



Criptografía y Seguridad en Redes

v.2013

Seminario #5

Titular a cargo: Prof.Ing.Miguel Solinas

msolinas@efn.uncor.edu

mksolinas@gmail.com





Agenda

- *Introducción*
- *Criptografía histórica*
- *Fundamentos teóricos*
- *Cifra de Bloque Moderna + DES + Modos de Uso*
- *Otras cifras de bloque, 3DES, IDEA, AES*
- *Criptografía Asimétrica, PKI*





Criptografía Asimétrica



Whitfield Diffie



Martin Hellman



Ralph Merkle



Taher Elgamal

Ron Rivest,
Adi Shamir
Leonard Adleman

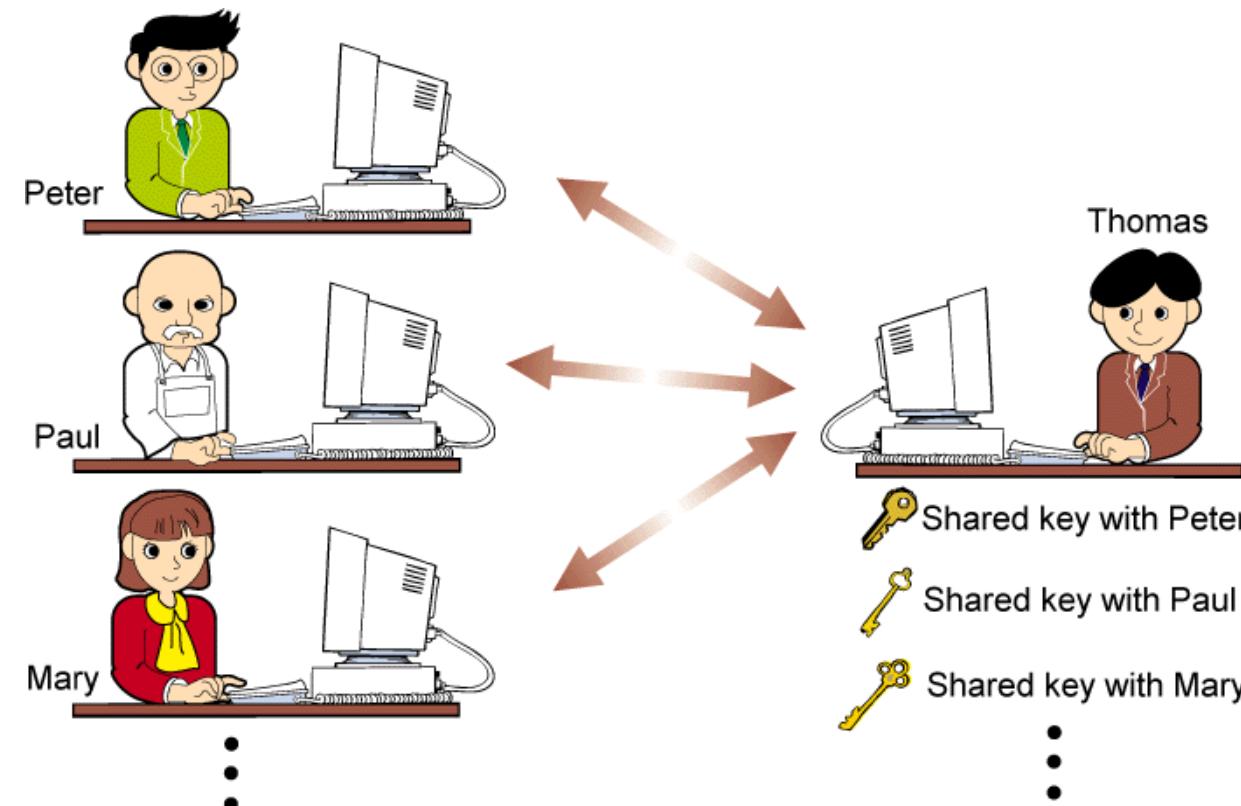




Criptografía Asimétrica

La distribución de claves en criptografía simétrica

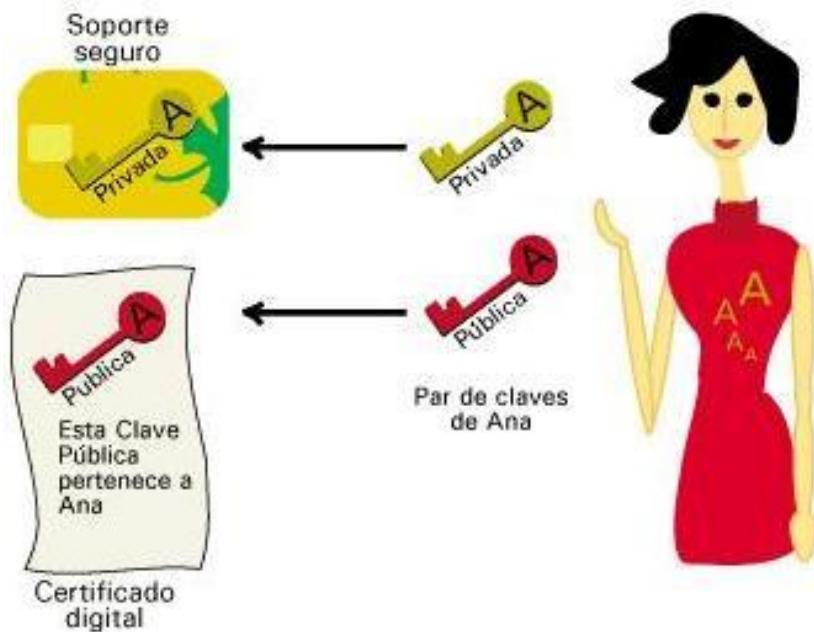
n	$n*(n-1)/2$
4	6
8	28
16	120
32	496
64	2016
128	8128
256	32640
512	130816
1024	523776





Criptografía Asimétrica

La criptografía asimétrica utiliza un único par de claves por usuario.



