Desarrollo e implementación de un prototipo de Notaría Digital

Francisco Rodríguez-Henríquez
CINVESTAV-IPN

Material desarrollado como parte de la tesis de maestría de:
Vladimir González García

Febrero de 2010
Universidad de TURABO

Francisco Rodríguez-Henríquez
Líneas de Investigación en Seguridad Informática

Introducción

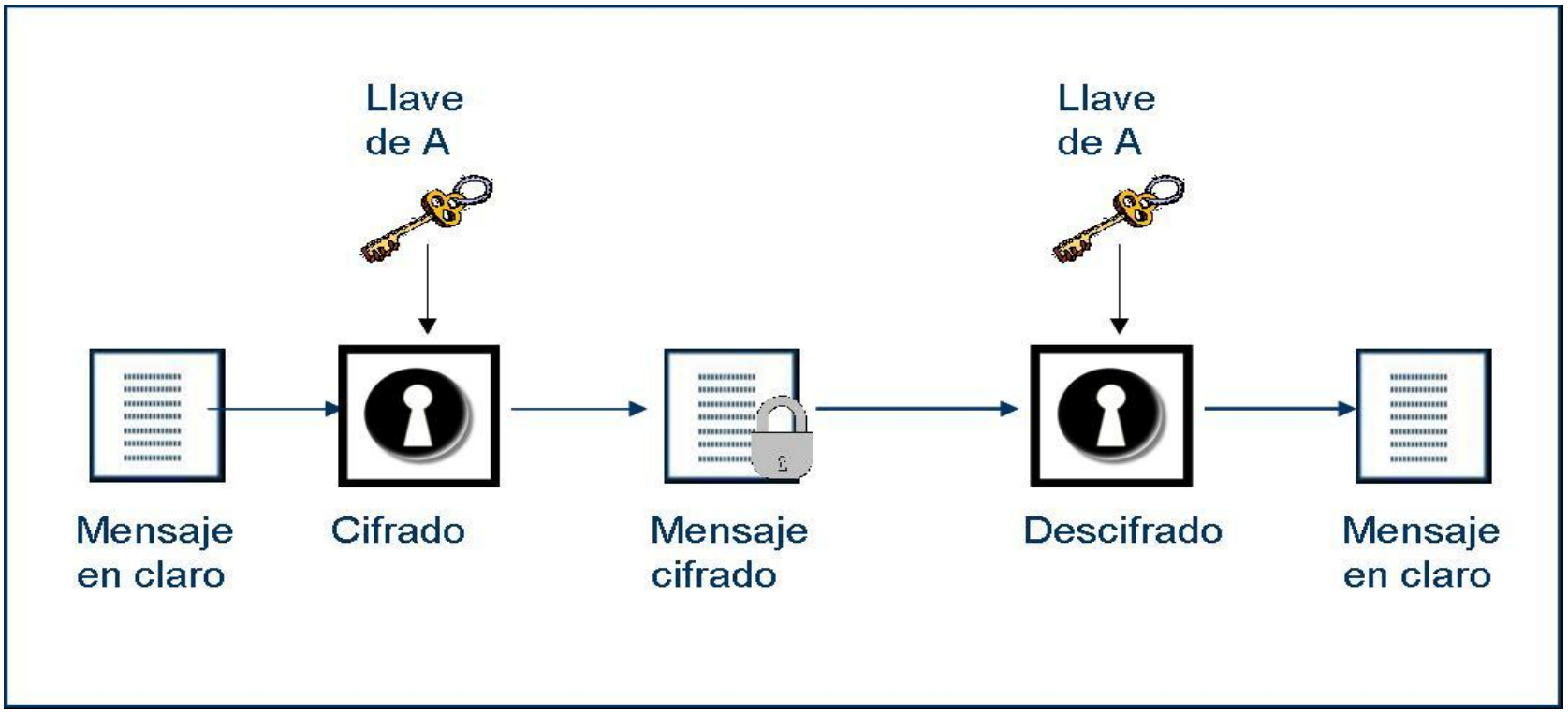
Papel contra Documento Digital

- Intercambio, reproducción.
- Integridad.
- Identidad y No repudio.

Ejemplo: Un documento digital cifrado con DES (1976) 54 bits, comprometido en menos de 24hrs.

