Una experiencia diferente con Tokens PKI

Rodrigo Quinta
rquinta@ces.com.uy

14 de marzo de 2015

Temas

- Introducción
  - Token
  - PKI
- Proyecto
  - Diseño
  - Investigación
  - Pruebas
  - Desarrollo
- Conclusiones

¿Quiénes somos?

- Especializados en servicios de testing
- Emprendimiento conjunto
- Vínculo Academia-Industria
- Símbolo de calidad

CENTRO DE ENSAYOS DE SOFTWARE

Fundación Julio Ricaldoni
INGENIERÍA EN EL URUGUAY

UNIVERSIDAD DE LA REPÚBLICA
URUGUAY

FACULTAD DE INGENIERÍA

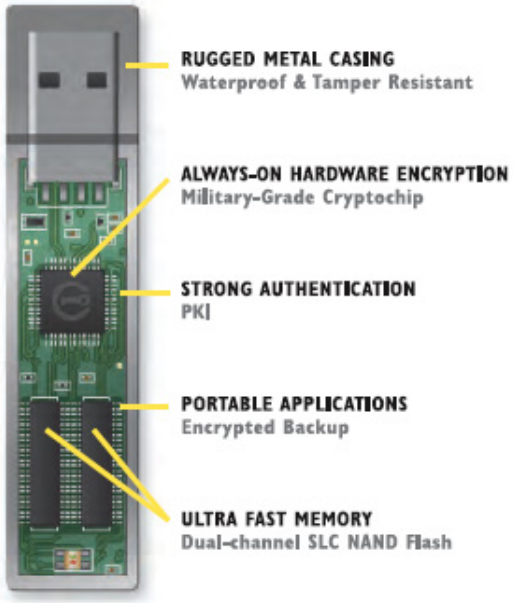
cuti

Introducción

- ¿Por qué testeamos?
  - encontrar errores
  - evaluar la calidad
- Hay mas …
  - desafíos no tradicionales

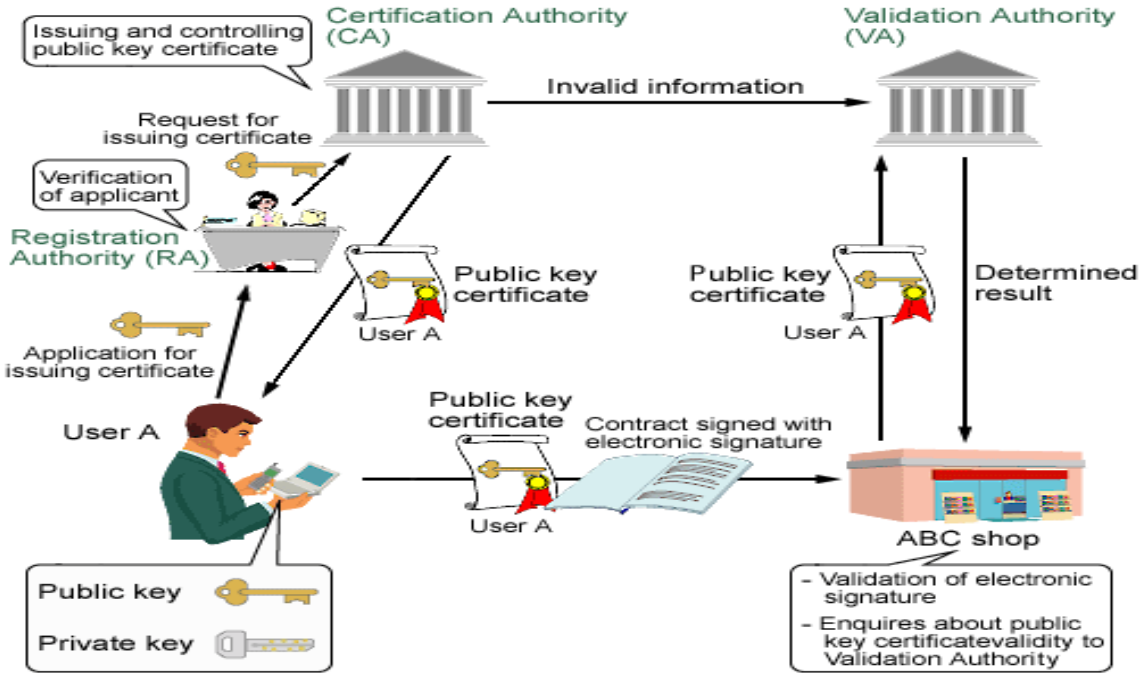
Tokens

- Token
  - dispositivo de hardware que permite almacenar certificados y firmas digitales
  - provee algoritmos de cifrado



PKI

- Public Key Infrastructure
  - combinación de hardware, software, políticas y procedimientos de seguridad
  - criptografía
    - ✓cifrado
    - ✓firmas.



