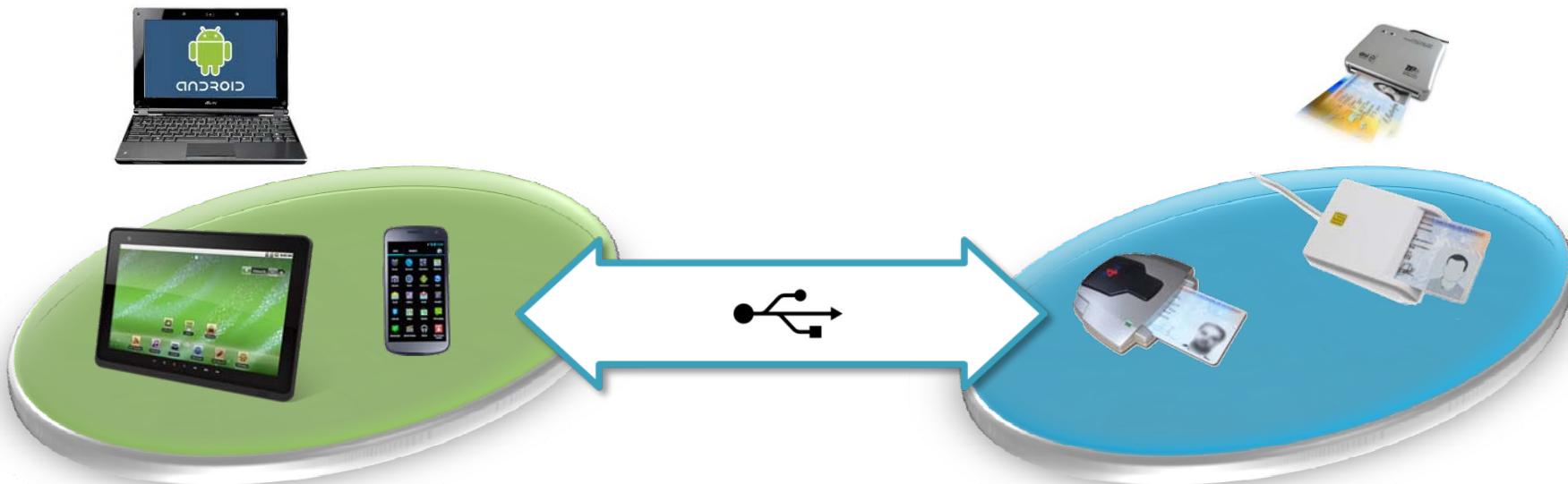




INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

Interaction of Android devices with the DNIe for authentication and signature, using a standard USB reader