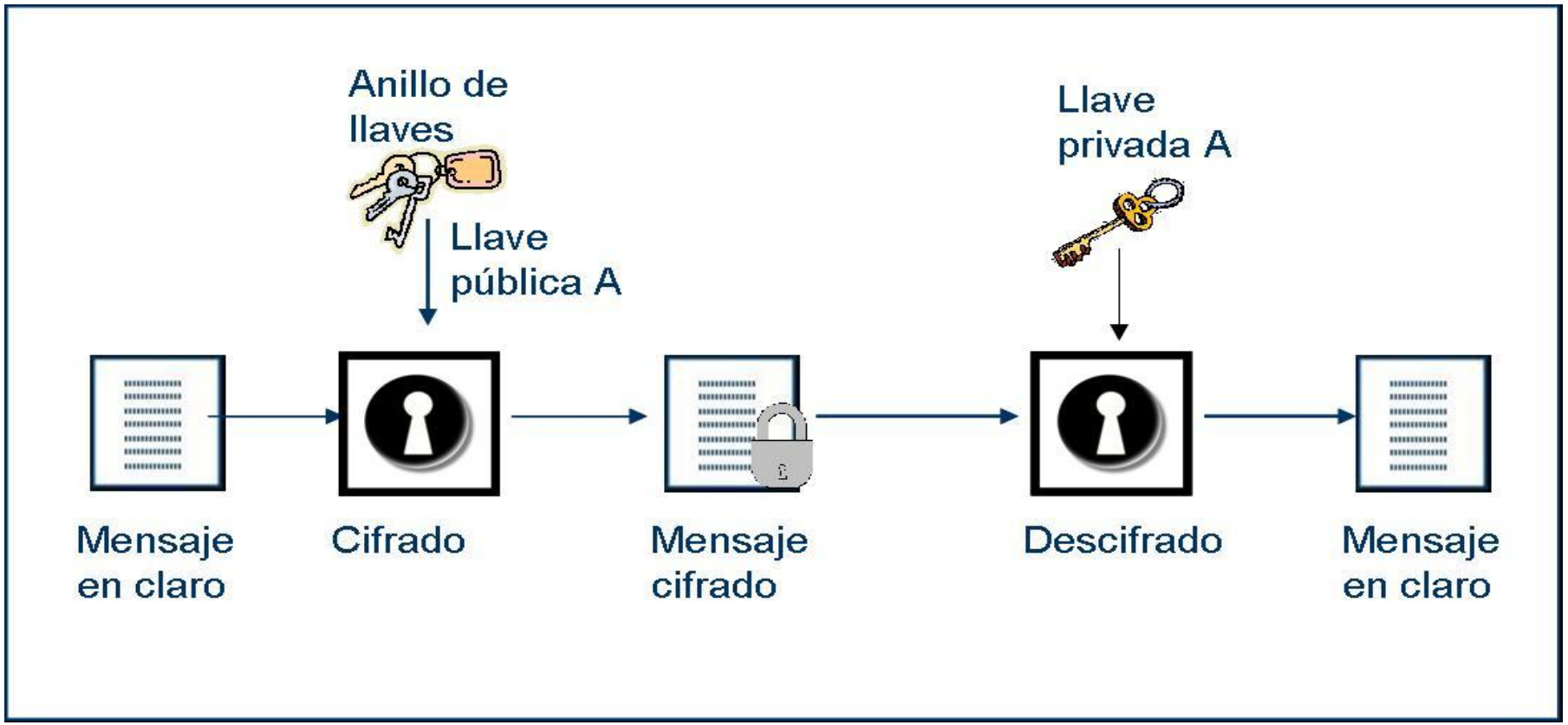
Conceptos básicos

Llave privada



Conceptos básicos

Llave pública

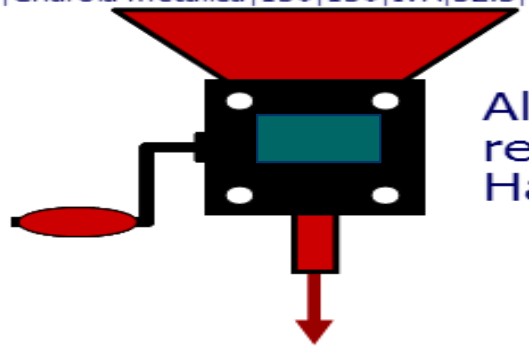


Conceptos básicos

Algoritmo de Resumen o *Hash*

Cadena Original

||A|1|2005-09-02T16:30:00|1|ISP900909Q88|Industrias del Sur Poniente, S.A. de C.V.|Alvaro Obregón|37|3|Col. Roma Norte|México|Cuauhtémoc|Distrito Federal|México|06700| Pino Suarez|23|Centro|Monterrey|Monterrey|NuevoLéon| México|95460|CAUR390312S87|Rosa María Calderó|Uriegas| Topochico|52|Jardines del Valle|Monterrey|Monterrey|Nuevo León|México|95465|10|Caja|Vasos decorados|20|200|1| pieza|Charola metálica|150|150|IVA|52.5||



