Transacciones electrónicas seguras

17/09/2014

Américo Alonso, CISSP, CIS

Gerente de Proyectos
Consultor en Seguridad BULL LATAM

About…

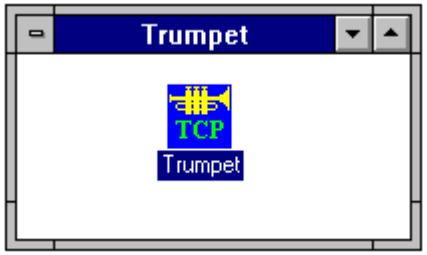
- Seguridad de la Información (CISSP, CIS, S+)
- Gestión (ITIL, COBIT, PMI)
- Cumplimiento(PCI, ISO27k)
- Infraestructura (Unicenter, Spectrum, Nagios, Zabbix, SCOM)

Agenda

1. Cómo llegamos aquí?
2. Desafíos y objetivos
3. PKI – Infraestructura de Clave Pública
4. Plataformas de Servicios de Confianza
5. HSM – Hardware Security Module
6. Preguntas

Cómo llegamos aquí?

Érase una vez…



ATDT09091234

Hasta que…

TIME Subscribe

MENU

ALL CONTENT | MAGAZINE | VIDEOS

Data Security

Nearly 5 Million Google Pas… Leaked on Russian Site

Home Depot Confirms Credit… Hack

Data Security

TECH CYBERSECURITY

Nearly 5 Million Google Passwords

Average Internet of Things device has 25 security flaws

In a study of ten devices including home thermostats, remote power outlets and door locks, HP found 250 potentially dangerous security vulnerabilities

Hackers To… Wallets

It was a cyber… Eastern Europ… major U.S. ret… deep into corp… what they had… Entering thro… Target's syste… and motion de…

nks and … But the …anks and … billion bill. …rld, have …gh Europe.

…r de

de liderar …

Your Debit …

…0.000

Citibank this … accounts were… with the same magnetic stripe technology is like lockbox with another padlock after someone just… battle and one the reasons why the U.S. retail in… it catches up with the rest of the world. [Time]

Extorsionaba a la compañía del sector informático exigiéndole 2.500 euros por no vender una base de datos con DNI, contraseñas y datos de empleados, colaboradores y distribuidores. La Policía lo ha detenido en Asturias

La pregunta no es “SÍ”, sino “CUÁNDO”

Desafíos y Objetivos

Desafíos

- Proveer un acceso seguro a los clientes que utilizan los servicios es un problema complejo. Los controles de seguridad suponen a menudo un impacto en el cliente que puede afectar al negocio (positiva o negativamente).

- El número de aplicaciones y usuarios se incrementa y la información de identidad y acceso a las mismas no tiene porque ser uniforme, la gestión se torna realmente complicada.

- Los mecanismos de autenticación son diversos (login/password, OTP, certificados, etc) y deben ser gestionados adecuadamente de forma transparente a las aplicaciones de negocio.

- La adquisición a terceros de certificados digitales implica un costo que debe ser asumido o trasladado al cliente final.

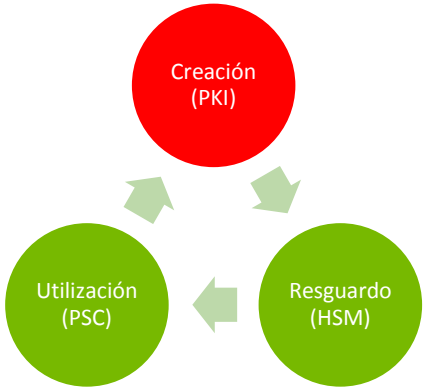
Objetivos

- Incluir seguridad, bajo la forma de integridad y no repudio, en aplicaciones que no la tienen
- Independencia tecnológica
- Operar con dominios de seguridad distintos
- Sin replicación de identidades
- Adecuación a regulaciones
  - “Se reconoce la admisibilidad, validez y eficacia jurídica del Documento Electrónico y Firma Electrónica…” (Ley 18.600)

Habilitadores

- Criptografía de Clave Pública (asimétrica)
  - Habilita doble factor de AuthN
  - Habilita “2-men-control” (N de M – generación de par de claves)
  - Habilita AuthN mutua (SSL Handshake)

