agesic
agencia de gobierno electrónico
y sociedad de la información

PRESIDENCIA
República Oriental del Uruguay

Firma Electrónica Avanzada

@agesic
@ghdotta

guillermo.dotta@agesic.gub.uy

Objetivos

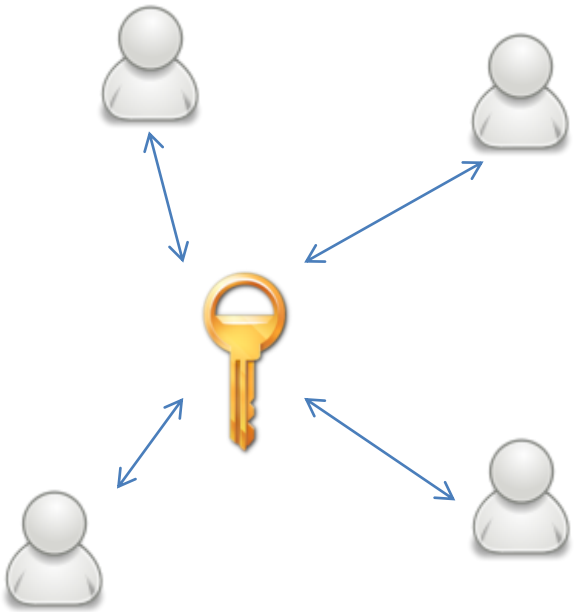
Introducir conceptos generales de Firma Electrónica Avanzada y de Infraestructura de Clave Pública

Mostrar el marco regulatorio y estado actual de implementación en Uruguay

Agenda

- Introducción
- Certificados Digitales
- Firma Electrónica
- Firma Electrónica en Uruguay – Marco Regulatorio

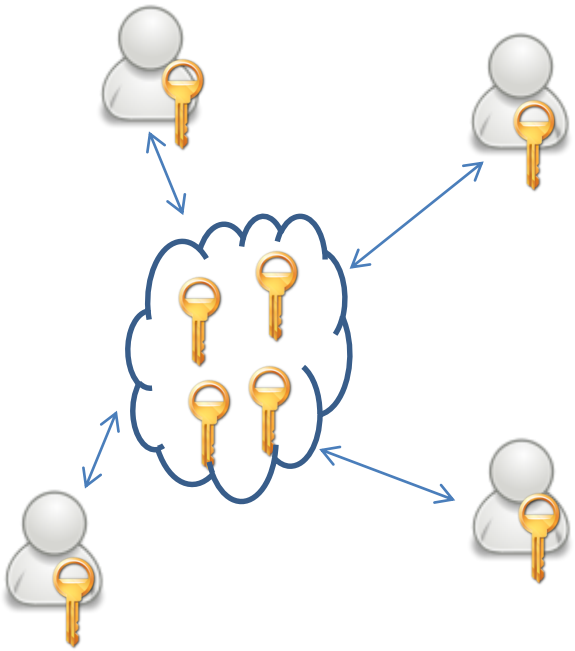
Introducción



- Criptografía simétrica es suficiente en muchos contextos

- Limitaciones:
  - Gestión y Distribución de Claves
  - Autenticación de origen – No Repudio