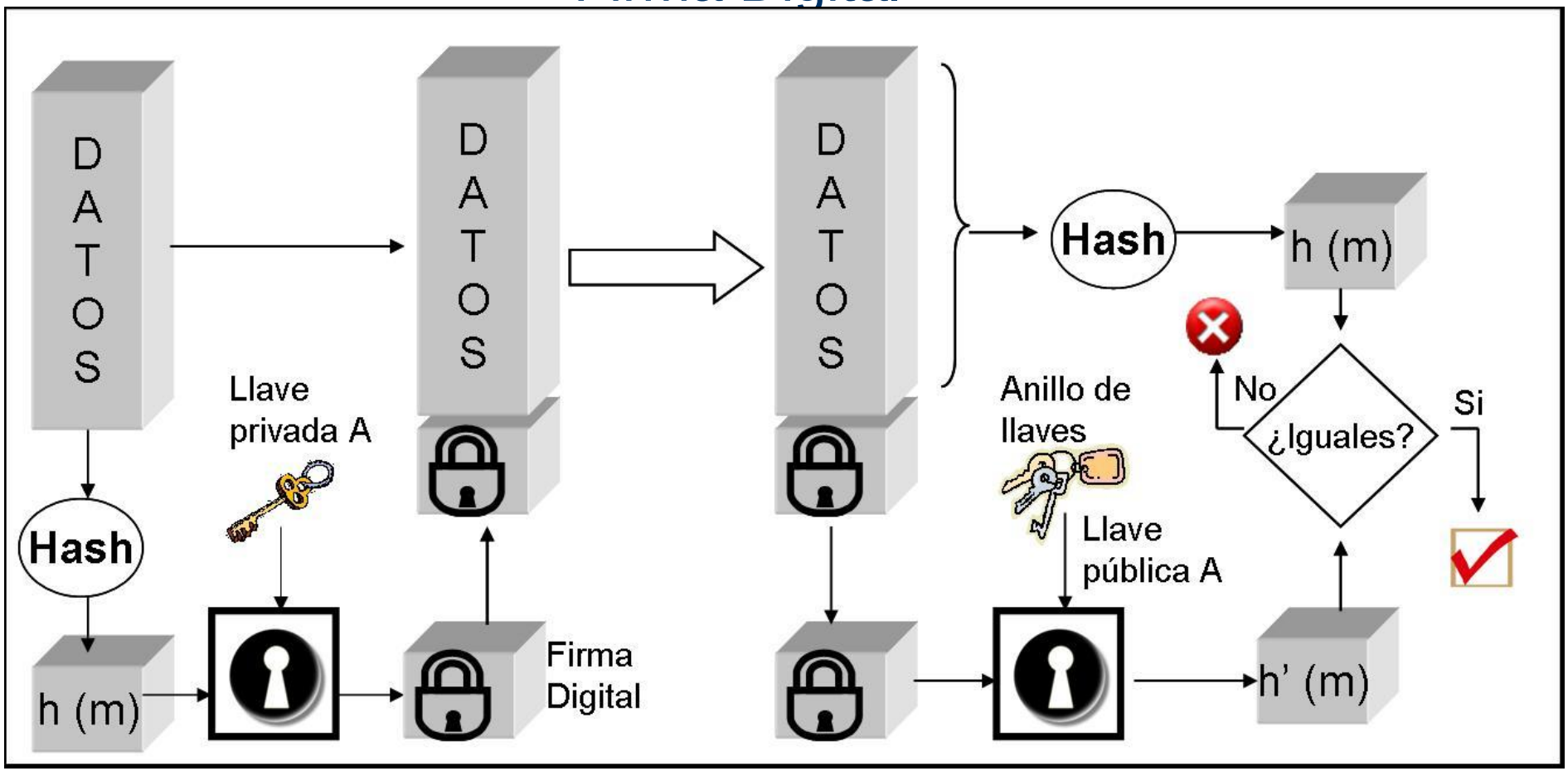
Algoritmo de resumen o Hash

8a a2 b6 17
94 44 27 35
36 97 e6 94
a2 e3 5a 07

Resumen o Hashing

Conceptos básicos

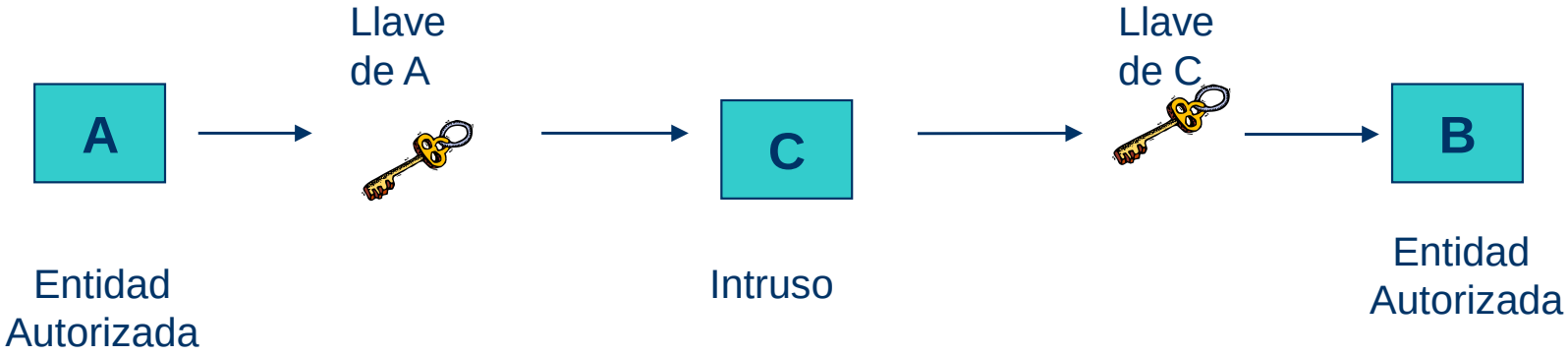
Firma Digital



Infraestructura PKI

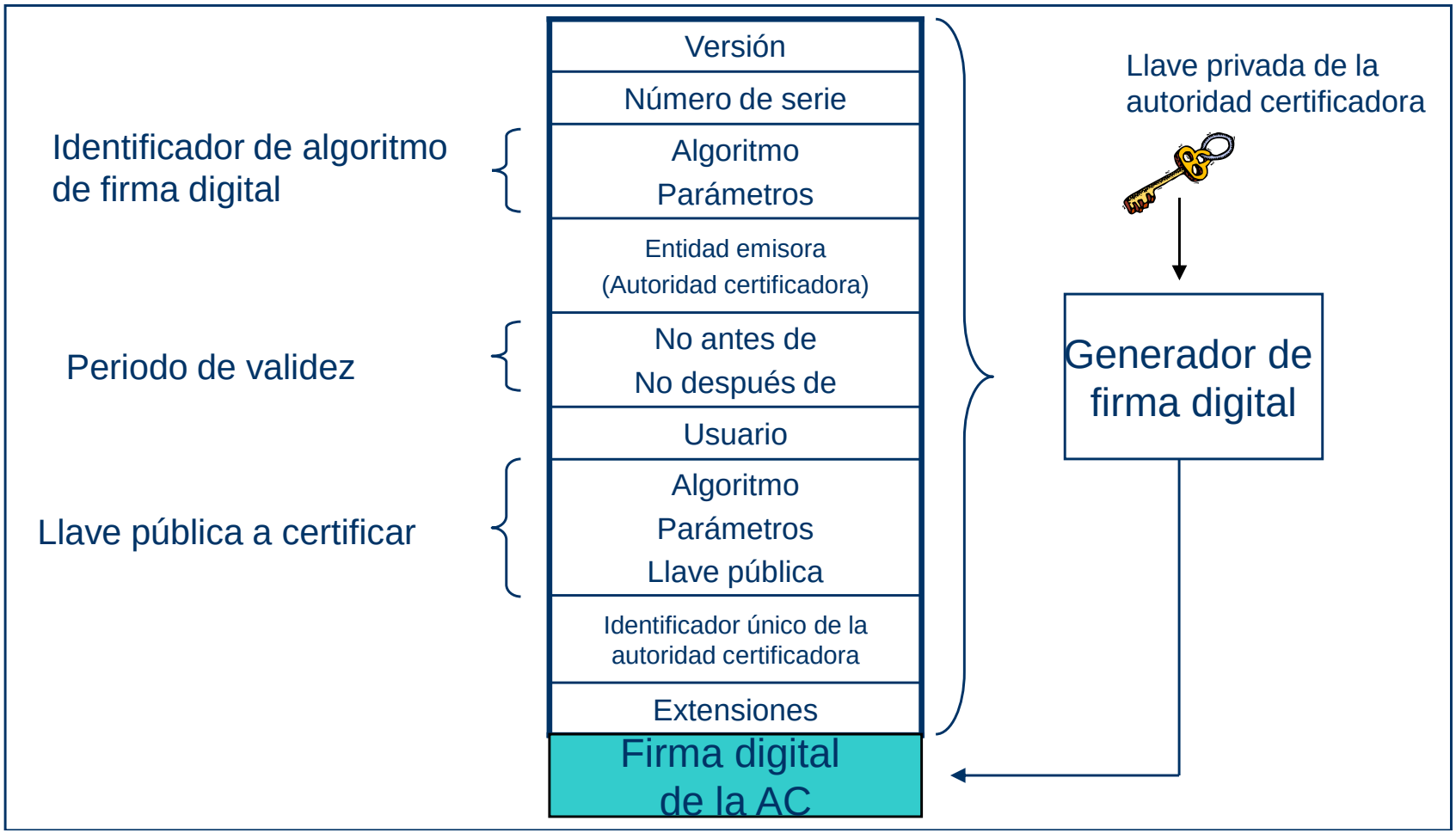
- ¿Cómo asegurar que la persona que firma un documento es quien dice ser?

  Existen varios ataques al intercambio de llaves, por ejemplo intruso en medio.



Infraestructura PKI

Certificado Digital X.509v3



Infraestructura PKI

Componentes de PKI

- Entidad final
- Autoridad de registro
- Autoridad certificadora
- Repositorio
- Emisor de CRL

