Firma Digital

Santiago Paz

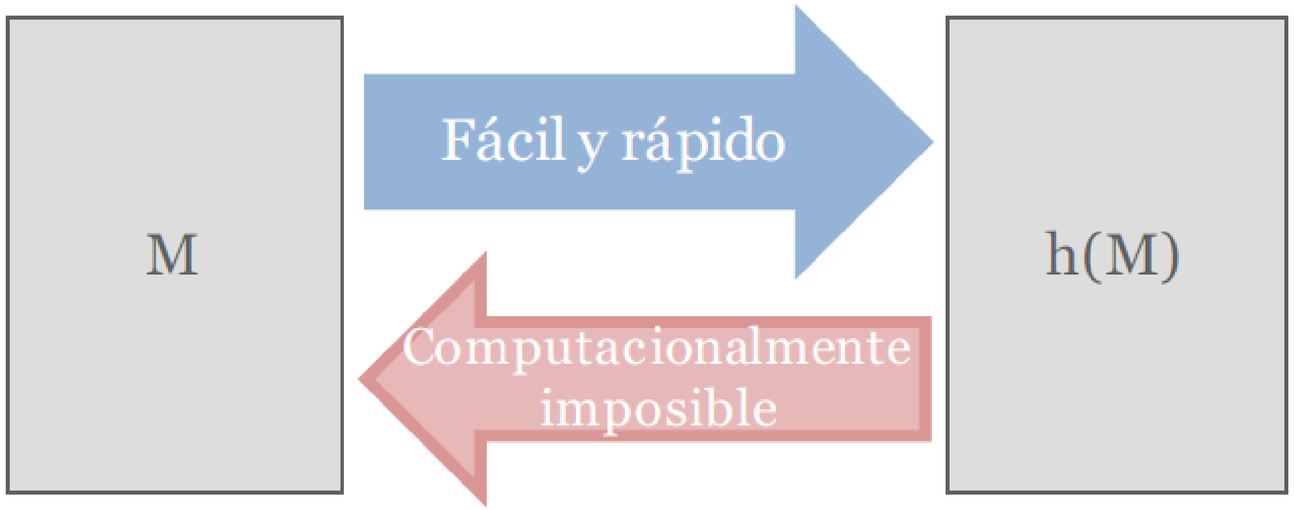
AGENDA

1. Funciones Hash
2. Criptografía Asimétrica
3. Firma Digital
4. Certificados X509
5. PKI
6. Casos de Uso

BID
Banco Interamericano de Desarrollo

Los Hash

Funciones que al aplicarlas sobre un mensaje, devuelven solo un “resumen” de largo fijo h(M). Encontrar M desde h(M) será muy complejo o imposible (?)

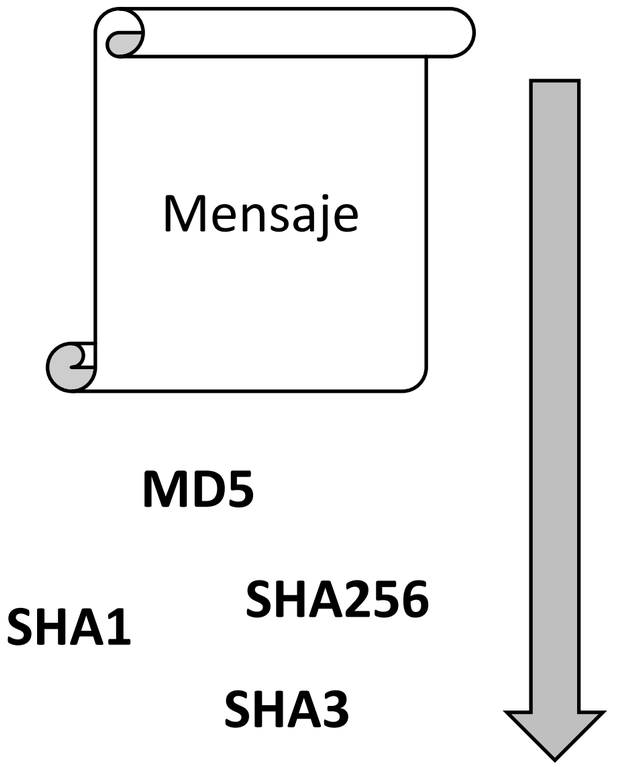


BID
Banco Interamericano de Desarrollo

Los Hash

Caracteristicas

- Unidireccionalidad
- Compresión
- Facilidad de calculo
- Difusión
- Resistencia a colisiones



