



Encuentro Sociedad y Tecnologías de la Información

La firma digital y su aplicación en la nueva economía

Expositor

Roberto Opazo Gazmuri
(roberto@opazo.cl)

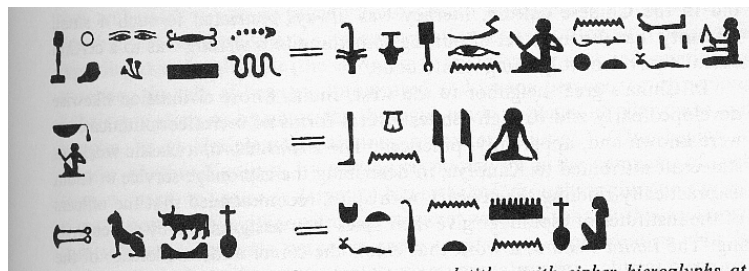
**Profesor del curso “Seguridad de Datos y Firmas Digitales”,
en el DCC de la Universidad de Chile.**

Gerente General de Acepta.com y Custodium.com

Criptografía

La firma digital y su aplicación en la nueva economía

- En 1900 AC, en Egipto, un anónimo escribió en columnas de la tumba de Khnumhotep II usando geroglifos distintos de los habituales un mensaje difícil de leer: “Khnumhotep se levanto en servicio del faraón Amenemhet II”.



Criptografía (Cont...)

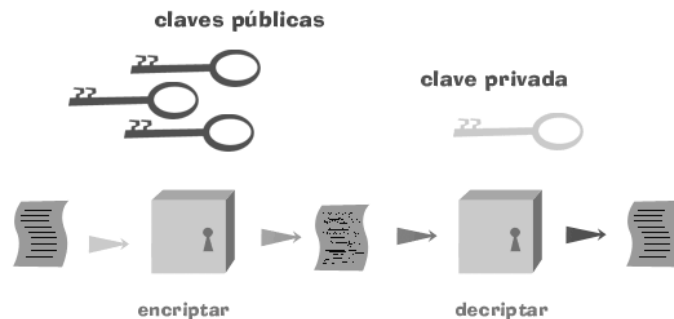
La firma digital y su aplicación en la nueva economía



Encriptamiento asimétrico

La firma digital y su aplicación en la nueva economía

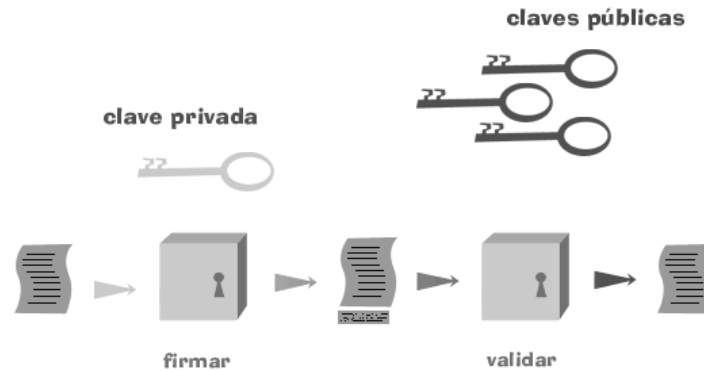
Diagrama de Encriptamiento



Firma Digital

La firma digital y su aplicación en la nueva economía

Diagrama de Firma Digital



Roberto Opazo Gazmuri (roberto@opazo.cl)

5

Qué es una Identidad Digital

La firma digital y su aplicación en la nueva economía

- Una identidad digital es el equivalente al Carné de Identidad
 - Permite firmar digitalmente
 - Cualquier persona puede validar las firmas generadas
 - Nadie puede generar firmas de otra persona
 - Nadie puede modificar lo que otro ha firmado

Roberto Opazo Gazmuri (roberto@opazo.cl)

6

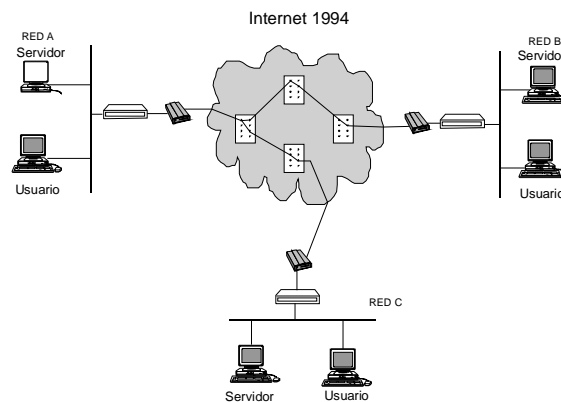
Qué es una Identidad Digital

La firma digital y su aplicación en la nueva economía

- Una identidad digital es el equivalente de Identidad
 - Permite firmar
 - Cuando se firman las firmas generadas
 - No se puede modificar lo que otro ha firmado