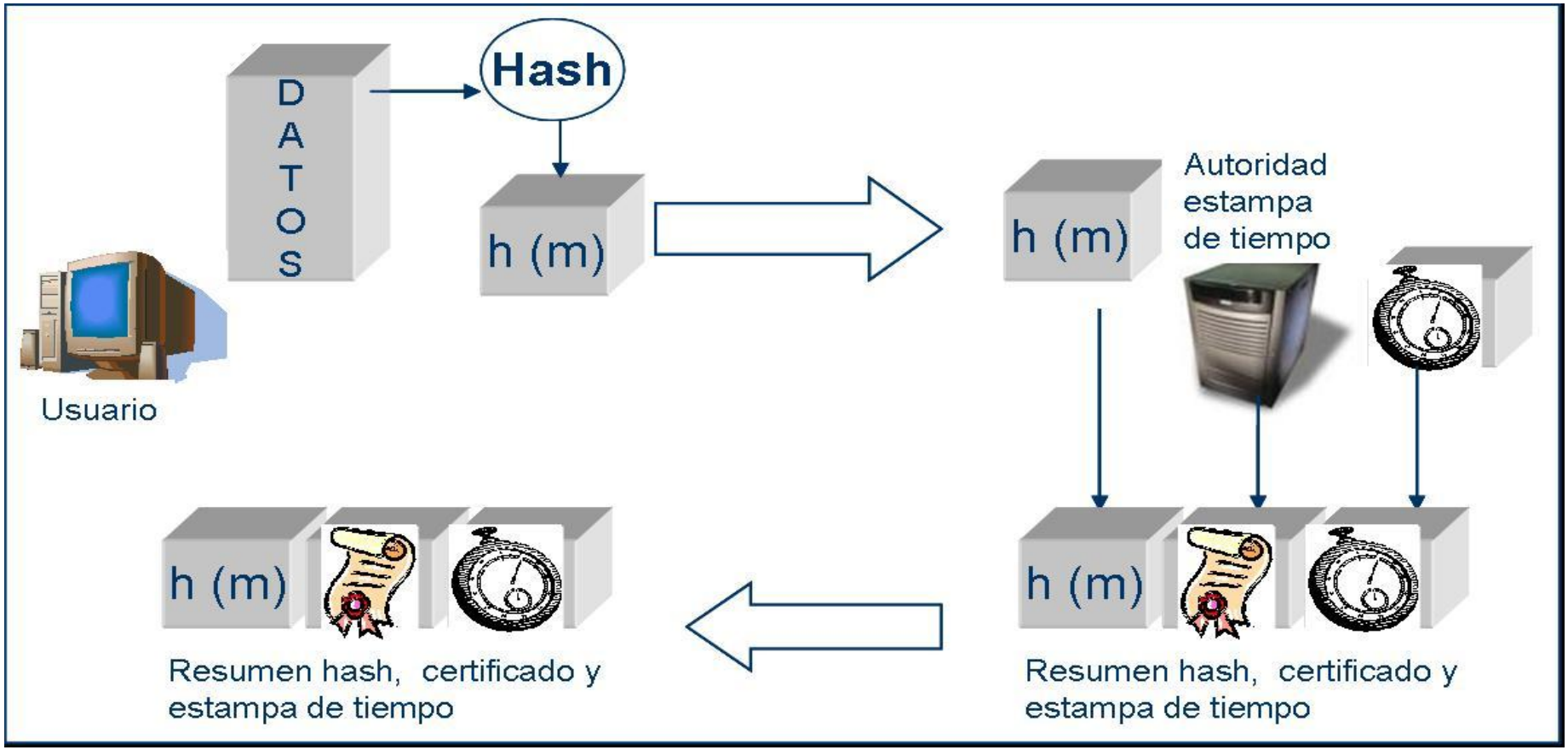
Notaría Digital

- La función notarial
- Necesidad en documentos
- Necesidad en documentos digitales
- Notaria digital

Al certificar documentos electrónicos se evita el plagio de la información y se garantiza que el documento no ha sido modificado.

Notaría Digital

Estampa de tiempo

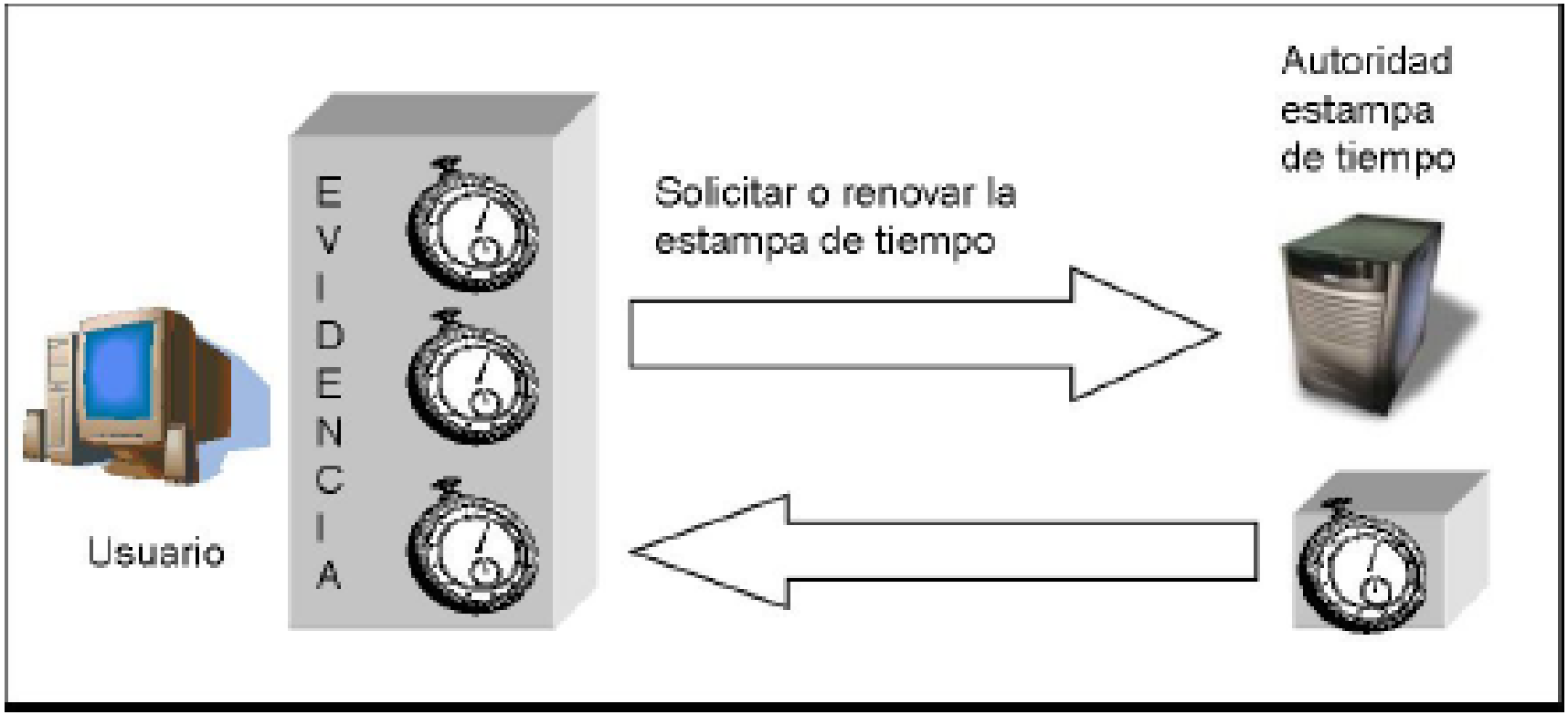


Notaría Digital

Servicios de protocolo Long Term Archive Notary Service (LTANS)

- ALMACENAMIENTO Enviar datos a un Servicio de Almacenamiento a largo plazo y solicitar la creación de información de evidencia para los datos.
- ESTADO Informar acerca del estado de los datos.
- VERIFICACIÓN Determinar la integridad y validez de los datos almacenados.
- EXPORTACIÓN Solicitar datos (incluyendo datos almacenados, meta-información y evidencia de la información) de un servicio de Almacenamiento a Largo Plazo.
- BORRADO Remover datos o evidencia de la información del servicio.