0920e7009b56c4418b9a04f87ffed351b5d1be5a

BID
Banco Interamericano de Desarrollo

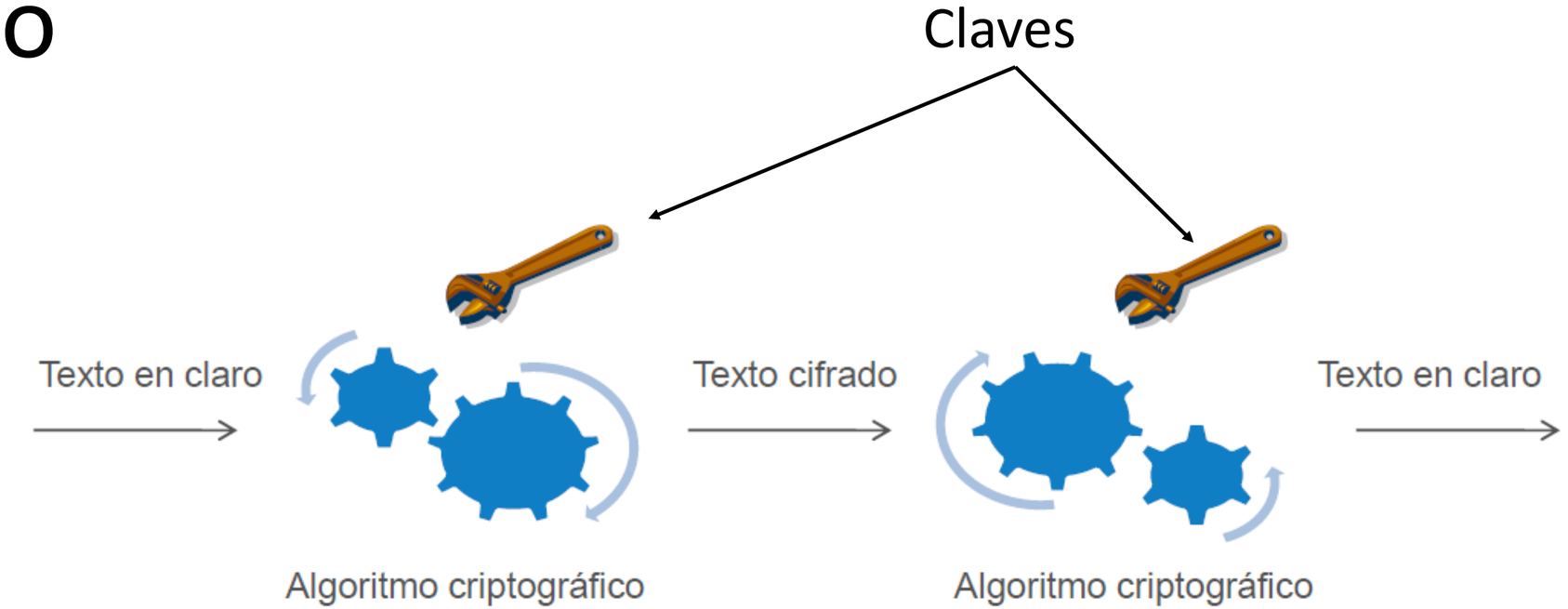
Cifrado



Transformar un mensaje de manera que un tercero que no vea no pueda reconocerlo

BID
Banco Interamericano de Desarrollo

Cifrado



Transformar un mensaje de manera que un tercero que no vea no pueda reconocerlo

BID
Banco Interamericano de Desarrollo

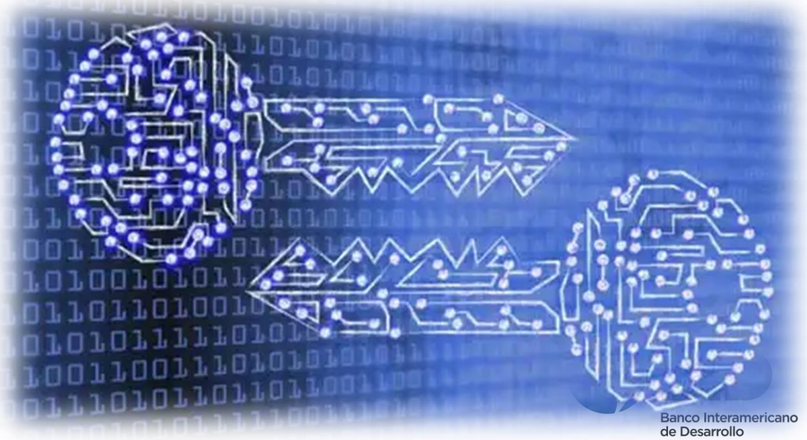
Criptografía

Simétrica

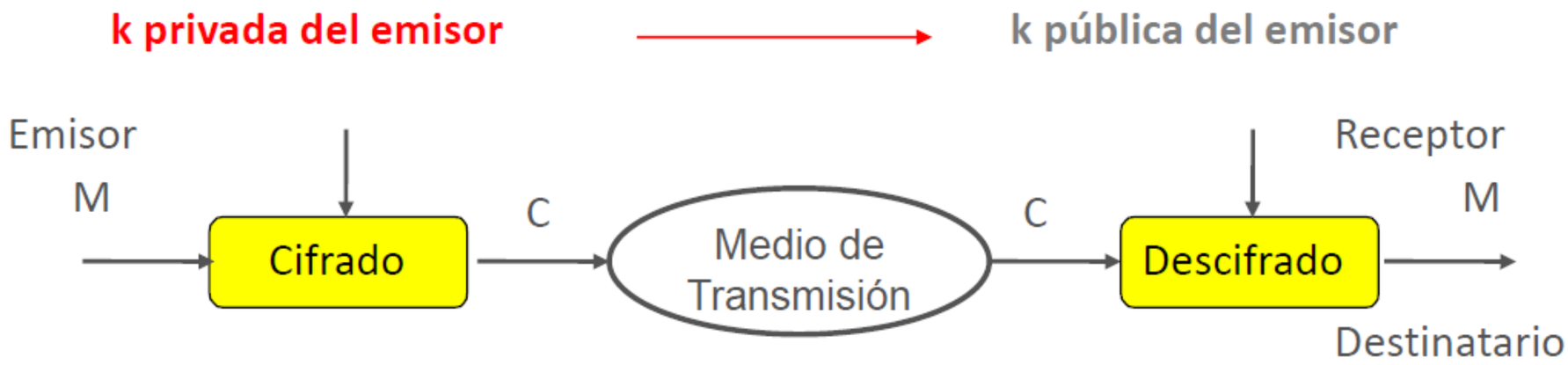
- DES
- 3DES
- AES
- IDEA
- RC4
- A5

Asimétrica

- DH
- RSA
- ECC
- ElGamal



Criptografía asimétrica



- Lo que hago con una lo deshago con la otra
- La k pública es realmente pública

BID
Banco Interamericano de Desarrollo

Características de la criptografía asimétrica

- Intercambio y distribución de claves ✓
- Largo de claves
- Duración de claves
- Performance
- Autenticidad de origen y no repudio

BID
Banco Interamericano de Desarrollo

Características de la criptografía asimétrica

- Intercambio y distribución de claves ✓
- Largo de claves ☒
- Duración de claves
- Performance
- Autenticidad de origen y no repudio

BID
Banco Interamericano de Desarrollo

Características de la criptografía asimétrica

- Intercambio y distribución de claves ✓
- Largo de claves ☒
- Duración de claves ✓
- Performance
- Autenticidad de origen y no repudio

BID
Banco Interamericano de Desarrollo

Características de la criptografía asimétrica

- Intercambio y distribución de claves ✓
- Largo de claves ☒
- Duración de claves ✓
- Performance ☒
- Autenticidad de origen y no repudio ✓

