Función HASH

- Son funciones de un solo sentido.
- La función Hash acepta como entrada mensajes M de longitud variable y da como resultado un Código Hash H(M) de longitud fija.

$$h = H(M)$$

- El hash de un mensaje es una función de todos los bits del mensaje que además brinda una capacidad de detección de errores: un cambio de un solo bit en el mensaje resulta en una modificación del hash resultante.

Propiedades de la Función HASH

- Produce una Huella Digital.
- Dado x debe ser computacionalmente imposible hallar un valor M / H(M) = x.
- Dado x debe ser computacionalmente imposible encontrar y $\neq$ x / H(x)=H(y).

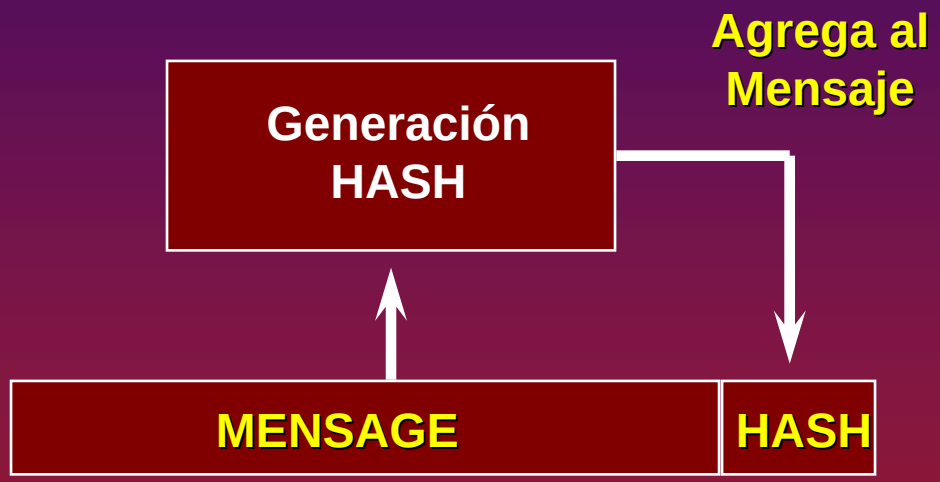
Función HASH

- Suponiendo una Función Hash de 99 bits, tendríamos:

$2^{99} = 633.825.300.114.114.700.748.351.602.688$

resultados posibles.

Función HASH



AUTENTICA LOS MENSAJES

Función HASH

Ejemplo de Función Hash

	bit1	bit 2	. . .	bit n
Bloque 1	bit_{11}	bit_{21}		bit_{n1}
Bloque 2	bit_{12}	bit_{22}		bit_{n2}
	.	.	.	.
	.	.	.	.
	.	.	.	.
Bloque m	bit_{1m}	bit_{2m}		bit_{m1}
Bloque Hash	C_1	C_2		C_n

Función HASH

- Algunas Funciones Hash.
  - SNEFRU (128/256 bits) de dos pasos, se puede quebrar usando una PC entre 3 min / 1 hora.
  - N-HASH
  - MD2/4/5 (Message Digest-2/3/4, Ron Rivest, 128 bits)
  - SHA/SHA-1 (Secure Hash Alg.,160 bits) usado en DSS.
  - RIPEMD 128 / RIPEMD 160 (estándar europeo)

Firma Digital

- Proceso que permite asegurar la
  - **IDENTIDAD** del autor del documento.
  - **INTEGRIDAD** del contenido del documento, luego de haber sido firmado.
  - **FECHA Y HORA** de la firma.

Firma Digital

- **Autenticación de mensajes con Criptografía Simétrica.**

  Protege de un tercero a las dos partes que intercambian mensajes.

- **Sin embargo, la autenticación no las protege de lo que se puedan hacer en-tre ellas.**

Firma Digital

- **Situaciones posibles**: Que **A** le envíe a **B** un mensaje autenticado, entonces:
  - **B** puede mostrar un mensaje distinto al recibido y asegurar que ese fue el que envió **A**.
  - **A** puede no haber enviado un mensaje. Pero dado que es posible para **B** fraguar un mensaje, no hay forma de demostrar que **A** realmente no envió un mensaje.