PKI

- Usos de la tecnología PKI
  - Autenticación de usuarios y sistemas
  - Cifrado de datos digitales
  - Firmado digital de datos (documentos, software, etc.)
  - Asegurar las comunicaciones
  - Garantía de no repudio

Experiencia Diferente

- ¿Por que una experiencia diferente?
  - Involucró varios SO y aplicaciones
  - Investigación
    - ✓estándares
    - ✓algoritmos
  - Distintos dispositivos
    - ✓celulares
    - ✓computadoras

Proyecto

- Diseñar e implementar un protocolo de verificación de compatibilidad
  - Estándares
  - Algoritmos
  - Middleware
- Crear instructivos de instalación y configuración

Proyecto

- No es típico proyecto de testing
- ¿Como encararlo?
  - diferentes objetivos
- Investigar
  - nuevas áreas de conocimiento
- Distintos tipos de pruebas

Pruebas

- Se identifican 3 tipos
  - Instalación y configuración en distintos sistemas.
  - Instalación de claves y certificados.
    - ✓Algoritmos soportados
  - Interacción con aplicaciones.
    - ✓Comprobar funcionamiento como usuario final
    - ✓Middleware

Pruebas

- Se identifican 3 tipos
  - Pruebas dependientes entre ellas.
  - El correcto funcionamiento de un tipo permite probar el siguiente tipo.

Clasificación

- Grado de compatibilidad
  - cuantas pruebas se ejecutan correctamente
- Se define un protocolo para verificación de compatibilidad
  - Futuros dispositivos
  - Actualizable
    - ✓Primera experiencia
    - ✓Mejoras en el horizonte

Sistemas

Windows 7	Microsoft Office - Outlook
Windows 8	Microsoft Office – Outlook
ubuntu	Libre Office – Thunderbird
CentOS	Libre Office – Thunderbird
Mac	Microsoft Office – Firefox
android	Manager de Token
iOS	Manager de Token

Desarrollo

- Instalación
  - Drivers
    - ✓Interacción con fabricantes
  - Manuales a nivel de usuario

- Dificultades
  - Falta de bibliotecas
  - Falta de soporte en algunos sistemas

Desarrollo

- Certificados
  - Necesario crearlos
    - ✓Openssl
  - Distintos algoritmos
    - ✓SHA
    - ✓RSA
  - Para firmar mails
- Importarlos al token

Desarrollo

- Interacción con aplicaciones
  - Firma de documentos
    - ✓MS Word
    - ✓Libre Office
    - ✓PDF
  - Firma de mails
    - ✓Outlook
    - ✓Mail
    - ✓Thunderbird

Desarrollo

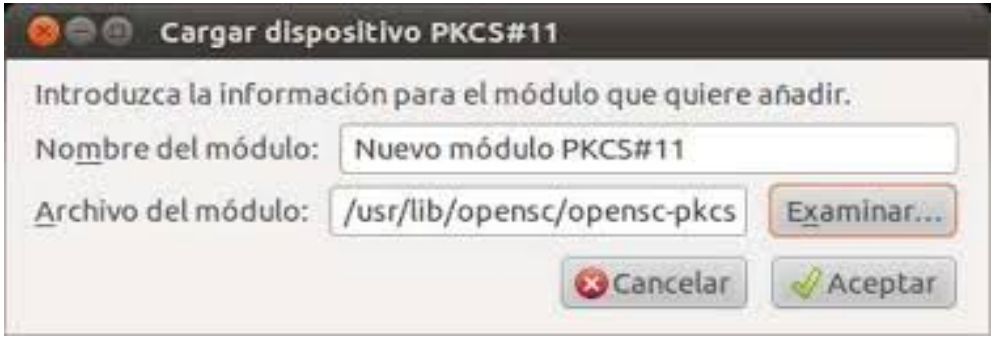
- Middleware
  - Implementación api PKCS#11
- PKCS#11 (Cryptoki)
  - **Cryp**tographic **Tok**en **I**nterface
  - estándar que define una api independiente de la plataforma
  - utilizar, agregar, modificar y borrar certificados y claves de los tokens

Desarrollo

- Middleware
  - Investigación de los estándares.
  - Conocimiento de la api y sus funciones.
  - ¿Cómo interactuar con la api?

Desarrollo

- Identificar el modulo que implementa la api.
- Configurarlo con aplicaciones
  - Firefox
  - Thunderbird



Conclusiones

- Experiencia enriquecedora
  - Nuevos conocimientos
  - Ideas a futuro
  - Enfoque diferente
    - ✓Definición de pruebas
    - ✓Como encarar cada una
  - Distintos dispositivos
  - Interacción con profesionales del área

Conclusiones

- Experiencia para poder encarar problemas similares
  - Compatibilidad
    - ✓Aplicaciones
    - ✓Hardware
    - ✓Estandares

¡Gracias!

Recomiendo charla sobre la Carrera
Próximos comienzos: ¡ya! ☺ y Julio

- Sitio: http://www.ces.com.uy
- Carrera: http://www.ces.com.uy/index.php/carrera-de-testing
- Twitter: @ces_com_uy
- Facebook: /CentroDeEnsayosDeSoftware
- Plataforma de capacitación: http://www.capacitacion.ces.com.uy
- Blog: http://blog.ces.com.uy
- Contacto: info@ces.com.uy
- Youtube: Centro de Ensayos de Software