BID
Banco Interamericano de Desarrollo

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

3. B Obtiene el certificado digital de A

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

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

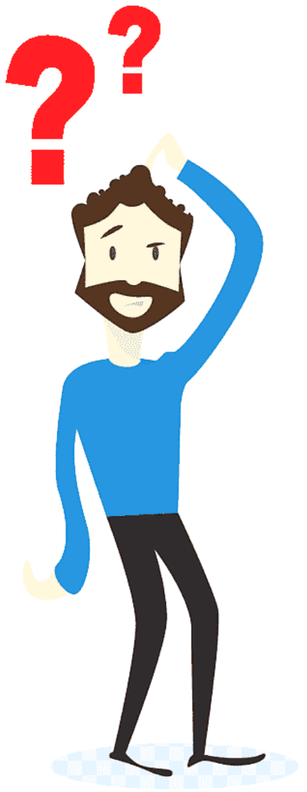




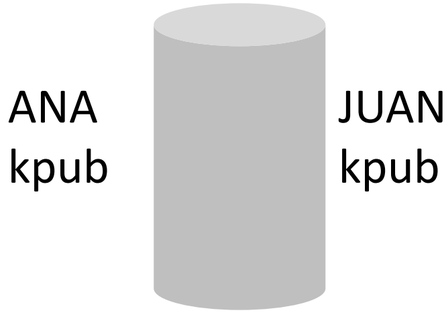


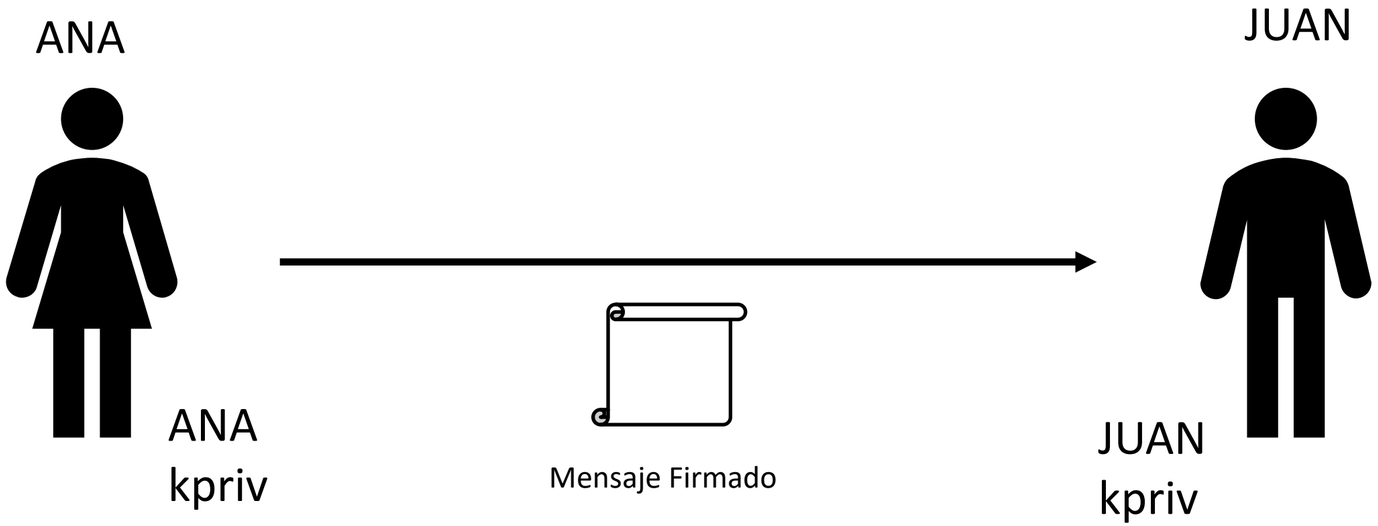
6. Siempre y cuando la validación del certificado esté bien hecha, B puede concluir que el documento fue efectivamente enviado por A (Autenticación y no Repudio) y nadie lo modificó en el camino (Integridad)

Certificados X.509



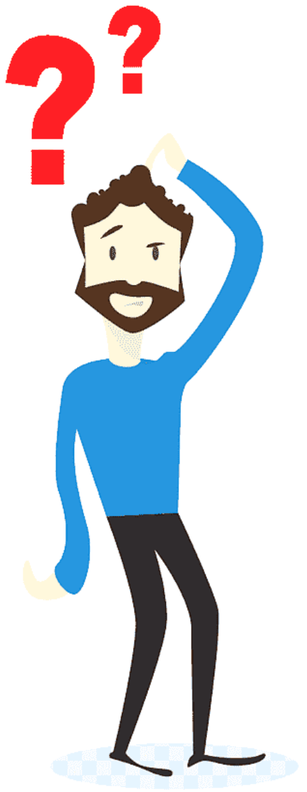
- Como se de quien es la clave???



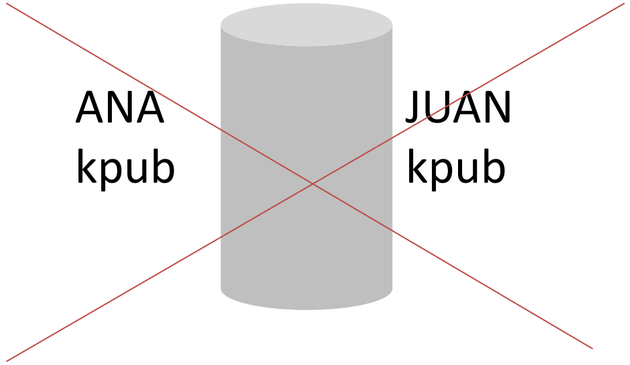


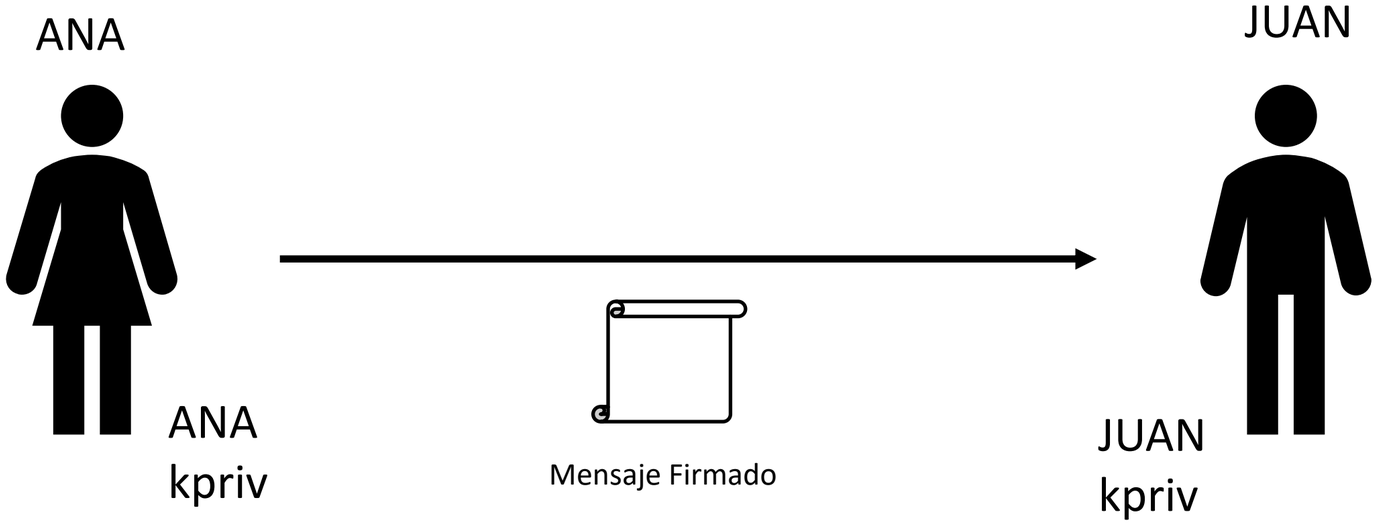
BID
Banco Interamericano de Desarrollo

Certificados X.509



- Como se de quien es la clave???



