Certificado Digital Accesible para la e-Administración

Boni García

boni@diatel.upm.es

Contenido

1. Introducción
2. Contexto
3. Certificado Digital Accesible
4. Verificación
5. Validación
6. Conclusiones

1. Introducción

- La **Administración electrónica** (e-Administración) tiene como objetivo lograr que los servicios telemáticos públicos sean accedidos por los ciudadanos de forma cómoda y eficaz
- El DNI electrónico (**DNIe**) puede ser usado para autenticar usuarios de cara a estos servicios telemáticos seguros

1. Introducción

- Problemas:
  - Los servicios de la e-Administración no son accesibles
    - Dificultad de uso
    - Barreras tecnológicas
  - El uso del DNIe no es accesible
    - No todas las personas que tienen un DNIe con el certificado generado han guardado la clave de utilización.
    - No todos los ciudadanos disponen de un ordenador configurado (drivers y lector de tarjetas)
    - Los certificados del DNIe caducan cada 20 meses y requieren renovación presencial en las oficinas de la Policía.

1. Introducción

- Alternativa al DNIe: certificados de identidad emitidos por la FNMT (**CERES**), y que son totalmente válidos para su uso en la administración electrónica
- Este trabajo propone un sistema accesible basado en el uso de certificados digitales CERES en un token criptográfico para romper las barreras de acceso a los servicios de la e-Administración

2. Contexto

- Este trabajo ha sido desarrollado en la **Universidad Politécnica de Madrid** en colaboración con la Federación Nacional **Aspaym** (Asociación de Lesionados Medulares y Grandes Discapacitados Físicos)
- Ha sido desarrollado en el ámbito del proyecto **ASTIC** (Accesibilidad en los Servicios Telemáticos Inteligentes para el Ciudadano)

http://www.tramitesaccesibles.aspaym.org/

2. Contexto

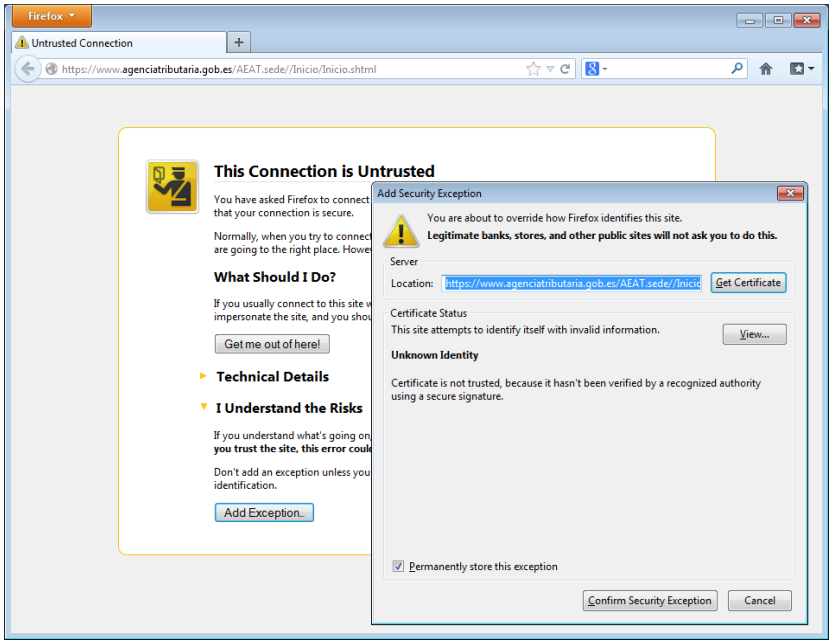
- En ASPAYM Madrid se realizó un análisis cuantitativo para averiguar cuales son las dificultades a las que se enfrentan las personas con discapacidades
- Perfil de usuarios:
  - Parálisis cerebral (PC)
  - Daño cerebral (DC)
  - Lesión medular (LM)