PKI – Infraestructura de Clave Pública

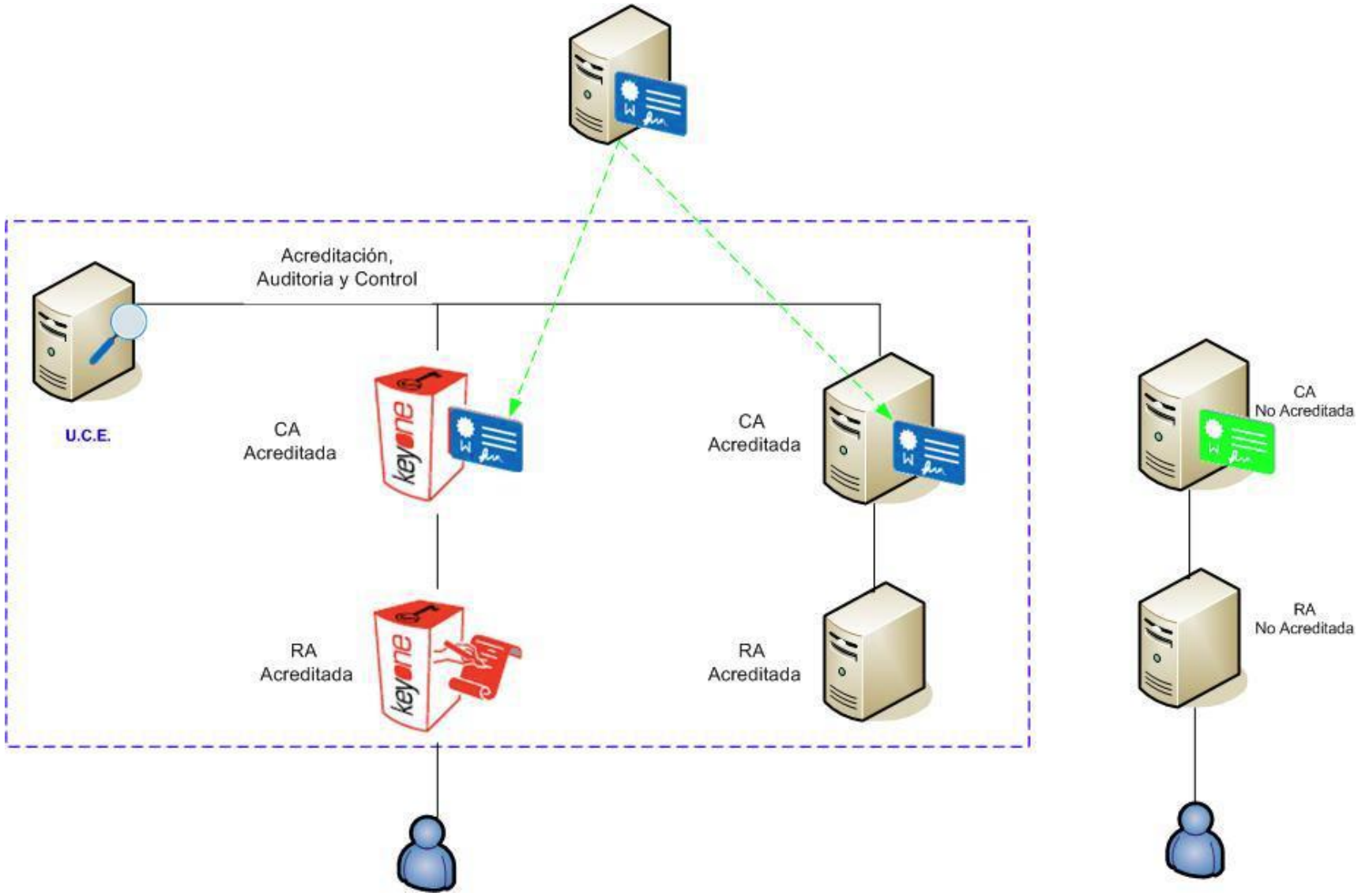


PKI – Infraestructura de Clave Pública

En criptografía, una infraestructura de clave pública (o, en inglés, PKI, Public Key Infrastructure) 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 o el no repudio de transacciones electrónicas.