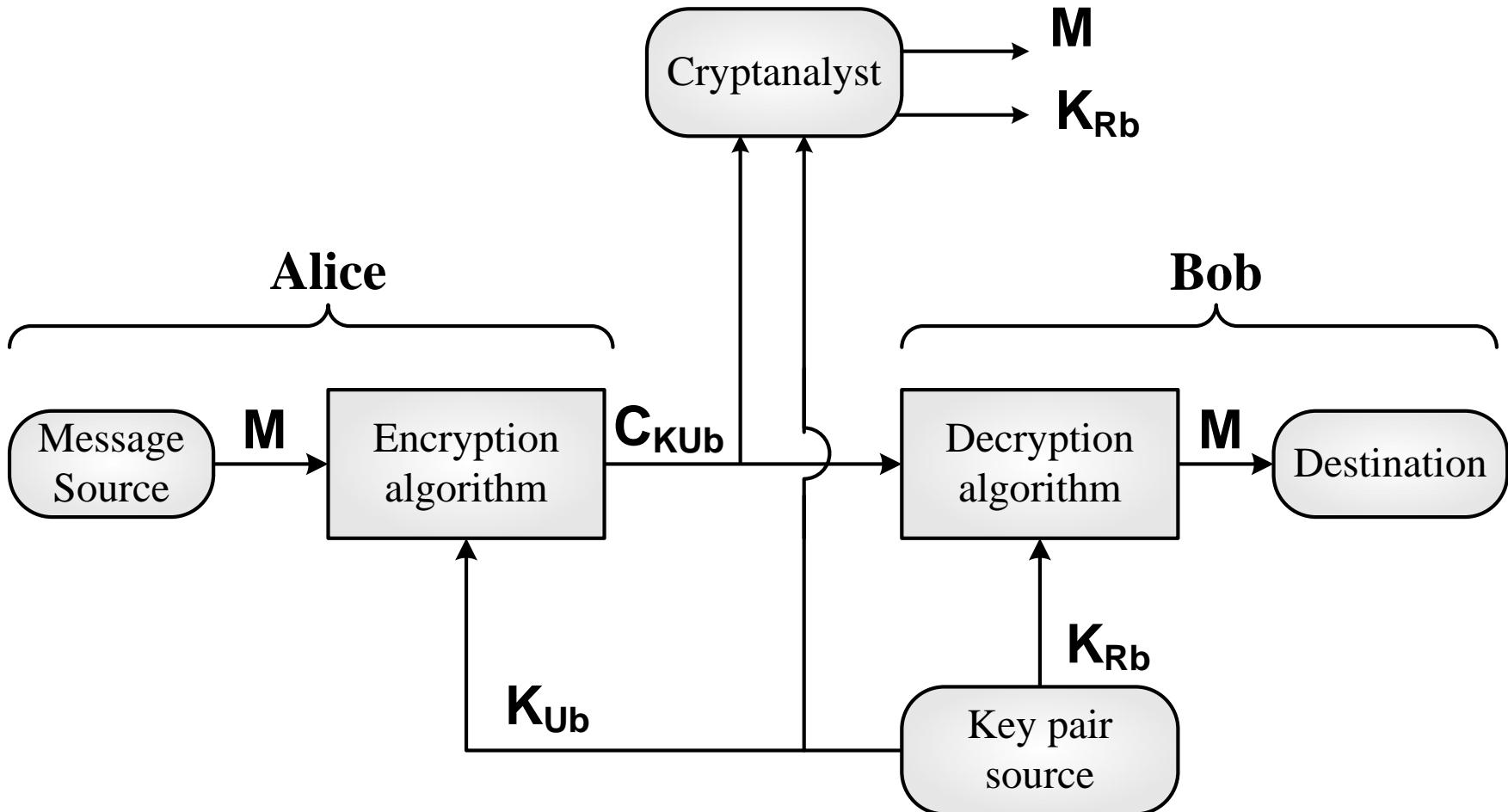
n	$n*(n-1)/2$	$2*n$
4	6	8
8	28	16
16	120	32
32	496	64
64	2016	128
128	8128	256
256	32640	512
512	130816	1024
1024	523776	2048