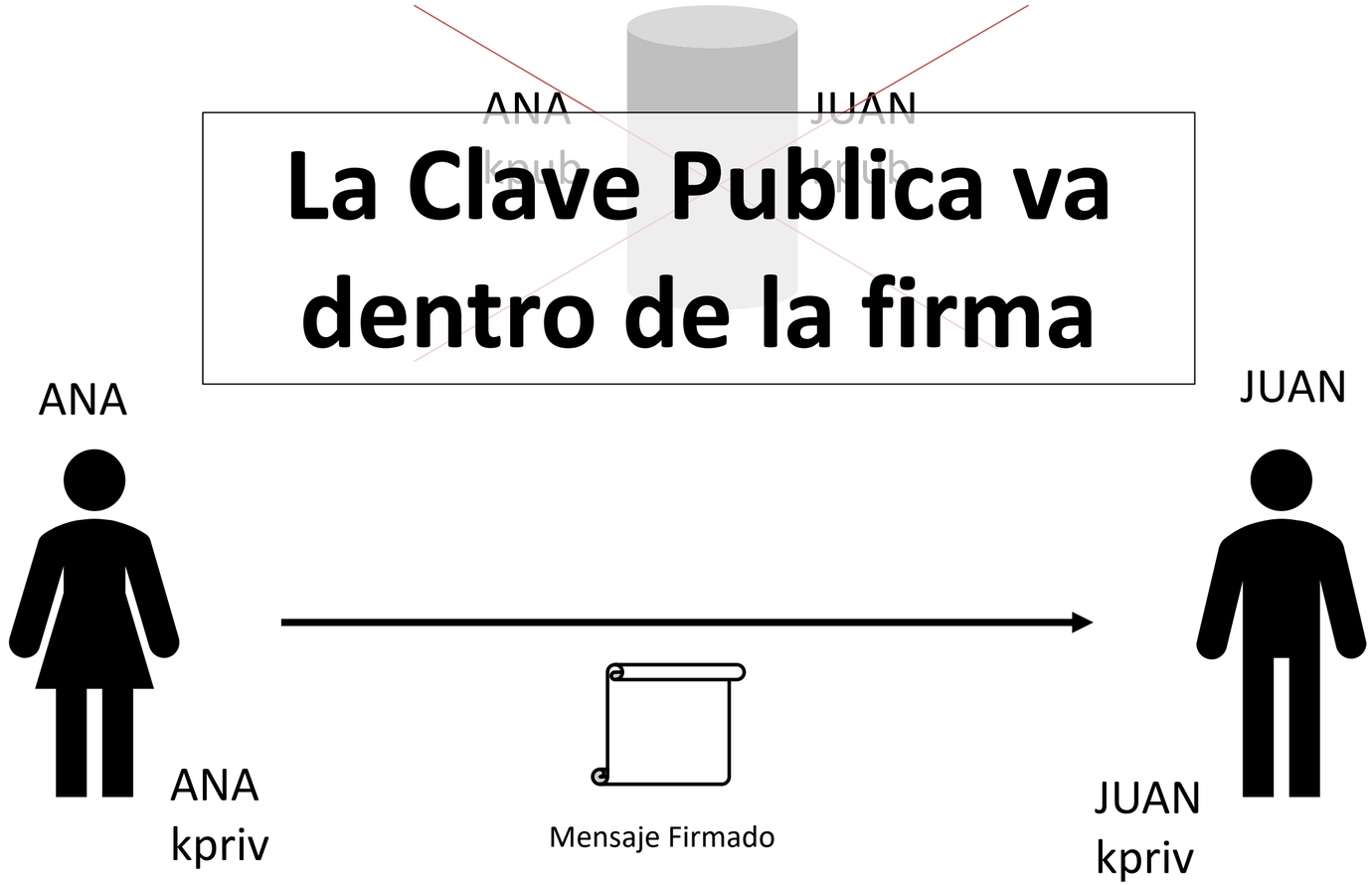


BID
Banco Interamericano de Desarrollo

Certificados X.509

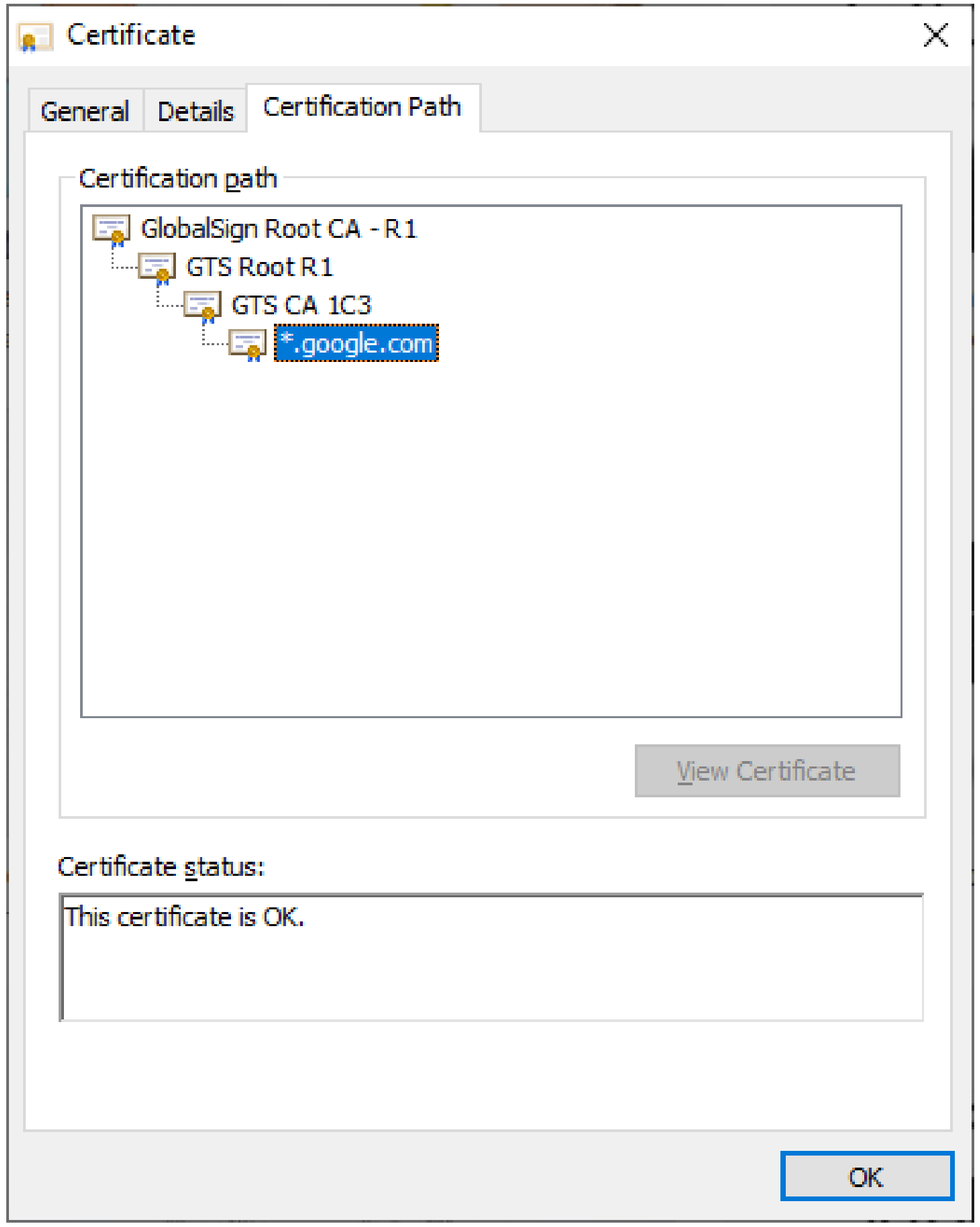


- Como se de quien es la clave???