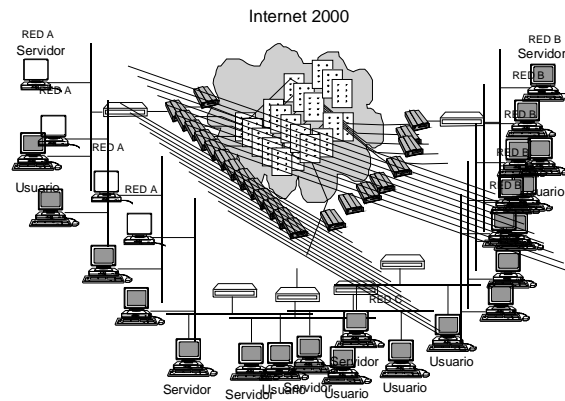
Necesidad

La firma digital y su aplicación en la nueva economía



Necesidad

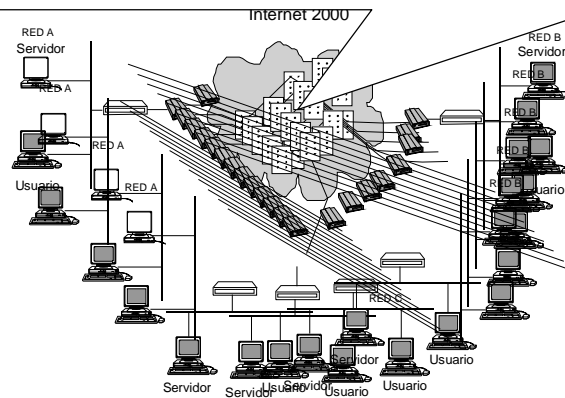
La firma digital y su aplicación en la nueva economía



Roberto Opazo Gazmuri (roberto@opazo.cl)

9

- Los mensajes pueden ser leídos por cualquiera (privacidad).
- Los documentos pueden ser negados por sus autores (repudiabilidad).
- Los usuarios deben recordar nombres de usuario/password para cada sitio (identidad).

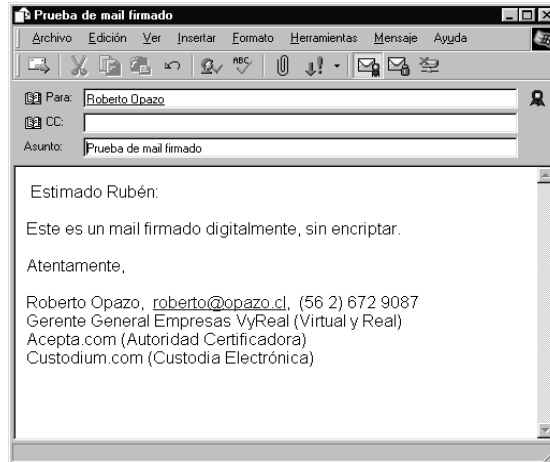


Roberto Opazo Gazmuri (roberto@opazo.cl)

10

Como se usa (Enviar mail firmado 1)

La firma digital y su aplicación en la nueva economía



Roberto Opazo Gazmuri (roberto@opazo.cl)

11

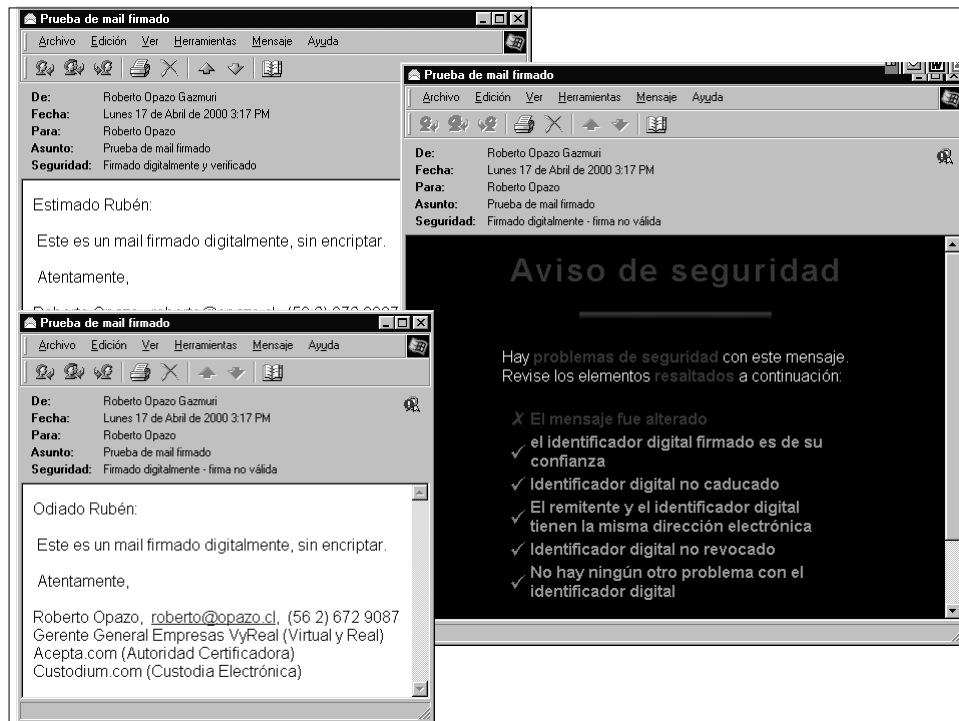
Como se usa (Enviar mail firmado 2)