Criptografía Asimétrica

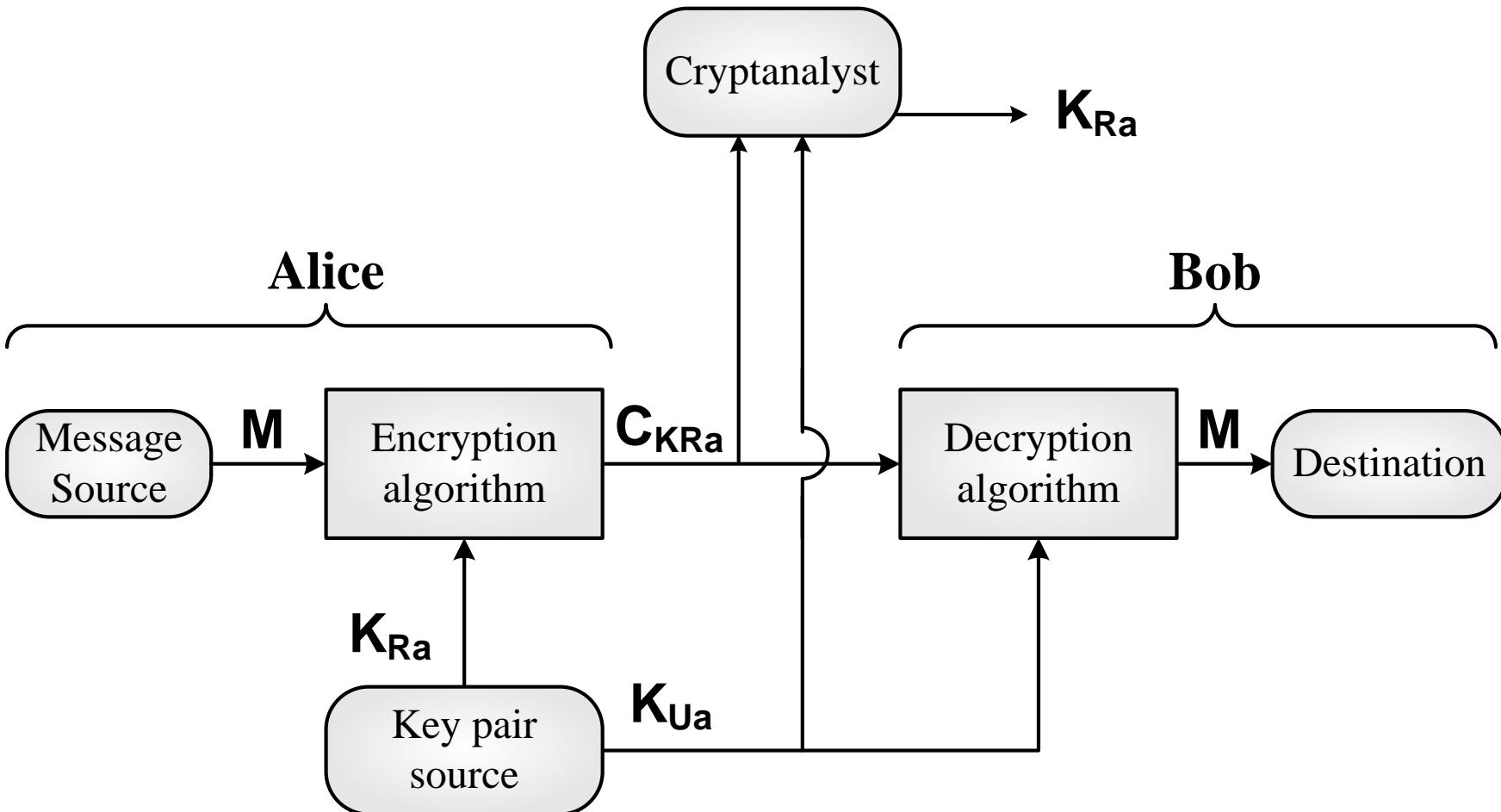
Confidencialidad





Criptografía Asimétrica

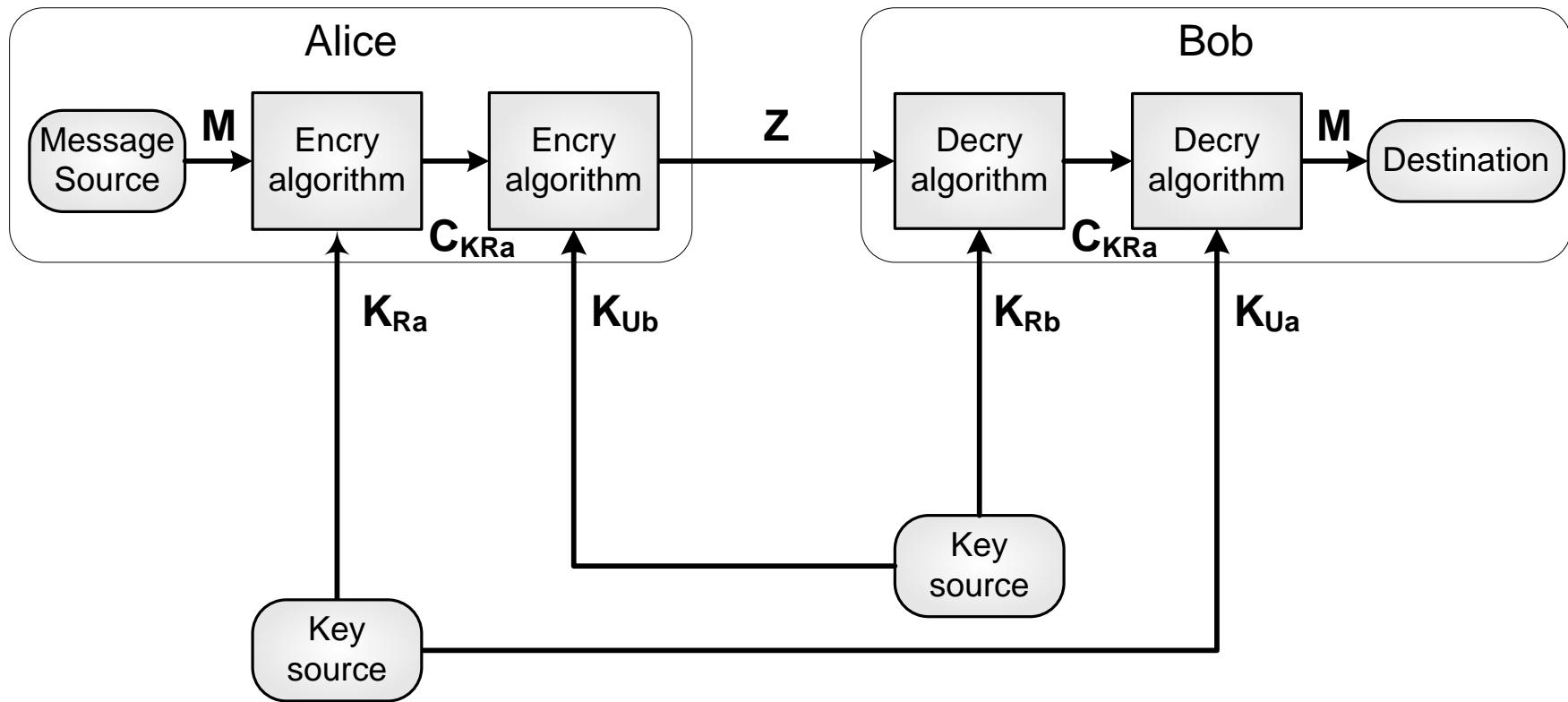
Autenticación





Criptografía Asimétrica

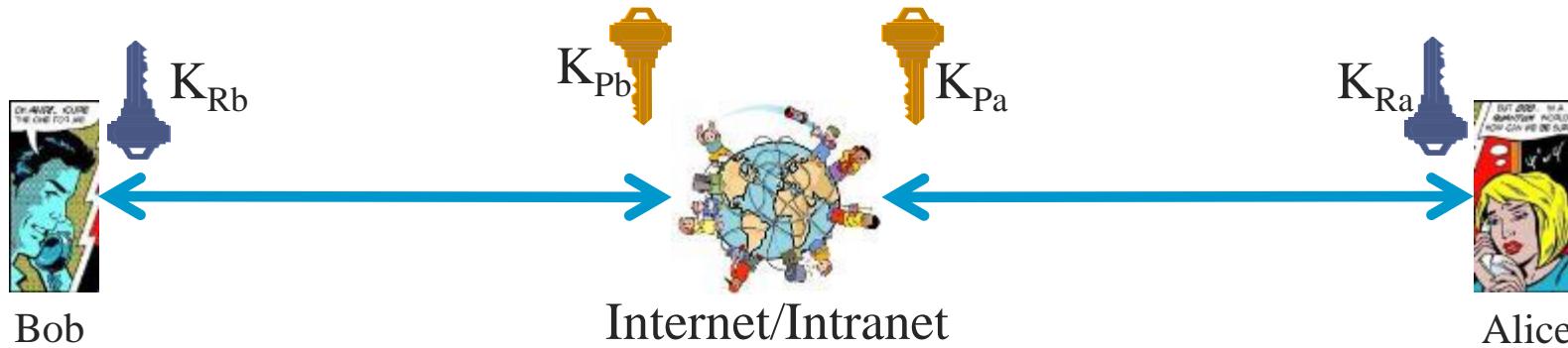
Confidencialidad y Autenticación





Criptografía Asimétrica

Firma Digital



UNA FIRMA DIGITAL ES UN ELEMENTO DE DATOS QUE DA FE DEL ORIGEN Y LA INTEGRIDAD DE UN MENSAJE

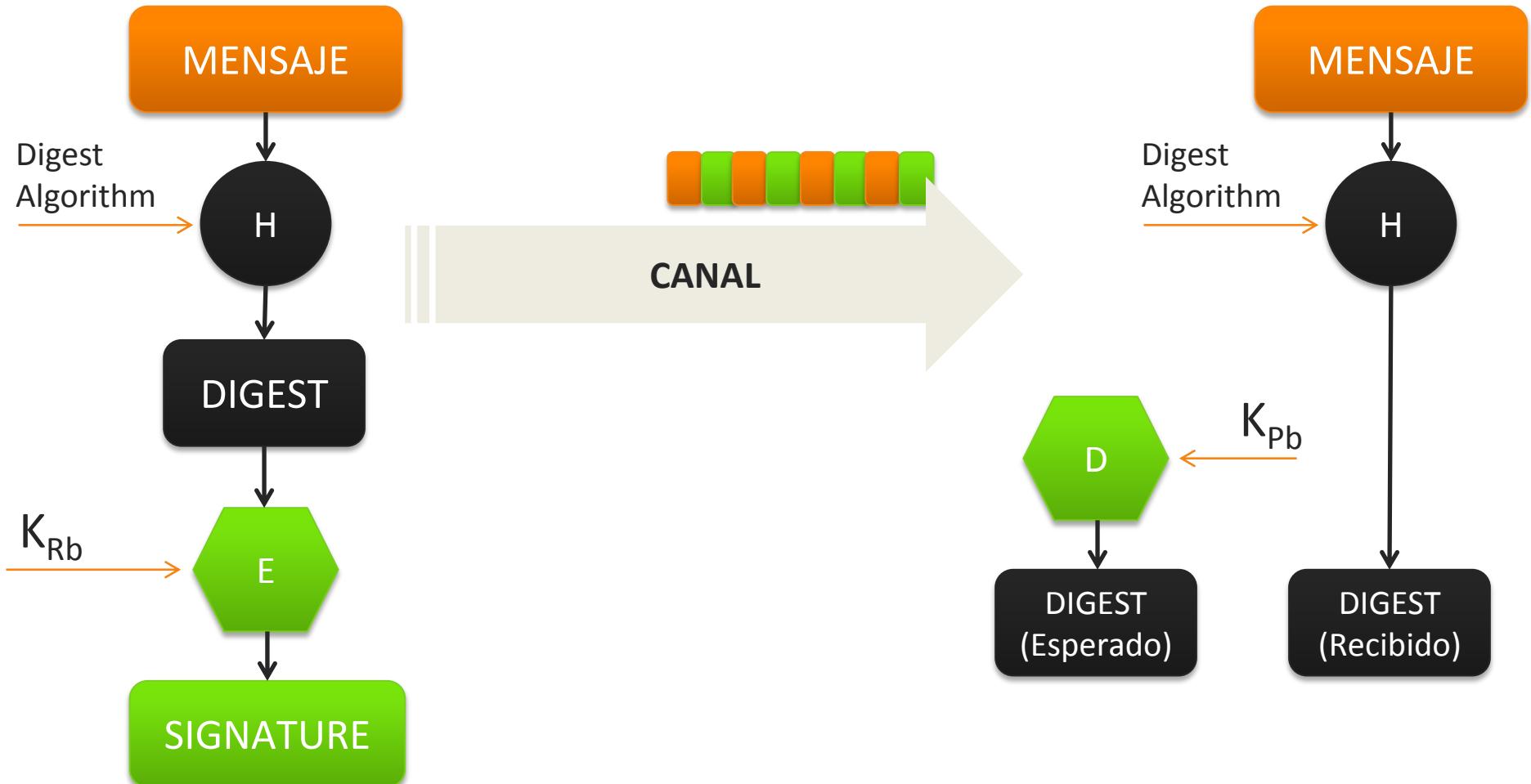
- El emisor del mensaje utiliza una clave de firmado (K_{Rb}) para firmar el mensaje y enviarlo al receptor junto con la firma digital.
- El receptor utiliza una clave de verificación (K_{Pb}) para verificar el origen del mensaje y que no ha sido alterado en la transmisión.