Certificados X.509v3

- Certificado
  - Versión
  - Número de serie del certificado
  - ID del algoritmo utilizado por el CA para firmar (típicamente RSA o DSA)
  - Emisor (CA)
  - Validez
    - No antes de
    - No después de
  - Sujeto, (sujeto titular) expresado en notación DN (Distinguished Name), compuesto por CN (Common Name), OU (Organizational Unit), O (Organization) y C (Country). El sujeto puede ser una persona, un servidor o un servicio.
  - Información de clave pública del sujeto
    - Algoritmo de clave pública
    - Clave pública del sujeto
  - Identificador único de emisor (opcional)
  - Identificador único de sujeto (opcional)
  - Extensiones (opcional)
    - ...
- Algoritmo usado para firmar el certificado
- Firma digital del certificado



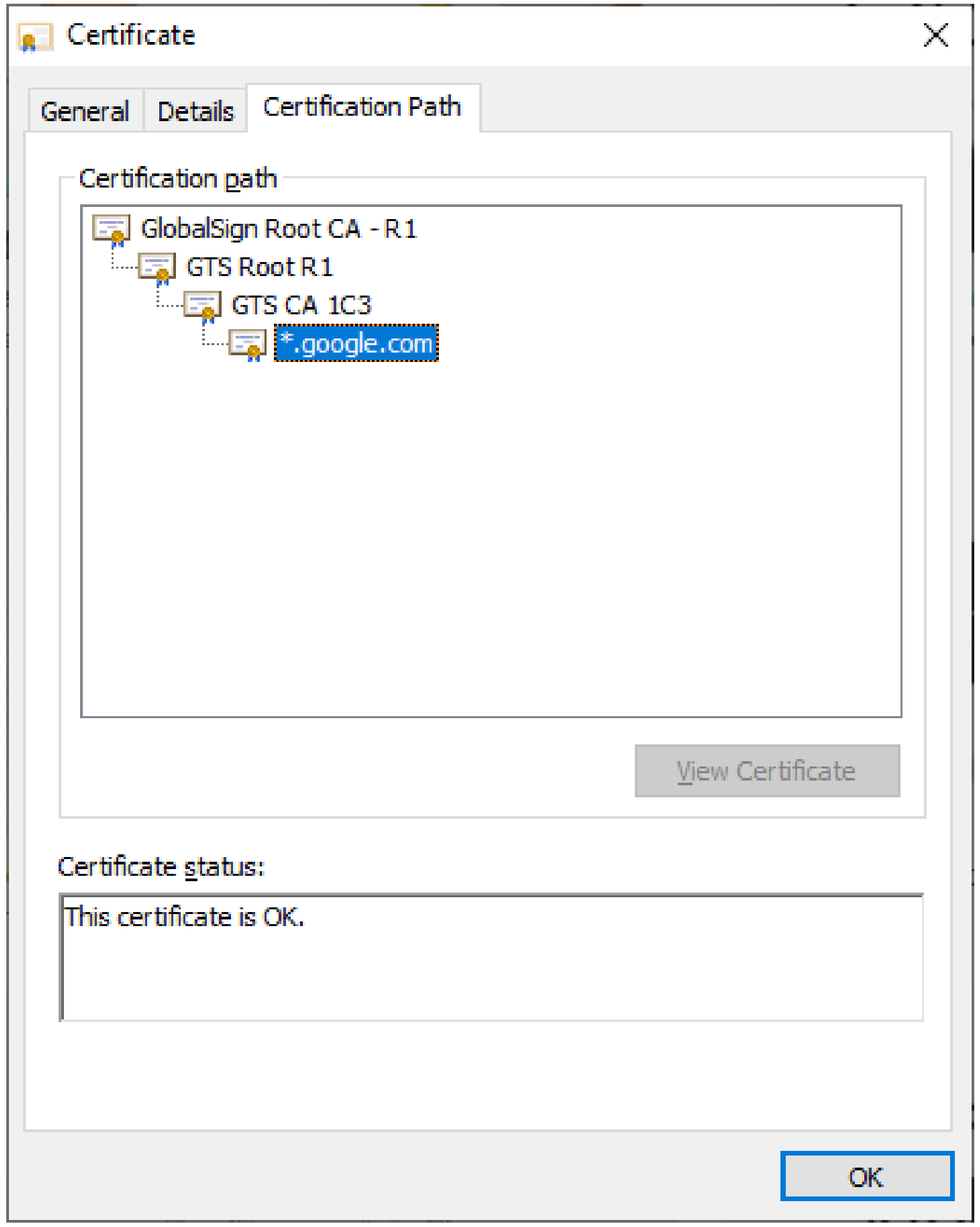
AGENDA

1. Funciones Hash
2. Criptografía Asimétrica
3. Firma Digital
4. Certificados X509
5. PKI
6. Casos de Uso

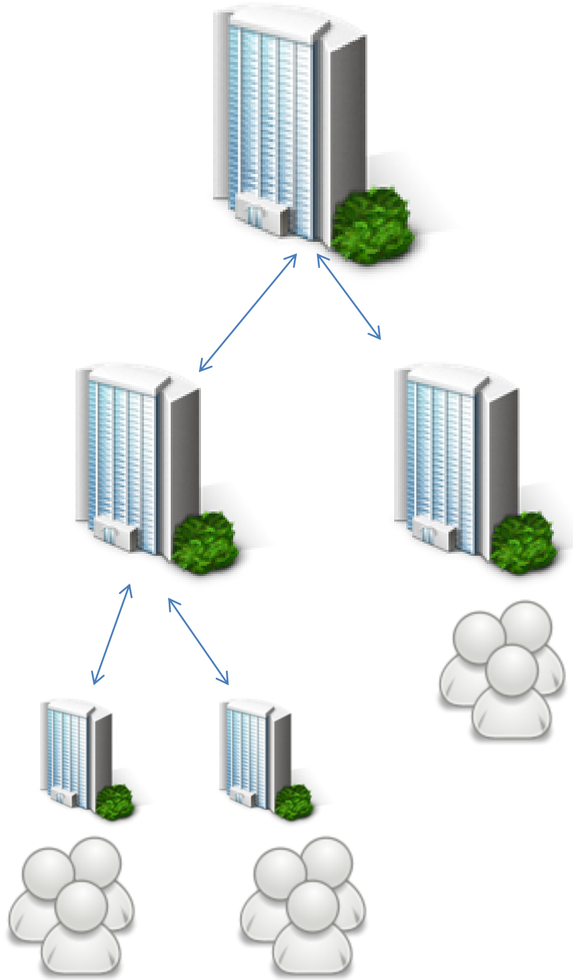
BID
Banco Interamericano de Desarrollo

Certificados X.509v3

- Certificado
  - Versión
  - Número de serie del certificado
  - ID del algoritmo utilizado por el CA para firmar (típicamente RSA o DSA)
  - Emisor (CA)
  - Validez
    - No antes de
    - No después de
  - Sujeto, (sujeto titular) expresado en notación DN (Distinguished Name), compuesto por CN (Common Name), OU (Organizational Unit), O (Organization) y C (Country). El sujeto puede ser una persona, un servidor o un servicio.
  - Información de clave pública del sujeto
    - Algoritmo de clave pública
    - Clave pública del sujeto
  - Identificador único de emisor (opcional)
  - Identificador único de sujeto (opcional)
  - Extensiones (opcional)
    - ...
- Algoritmo usado para firmar el certificado
- Firma digital del certificado



¿Cómo sé quién es un certificado?