Firma Digital

Propiedades

- Debe ser posible verificar quien es el autor de la firma, como así también la fecha y hora en que se realizó.
- Se debe estar en capacidad poder autenticar el contenido del documento al momento de poner la firma.
- La firma debe ser verificable por terceros a fin de resolver diferendos.

Firma Digital

Requerimientos.

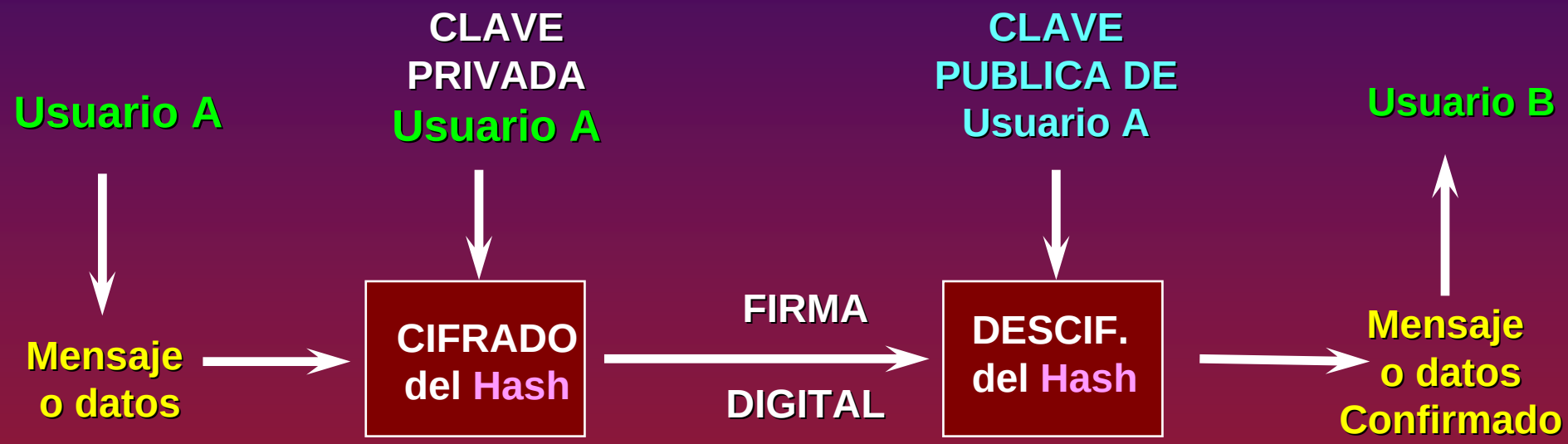
- Grupo de bits que dependa del mensaje al cual se pone la firma.
- Utilizar información que pertenezca sólo al remitente a fin de impedir simultáneamente falsificaciones y desconocimiento.
- Fácil de producir, reconocer y verificar.

Firma Digital

Requerimientos.