Introducción

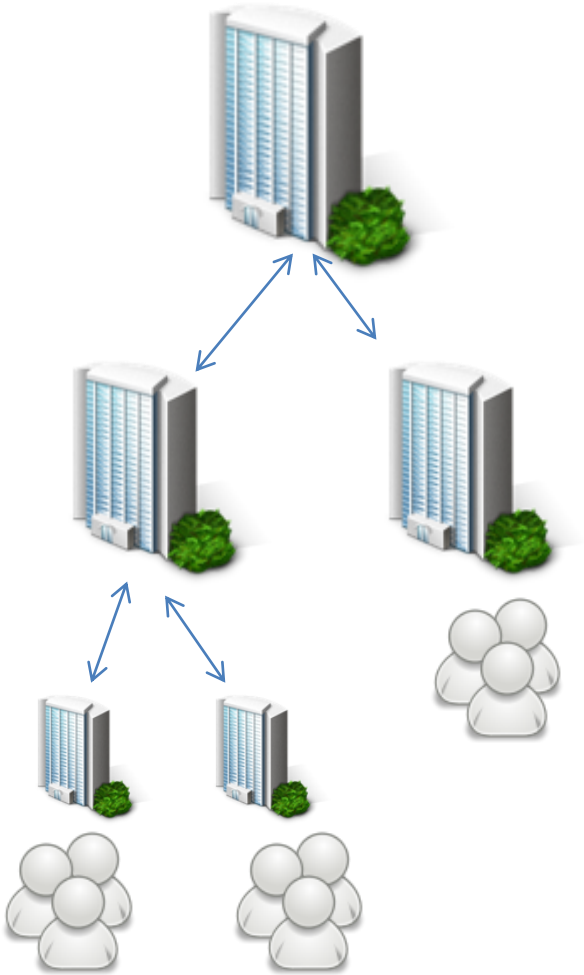


- Criptografía asimétrica: *Par de claves*
  - Una pública para distribuir
  - Una privada para uso exlcusivo, que *nunca se comparte*
- Distribución de claves *Públicas*
  - **PKI**
  - PGP
  - Otros…

¿Cómo sé de quién es una clave pública?

- Autoridades Certificadoras emiten certificado con:
  - Datos del suscriptor
  - Clave Pública
- Concepto de certificado aparece en 1978 [Kohnfelder's *Bachelor's* thesis]
- X.509 – "El estándar"
  - v.1 (1988) – sin extensiones
  - v.2 – No aporta mucho más
  - v.3 (1997) actual – incluye extensiones
  - RFC2459, 3280, **5280** – "La guía"

¿Cómo sé quién es una CA?



Infraestructura de Claves Públicas (PKI)

- Jerarquía de CA, con una raíz
- Método seguro, confiable y escalable para la distribución de claves públicas de forma segura, correcta y verificable.
- Establece globalmente una relación directa entre una clave pública y su "propietario"

Infraestructura de Claves Públicas

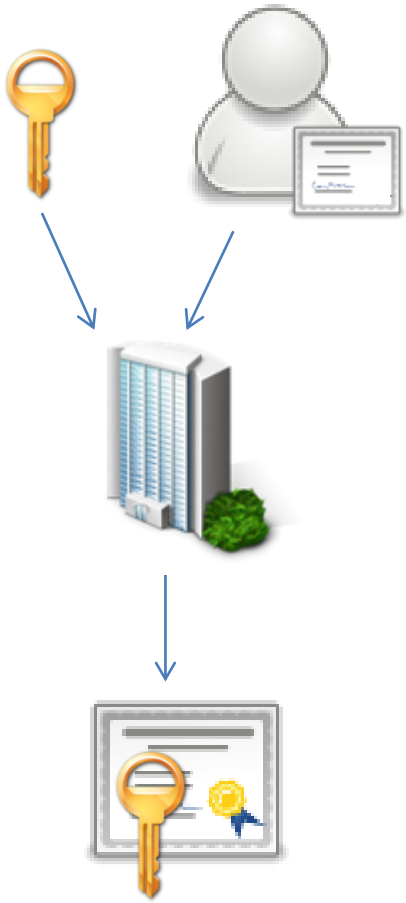
- Conjunto complejo de tecnologías y procedimientos que garantizan:
  - Autentificación
  - Confidencialidad
  - Integridad
  - No repudio
- En transacciones no presenciales a través de redes privadas o públicas utilizando criptografía de clave pública.

CONFIANZA!!!