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”

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

3. B Obtiene el certificado digital de A

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

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

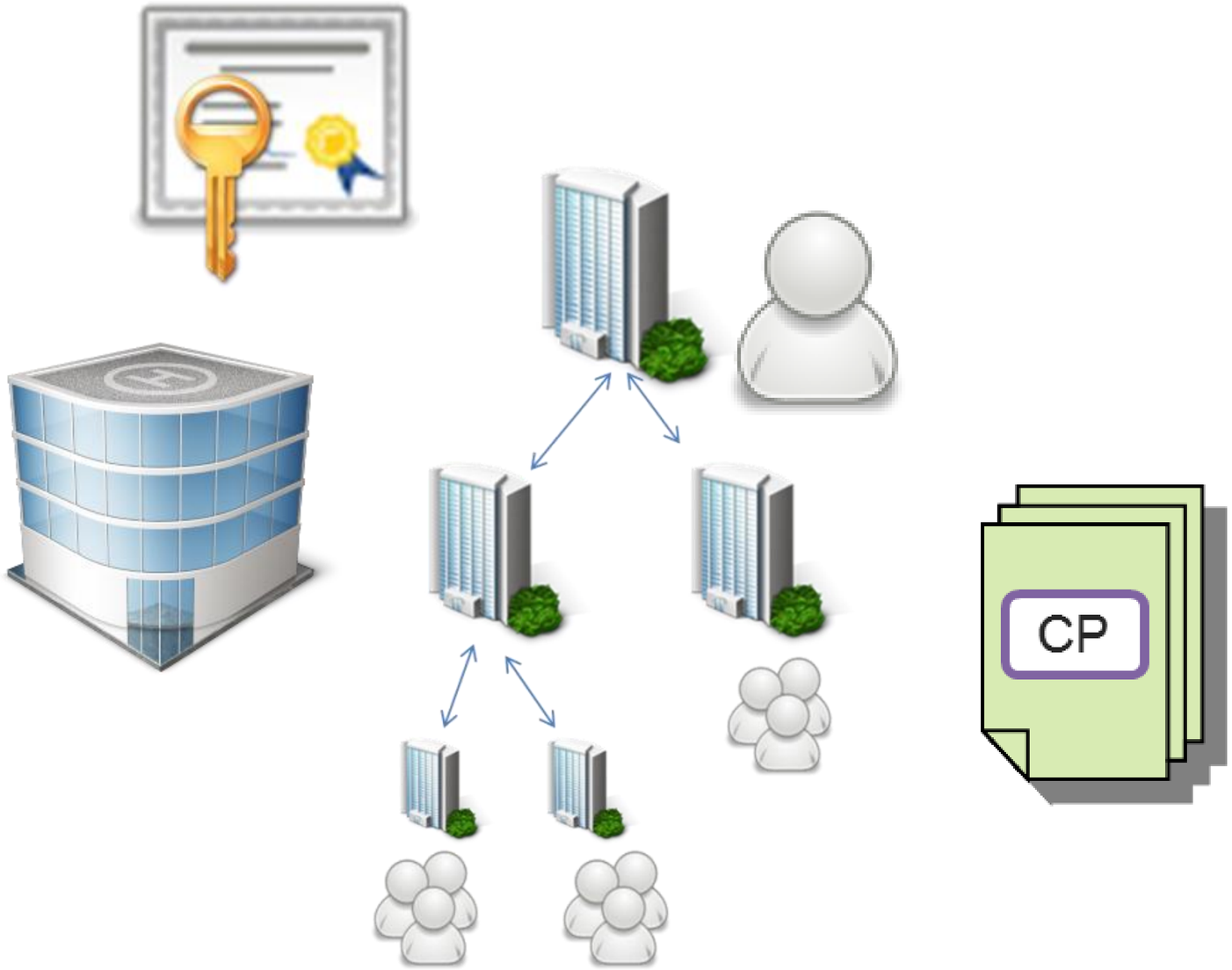




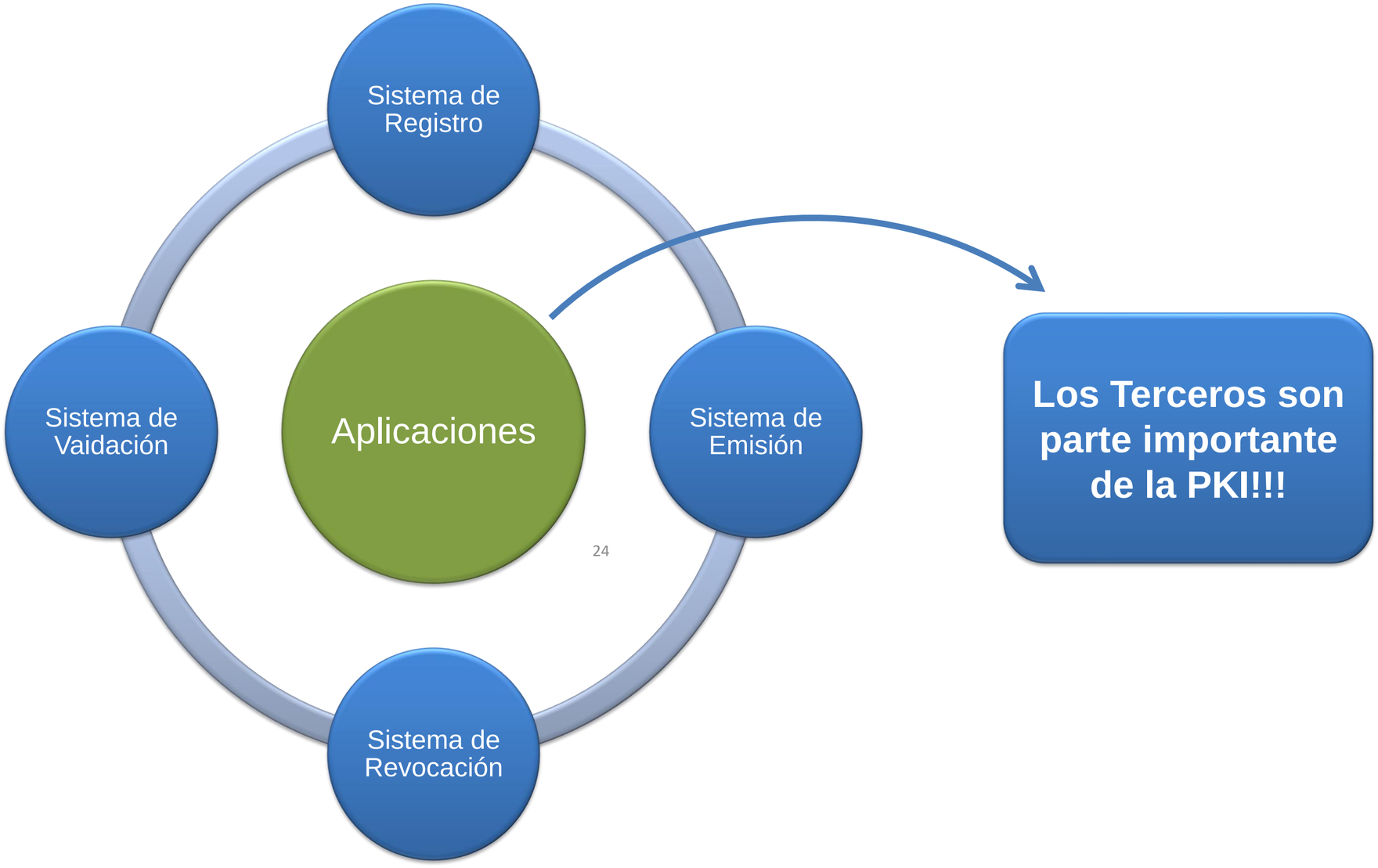


6. Siempre y cuando la validación del certificado esté bien hecha, B puede concluir que el documento fue efectivamente enviado por A (Autenticación y no Repudio) y nadie lo modificó en el camino (Integridad)

COMPONENTES DE UNA PKI

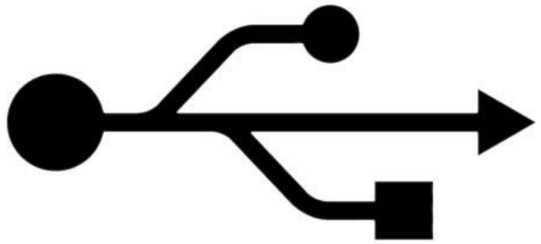


Componentes Mínimos



BID
Banco Interamericano de Desarrollo

No hay que inventar demasiado







Estándares Internacionales

- ITU-T X.509
- RFC 3647, 4211, 5280, 6277, etc
- ETSI TS 102 042 / ETSI TS 101 456
- Web Trust para CA
- CEN-CWA 14167
- CEN-CWA 14169
- Familia PKCS#

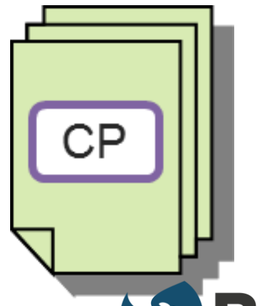
BID
Banco Interamericano de Desarrollo

Se necesitan políticas para "instanciar"

Política de Certificación

- Detalla **los requerimientos** que las **CA y Terceros** deben cumplir en cada componente