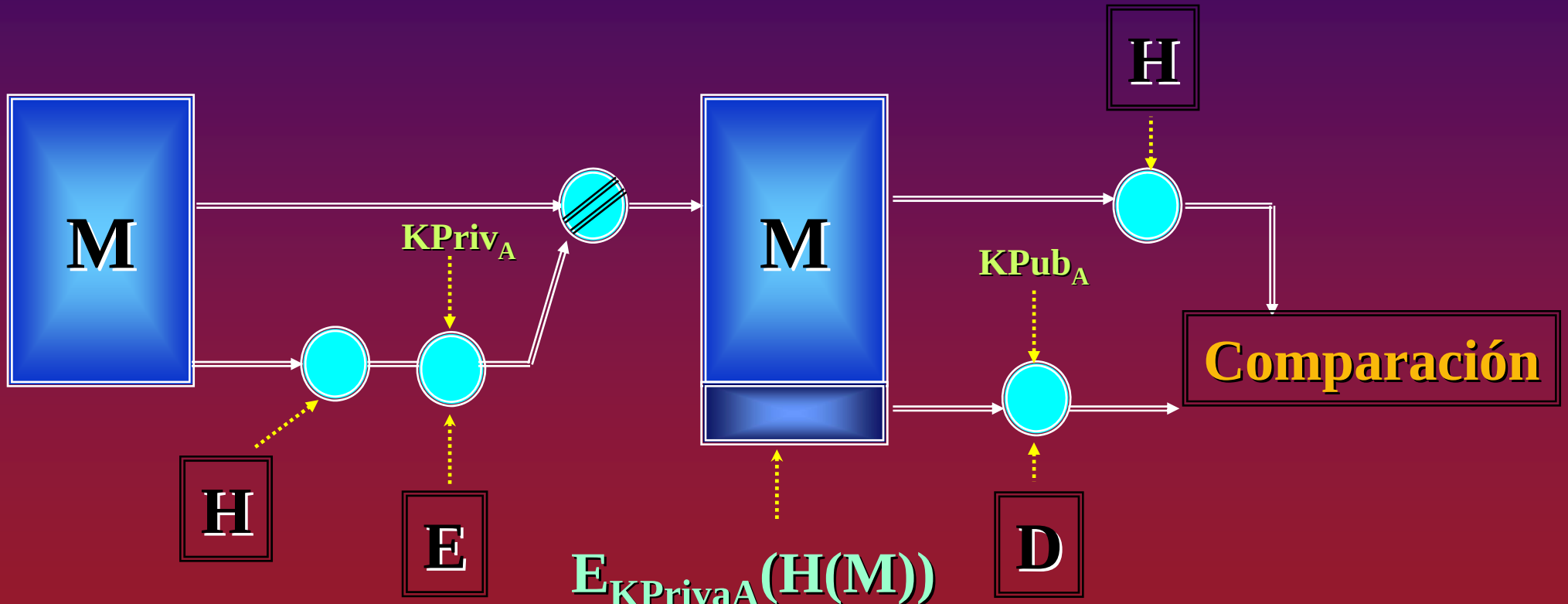
- Computacionalmente impracticable falsificar una firma digital ya sea armando un nuevo mensaje para una firma existente o bien realizando una firma digital fraudulenta para un mensaje dado.
- Factible poder mantener almacenada una copia de la firma digital.

Firma Digital



INTEGRIDAD – CERTIFICACION – NO REPUDIO

Firma Digital



Firma Digital

- Problema para distribuir Claves Públicas.
- La solución está dada por

CERTIFICADOS DE CLAVE PUBLICA

Firma Digital

Cadena de confianza

- Documento de J. R. García.
  - Firmado: H. K. Pérez.
- Certifico que la firma que antecede es válida y corresponde a H. K. Pérez.
  - Firmado: Banco Nación.
- Certifico que la firma que antecede es válida y corresponde a BANCO NACION.
  - Firmado: Banco Central.

Certificado Digital

- Un **Certificado** es una estructura de datos firmada digitalmente, definida en el standard X.509, que liga la identidad del poseedor del certificado con su clave pública.
- La protección de la clave privada debe realizarse con un algoritmo simétrico.
- El usuario mantiene una base de datos donde almacena su certificado, claves y certificados que provienen de otros usuarios.

Administración de claves y certificados

Emisión de un certificado

- Para establecer la identidad, al solicitar un pasaporte, se requiere de:
  - Registrar la siguiente información.
    - Lugar y fecha de nacimiento, Domicilio, Estado Civil, Condenas judiciales.
  - Aportar la siguiente documentación.
    - Partida de Nacimiento, Certificado de Matrimonio, DNI.
  - Fotografías actualizadas.
  - Hacer el trámite en forma personal.
  - Hacer colas (por lo menos tres (3) horas).
  - Pagar tasa fiscal.
  - Entrega al cabo de cierto tiempo.