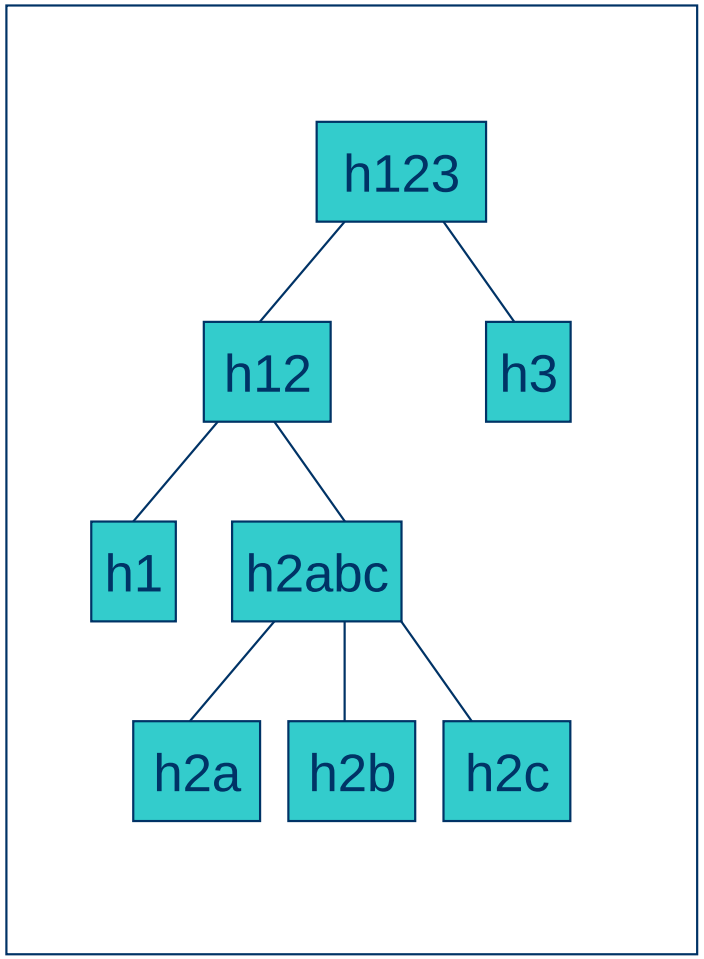
Generación del Registro de evidencia



Notaría Digital

Árboles *hash*

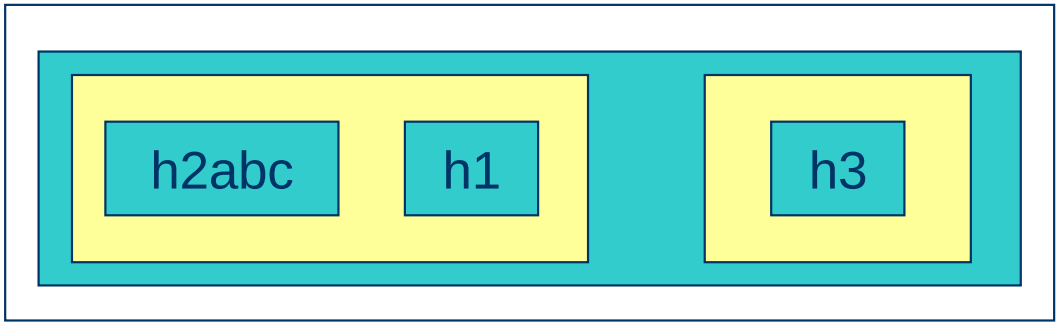
- h1 = H (d1) donde d1 es el único objeto del grupo 1
- h3 = H (d3) donde d3 es el único objeto del grupo 3
- h12 = H (concatenación y ordenación binaria de (h1, h2abc))
- h123 = H (concatenación y ordenación binaria de (h12, h3))
- h2abc = H (concatenación y ordenación binaria de (h2a, h2b, h2c))



Notaría Digital

Reducción árbol hash

1. Seleccionar y concatenar los valores hash que tengan el mismo padre
2. Realizar el resumen de la concatenación
3. Repetir los pasos hasta tener un solo valor hash (la raíz)



Reducción para grupo de datos 1

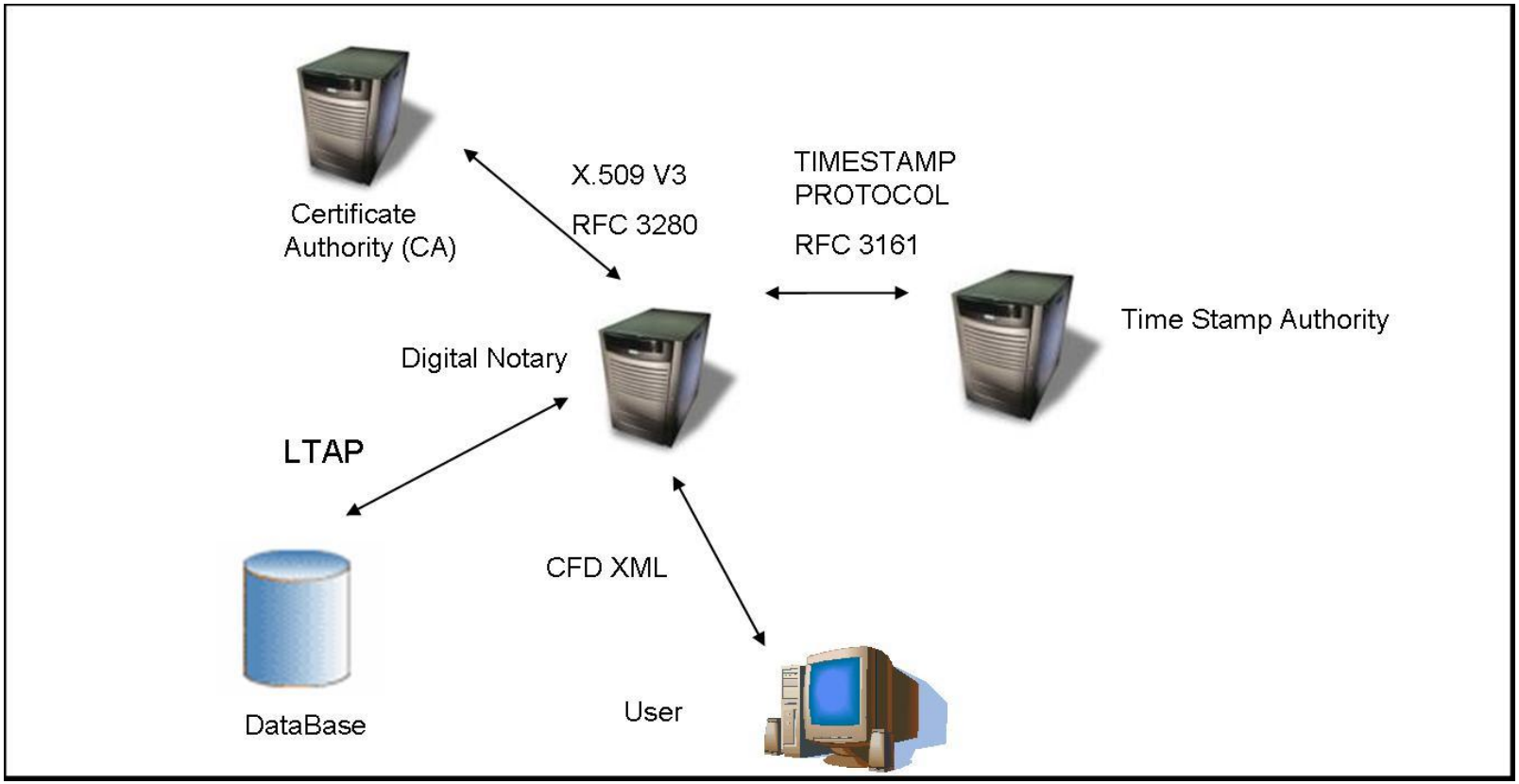
Notaría Digital

Protocolo LTANS

- Estampa de Tiempo de Almacenamiento
- Cadena de Estampas de Tiempo de Almacenamiento
- Secuencia de Cadenas de Estampas de Tiempo de Almacenamiento