  - Actores
  - Roles y Responsabilidades tipo
  - Funciones

- Perfil de certificado
  - Indican su contenido y los niveles de seguridad mínimos para su gestión.



BID
Banco Interamericano de Desarrollo

A veces es necesario algo más…



Declaración de Prácticas de Certificación (CPS)

- Documento que describe en forma **DECLARATIVA**
  - Los servicios ofrecidos
  - Los procedimientos de gestión del ciclo de vida de los certificados
- Contiene información detallada sobre:
  - El sistema de seguridad, soporte, administración y emisión de los certificados

BID
Banco Interamericano de Desarrollo

Sistema de Registro

- «La RA»
- Es el responsable de la identidad de los suscriptores
  - Presencial
  - Remoto
  - Batch

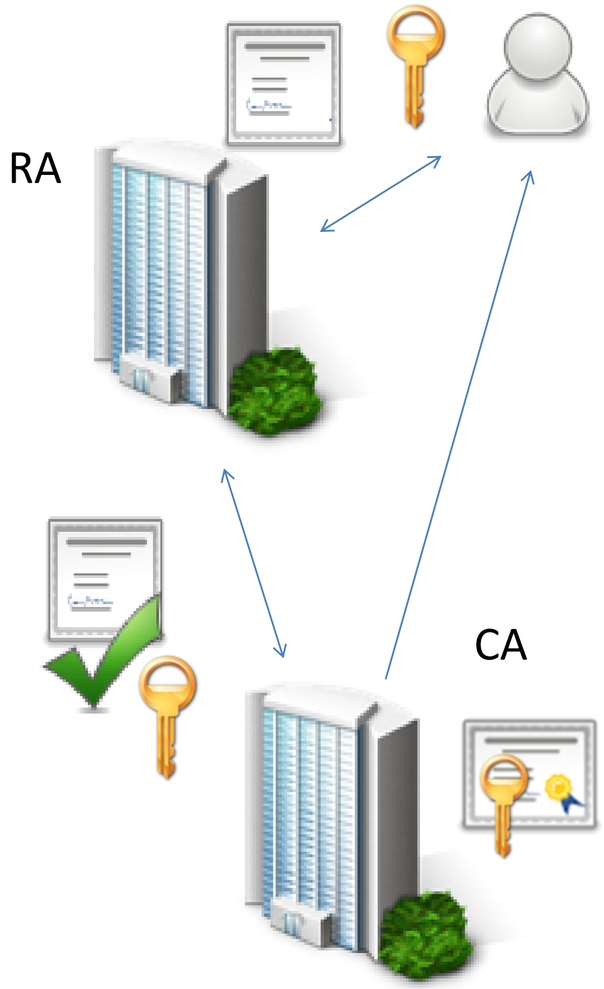
- Puede ser el componente más caro y complejo!



Sistema de Emisión

- «La CA»
- Generación de claves
  - Hardware de Seguridad
  - Procedimientos
  - Auditoría y Testigos
  - Generación por el usuario o batch?
- Esencialmente emite lo que la RA le diga

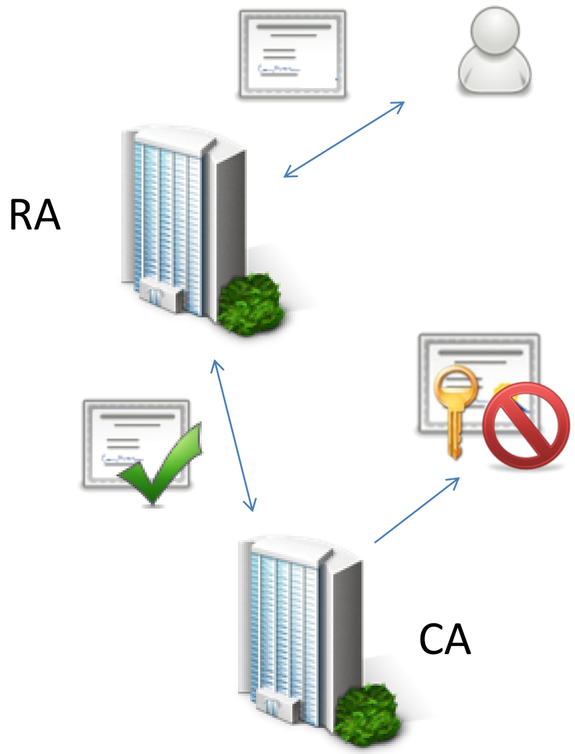
- Respaldo y Escrow de Claves?



