30

PKI INTERNA EN EL MINISTERIO DEL INTERIOR

Francisco Romero Royo
Jefe del Área de Redes y Comunicaciones
S. G. del Centro de Sistemas de Información. Subsecretaría. Ministerio del Interior

VOLVER

QUÉ ES UNA P. K. I.

- P.K.I. = Infraestructura de Clave Pública
- Un conjunto de componentes tecnológicos y procedimientos que proveen servicios de:
  - Autenticación
  - Confidencialidad
  - Integridad
  - No repudio
- Permite securizar el intercambio y almacenamiento de información por medio de criptografía de clave pública
- Equivalente a la firma, ensobrado y sellado tradicionales
- Requiere tanto componentes tecnológicos como procedimientos normalizados:
  - "La cadena es tan fuerte como el más débil de los eslabones"

IMPLEMENTACIÓN: ÁMBITO

- Altos cargos del Ministerio y extensión progresiva a resto de usuarios
- Red de Subsecretaría (inicio del proyecto)
  - 8 edificios
  - 1200 puestos de trabajo (unos 300 con lectores SmartCard)
  - Redes locales Ethernet 100Mbps, enlaces de 512 a 2048Kbps
  - Direccionamiento oficial Intranet Administrativa (10.11.x.x)
  - Servidores de aplicaciones Sparc / Solaris e Intel / Linux
  - Servidores de disco Intel / Windows 2000
  - Puestos de trabajo Windows 2000 y Windows NT
  - Gestión de usuarios utilizando Microsoft Active Directory (login único)
- Resto de unidades del Departamento
  - Enlaces a 2048Kbps (anillo red InterLAN)
  - Firewall en cada punto de conexión InterLAN
  - Direccionamiento oficial (utilizando NAT en algún caso)

IMPLEMENTACIÓN: SOLUCIÓN ADOPTADA

- Se optó por "KeyOne" de Safelayer
- Autoridad de Certificación (CA) y Servidor de Recuperación de Claves (KA) en una misma máquina (Sun Sparc, s.o. Solaris)
- Gestión de CA/KA y autoridad de registro (RA) sobre Windows 2000
- Ambas máquinas en una misma red local aislada del resto por un firewall (Firewall-1 de Checkpoint, funcionamiento en cluster de Stonesoft, hardware de Sun con s.o. Solaris)
- Otros equipos directamente relacionados (en la intranet):
  - Almacenamiento en Oracle corporativo (Cluster Sun Solaris)
  - Servidor LDAP para publicación de certificados/CRL (Active Directory de Microsoft)
  - Servidor Web para publicación de certificados/CRL (Apache sobre Linux)

VOLVER

  - Autoridad de registro (RA) móvil (equipo portátil) sobre Windows 2000
- Tarjetas criptográficas Gemplus personalizadas "on site" (varios modelos de lectores distintos)

IMPLEMENTACIÓN: CARACTERÍSTICAS DE LA P.K.I.

- Clave raíz generada en ceremonia presidida por la Subsecretaria
  - 4096 bits
  - 30 años de vigencia
  - Almacenada en dispositivo criptográfico nCypher conectado a la CA
  - Claves de acceso almacenadas en 3 tarjetas asignadas a diferentes personalidades
  - Acceso a la clave raíz requiere dos tarjetas
- Las tarjetas de usuario contienen 3 certificados (asociados al correo electrónico) cada uno para un propósito diferente:
  - Autenticación
  - Firma (integridad / no repudio)
  - Cifrado
- Autenticación y firma se mantienen separados para no confundir el acceso a un sistema con la aprobación de un documento
- Cifrado se mantiene separado del resto porque las claves privadas se almacenan en la KA, para poder recuperarlas en caso de inutilizarse la tarjeta
- Las claves públicas se publican en Active Directory y en un servidor web
- Además de los certificados necesarios para el funcionamiento de la P.K.I. y de los de usuario, la CA permite generar todo tipo de certificados estándar como por ejemplo:
  - Para controladores de dominio Windows 2000
  - Para servidores Web seguros (HTTPS://)
  - Para administración de servidores por SSH
  - Para conexiones entre equipos (stunnel, IPSec, VPN...)