Criptografía Asimétrica

Firma Digital





Criptografía Asimétrica

Primero: requerimientos para los algoritmos

1. Que sea fácil, desde el punto de vista del cálculo, para **B** generar el par (K_{Ub}/K_{Rb}) .
2. Que sea fácil para un emisor **A**, conociendo K_{Ub}/M , generar $C = E_{KUb}(M)$
3. Que sea fácil para el receptor **B**, usando K_{Rb} , recuperar el mensaje M , con
$$M = D_{KRb}(C) = D_{KRb}[E_{KUb}(M)]$$
4. Que sea difícil para un atacante, conociendo K_{Ub} determinar K_{Rb} .
5. Que sea difícil para un atacante, conociendo K_{Ub}/C , recuperar M .
6. Las funciones de encripción y desencripción se pueden aplicar en cualquier orden.

$$M = D_{KRb}[E_{KUb}(M)] = E_{KUb}[D_{KRb}(M)]$$





Criptografía Asimétrica

Algoritmos mas populares

1. RSA
2. Elgamal
3. Diffie Hellman





Criptografía Asimétrica

¿Solucionamos el problema de distribución de claves?





Criptografía Asimétrica

Segundo: No solo que no se solucionó sino que ahora PERSISTE EL PROBLEMA DE LA IDENTIDAD DEL FIRMANTE...!!

¿Por qué debería confiar en lo que el remitente dice ser?

nos movemos hacia una PKI...





Certificado Digital

Es un vínculo entre la clave pública de la entidad y uno o más atributos relativos a su identidad.

- La entidad puede ser una persona, un componente de hardware, un servicio, etc.
- Un Certificado Digital es emitido (y firmado) por alguien.
- Por lo general ese «alguien» es una tercera parte confiable!!
- Un Certificado auto-firmado por lo general no es confiable.



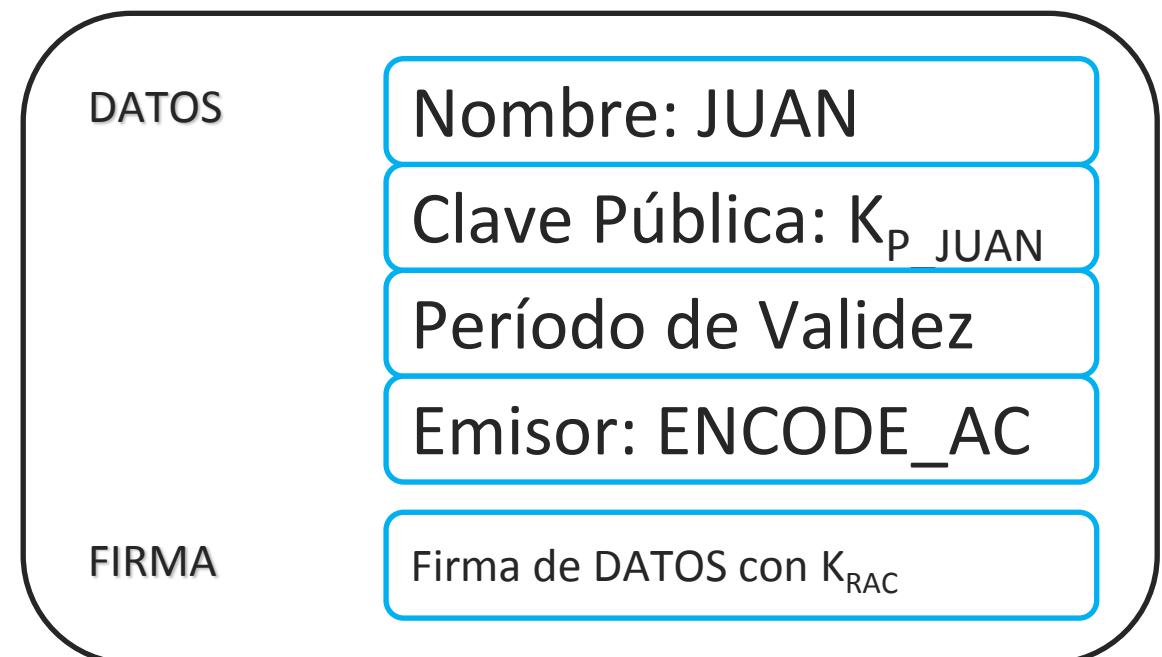


Certificado Digital

CERTIFICADO DE «JUAN» GENERADO O EXPEDIDO POR «ENCODE_AC»
ENCODE_AC<<JUAN>>

Formato

*SIMPLIFICADO de un
certificado de clave
pública*

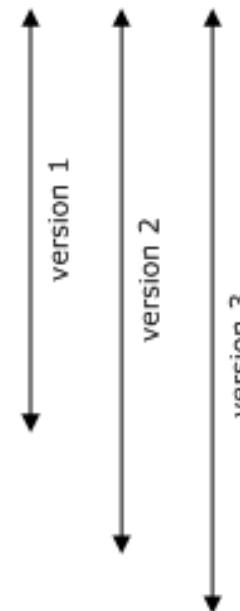




Certificado Digital

EL ESTÁNDAR DE CERTIFICADO DE CLAVE PÚBLICA X.509 SE HA
REVISADO VARIAS VECES DESDE SU CREACIÓN

Version
Serial Number
Signature Algorithm Identifier
Issuer Name
Validity Period
Subject Name
Public Key Information
Issuer Unique ID
Subject Unique ID
Extensions