Certificados Digitales

Certificado Digital

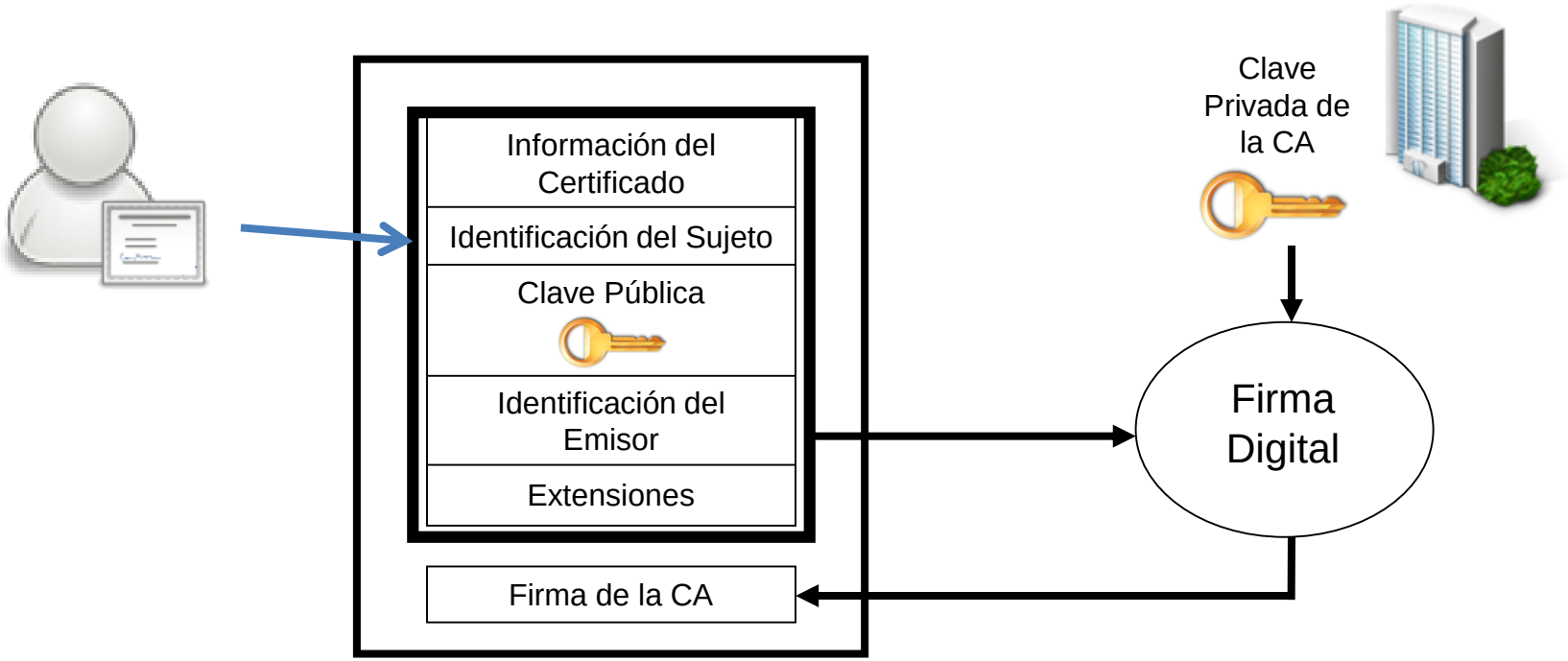
- Documento electrónico emitido por la CA, que vincula la **identidad de un sujeto** con su clave pública
  - Codificación ASN.1
  - Estructura X.509
  - Contenido depende de la PKI, de la CA y del sujeto
    - ***Políticas de Certificación***



Certificado Digital

- Clave pública es la del sistema criptográfico subyacente
  - RSA, curvas elípticas u otro
- Datos del sujeto dependen del sujeto!
  - Persona física
  - Persona jurídica (empresa)
  - Sitio web
  - Autoridad de Certificación!

Creación de un Certificado X.509 Completo



Uso de Certificados Digitales

- A quiere enviar documento firmado a B

1. A firma el documento con su clave privada

2. A envía el documento firmado a B

4. B Obtiene clave pública de A del certificado y valida la firma del certificado para verificar su integridad

5. B valida el certificado de A para verificar su identidad

5. Siempre y cuando la validación del certificado esté bien hecha, B puede concluir que el documento fue efectivamente enviado por A (Autenticación y no Repudio) y nadie lo modificó en el camino (Integridad)

Observaciones

- El firmante solo usa su clave privada
- El validador solo usa el certificado público
- Si el documento es un número aleatorio previamente enviado por B, se tiene autenticación
  - Certificados de SSL y TLS
  - Login mediante certificados

Observaciones (cont.)

- ¿De dónde saca B el certificado?
  - Lo tiene previamente
  - Directorio público
  - Del documento mismo – **Estándares de Firma**

Validación del certificado

- Identidad del sujeto actuante
  1. Codificación y Estructura – ASN.1 y X.509
  2. Vigencia
  3. Status de revocación – CRL, OCSP
  4. Cadena de Confianza – Firma de la CA
     - Validación de certificado de la CA
     - Hasta una raíz de confianza (*Trust Anchor*)

Validación del certificado (cont.)