APLICACIONES DE LA P.K.I. CORREO SECURIZADO

- Fue la aplicación para la que se diseñó inicialmente
- Uso de estándares: S/MIME
- Cualquier cliente estándar (se necesita acceder al certificado y por lo tanto ha de tener soporte de SmartCard)
- En la práctica se accede con tres clientes:
  - Outlook Express (80% de los usuarios)
  - Outlook
  - Webmail
- En Windows, plataforma completamente integrada (CryptoAPI)
- En los clientes Outlook y Outlook Express se detectaron graves deficiencias en su implementación (subsanables)

VOLVER

- Acceso a claves públicas y CRL: por LDAP, listín en Web y distribución inicial de certificados a las libretas de usuarios
- Para Webmail, se generó un componente ActiveX
  - El cliente ha de tener acceso al certificado (soporte de SmartCard)
  - Conexión securizada cliente/servidor
  - No se transmiten las claves privadas
  - No se transmite el mensaje completo
  - Solo se transmiten las claves simétricas de cifrado del mensaje (descifrado) o el hash del mensaje (firma)
  - Permite generar notificaciones de envío y recepción firmadas por el servidor

APLICACIONES DE LA P.K.I. SMARTCARD LOGON

- Permite autentificarse en el dominio Windows 2000 por medio de tarjeta criptográfica
- Puede forzarse como único método para usuarios determinados (por seguridad)
- Proceso:
  - En cada Controlador de Dominio se genera petición de certificado
  - La CA procesa la petición y firma el certificado
  - Se instala el certificado en cada Controlador de Dominio
- Los certificados (claves públicas) de los usuarios y el raíz de la CA se almacenan en el AD (disponibles en todo el dominio por medio de CryptoAPI y por medio de LDAP)

APLICACIONES DE LA P.K.I. CERTIFICADOS PARA SERVIDORES WEB

- Permiten acceso securizado
- Multiplataforma
- El cliente ha de tener instalado el certificado raíz
- Total de certificados en la actualidad: 10
- Aplicaciones:
  - Webmail
  - Registro Telemático de entrada de documentos
  - Servidores web corporativos (Intranet / Internet)

APLICACIONES DE LA P.K.I. VOTO ELECTRÓNICO

- Utilizado en la prueba de Voto No Presencial (por internet) en la Elecciones Generales del 14 de Marzo de 2.004
- Se generaron tarjetas para los ciudadanos participantes en la prueba (unas 280)
- Se generaron certificados para los servidores del sistema (recepción de votos, almacenamiento, recuento)
- Se generaron tarjetas para los Depositarios de Votos

APLICACIONES DE LA P.K.I. REGISTRO TELEMÁTICO DE SALIDA

- En fase de desarrollo
- Para el Registro de Entrada, el certificado de la web ha sido generado por la CA
- Para el de salida se precisa enviar las comunicaciones a la D.A.U. del ciudadano, gestionada por Correos
- Las comunicaciones se cifran y firman por medio de un certificado generado por la CA
- Las claves públicas y acceso a CRL se proporcionan a Correos para que pueda verificar las comunicaciones recibidas

APLICACIONES DE LA P.K.I. FIRMA ELECTRÓNICA INTERNA

- La plataforma de usuario ha de soportar el acceso a las SmartCard. Eso implica Windows hoy por hoy.
- La integración CryptoAPI facilita mucho el acceso desde clientes Windows
  - Permite usar la infraestructura del s.o.
  - Integrado con Internet Explorer
  - Acceso simplificado con CAPICOM (similar a aplicaciones desarrolladas en Patrimonio)
- Los certificados y documentos con firma generados se pueden procesar en entorno multiplataforma (herramientas OpenSSL en Linux), gracias a seguirse estándares

CONCLUSIONES

- Tecnología suficientemente madura
  - Pese a encontrarse errores en las implementaciones o algunas dificultades por ser tecnología emergente, es posible conseguir una funcionalidad completa
  - El soporte a nivel software es muy completo en los principales sistemas operativos
  - A nivel hardware, en la actualidad solo se consiguió soporte fiable, sencillo y operativo sobre Windows con CryptoAPI. En Linux existen varias iniciativas pero por el momento son limitadas.
- Una experiencia positiva.
  - Hasta el momento, todas las funcionalidades que se han ido exigiendo a la P.K.I. han podido ser resueltas satisfactoriamente.
  - Aparte de las funcionalidades directas conseguidas, constituye una muy interesante preparación para el futuro, con la inminente P.K.I. a nivel nacional (D.N.I. electrónico) ya que el sistema es funcionalmente equivalente.

VOLVER