< Criptografía: la herramienta que garantiza la seguridad máxima en los procesos de banca >

Criptografía

Del griego κρύπτος '(criptos), «**oculto**», y γραφη (grafé), «**escritura**», literalmente «**escritura oculta**»

Hoy: Estudio de los algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad a las comunicaciones, a la información y a las entidades que se comunican.

Tipos de Criptografía

Simétrica

Clave común

Ventaja

Velocidad

Aplicación

- Alto volumen de transacciones en canales seguros

Ej. Verificación de PIN

Asimétrica

Clave Publica y Privada

Ventaja

- Robustez / Seguridad
- Las Claves Privadas nunca se comparten

Aplicación

- Intercambio de claves para crear canales seguros
- Aplicaciones que requieren mayor seguridad en el cifrado

E.j. Firma Digital, Cifrado de Documentos, etc.

Usos Criptografía

- **Comunicaciones Electrónicas**: PPP, SSH, SSL, TLS, IPSec, Kerberos
- **Medios de Pago:** X9.24, ISO 9564, ISO 7816, ISO 14443, and ISO 8583, **EMV**
- **Firma Digital y Cifrado**: x509, GnuPG
- **Otras Aplicaciones:** Correo Electrónico, Cedulas de Identidad, Tarjetas Inteligentes
- Y muchas mas!

Criptografía y Medios de Pago

EMV o Tarjetas Microcircuito

EMV es un estándar de interoperabilidad de tarjetas microcircuito y TPV, para la autentificación de pagos mediante tarjetas de crédito y débito.

1996 EMV: **E**uropay, **M**astercard y **V**isa.

2015 EMV 4.3: American Express, Discover, JCB, MasterCard, UnionPay, and Visa

Organos Reguladores

- **EMVCo**
  - http://www.emvco.com/

- **PCI DSS**
  - https://www.pcisecuritystandards.org/security_standards/

- **SmartCard Alliance**
  - http://www.smartcardalliance.org/

Tecnología Requerida

HSM – Hardware Security Module

Dispositivos Físicos Criptográficos utilizados para la generación, almacenaje y gestión de claves y certificados.

Deben cumplir estrictas normativas internacionales:

- NIST (US National Institute of Standard & Technology)
  - **FIPS 140-2 Nivel 3** o Superior
- Common Criteria
  - **EAL4+** o Superior
- PCI Security Standards Council
  - **PCI HSM**

A quien Afecta?

- **Emisores de Tarjetas → HSM para Personalización**
  - Petición y gestión de Certificados/claves de las marcas
  - Emisión de Tarjetas
- **Procesadores de Transacciones → HSM Bancario**
  - Gestión de transacciones EMV
- **Redes de Cajeros / ATMs → HSM para Carga de Claves**
  - Solicitud y gestión de certificados/Claves a Fabricantes de Cajeros
  - Inyección / Renovación de Certificados de los Cajeros
  - Carga Remota de Claves
- **Comercios con TPVs y Dispensadores de Gasolina → HSM para Carga de Claves**
  - Inyección / Renovación de Certificados de los ATMs
  - Carga Remota de Claves

"Todos los actores están obligados garantizar por su parte la seguridad de las transacciones/operaciones que involucren tarjetas EMV"

EMV – Seguridad
Donde requiere cifrado?

- **Tarjetas**:
  - Generar Ficheros de Personalización
  - Grabado de información en microcircuitos
  - Generación/Cambio de PIN
  - Transacciones (ARQC, ARPC, AAC, TC)
  - …
- **ATMs / Cajeros / TPVs:**
  - Inyectar las claves maestras
  - Transacciones
  - …

EMV – Pros & Cons

Pros

- Reduce prácticamente a **cero** el fraude en transacciones donde la tarjeta esta presente
- Actualmente es imposible duplicar una tarjeta EMV
- Permite nuevas aplicaciones de las tarjetas bancarias

Cons

- Elevado coste de la migración tecnológica
- El fraude **online** y el relacionado con operaciones donde la **tarjeta no esta presente** aumenta

EMV Hace posible

Google wallet

Visa payWave

Pay

MasterCard paypass™

Square

Infraestructura de Seguridad

Con el fin de luchar contra otros tipos de fraude las empresas deben implantar:

- Políticas de **Seguridad física** (ej. Perimetral) y **lógica** (BOYD – Bring your own device)
- Mecanismos para el **Cifrado**, **Firma** y **Verificación** de Documentos
- Instrumentos para la correcta **Identificación** y **Autenticación** de usuarios y roles

Infraestructura de Clave Publica

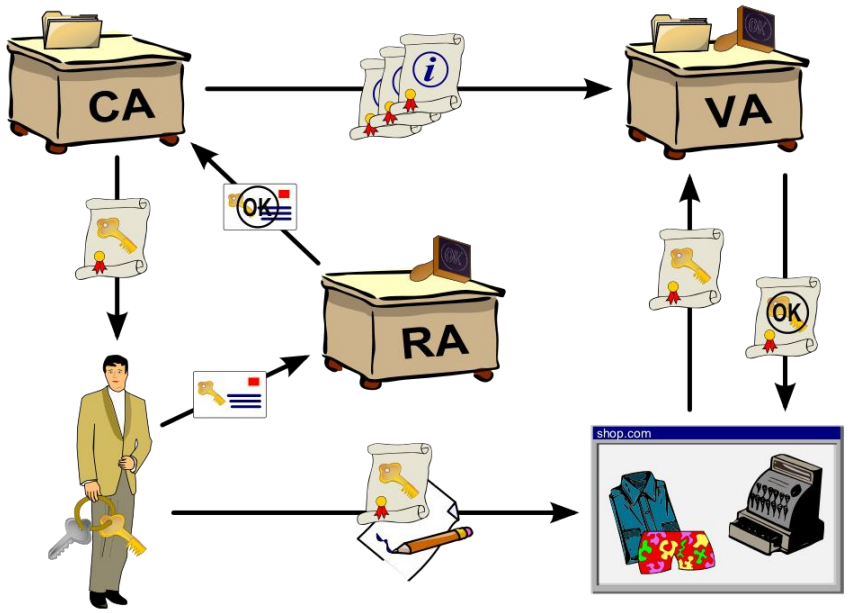
PKI es una combinación de **hardware** y **software**, **políticas** y **procedimientos** de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital.