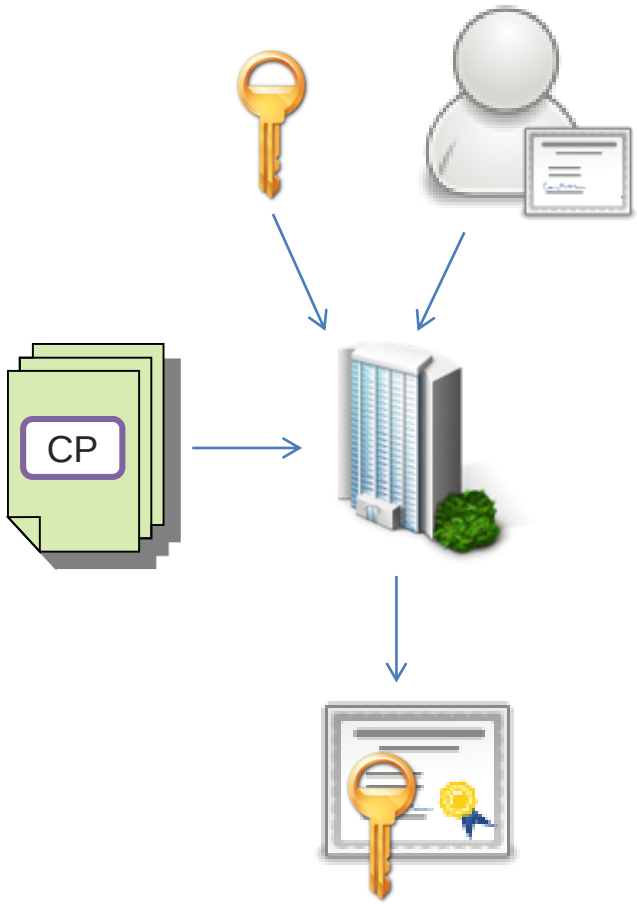
- Tipo de sujeto actuante
  1. Uso general – Si es de CA o no
  2. Uso Específico – Certificate Policies, OID

A = ?

¿Qué pasa con la Autorización?

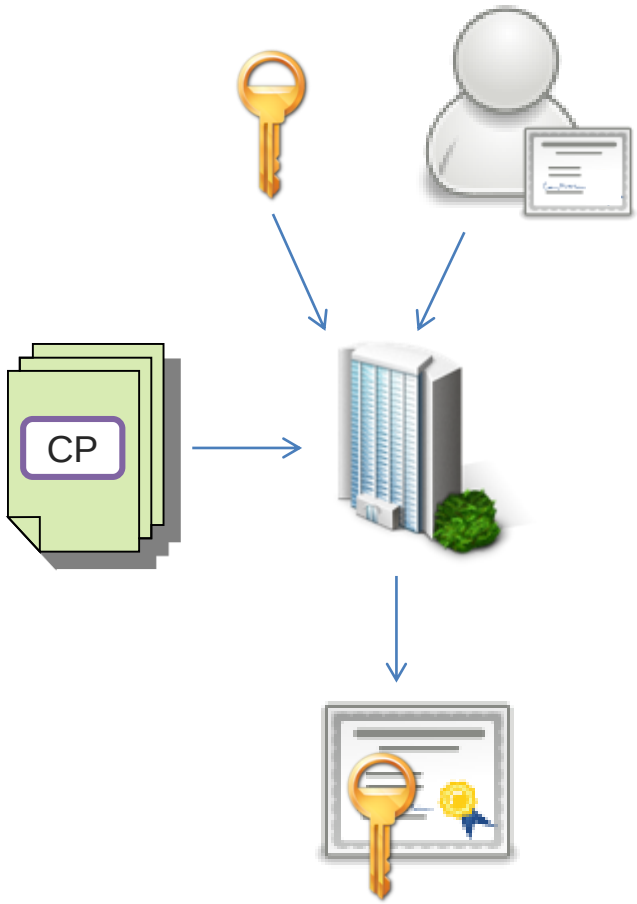
Perfil del Certificado

- Características que deben cumplir los certificados digitales emitidos por una Autoridad Certificadora para unas condiciones de uso determinadas.