Fuente: wikipedia

PKI Uruguay

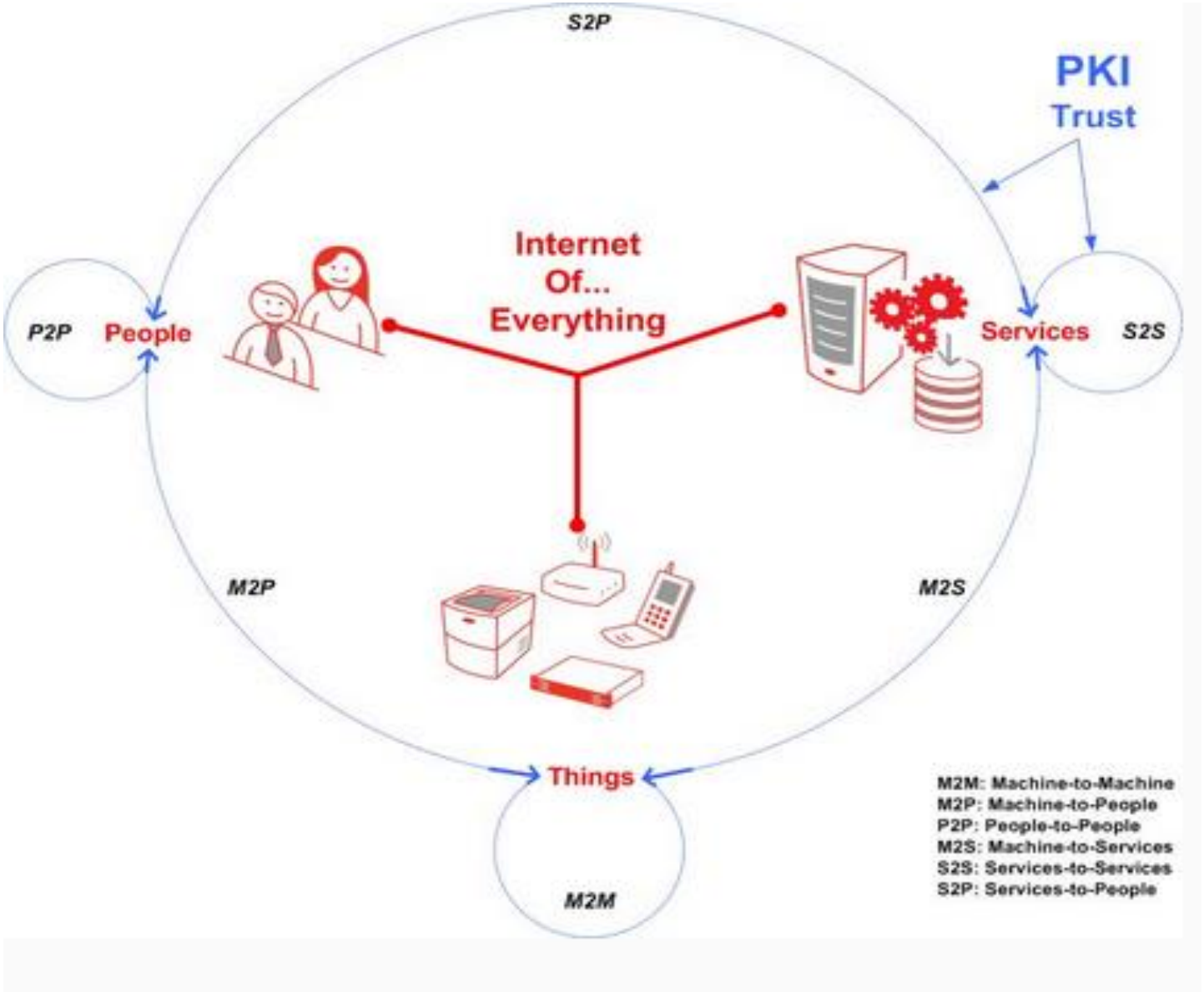


PKI – Usos de la tecnología

- Autenticación de usuarios y sistemas (*login*)
- Identificación del interlocutor
- Cifrado de datos digitales
- Firmado digital de datos (documentos, software, etc.)
- Asegurar las comunicaciones
- Garantía de no repudio (negar que cierta transacción tuvo lugar)

Fuente: wikipedia

IoT (Internet of Things) / IoE (Internet of Everything)



PKI – KeyOne

- Familia de productos KeyOne incluye los componentes necesarios para el despliegue de servicios avanzados de certificación electrónica:
  - Autoridad de Certificación (CA)
    - ITU-T X.509v3 - Sistema de gestión de certificados digitales
    - ICAO/EAC – Extensiones para pasaporte electrónico
  - Autoridad de Registro (RA)
  - Autoridad de Validación (VA)
    - IETF OCSP - Sistema de validación de certificados
  - Autoridad de Sellado de Tiempo (TSA)
    - IETF TSP - Sistema de sellado de tiempo