Certificado del mundo real: Pasaporte

- **Nombre:** Identifica al poseedor o sujeto del pasaporte.
- **Lugar y fecha de nacimiento:** Información adicional del poseedor.
- **Fotografía y firma:** Son para poder hacer comparaciones.
- **País emisor:** País que certifica la identidad del poseedor.
- **Número único:** Número de serie que identifica en forma unívoca a cada pasaporte.
- **Fecha de emisión:** Fecha a partir de la cual el pasaporte tiene validez.

Certificados del mundo real

- **Fecha de caducidad:** Fecha a partir de la cual pierde su validez.
- **Firma de la autoridad emisora:** Firma, marcas holográficas o de seguridad para evitar fraude.
- **Número de página:** Las páginas están numeradas y tienen el número de serie grabado en las mismas para evitar que se puedan cambiar o agregar fácilmente.
- **Información adicional:** Tipo de pasaporte, condiciones de uso y cualquier otra información, como hijos menores.

Certificado Digital

Versión (Version)		***Número de versión del formato X.509***
Número de Serie (Serial Number)		***Único número identificador del certificado generado por el emisor del mismo.***
Firma (Signature)	**ID del Algoritmo**	***Algoritmo usado para firmar el certificado***
Emisor (Issuer)		***Nombre del emisor del certificado (en formato X.500)***
Validez (Validity)	**No antes de (Not Before)**	***Fecha de inicio de validez***
	No después de (Not After)	***Fecha de finalización***

Certificado Digital

Titular (Subject)		***Nombre del titular del certificado (en formato X.500)***
Información de la Clave Pública del Titular. (Subject's Public Key)	**ID del Algoritmo**	***Algoritmo de firma del titular***
	Parámetros	***Parámetros aplicables a la clave pública***
	Clave Pública	***Clave Pública del titular***
Extensiones. (Extensions)	**(Opcional)**	***Extensiones agregadas a los certificados tal como lo indica el estándar.***
Firma del Emisor (Encrypted)	**ID del Algoritmo**	***Algoritmo usado para esta firma***
	Cifrado del resultado de la función de Hash sobre el certificado	

Contenido de un Certificado

Version		X.509 Version 3
Serial Number		Ox3E29...
Aigorithm Identifier		MD5 hash and RSA signing
Issuer:		
	Organization	Verisign Trust Network
	Organizational Unit	Verisign, Inc.
	Organizational Unit	Verisign International server CA = Class 3
	Organizational Unit	www.verisign.com/cps ...
Validity:		
	Not Before	1998-12-03 00:00.00 UTC
	Not After	1999-12-11 23:59.59 UTC
Subject:		
	Country	New Zealand.
	State or Province	Auckland.
	Locality	Auckland
	Organization	ASB Bank Limited
	Organizational Unit	Information Services
	Common Name	www.asbbank.co.nz
Public Key Information:		
	Aigorithm	RSA
	Public Key	Ox308188...
Extensions:		
	International Step-Up Server Gated Cryptography various VeriSign extensions	
Aigorithm Identifier		MD5 hash with RSA signing
Signature		Ox4C2170...

Certificado Digital

- Uso de los certificados en aplicaciones.
  - Secure Socket Layer: *https://www.bank.com/*
  - Correo Electrónico Seguro.
  - Redes Privadas Virtuales.

Infraestructra de Clave Pública (PKI)

- Porqué es necesaria:
  - Creación de claves seguras.
  - Validación inicial de identidades.
  - Emisión, renovación y baja de certificados.
  - Validación de Certificados.
  - Distribución de certificados y la información asociada.
  - Guarda segura y recuperación de claves.
  - Generación de firmas y marcas de tiempo.
  - Establecimiento y manejo de relaciones de confianza.
  - Autenticación del Usuario.

PKI

Autoridades de Certificación

- Son terceras partes en la cual confían sus usuarios para que les extienda certificados de Clave Pública y garanticen la precisión de los datos críticos contenidos en los certifi-cados que extienden.

- El dominio de un certificado comienza por la parte superior de la cadena, conocida como la **Autoridad Raíz** ***(Root Authority).***

PKI

- Requiere equipamiento e instalaciones especiales, procedimientos y mecanismos para asegurar canales seguros o “trusted paths”, personal seleccionado, almacenamiento seguro.