Notaría Digital

Arquitectura de **Notaría Digital**



Factura Electrónica

- Escenarios
  - Notario Electrónico
  - Factura Electrónica
- Objetivos
  - Comprobar que los documentos son copias legítimas de los originales
  - Autenticación de las partes involucradas
- Herramientas
  - Criptografía de llave pública
  - Certificados Digitales
  - Autoridades Certificadoras y de estampas de tiempo

CATE

1 El contribuyente pide cita al centro de Atención Telefónica Externo *(01 800) 849 93 70*

2 Se le asigna cita al contribuyente

3 El contribuyente obtiene aplicación SOLCEDI y genera archivo .key y archivo .req

SAT.GOB.MX

4 El contribuyente Acude a cita

Local

5 Obtiene certificado de firma electrónica avanzada

Contribuyente
- Acude a cita
- Entrega documentos Entrega archivo .req

ALAC
- Revisa documentos
- Genera certificado de firma electrónica avanzada

CICLO DE GENERACIÓN

Seguridad

- Los estándares de Seguridad empleados en la Firma Electrónica Avanzada y el Comprobante Fiscal Digital están basadas en la tecnología de Llaves Publicas.

- Llaves de 1024 bits RSA (Llave Privada y Publica)
  - Se estima que se requieren de más de 70 años con las computadoras más potentes y un presupuesto de mas de 100 millones de dólares para poder 'quebrar' este algoritmo.
  - Los certificados de Firma Electrónica Avanzada y de Sellos Digitales tienen una validez de 2 años lo cual elimina la posibilidad de que alguien quiebre esta llave.

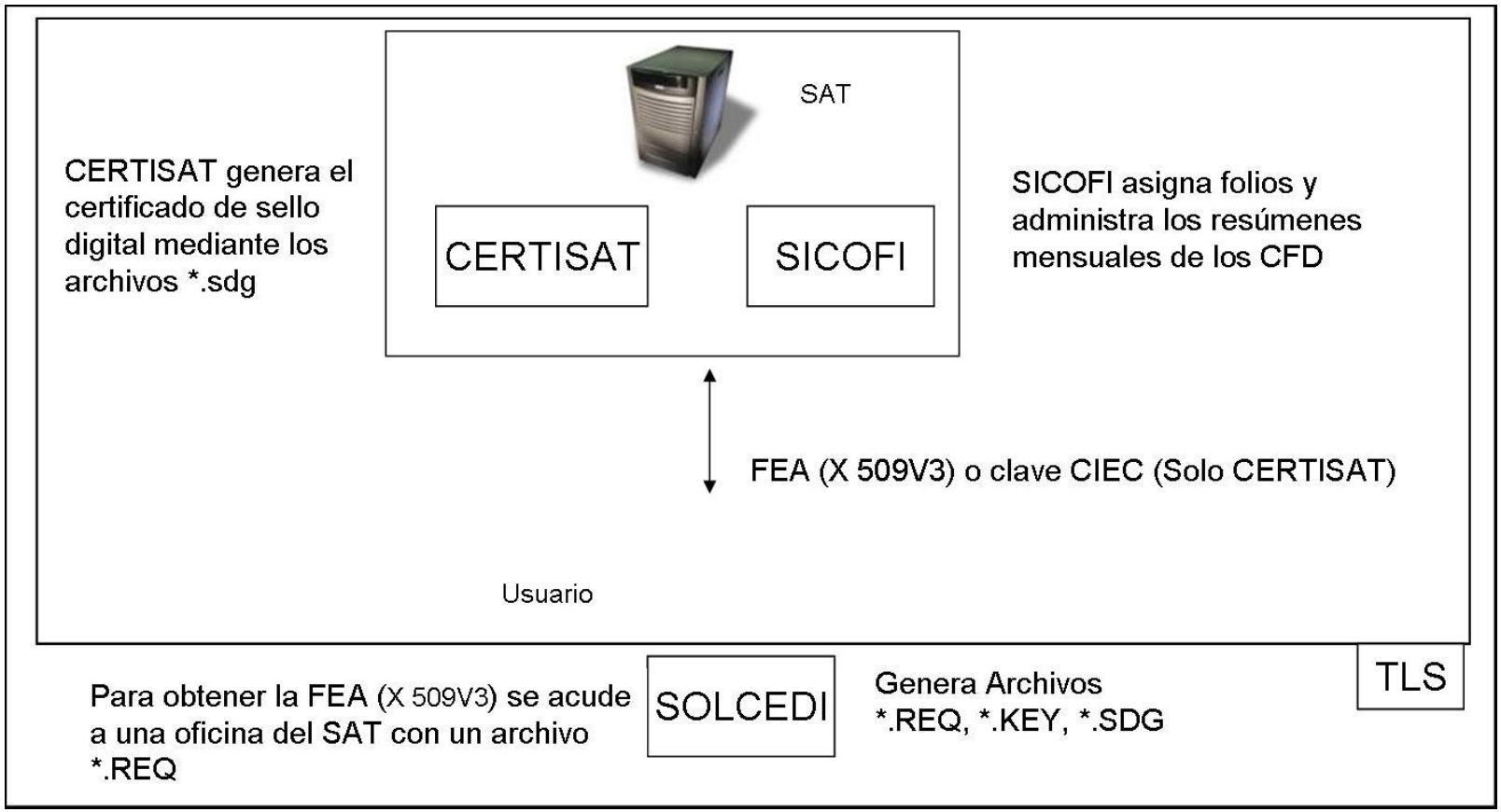
- Encriptación 3 DES (Encriptación de Seguridad en la Llave Privada)
  - Si con un hardware especial se pudiera desencriptar algo encriptado con DES en 1 segundo, se requerirían 2,285 billones de años para 'quebrar' un encriptamiento con Triple DES con el mismo hardware.
  - Se requirieron 22 horas y 100,000 computadoras para 'quebrar' el algoritmo DES en su ultima prueba.

*** Number 13 - April 2000* - Bulletin**
A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths
Robert D. Silverman, RSA Laboratories

**** Data Encryption Standard" FIPS 46**
Extracting a 3DES key from an IBM 4758
***** FIPS 180-1 / 180-2**

Comprobantes Fiscales Digitales del SAT

Sistema de Comprobantes Fiscales Digitales del SAT



Comprobantes Fiscales Digitales del SAT

Firma Electrónica Avanzada

- Generar *.req (PKCS#10) y *.key (PKCS#8). RSA 1024 bits.
  - Requisitos: RFC, CURP, EMAIL, Contraseña de acceso y Contraseña de revocación
- Obtener el certificado (X.509v3) en el SAT
  - Contenido: Nombre o razón social, RFC, CURP
- Entrega certificados, Renovación, Revocación.