Habilita la garantía de 3 principios de la información:

- Integridad
- No repudio
- Confidencialidad

Una completa PKI se compone de:

- Autoridad de Certificación
- Autoridad de Registro
- Autoridad de Verificación
- Autoridad de Sellado de Tiempo

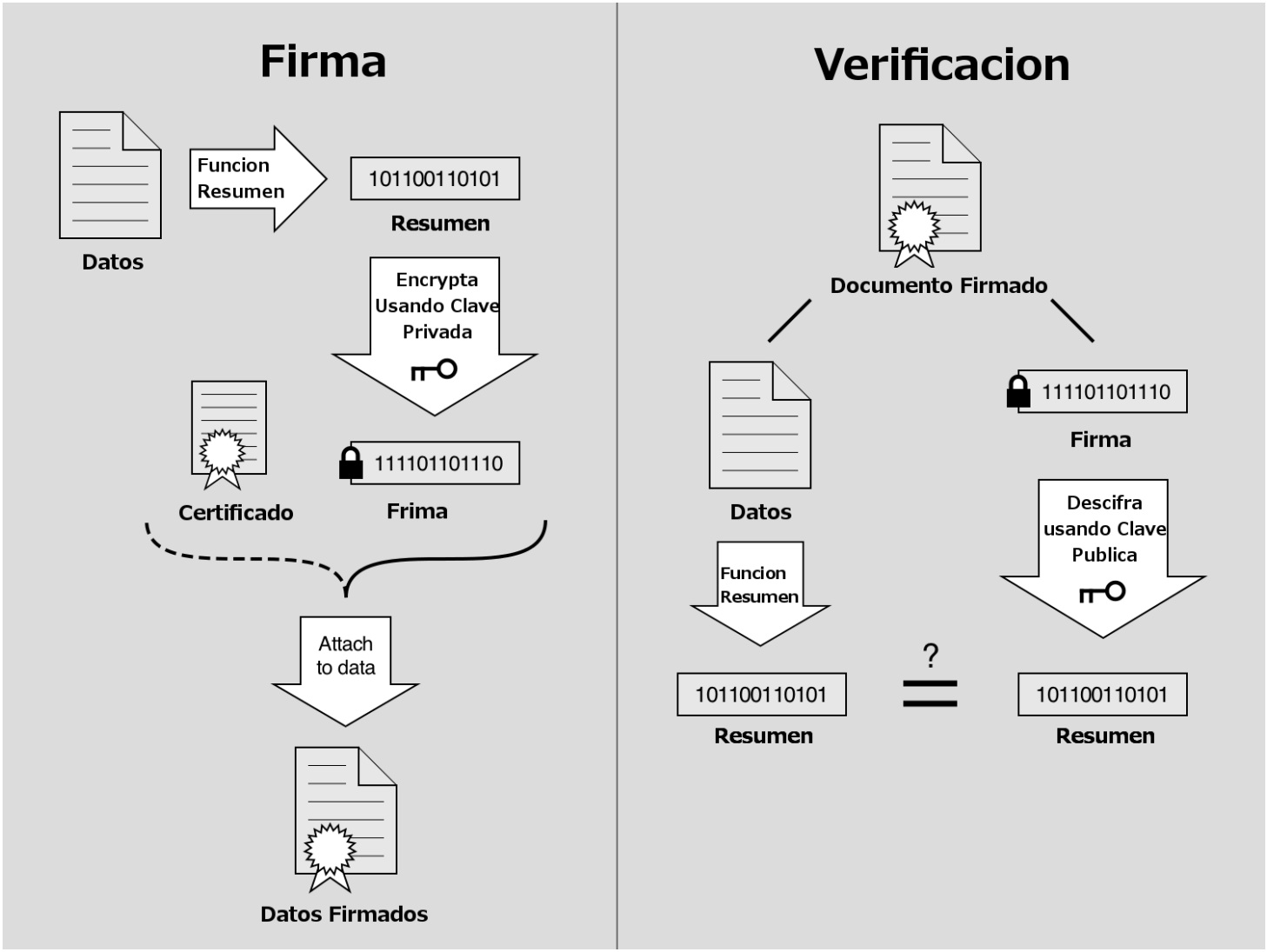


Firma Digital

Mecanismo criptográfico que permite verificar el de origen de un mensaje (**no repudio**), y confirmar que el mensaje no ha sido alterado desde que fue firmado (**integridad**).

La firma digital se aplica en aquellas áreas donde es importante poder verificar la autenticidad y la integridad de ciertos datos, por ejemplo documentos electrónicos o software, ya que proporciona una herramienta para detectar la falsificación y la manipulación del contenido

Firma Digital



realsec
The key to protect your business

Gracias

Sebastian Munoz
smunoz@realsec.com