ENCODE_AC<<JUAN>>

ID de extensión

Crítica / NO Crítica

Valor





Certificado Digital

EXTENSIONES DEL CERTIFICADO X.509 V3

- *Relacionadas con las claves y las políticas*
- *Sobre atributos relativos a la entidad propietaria del certificado y a la AC emisora*
- *Relativas a restricciones sobre el camino de certificación*

ENCODE_AC<<JUAN>>

ID de extensión

Crítica / NO Crítica

Valor





Certificado Digital

CAMPOS DE LA VERSIÓN 1

Campo	Descripción
Versión	Número de versión del certificado codificado. Valores posibles 0, 1 o 2.
Número de serie	Entero positivo único asignado por la AC.
Algoritmo de firma	OID que especifica el algoritmo usado por la AC para firmar el certificado. Ej.: 1.2.840.113549.1.1.5 especifica un algoritmo hash SHA-1 combinado con el algoritmo de cifrado RSA de RSA Laboratories.
Emisor	Nombre distintivo (DN) X.500 de la entidad de certificación que creó y firmó el certificado.
Validez	Intervalo de tiempo durante el cual el certificado es válido.
Sujeto	Nombre distintivo X.500 de la entidad asociada con la clave pública contenida en el certificado.
Clave pública	Clave pública e información de algoritmo asociada.





Certificado Digital

CAMPOS DE LA VERSIÓN 3

Campo	Descripción
ID de clave de entidad emisora	ID de la K _{PAC} correspondiente a la K _{RAC} utilizada para firmar el certificado.
Restricciones básicas	Especifica si la entidad se puede utilizar como una AC. En caso afirmativo, el número de AC subordinadas que pueden existir por debajo.
Directivas del certificado	Especifica las directivas con las que se ha emitido el certificado y los fines para los que se puede utilizar.
Distribución CRL	Contiene el URI de la lista de revocación de certificados (CRL) de base.
Uso de claves	De que manera se puede utilizar la clave pública del CD.
Nombre Alt.del emisor	Especifica una o más formas de nombre alternativos para el emisor de la solicitud de certificado.
Uso de claves	Restricciones en las operaciones que puede realizar la K _P del CD.
Restricciones de nombre	Espacio de nombres en el que deben encontrarse todos los nombres de firmantes en una jerarquía de certificados. Solo en un certificado de CA.





Certificado Digital

CAMPOS DE LA VERSIÓN 3

Campo	Descripción
Restricciones de directiva	Restringen validación de rutas. Prohibe asignación de directivas o exige que c/CD de la jerarquía tenga un ID de directiva aceptable. Idem Anterior.
Asignaciones de directiva	Especifica las directivas de una CA subordinada correspondientes a directivas de la CA emisora.
Período de uso de clave privada	Especifica un período de validez distinto para la clave privada que para el certificado con el que la clave privada está asociada.
Nombre alternativo del firmante	Especifica una o más formas de nombre alternativas para el firmante de la solicitud de certificado. Algunos ejemplos de formas alternativas son direcciones de correo electrónico, nombres DNS, direcciones IP y URI.
Atrib.de directorio de firmantes	Contiene atributos de identificación como la nacionalidad del firmante del CD. El valor de extensión es una secuencia de pares de valores OID.
Identificador de clave del firmante	Diferencia entre varias K _P de las que el firmante del certificado es titular. El valor de extensión suele ser un hash SHA-1 de la clave.





Certificado Digital

MUÉSTRAME UN CERTIFICADO DIGITAL !!





Certificado Digital

PROBLEMAS:

- *¿Cómo se emiten los Certificados Digitales?*
- *¿Quién los emite?*
- *¿Por qué habría de confiar en el emisor?*
- *¿Cómo chequear la validez de un Certificado Digital?*
- *¿Cómo revocar un Certificado Digital?*
- *¿Quién puede revocar un Certificado Digital?*

nos movemos hacia una PKI...





Una Public Key Infrastructure (PKI) es una infraestructura tecnológica y organizacional para dar soporte y gestionar Certificados Digitales basados en clave pública





PKI

Una PKI es un conjunto de estándares acordados, Autoridades de Certificación (CA), la estructura entre CAs, métodos para descubrir y validar rutas de certificación, protocolos operativos, protocolos de gestión, herramientas interoperables y legislación de apoyo.





FOCO EN :

- X509 PKI
- X509 Digital Certificates

Estándares definidos por el IETF, PKIX WG: <http://www.ietf.org/>





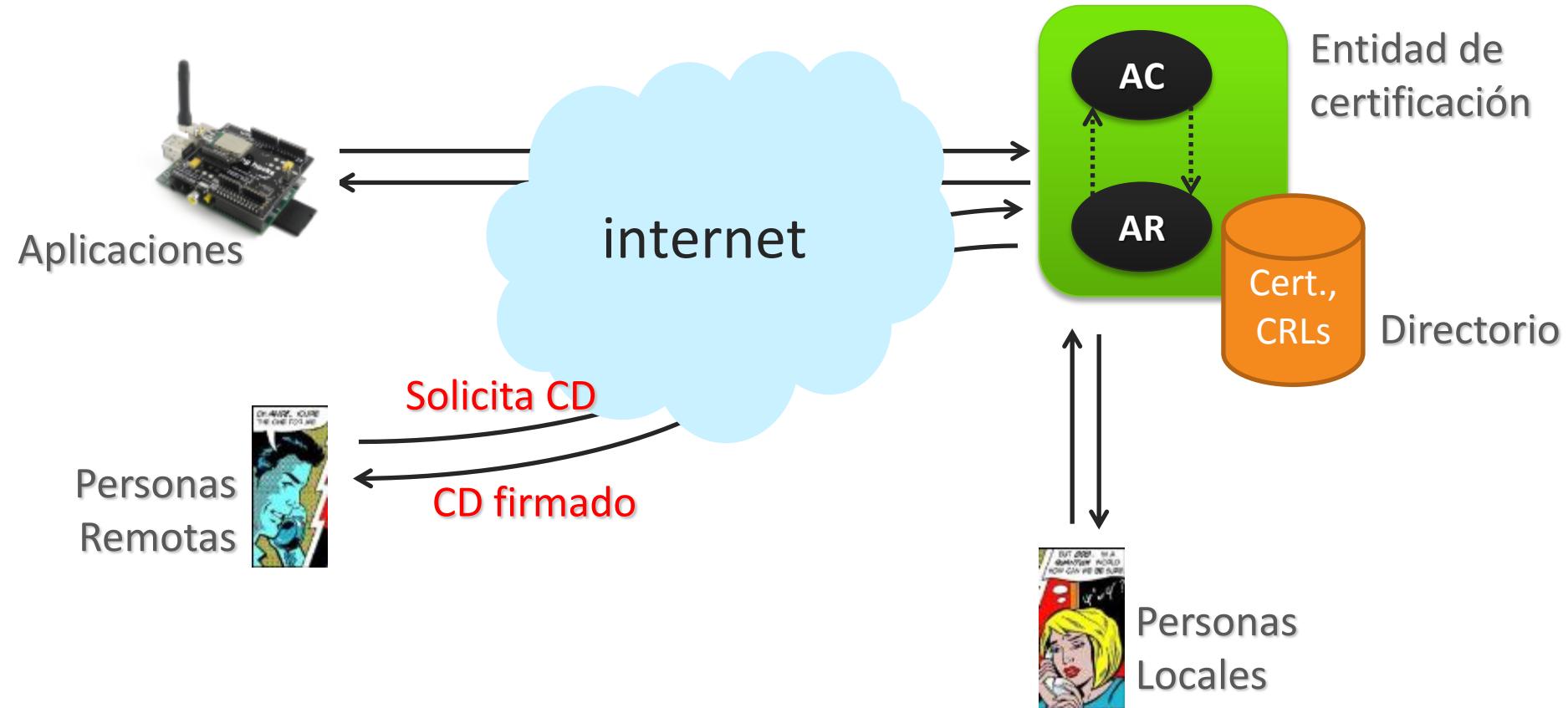
COMPONENTES BÁSICOS:

- Autoridad de Certificación (AC)
- Autoridad de Registro (AR)
- Sistema de distribución de certificados
- Aplicaciones habilitadas para utilizar la PKI





UN MODELO SENCILLO





TAREAS BÁSICAS DE UNA “AC”

- Generación de claves
- Generación de Certificados Digitales
- Emisión y distribución de CD
- Revocación
- Sistema de recuperación y backup de claves
- Certificación cruzada





TAREAS BÁSICAS DE UNA “AR”

- Registro de información de Certificados
- Registro cada a cara
- Registro remoto
- Registro automático
- Revocación





SISTEMA DE DISTRIBUCIÓN DE CD

- Certificados Digitales
- Certificate Revocation Lists (CRLs)

Generalmente se trata de:

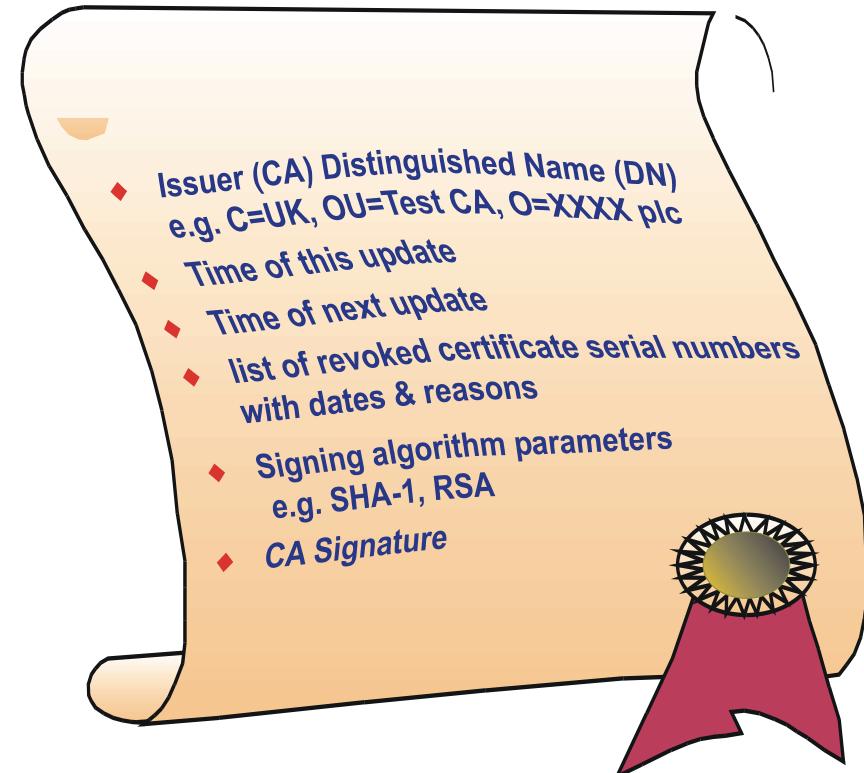
- Base de datos de propósitos generales
- Directorios LDAP





CRL

Los Certificados Revocados permanecen en la CRL hasta que
expiran





CRL

Las CRLs son publicadas por la AC a intervalos de tiempo bien definidos.

Es responsabilidad de los “usuarios” de certificados bajar un CRL y verificar si un certificado ha sido revocado.

Las aplicaciones de usuarios deben hacer frente a los procesos de revocación.





ONLINE CERTIFICATE STATUS PROTOCOL (OCSP)

Una alternativa a las CRLs.

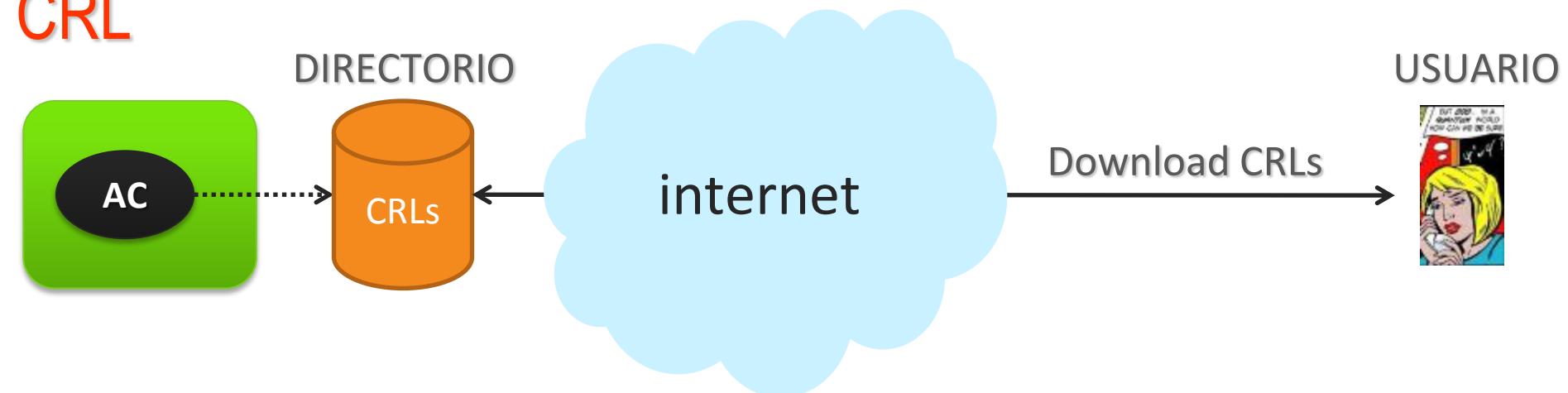
Es el estándard IETF/PKIX para chequear en tiempo real si un certificado ha sido revocado/suspendido.

Requiere que el Servidor de OCSP brinde un servicio de alta disponibilidad.