Elementos de PKI

- Autoridad de Certificación.
  - Autoridad de Registro.
  - Servidor de Certificados.
  - Depósito de Certificados.
- Validación de Certificados.
- Servicio de Recuperación de Claves.
- Servidor de tiempo.
- Servidor de firmas.

Autoridades de Certificación

- Las reglas que delinean los distintos aspectos de como las AC son operadas y sus limitaciones, la descripción de cómo la AC debe proteger las claves, que información debe ser puesta en el certificado y cada cuanto se debe generar la información de revocación, etc. están definidas en un documento denominado:

  - Certification Practices Statement (CPS) o Declaración sobre las Actividades de Certificación.

Depósito de Certificados

- Un depósito de certificados es el lugar que los mecanismos de publicación utilizan para distribuir los certificados públicos.
- Los depósitos son directorios de LDAP (Lightweight Directory Access Protocol).
- Los certificados pueden ser de distribuidos directamente a un usuario específico, cuando el propietario del certificado inicia una conexión con el usuario del certificado.

Validación de Certificados

- Los usuarios de los certificados necesitan validar aquellos certificados que reciben. Este proceso requiere:
  - Verificar la firma del firmante del certificado.
  - Asegurar la validez del certificado controlando la fecha de vigencia.
  - Controlar la concordancia entre el uso que se quiera dar al certificado y cualquier restricción de oren político especificada en el mismo por la AC.
  - Verificar que el certificado no fue anulado por la AC.

Servicio de Recuperación de Claves

- Cualquiera sea el método de generación de claves:
  - Navegador.
  - Tarjeta Inteligente.
  - Servidor Central de Claves.

se debe proporcionar un mecanismo que realice el cifrado de claves y permita recuperarlas si se pierden, por orden judicial, enfermedad o muerte del poseedor de las mismas.

Servidor de Tiempo

- Las firmas digitales permiten que se emita una constancia de fecha y hora.
- Se necesita que el tiempo se tome de una fuente precisa, confiable y monótonamente creciente desde la cual se transfiera, en forma segura, la constancia temporal, sin que pueda ser interceptada o reemplazada.
- La constancia es firmada de modo que se pueda verificar al emisor de la fuente de tiempo confiable.
- Aplicable a logs de auditoría, sistemas de acuse de recibo y documentos electrónicos, incluyendo contratos.

Administración de claves y certificados

Cuál es la vida útil de la clave?

- Si la información a proteger se la cifra con RSA de 760 bits de clave, serán necesarios 600 meses o 50 años para quebrarla. Con 1024 el tiempo requerido es de 3 millones de años.
- Las claves pueden ser descubiertas debido a inadecuadas implementaciones por software, análisis del hardware de almacenamiento de las claves, falta de celo del propietario al momento de proteger el acceso a las claves, ingeniería social, etc.
- Como resultado de esto, las normas de seguridad recomiendan un cambio periódico de clave, siendo ésta una de las razones para fijar períodos de validez de los certificados.

Administración de claves y certificados

Validación de certificados.

- Debe contener una firma criptográfica válida.
- La clave pública del emisor debe emplearse para verificar la firma del certificado.
- Las fechas deben indicar que el certificado está vigente.
- Debe ser utilizado para el propósito para el cual fue originalmente creado. Por ejemplo, claves y certificados destinados para solamente firmar aplicaciones no pueden ser empleados en operaciones de cifrado.
- No tiene que estar anulado. Aunque toda la información interna del certificado indique que el mismo es válido

Administración de claves y certificados

Revocación de certificados.

Las razones que fundamentan la desactivación de las claves, previa a la fecha de caducidad del certificado, son:

- Sospecha o certeza de que la clave privada está comprometida.
- El usuario mencionado en el certificado ya no tiene autoridad para usar la clave (cambio en el status o asignación laboral, etc.)
- La información en el certificado no es precisa debido a cambios en nombres o autoridad atribuida a un individuo en particular.