La firma digital y su aplicación en la nueva economía

[Ver archivo generado](#)

Roberto Opazo Gazmuri (roberto@opazo.cl)

12





Como se usa (Enviar mail encriptado y firmado)

La firma digital y su aplicación en la nueva economía

Prueba de mail firmado y encriptado

Para: Roberto Opazo

CC:

Asunto: Prueba de mail firmado y encriptado

Estimado Rubén:

Este mail está firmado y encriptado.

Atentamente,

Roberto Opazo, roberto@opazo.cl, (56 2) 672 9087
 Gerente General Empresas VyReal (Virtual y Real)
 Acepta.com (Autoridad Certificadora)
 Custodium.com (Custodia Electrónica)

Roberto Opazo Gazmuri (roberto@opazo.cl)

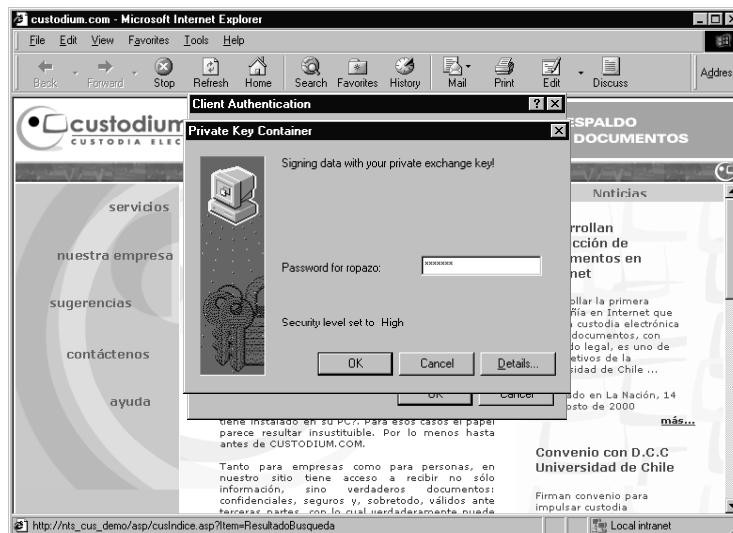
Como se usa (Enviar mail encriptado y firmado 2)

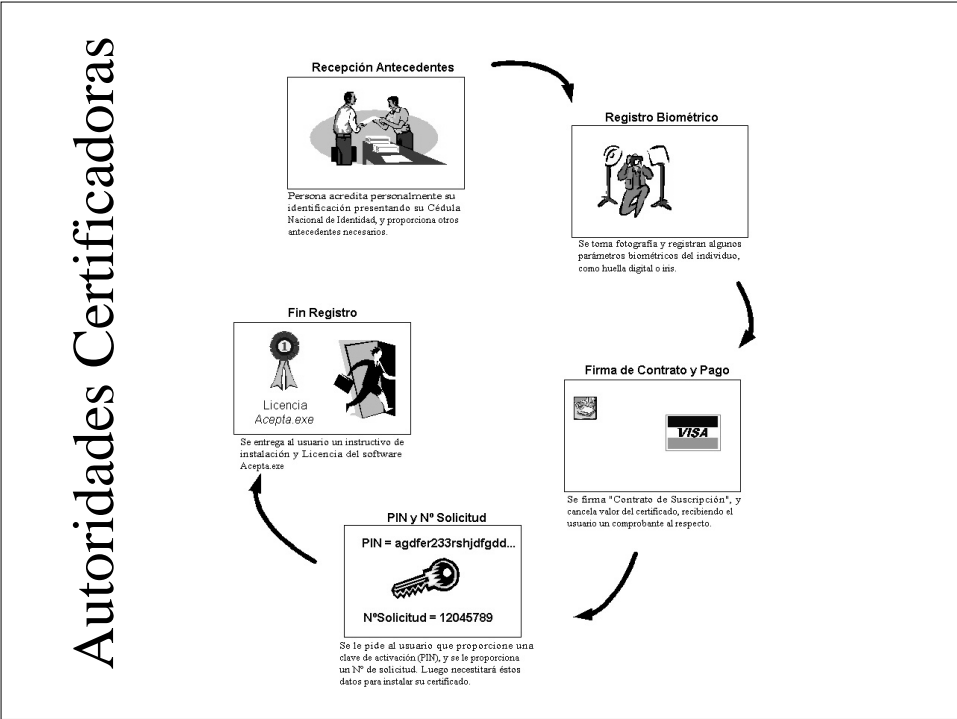
La firma digital y su aplicación en la nueva economía