Perfil del Certificado

- Eso se especifica en la **Política de Certificación** asociada
  - Elaborada por la CA, por la Root o por organismo regulador
    - En Uruguay, por la UCE
  - RFC 3647
  - Define comunidad objetivo, usos permitidos, controles de seguridad y ***contenido***
  - *OID*



Perfil del Certificado

- Política 1
  - Subject: C=UY, CN=GUILLERMO DOTTA, SerialNumber=DNI40906816
  - KeyUsage: digitalSignature, contentCommitment
  - ExtendedKeyUsage: clientAuth
  - Basic Constraits: CA=False
  - Certificate Policies: 2.16.858.10000157.66565.2
- Política 2
  - Subject: C=UY, O=Empresa S.A. CN=CA de Empresa
  - KeyUsage: keyCertSign, CRLSign
  - Basic Constraits: CA=True, maxPathLen=0
  - Certificate Policies: 2.16.858.10000157.66565.0

Y esto es sólo la parte visible…

Firma electrónica

¿Qué dice?

```
50 61 72 61 20 70 6F 64 65 72 20 6C 65 65 72 20 63 75 61 6C
71 75 69 65 72 20 64 6F 63 75 6D 65 6E 74 6F 2C 20 6E 65 63
65 73 69 74 6F 20 63 6F 64 69 66 69 63 61 63 69 6F 6E 20 79
20 65 73 74 72 75 63 74 75 72 61
```

- Aplicando UTF-8
  - «Para poder leer cualquier documento, necesito codificacion y estructura»

Con la firma pasa lo mismo, tengo que saber interpretarla!

Estándares de Firma

- Definen
  - Alcance de la firma
  - Reglas de canonicalización
  - Codificación del Digest y la firma
  - Estructura de la metadata
  - Certificado del firmante

- Dependen del tipo de Documento

```
<Signature>
  <SignedInfo>
    <CanonicalizationMethod />
    <SignatureMethod />
    <Reference>
       <Transforms>
       <DigestMethod>
       <DigestValue>
    </Reference>
    <Reference /> etc.
  </SignedInfo>
  <SignatureValue />
  <KeyInfo />
  <Object />
</Signature>
```

Estándares de Firma

- XMLDsig, XAdES-BES, XAdES-T, XAdES-C

- PDF-Signature, PAdES

- PKCS#7, CMS, CAdES

¿ HL7 INTERNATIONAL ?