Administración de claves y certificados

- **Lista de Revocación de Certificados (CRL)**
  - Es una lista de certificados que fueron revocados antes de su fecha de expiración.
  - Son creadas, mantenidas y puestas a disposición de los usuarios por la AC.
  - Solamente contiene la nómina de los certificados con fecha de caducidad posterior a la fecha de publicación.

Administración de claves y certificados

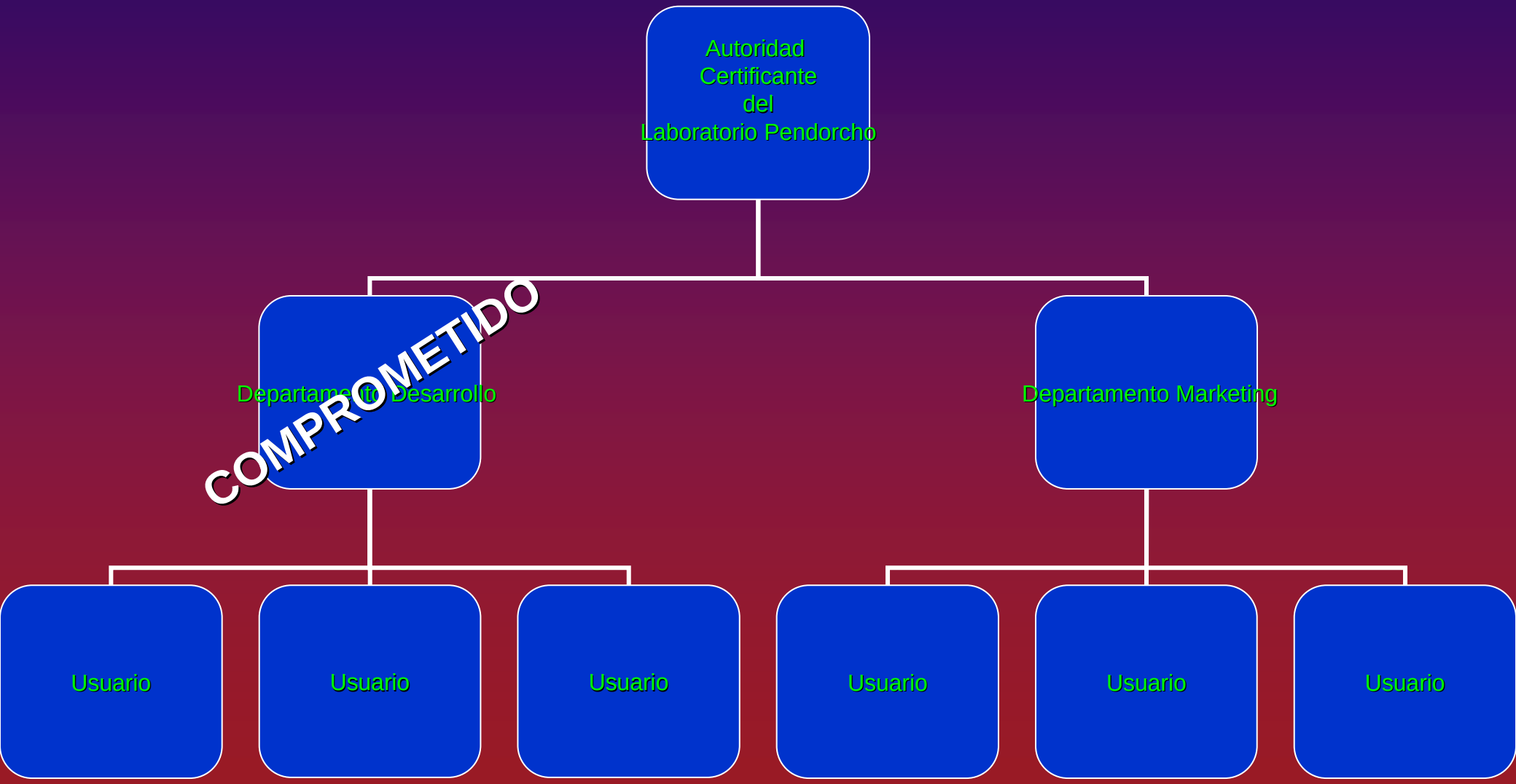
- **Recorridos de la certificación.**
  - Una sola AC de gran tamaño no es una solución razonable.
  - Qué ocurre si se ve comprometida la Clave Privada de una AC de proporciones?
    - Anulación de certificados
    - Usuarios que deberán pasar por un nuevo proceso de registro.
  - Se requiere un modelo que permita el despliegue de múltiples AC en diferentes momentos.