[Ver archivo generado](#)

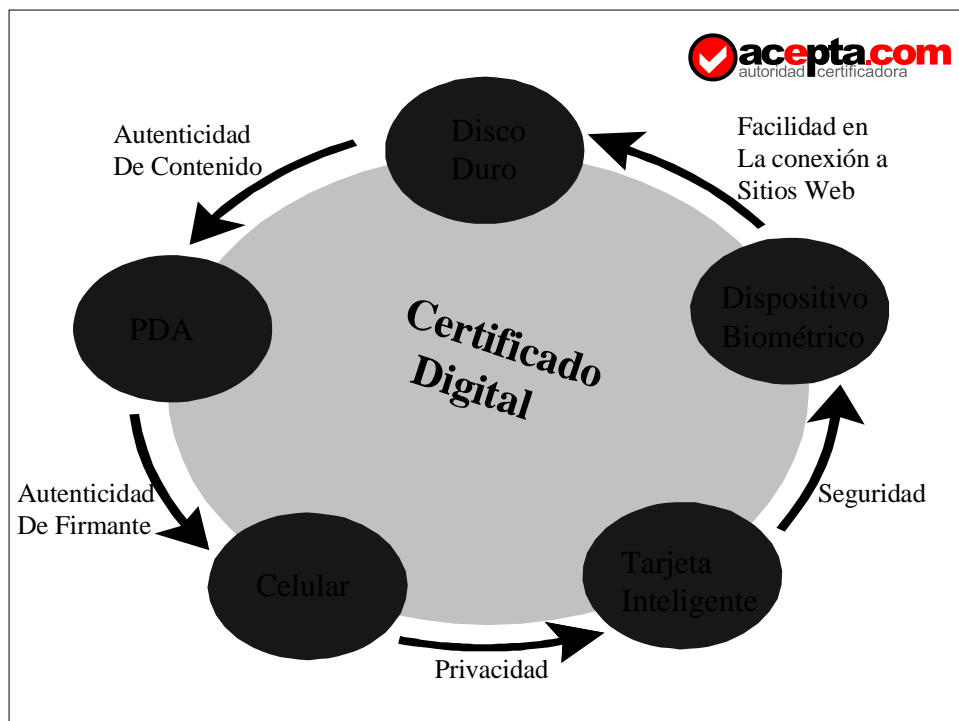
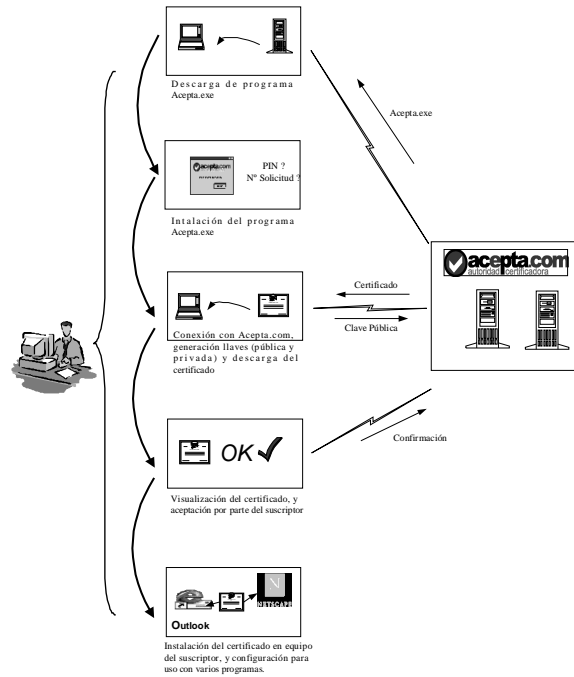
Roberto Opazo Gazmuri (roberto@opazo.cl)

