

Habemus raíz

Autoridad Certificadora Raíz Nacional de Uruguay



@agesic
@certuy
@fcm_uy

#GEa11

Ing. Fernando Cócaro
fernando.cocaro@agesic.gub.uy

Agenda



- Infraestructuras de Clave Pública
 - Componentes, estándares, políticas y prácticas de certificación, Autoridades y funciones
 - Modelo de operación en Uruguay
 - Participantes, roles y su relación
- Puesta en marcha de una PKI
 - Ceremonia de Claves
 - Resultados
 - Trabajos a futuro

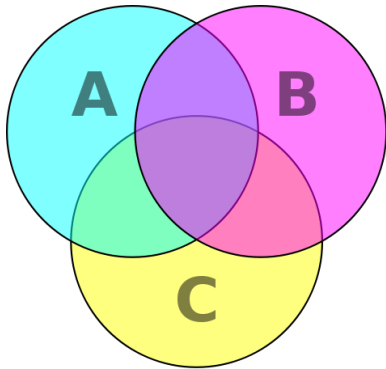
Infraestructura de Clave Pública

¿Qué es?

- Sistema para la gestión de Certificados Electrónicos y aplicaciones de Firma Electrónica (Avanzada)
- Debe proporcionar garantías de:
 - Integridad
 - Autenticidad
 - No repudio
 - Confidencialidad



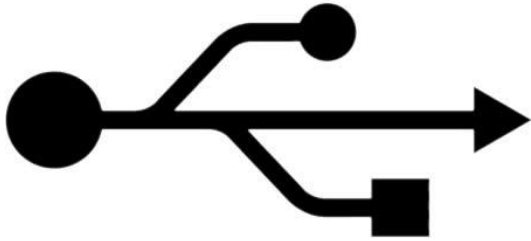
Infraestructura de Clave Pública



Conjunto de componentes

- Hardware, Software, Políticas, Procesos y Procedimientos (CP, CPS)
 - Permite realizar operaciones criptográficas con garantías
- Arquitectura diseñada para probar la identidad de entidades en la red

Estándares Internacionales



Definen requisitos de conformidad internacional:

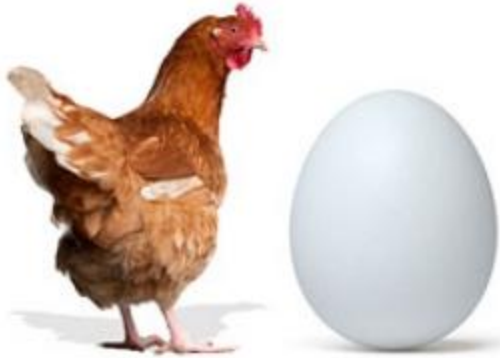
- ITU-T X509
- RFC 3647, 4211, 5280, 6277, etc
- ETSI TS 102 042 / ETSI TS 101 456
- Web Trust para CA
- CEN-CWA 14167
- CEN-CWA 14169



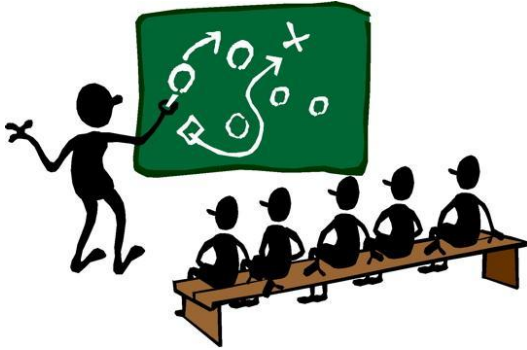
Cadena de confianza

¿Cómo hace una CA para firmar?

- Cuenta con un Certificado propio
- Utiliza la clave privada para firmar los certificados emitidos por ella
- Se necesita de un certificado raíz que permita firmar otros certificados
 - Certificado Auto-firmado
 - Se forma una jerarquía de CAs



Políticas y procedimientos



- Política de Certificación (CP)
 - Se detalla la infraestructura (Actores, Roles, Funciones, etc.)
 - Tipos de certificado
 - Indican el nivel de seguridad mínimo asociado.