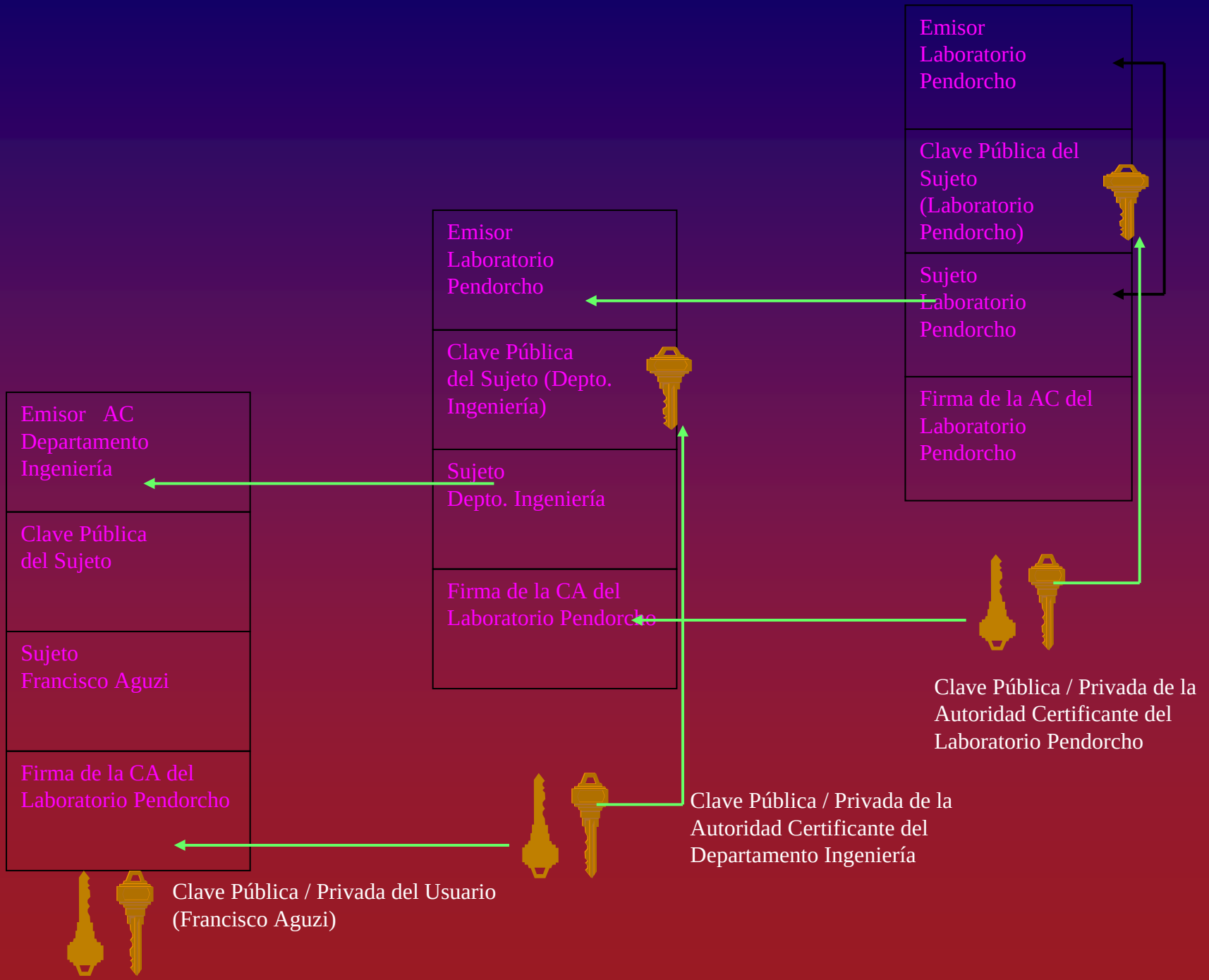
Administración de claves y certificados

Jerarquías de los Certificados

- Las AC están en capacidad de certificar la identidad de usuarios o routers de redes, y además pueden certificar la de otras AC.
- En este modelo, la AC en la cual se confía puede respaldar la identidad de otra AC.
- Como resultado muchas identidades y AC son consideradas subordinadas a otras identidades y AC. En entornos muy grandes es frecuente hallar AC que tienen como único objetivo el identificar a otras AC. La jerarquía resultante se muestra en la figura siguiente:

Administración de claves y certificados




Emisor
Laboratorio
Pendorcho
Clave Pública del
Sujeto
(Laboratorio
Pendorcho)
Sujeto
Laboratorio
Pendorcho
Firma de la AC del
Laboratorio
Pendorcho
Emisor
Laboratorio
Pendorcho
Clave Pública
del Sujeto (Depto.
Ingeniería)
Sujeto
Depto. Ingeniería
Firma de la CA del
Laboratorio Pendorcho
Emisor AC
Departamento
Ingeniería
Clave Pública
del Sujeto
Sujeto
Francisco Aguzi
Firma de la CA del
Laboratorio Pendorcho
Clave Pública / Privada de la
Autoridad Certificante del
Laboratorio Pendorcho
Clave Pública / Privada de la
Autoridad Certificante del
Departamento Ingeniería
Clave Pública / Privada del Usuario
(Francisco Aguzi)
2009

Administración de claves y certificados

- **Tipos de claves**
  - **Cifrado de claves:** transporte o intercambio
  - **Cifrado de datos.**
  - **Claves para firma digital.**

Administración de claves y certificados

- Distribución de certificados.
  - Distribuido con el protocolo.
    - Correo Electrónico (protocolo S/MIME).
    - Lado Cliente en Autenticación SSL.
  - Distribuido a través de un repositorio.