15





Autoridades Certificadoras



Aplicaciones en la Industria

La firma digital y su aplicación en la nueva economía

- Agencia Tributaria Española
 - Declaraciones de impuestos
- Proyecto Identrust
 - Consorcio de Bancos de USA
- Banco de Bermudas
 - Autenticación interna, VPN, firma de documentos
 - Plan para ampliarse a usuarios externos (10.000 usuarios)
- Mackenzie Financial Corporation (USA)
 - Autenticación segura de consultores financieros, para acceso a cuentas y portfolios de inversión, usando certificados digitales.
 - Instauración de su propia AC
 - Red interna

Aplicaciones en la Industria (Cont 1...)

La firma digital y su aplicación en la nueva economía

- New York Life (USA)
 - Empresa de seguros, Uso de certificados para autenticar a agentes y brokers que requieren acceso a información de clientes, Uso de encriptación y e-mail seguro para envío de información confidencial, Emisión de certificados a empleados, Instauración de AC interna
- Royal Mail (UK)
 - Uso de tecnología de seguridad para transmisión segura de documentos, Entidades de negocios autenticadas con certificados digitales
- Chase Manhattan Bank
 - Uso de software de AC interna
 - Uso de PKI para envío seguro de instrucciones de pago y archivos de información a través de Internet

Aplicaciones en la Industria (Cont 2...)

La firma digital y su aplicación en la nueva economía

- ARCO (Alaska)
 - Compañía de exploración de gas en Alaska, Administradores de proyectos usan certificados digitales para enviar instrucciones por correo seguro, Usan AC propia para emitir certificados
- General Electric Corporate Research Center (USA)
 - Usa PKI para distribuir información sensitiva entre contratistas y equipos de proyectos, Certificados digitales para autenticación, AC propia, Comunicación segura a través de Internet le ofrece menor costo.

Aplicaciones en la Industria (Cont 3...)

La firma digital y su aplicación en la nueva economía

- Muchos otros
 - Bechtel BWXT Idaho (USA)
 - TeleCash Kommunikations-Service GmbH (Alemania)
 - AMN AMBRO Bank
 - PTT Post (Netherlands)
 - Kommunedata (KMD)
 - Universal P...
- Recientemente la UIT (Unión Internacional de Telecomunicaciones) aprobó en Ginebra un modelo internacional para asegurar Internet, basado en PKI.
- ...
 - Parlamento de Comercio (USA)
 - US Department of Labor
 - U.S. Department of Veteran Affairs
 - US Postal Service Electronic Change of Address
 - US Department of Education--Free Application for Student Aid
 - ...

Situación en Chile

La firma digital y su aplicación en la nueva economía

- **Poder Legislativo**
 - Proyecto en el senado
 - Proyecto en la cámara baja
- **SII (Proyecto Módulos Internet 2000)**
 - Módulo de autenticación de usuarios con identidad digital en proceso de licitación.
 - La próxima declaración de renta se podrá realizar usando identidad digital.
- **SAFP (Circular N° 1143)**
 - Autoriza y regula el uso de Internet para pagar las Cotizaciones Previsionales y Aportes de Indemnización.
 - Se exige a los intermediarios (Empresas que reciben las cotizaciones) el uso de identidad digital.
 - Es opcional para las empresas el uso de identidad digital.
- **SVS (Circular N° Borrador)**
 - Autoriza y regula el uso de Internet para la venta de seguros.
 - Se exige a los intermediarios (empresas y corredores) el uso de identidad digital.
 - Es opcional para los clientes.

Iniciativas Privadas en Chile

La firma digital y su aplicación en la nueva economía

- **Primeras 3 Autoridades Certificadoras**
 - Acepta.com
 - CNC-ONCE
 - e-CertChile
- **Primera empresa de Custodia Electrónica**
 - Custodium.com

La nueva Nueva Economía

La firma digital y su aplicación en la nueva economía

- **Habilitadores**
 - Autoridades Certificadoras
 - Empresas de Custodia Electrónica
- **Aplicaciones**
 - Eliminación del papel en procesos actuales
 - Comprobantes, facturas, cartolas, cuentas...
 - Contratos
 - Cotización, OC, ...
 - Comercio
 - Farmacia, exámenes clínicos, notaría, contratación de servicios, ...

Conclusiones

La firma digital y su aplicación en la nueva economía

- Se requieren identidades digitales
- Los usuarios ya tienen la tecnología
- Es la dirección mundial
- Es la dirección en Chile
- Esto potencia la nueva economía al cerrar procesos de negocio electrónicos