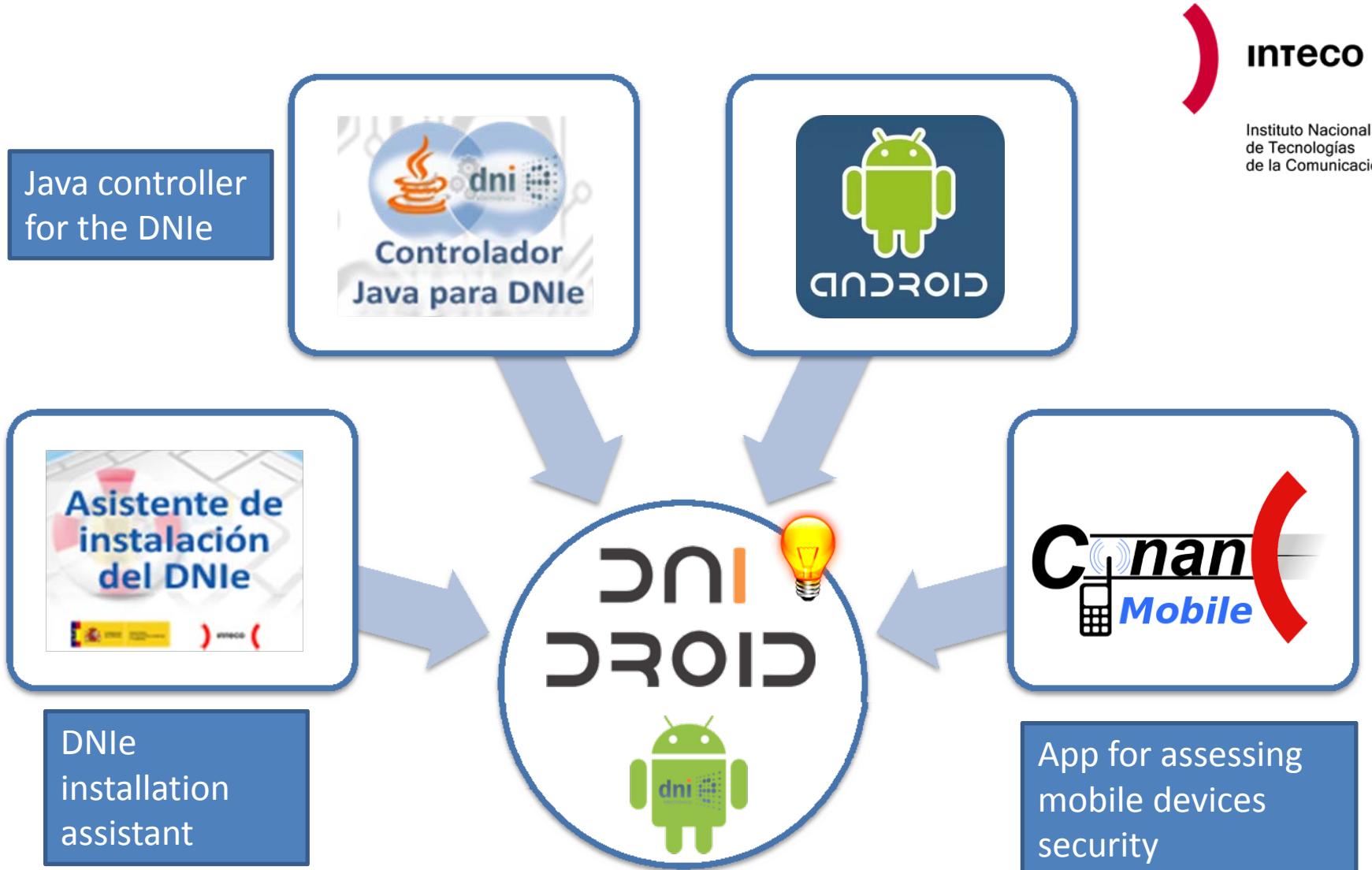


R&D project led by
INTECO

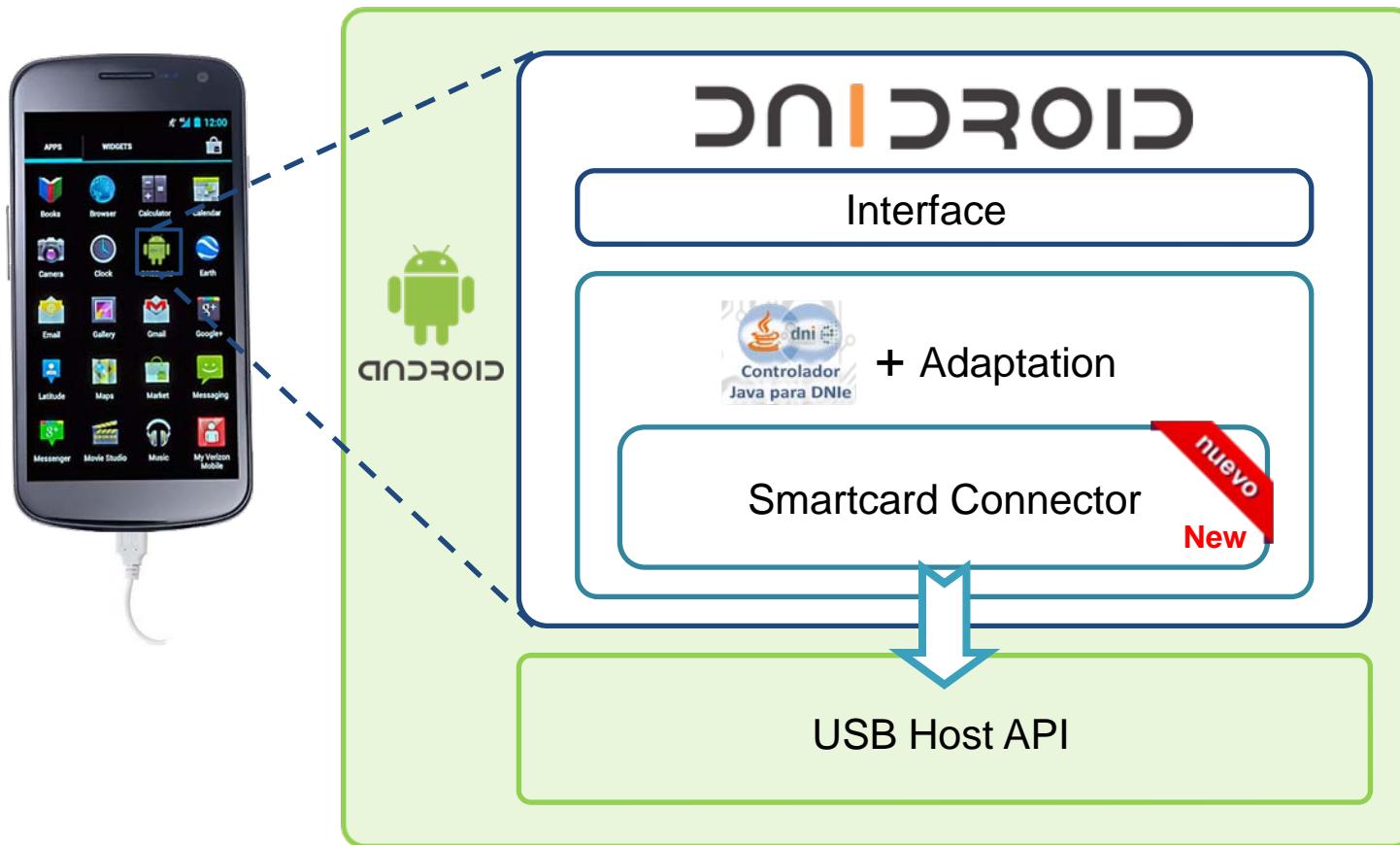


@dministración
electrónica

Background – Previous projects



The feasibility of the project has been demonstrated through the proof of concept performed



Standard USB reader
(compatible with CCID, which is typical) + USB adapter (if required)



Proof of concept (video):

<http://www.youtube.com/watch?v=QB2GJLhzdeg>



Demonstration application “Mi DNIe” in Google Play:

<https://play.google.com/store/apps/details?id=es.inteco.labs.dnie.android.midnie>

Allows to interact with the DNIe in Android terminals using internally source code from DNIEdroid project. It provides access to some services that require DNIe

- Working Life report (Social Security)
- Checking the balance of the Driver's license points (Traffic)

DNIEdroid source code publication

<http://zonatic.usatudni.es/aplicaciones/dniedroid>

It will allow companies and developers to easily create Java based applications that make use of the DNIe



Thank you



The screenshot shows the homepage of the PAe portal. At the top, there's a banner with the European Union flag, the Spanish flag, and the text "PAe portal administración electrónica". Below the banner, the word "Bienvenidos" (Welcome) is displayed. On the right side of the header, there are links for "Escuchar" (Listen), "Identificarse | Registrarse" (Log in | Register), and a search bar with a magnifying glass icon.

The main navigation menu includes "Actualidad", "Estrategias", "Soluciones - CTT", "Observatorio - OBSAE", "Documentación", and "Organización". A breadcrumb trail indicates the user is at "Inicio".

A sidebar on the left lists categories: "Administración electrónica", "Indicadores Ae", "CTT", "Firma Electrónica", "Interoperabilidad", and "Movilidad Ae". Each category has a small thumbnail image and a brief description.

In the center, there's a section titled "Iniciativas, entidades y proyectos relacionados con la Administración Electrónica en España. Consulta la información básica." It also features a "Campaña" message: "-Actualízate tus datos!" with an exclamation mark icon.

At the bottom, there are three blue buttons: "Noticias Administración Electrónica", "Lo que debes saber de la Ae", and "La Administración en la Red".

<http://administracionelectronica.gob.es>