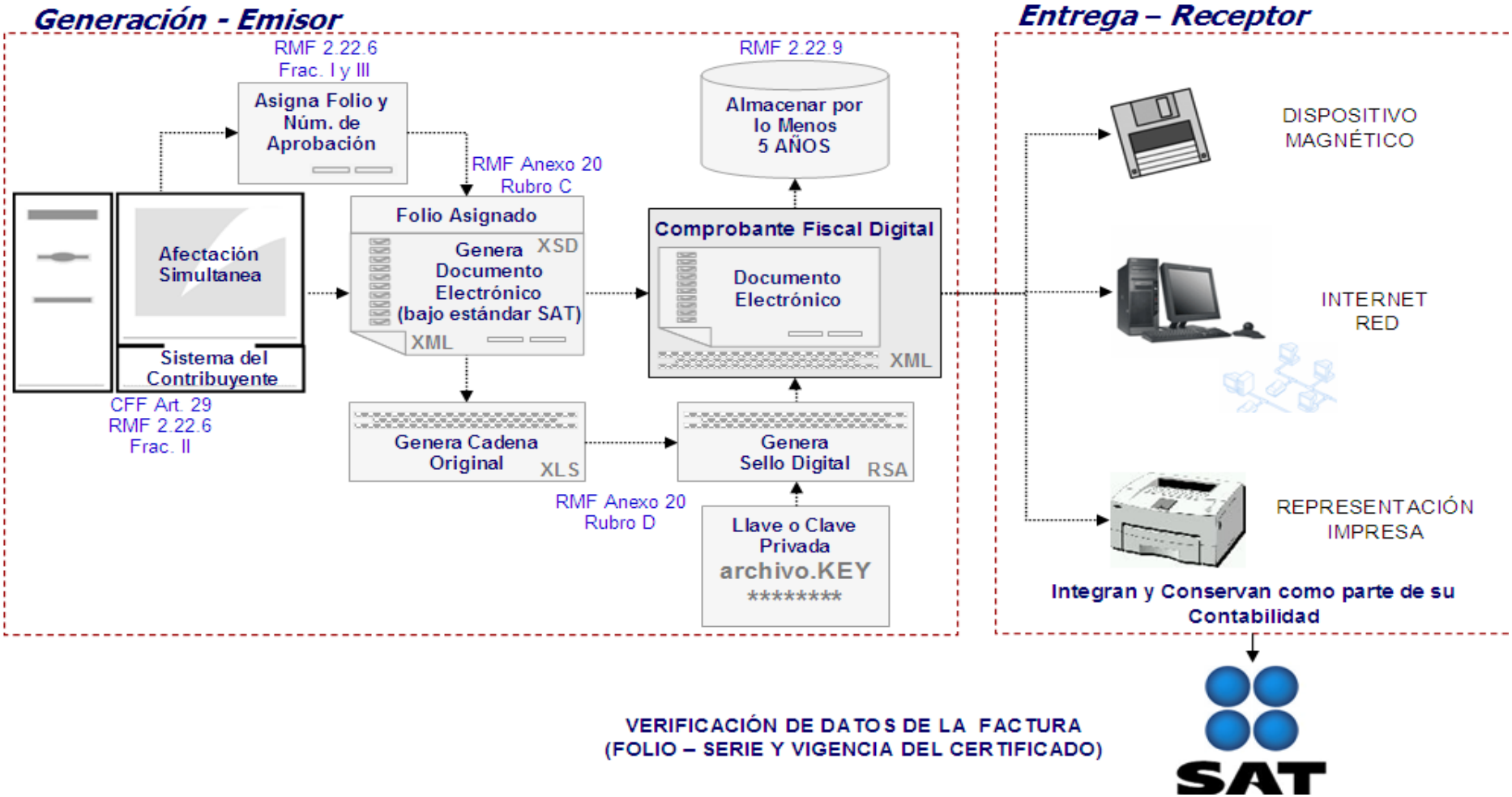
Comprobantes Fiscales Digitales del SAT

Certificado de sello digital

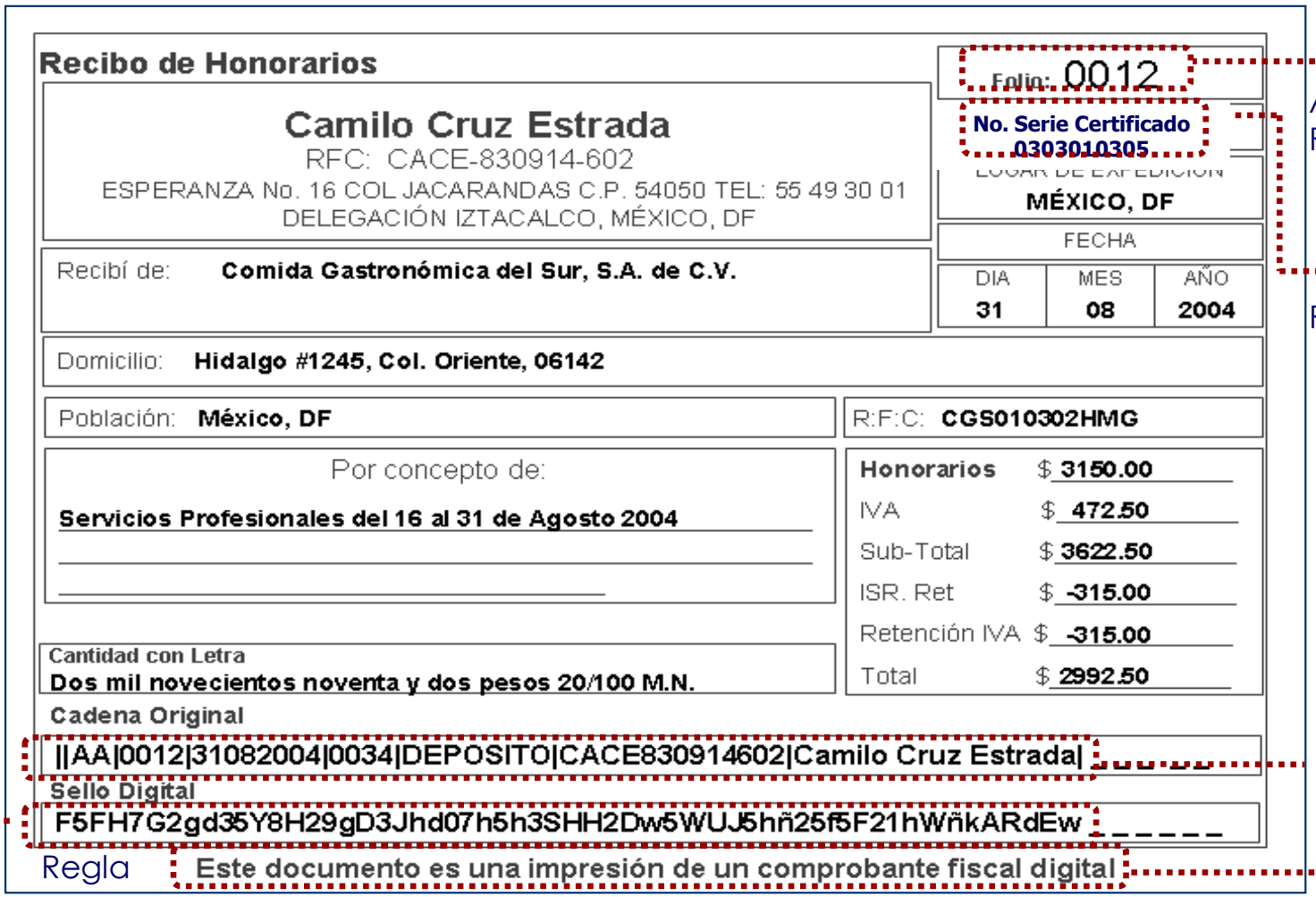
- Generar *.req, *.key y ensobretar *.req convertir a *.dsg
- Enviar por Internet el archivo *.dsg en el programa CertiSAT Web.
- CertiSAT: Revocar, Seguir, Descargar y Solicitar certificados de sello digital