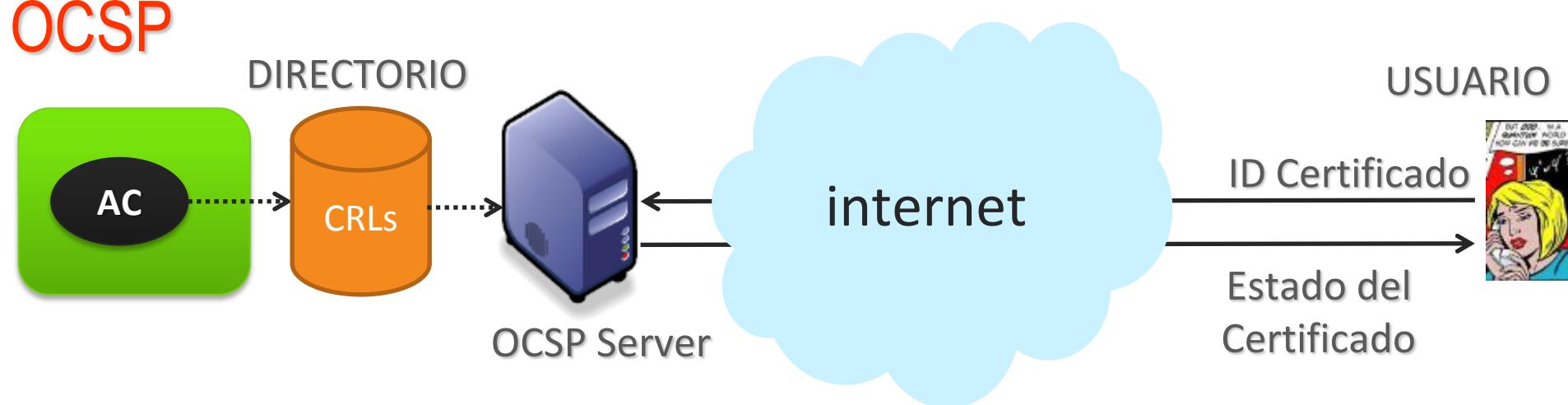




CRL



OCSP





FUNCIONALIDAD REQUERIDA DE UNA APLICACIÓN

- Capacidad para ejecutar primitivas criptográficas
- Almacenamiento seguro de información personal
- Manejo de Certificados Digitales
- Acceso a Directorios
- Infraestructura de comunicaciones





Aspectos legales y de confianza





¿ PORQUE DEBERÍA CONFIAR EN UNA AC ?

- Jerarquía de certificación
- Certificación cruzada

¿ CÓMO FIJAR LA RESPONSABILIDAD DE UNA AC ?

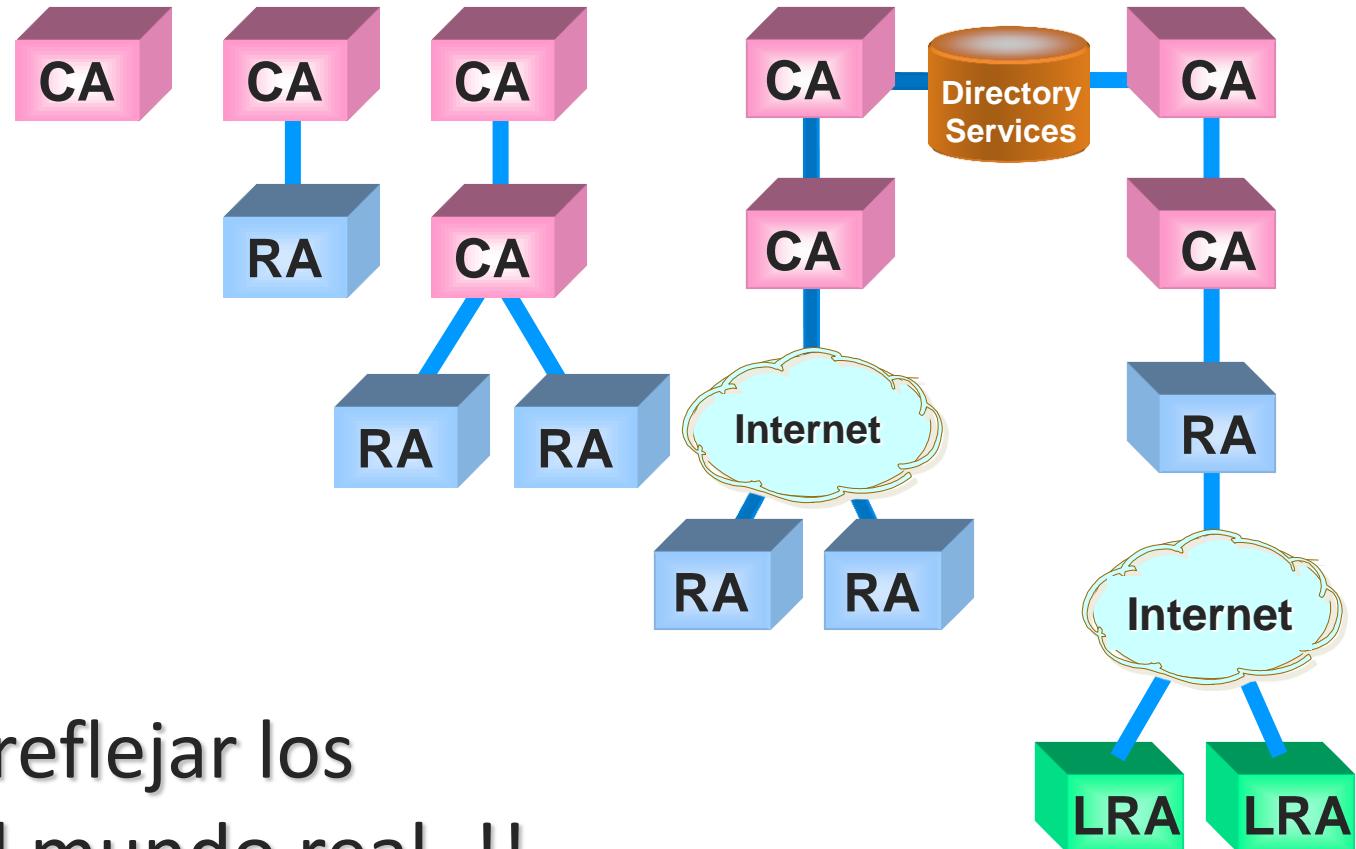
- Política de Certificación ó Certificate Policies (CP)
- Manual de Procedimientos ó Certificate Policy Statement (CPS)





EVOLUCIÓN DE LA TECNOLOGÍA DE AC

'90



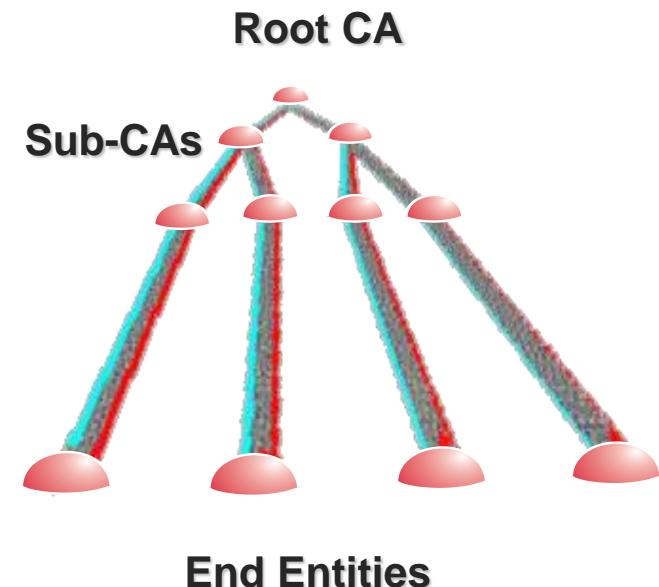
Intentando reflejar los
modelos del mundo real..!!