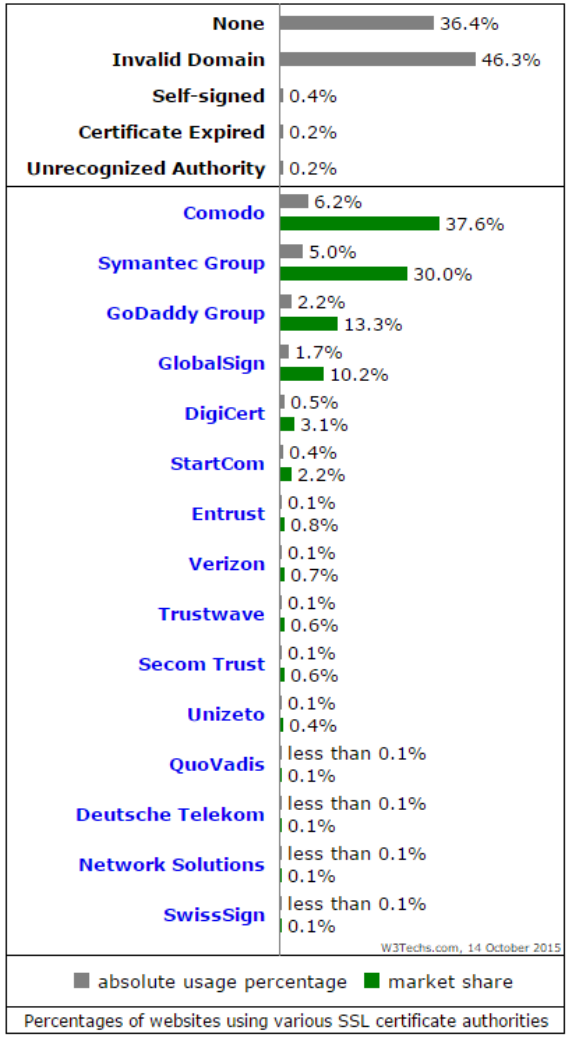
2. Contexto

- Este colectivo encuentra doble dificultad para acceder a los servicios de la e-administración
  - Problemas de accesibilidad para acceder a muchos edificios, o dificultad para llegar hasta ellos (transporte público inaccesible, problemas de aparcamiento)
  - Dificultad para acceder a través del formato telemático debido a los problemas para utilizar un ordenador o dificultad para entender cierta información

2. Contexto

- Ejemplo de dificultad técnica:





http://w3techs.com/technologies/overview/ssl_certificate/all

3. Certificado Digital Accesible

- El dispositivo accesible que proponemos como alternativa al DNIe para almacenar la identidad digital para los usuarios se ha bautizado con el nombre de CDA (**Certificado Digital Accesible**)

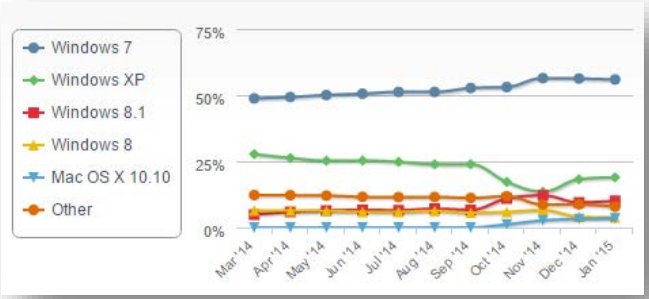
3. Certificado Digital Accesible

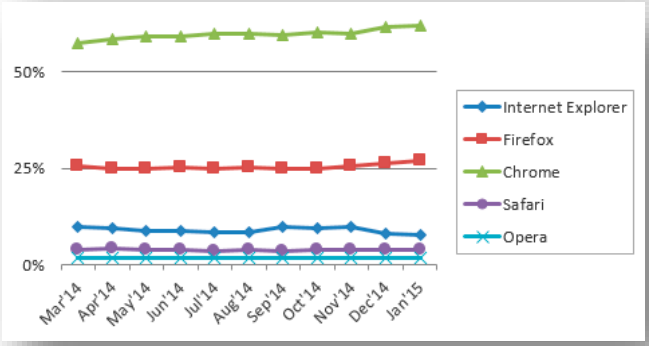
- Requisitos CDA:

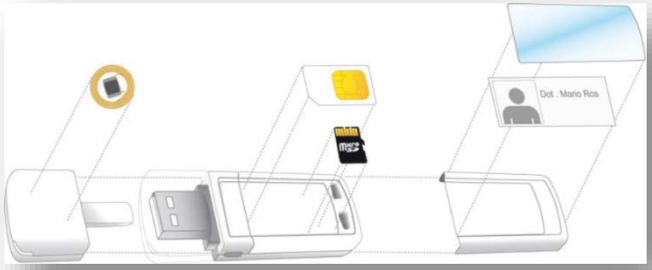
1. Se usará un token criptográfico para almacenar el **certificado digital** del usuario
2. El token además tendría un navegador web portable completamente configurado y listo para su uso en aplicaciones web seguras
3. Cuando se conectase el token por USB al ordenador del usuario, se debería lanzar y actualizar automáticamente dicho navegador portable
4. Cuando el usuario cerrase el navegador, se expulsaría automáticamente de forma segura el dispositivo USB

3. Certificado Digital Accesible

- Sistema operativo: **Windows**
- Navegador web: **Firefox**
  - Usa el almacén de certificados de NSS (*Network Security Services*)
- Token Criptográfico: **iAM**

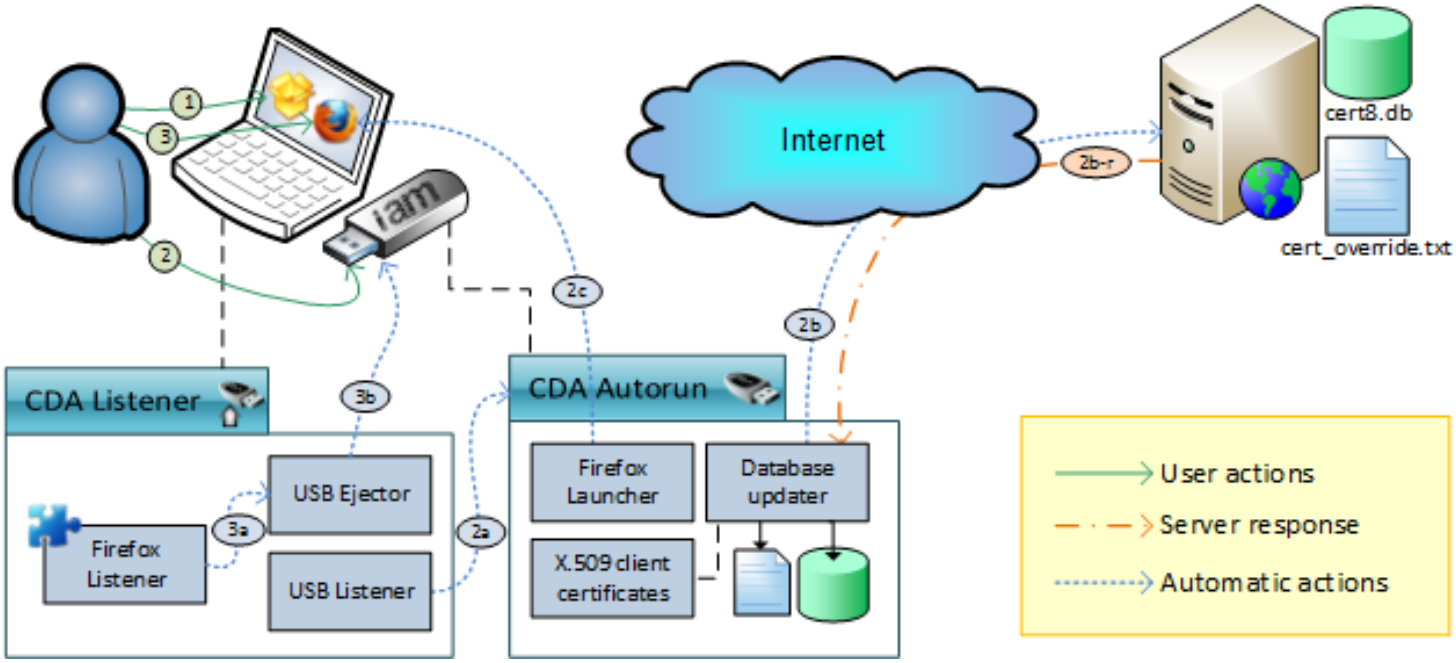






3. Certificado Digital Accesible

- Escenario de uso



3. Certificado Digital Accesible

- CDA-Listener
  - USB Listener: C#
  - Firefox Listener: Plugin de Firefox creado con Add-on Builder (https://builder.addons.mozilla.org/)
  - USB Ejector: USB Disk Ejector (http://quickandeasysoftware.net/software/usb-disk-ejector)
- CDA-Autorun: C#
  - Database updater: cURL y *certutil* (paquete NSS)

4. Verificación

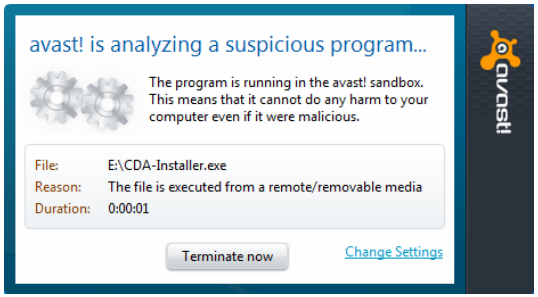
- Pruebas con diferentes combinaciones de sistema operativo y Antivirus
- Proceso:
  1. Instalar CDA-Listener
  2. Conectar token
  3. Comprobar que se ejecuta automáticamente CDA-Autorun y se actualizan los certificados del navegador Firefox portable
  4. Comprobar que el Firefox portable no entra en conflicto con un Firefox previamente instalado en el sistema
  5. Navegar con el Firefox portable usando el certificado digital de usuario del token