Comprobantes Fiscales Digitales del SAT

Funcionamiento del SAT



Comprobantes Fiscales Digitales del SAT



Recibo de Honorarios

Folio: 0012

Camilo Cruz Estrada
RFC: CACE-830914-602
ESPERANZA No. 16 COL JACARANDAS C.P. 54050 TEL: 55 49 30 01
DELEGACIÓN IZTACALCO, MÉXICO, DF

No. Serie Certificado 0303010305

LUGAR DE EXPEDICIÓN: MÉXICO, DF

Recibí de: **Comida Gastronómica del Sur, S.A. de C.V.**

FECHA

DIA	MES	AÑO
31	08	2004

Domicilio: **Hidalgo #1245, Col. Oriente, 06142**

Población: **México, DF**

R.F.C: **CGS010302HMG**

Por concepto de:

Servicios Profesionales del 16 al 31 de Agosto 2004

Honorarios	$ **3150.00**
IVA	$ **472.50**
Sub-Total	$ **3622.50**
ISR. Ret	$ **-315.00**
Retención IVA	$ **-315.00**
Total	$ **2992.50**

Cantidad con Letra
Dos mil novecientos noventa y dos pesos 20/100 M.N.

Cadena Original

||AA|0012|31082004|0034|DEPOSITO|CACE830914602|Camilo Cruz Estrada|

Sello Digital

F5FH7G2gd35Y8H29gD3Jhd07h5h3SHH2Dw5WUJ5hñ25f5F21hWñkARdEw

Este documento es una impresión de un comprobante fiscal digital

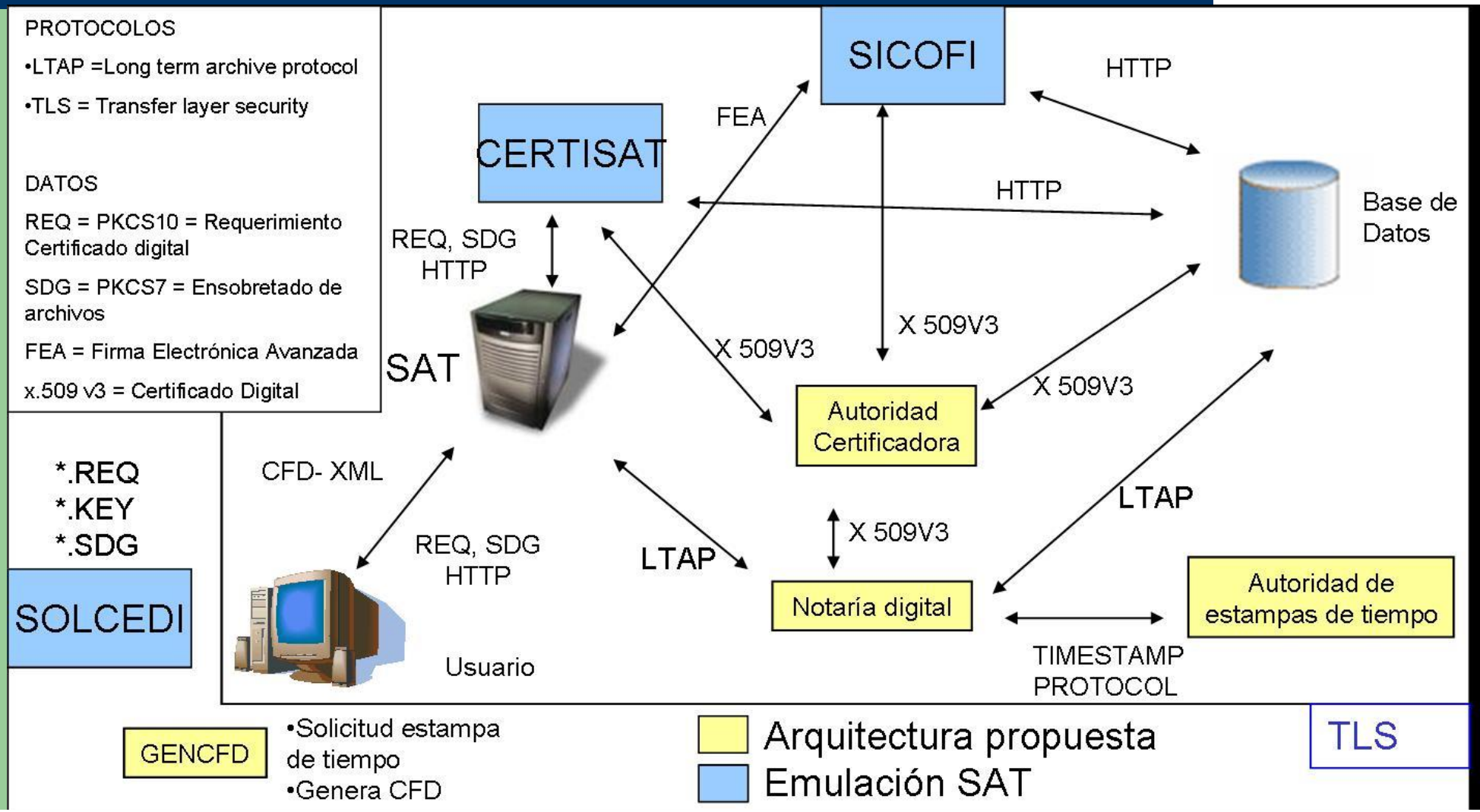
Folio
Art. 29 fracción III, Regla 2.22.8.

Regla 2.22.8.

Regla 2.22.8.

Sello digital
Art. 29 fracción I, 2.22.8.

Regla

Leyenda

Arquitectura integrada con el Sistema del SAT