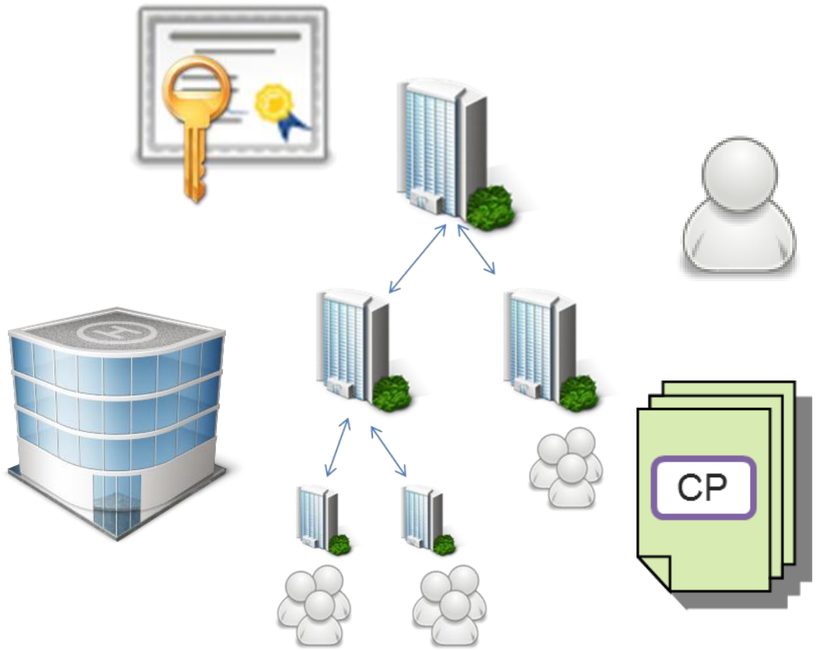
BID
Banco Interamericano de Desarrollo

Sistema de Revocación

- RA Registra – Quién la pide?
- CA Efectiviza
- Es esencial para poder cortar la vida de algunos certificados
  - Extravío
  - Compromiso
  - Incumplimiento de condiciones



Resumen



- Mucho más que sólo CA y Certificados.
- Políticas, procesos, usuarios finales, terceros, etc.
- **Se tienen que tener en cuenta todos los actores y su interacción!**

BID
Banco Interamericano de Desarrollo

FIRMA ELECTRÓNICA



BID
Banco Interamericano de Desarrollo

¿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!

BID
Banco Interamericano de Desarrollo

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>
```


BID
Banco Interamericano de Desarrollo

Estándares de Firma



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



- PDF-Signature, PAdES

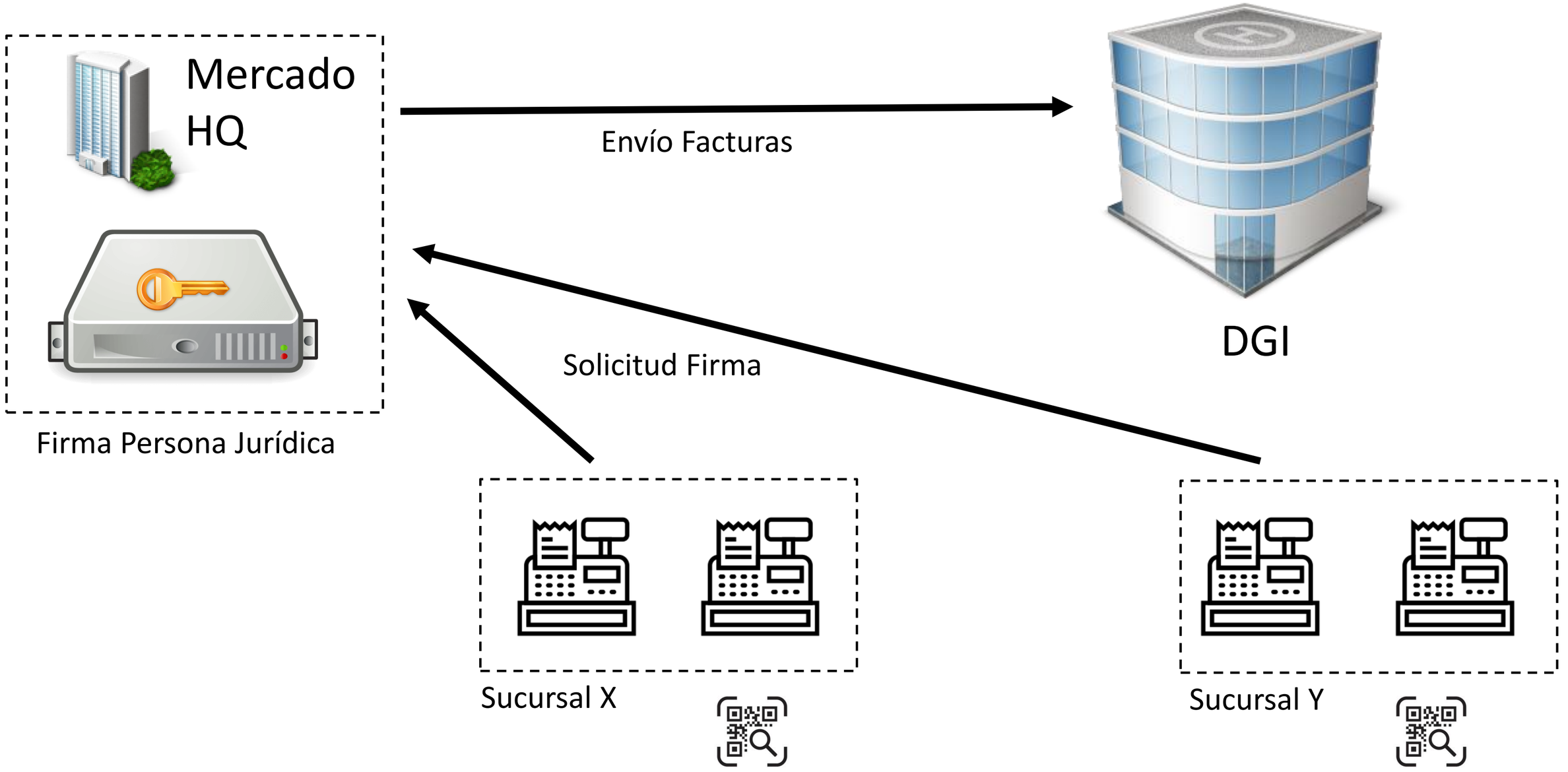
- PKCS#7, CMS, CAdES

Otros

AGENDA

1. Funciones Hash
2. Criptografía Asimétrica
3. Firma Digital
4. Certificados X509
5. PKI
6. Casos de Uso

Facturación Electrónica DGI Uruguay



Gracias