- Declaración de Prácticas de Certificación (CPS)
 - Servicios ofrecidos y procedimientos de gestión de los certificados
 - Información detallada del ciclo de vida

Autoridad de Certificación

Emisión de Certificados Electrónicos

- De acuerdo a sus CPs (perfiles de certificados)
 - Opera de acuerdo a su CPS
- Entidad conocida y aceptada, en la que confían todos los participantes
- Certifica con su firma que la información del certificado fue validada
 - Asocia identidad con una clave pública
 - El sujeto del certificado es quién dice ser



Autoridad de Registro

Inicio de la solicitud de un certificado

- Entidad de confianza dependiente de una Autoridad de Certificación
 - Registra las solicitudes de certificados
- Comprueba la veracidad de los datos suministrados por el solicitante
- Solicita a su CA la emisión del certificado



La Autoridad Certificadora Raíz Nacional



- Primer Autoridad de Certificación en la cadena de confianza
 - Toda CA subordinada:
 - Hereda la confianza de ésta
 - Sometida a sus políticas
 - Emite ante resolución de la UCE
- Habilitador tecnológico
 - Gestionado por AGESIC (Ley 18.600)

A nivel internacional



Gobiernos con un esquema de PKI

- Modelo de acreditación con una raíz
 - Argentina, Brasil, Chile, Australia, entre otros
- Modelo Federado
 - Estados Unidos
 - Una PKI por federación más una CA bridge para “integrarlas”

Implantación



- Inicia con la adjudicación de la Licitación 02/2010 – Nov. 2010
 - Servicios de consultoría
 - Software y hardware
- Definiciones, modelos de gobernabilidad y operación
 - Estudios regionales y de referencia
 - Escritura de la CP y CPS

Definiciones

- Política
 - Dueño del documento (UCE)
 - Algoritmo de hash (sha256)
 - Validez de la clave privada
 - De la ACRN (20 años)
 - De los Prestadores (10 años)
 - Adecuación a la Ley 18.600
 - ¿Cómo opera la RA?
- Declaración de Prácticas
 - Como ajustar el documento a la CP



Ceremonia de Clave



- Proceso de inicialización de la CA
 - De forma segura, confiable y con garantías de auditoría
 - Instalación de los sistemas
 - **Generación del par de claves** que firmarán los certificados de los PSCA
 - Se sigue un guión detallado de cada acción a tomar
 - Se realiza en presencia de testigos, auditores y otros interesados
 - Se mantiene un registro fílmico de toda la jornada

3 de Noviembre de 2011



El día de la ceremonia de claves

- En instalaciones de Presidencia
- Asistieron más de 30 personas
 - No fue un evento público
- Insumió más de 9 horas
- Se siguió punto a punto el plan marcado
- Se mantuvo el registro fílmico del evento
- Todo el material utilizado y generado se encuentra en una caja fuerte

La clave privada

Es fundamental garantizar su seguridad



- 4 perímetros para llegar a la CA
- CA offline dentro de una caja fuerte
- Tuning al Sistema Operativo
- Clave dentro de un HSM
 - Activación de la clave privada con 3 de 8 custodios
 - Tanto para producción como para backup
- Toda acción es auditada
 - Son necesarias 4 personas para operar

Resultados

- Política de Certificación
 - www.uce.gub.uy/informacion-técnica/politicas/cp_acrn.pdf
- Declaración de Prácticas de Certificación
 - www.agesic.gub.uy/acrn/cps_acrn.pdf
- Primer Lista de Revocación
 - www.agesic.gub.uy/acrn/acrn.crl
- Certificado auto firmado
 - www.agesic.gub.uy/acrn/acrn.cer



Resultados (Cont.)