JERARQUÍA DE CERTIFICACIÓN SIMPLE

- Cada entidad tiene su propio CD (puede tener mas de uno).
- El CD de la AC raíz está autofirmado.
- Cada sub-AC tiene su CD firmado por la AC padre.
- Cada AC puede (debe) emitir sus CRL. Las de menor jerarquía lo hacen mas frecuentemente.
- Las entidades finales necesitan encontrar el camino de certificación a una AC de confianza.

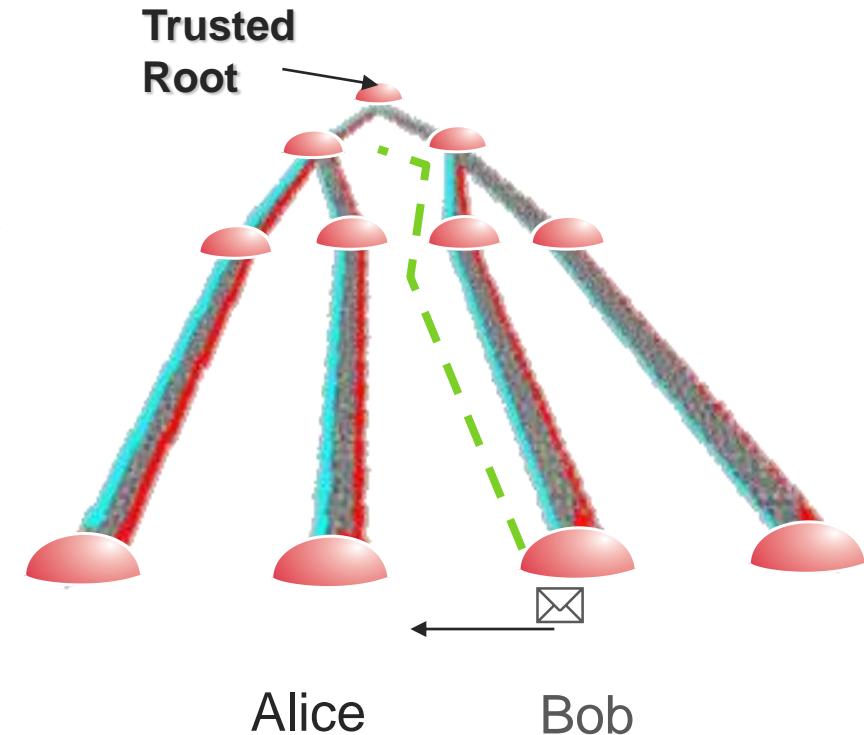




JERARQUÍA DE CERTIFICACIÓN SIMPLE

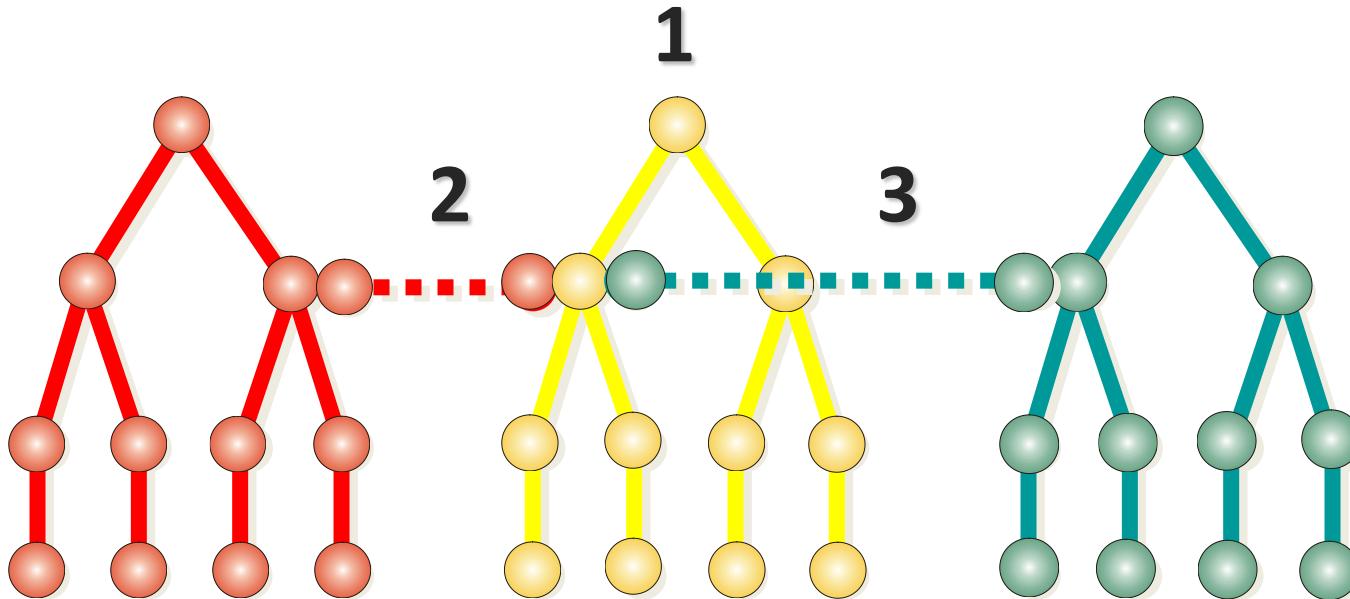
- Alice confía en la AC Raíz.
- Bob envía mail a Alice.
- Alice necesita el CD de Bob mas el CD de la AC que firmó el CD de Bob, hasta la AC Raíz.
- Alice necesita las CRLs de cada AC.

Sólo así Alice puede verificar que el CD de Bob es válido y confiable y así verificar su firma.





MULTIPLES JERARQUÍA Y CERTIFICACIÓN CRUZADA



1. Múltiples raíces
2. Certificación cruzada simple
3. Certificación cruzada compleja





PKI

Política de Certificación y Manual de Procedimientos de Certificación



Criptografía y Seguridad en Redes



POLÍTICA DE CERTIFICACIÓN

- Documento que establece los derechos, deberes y obligaciones de cada una de las partes de una infraestructura de clave pública.
- La Política de Seguridad usualmente tiene efectos legales.
- LA AC debe hacer pública la Política de Seguridad, por ejemplo en su sitio web.





Aspectos Generales

Perfil de Certificados y CRL

Controles Técnicos y de Seguridad

Requerimientos Operativos

Comunidad y Aplicabilidad

POLÍTICA DE CERTIFICACIÓN

Derechos, Resp. y Obligaciones

Identificación y Autenticación





MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN

- Documento que establece lo que sucede en la práctica para apoyar las declaraciones políticas realizadas en la PC de una PKI.
- Es un documento que puede tener efecto jurídico bajo determinadas circunstancias.





Administración de
Especificaciones

Introducción

Perfil de
Certificados y CRL

MANUAL DE PROCEDIMIENTOS DE CERTIFICACIÓN

Disposiciones
Generales

Controles Técnicos
y de Seguridad

Identificación y
autenticación

Procedimientos
Físicos y de Personal

Requerimientos
operativos





MUÉSTRAME UNA PC Y UN MPC...!!





¿ Y CON QUE HERRAMIENTA PODEMOS
CONSTRUIR UNA PKI ?





- ✓ Enterprise Java Bean Certification Authority (EJBCA)
- ✓ OpenCA
- ✓ Windows Server