agesic
agencia de gobierno electrónico
y sociedad de la información

PRESIDENCIA
República Oriental del Uruguay

Firma electrónica en Uruguay

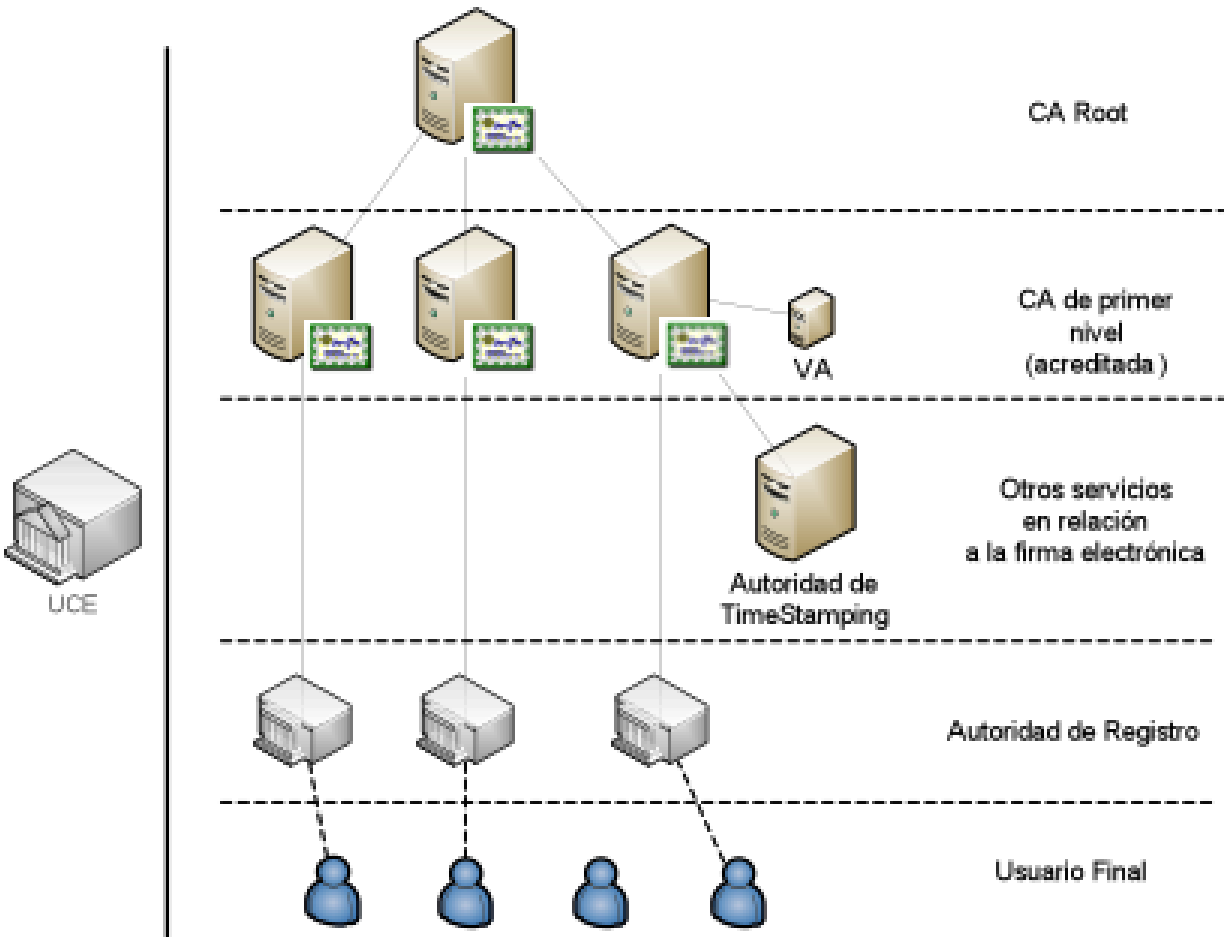
Marco Regulatorio

Ley de Firma Electrónica

- Ley 18.600:
  - Firma Electrónica
  - Firma Electrónica avanzada
- Infraestructura Nacional de Certificación Electrónica
  - Unidad de Certificación Electrónica
    - Consejo Asesor