    - E-mail.

Autoridades de Certificación

- **Quién puede ser una AC?**
  - Empresas cuyo negocio es brindar los servicios profesionales de una AC al público en general.
  - Compañías, organizaciones, entidades gubernamentales, etc. que por razones de seguridad, costo, control, etc. desean hacerlo por su cuenta.

Administración de claves y certificados

- CA pública.
- CA dentro de la empresa.
- CA externa a la empresa.

Ataques a Certificados

- **Posibles amenazas a los certificados:**
  - Ingreso subrepticio a una instalación perteneciente a un elemento de la JCC con fines de robo o copia de su clave privada.
  - Obtención de la clave privada por criptoanálisis.
  - Emisión compulsiva de un certificado con identidad falsa.

Servicios Opcionales

- Generación del par de claves pública / privada del usuario.
- Guarda de los pares de claves del usuario.
- Recuperación de datos (Key Escrow).
- Programación de tokens de seguridad.
- Certificación cruzada con otros dominios de certificación.

Servicios Opcionales

- **Distribución de Certificados.**
  - Para que dos partes utilicen criptografía asimétrica, cada una de ellas debe de estar en posesión de las claves públicas de la otra.
  - El método más común para difundir los certificados es publicarlos en boletines, páginas Web o directorios.
  - Certificados compartidos por los usuarios.

Firma Digital

- **TIPOS DE CERTIFICADOS DIGITALES**
  - **Clase 1: Certificado de e-mail**
  - **Clase 2: Certificado ID personal ante 3ros. (DNI, Domicilio, etc.) Apto e-commerce. Usado por SSL.**
  - **Clase 3: Institucional , vinculado a la empresa o institución a la que se pertenezca.**