  6. Cerrar el Firefox portable
  7. Comprobar que se expulsa automáticamente

4. Verificación

- Resultado:

	Sin antivirus	Security Essentials/ Windows Defender	Avast
Windows XP	✓	✓	✓
Windows Vista	✓	✓	X
Windows 7	✓	✓	X
Windows 7		✓	X
Windows 8.1		✓	X

- Problema con Avast:



5. Validación

- Validación con usuarios finales fue llevada a cabo en ASPAYM Madrid
  - ASPAYM es entidad gestora de la creación de las certificados digitales CERES (a través de Camerfirma)
  - ASPAYM pide el DNI y una fotocopia, genera el certificado digital que es almacenado de forma segura en el token criptográfico
  - De esta forma se evitan las barreras arquitectónicas para los usuarios de ASPAYM
- 30 tokens CDA fueron distribuidos entre voluntarios con diferentes tipos de discapacidades físicas
- El 60% de los usuarios completaron el proceso

6. Conclusiones

- Los sistemas telemáticos siguen teniendo problemas de accesibilidad
- El DNI electrónico proporciona un sistema de autenticación para usuarios finales, pero debido a su dificultad no es ampliamente usado
- El sistema CDA (Certificado Digital Accesible) trata de proporcionar accesibilidad y seguridad para los servicios telemáticos usando un certificado digital almacenado de forma segura en un token criptográfico
- En las primeras pruebas, CDA ha sido encontrado útil por más de la mitad de los usuarios de ASPAYM Madrid

6. Conclusiones

- El proyecto ASCIT ha recibido el premio **Discapnet** de la Fundación ONCE a las Tecnologías Accesibles (septiembre 2015)

http://premios.discapnet.es/candidaturasAceptadas.php