PKI Uruguay

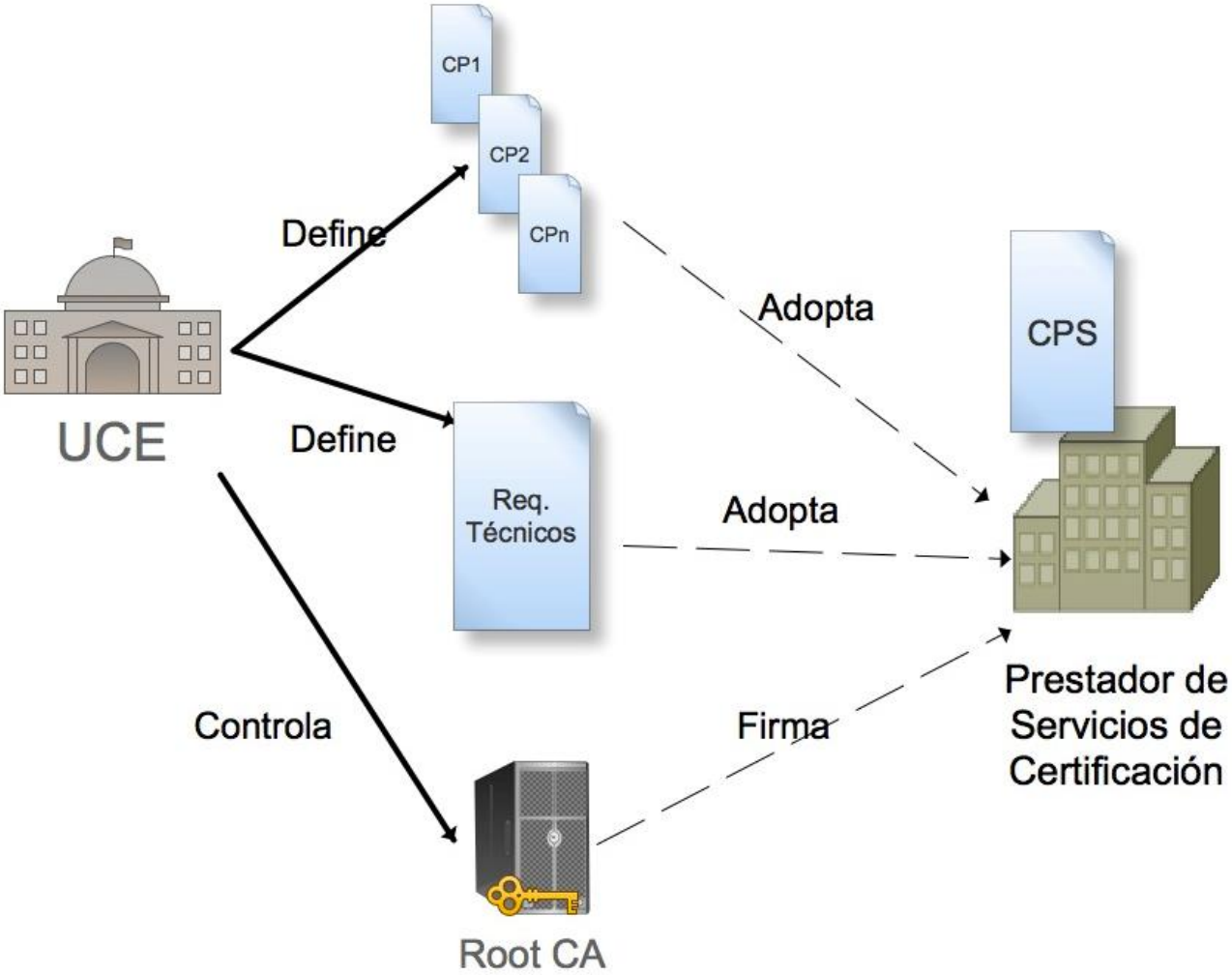
- La UCE es el órgano de control de la infraestructura.



Prestadores de Servicio de Certificación

- Decreto 436/2011
  - Requerimientos formales
  - Garantías financieras
  - Requerimientos técnicos
  - Condiciones de suspensión
  - Esquemas de salida

Modelo de de regulación



Tipos de Certificados

Prestadores de Servicios de Certificación

- CP PSC

Personas Físicas

- CP Persona Física

Personas Jurídicas

- CP Persona Jurídica

Persona Física

- Identifica la firmante como el titular del certificado
- Requiere verificación fisica del titular con documentación:
  - CI o Pasaporte
- Emisión “on-line” o Batch (con proceso auditado)
- Emisión únicamente sobre dispositivo criptográfico seguro
- Revocación:
  - 24x7
  - Plazo de efectivo 12hrs
  - Automática, presencial o remota

Persona Jurídica

- Certifica que el emisor de un documento electrónico emanado de un sistema es la persona jurídica titular del certificado.
- Crea figura del:
  - Titular
  - Referente
- Requiere verificación de documentación del titular y referente
- Emisión “on-line” o Batch (con proceso auditado)

- Emisión en dispositivo criptográfico seguro o software
- Revocación:
  - Horario de Oficina
  - Efectivo 24 hrs
  - Presencial o “de oficio”

Situación Actual en Uruguay

- Aplicaciones:
  - PJ: Factura Electrónica, DUA, Plataforma de eGov, BROU, MIEM, eNotificaciones, URCDP, Caja Notarial, HCEO, Teleimagenología
  - PF: BCU, BROU, DGI, JUTEP, Expediente Electrónico, Trámites en Línea, MEF, eNotificaciones, Control de Acceso Federado, Caja Notarial
- Prestadores:
  - El Correo Uruguayo
  - Abitab
  - Ministerio del Interior (cédula electrónica)

agesic
agencia de gobierno electrónico
y sociedad de la información

PRESIDENCIA
República Oriental del Uruguay

Preguntas