Lista de revocaciones de certificados

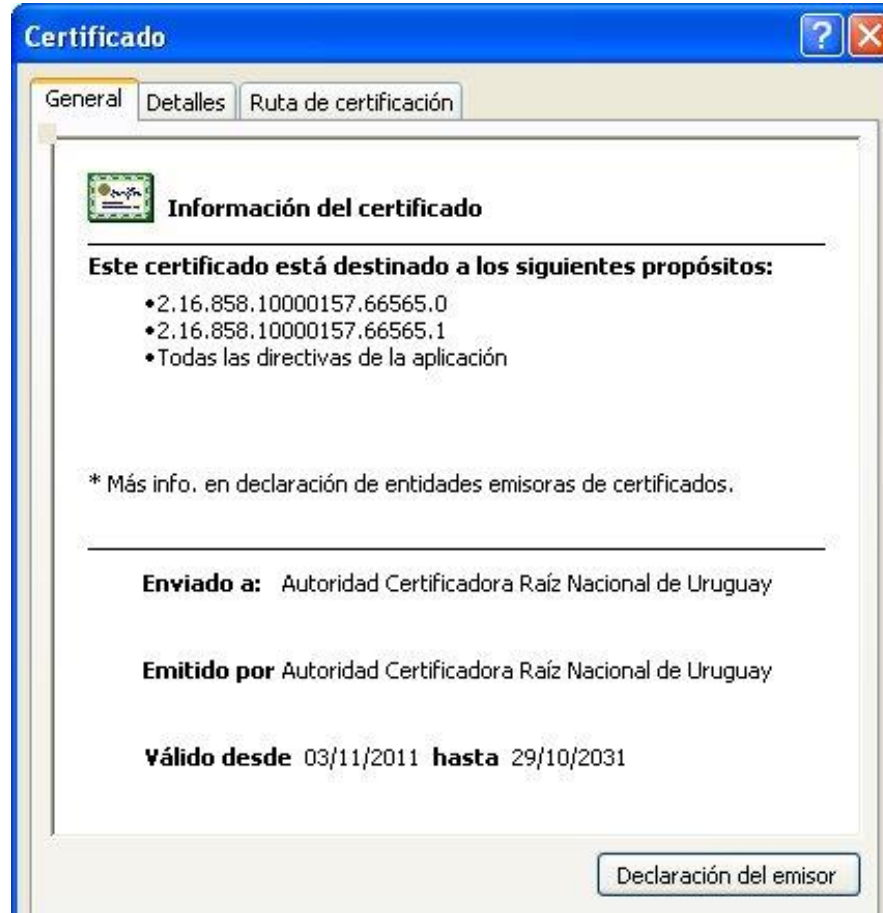
General Lista de revocaciones

 **Información de la lista de revocación de certificados**

Campo	Valor
Versión	V2
Emisor	UY, AGESIC, Autoridad Certificado...
Fecha efectiva	jueves, 03 de noviembre de 2011 ...
Próxima actualización	miércoles, 01 de febrero de 2012 ...
Algoritmo de firma	sha256RSA
Número CRL	1

Valor:

Resultados (Cont.)



The screenshot shows a window titled "Certificado" with three tabs: "General", "Detalles", and "Ruta de certificación". The "General" tab is active, displaying the following information:

Información del certificado

Este certificado está destinado a los siguientes propósitos:

- 2.16.858.10000157.66565.0
- 2.16.858.10000157.66565.1
- Todas las directivas de la aplicación

* Más info. en declaración de entidades emisoras de certificados.

Enviado a: Autoridad Certificadora Raíz Nacional de Uruguay

Emitido por: Autoridad Certificadora Raíz Nacional de Uruguay

Válido desde: 03/11/2011 **hasta:** 29/10/2031

Declaración del emisor

Resultados (Cont.)

Certificado

General Detalles Ruta de certificación

Mostrar: <Todos>

Campo	Valor
Emisor	UY, AGESIC, Autoridad Certifi...
Válido desde	jueves, 03 de noviembre de 2...
Válido hasta	miércoles, 29 de octubre de 2...
Asunto	UY, AGESIC, Autoridad Certifi...
Clave pública	RSA (4096 Bits)
Puntos de distribución CRL	[1]Punto de distribución CRL: ...
Bases del certificado	[1]Directiva de certificado:Ide...
Identificador de clave de as...	92 9e 91 b8 55 28 3d 77 42 2c...

[1]Punto de distribución CRL
Nombre del punto de distribución:
Nombre completo:
Dirección URL=<http://www.agesic.gub.uy/acrn/acrn.crl>

[2]Punto de distribución CRL
Nombre del punto de distribución:
Nombre completo:
Dirección URL=<http://www.uce.gub.uy/acrn/acrn.crl>

Modificar propiedades... Copiar en archivo...

Próximos pasos de la UCE



- Normas
 - Documento de Requisitos Técnicos para los Prestadores (PSC)
 - Políticas de Certificación para certificados emitidos por PSCA
 - Procedimientos de Acreditación
 - Procedimientos de control
- Acciones
 - Acreditación de Prestadores (PSC)
 - Acreditación Internacional
 - Completar la Integración del Consejo Consultivo y Convocarlo



¿Preguntas?



¡Muchas gracias!

fernando.cocaro@agesic.gub.uy



@agesic

@certuy

#GEa11