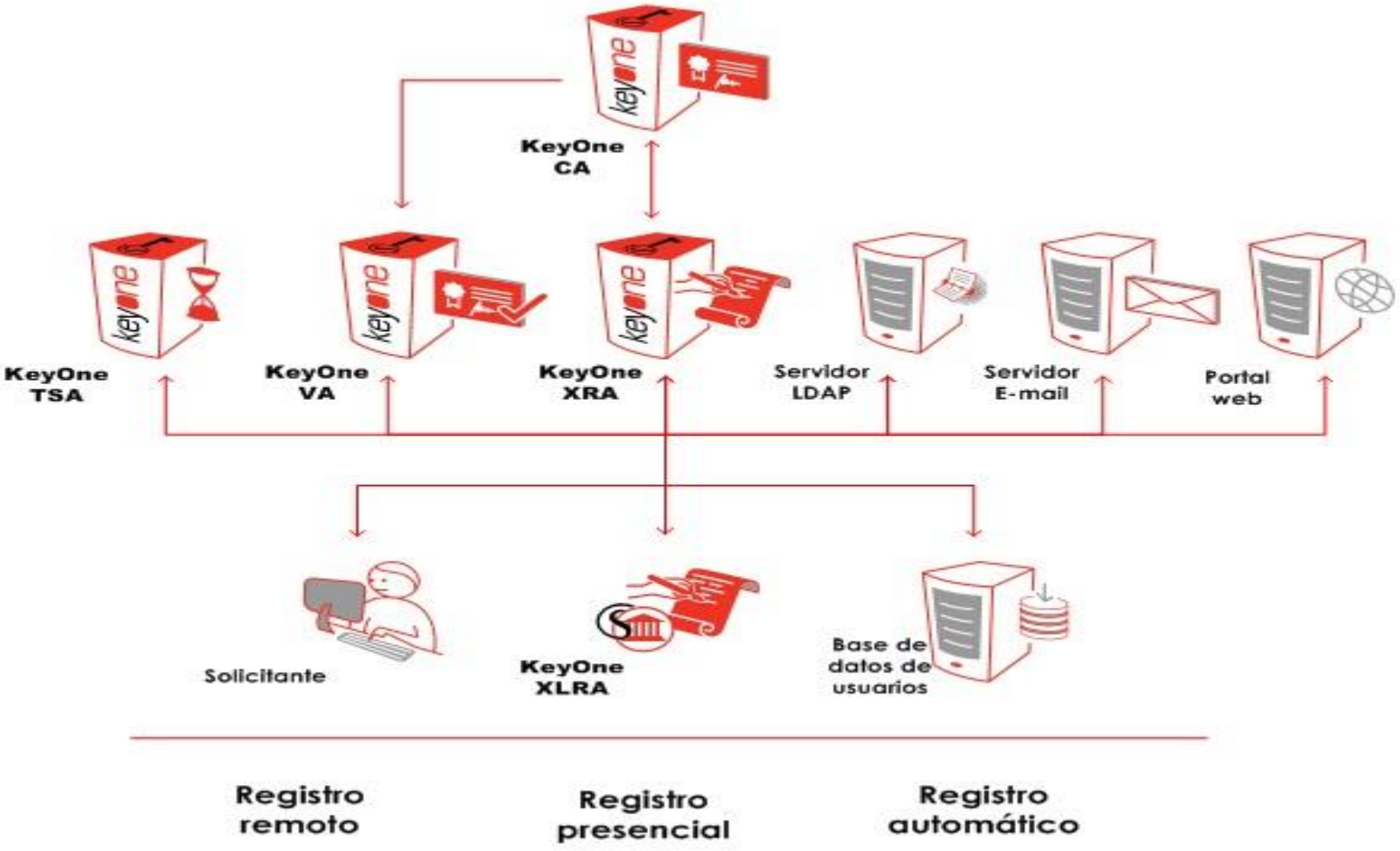
KeyOne

- Mayor seguridad y control:
  - Certificado según la norma Common Criteria con nivel EAL4+ bajo el Perfil de Protección CIMC de nivel de seguridad 3 (gama completa de productos) (*)
  - KeyOne se ha diseñado para facilitar el cumplimiento de los requisitos CWA 14167-1 para Sistemas Confiables de Gestión de Certificados Digitales y Firma Electrónica
  - Único producto PKI en proceso de aprobación NATO por SECAN (**)
  - Soporte completo de algoritmos criptográficos (RSA, DSA, EC-DSA, AES256, SHA-2, etc.)

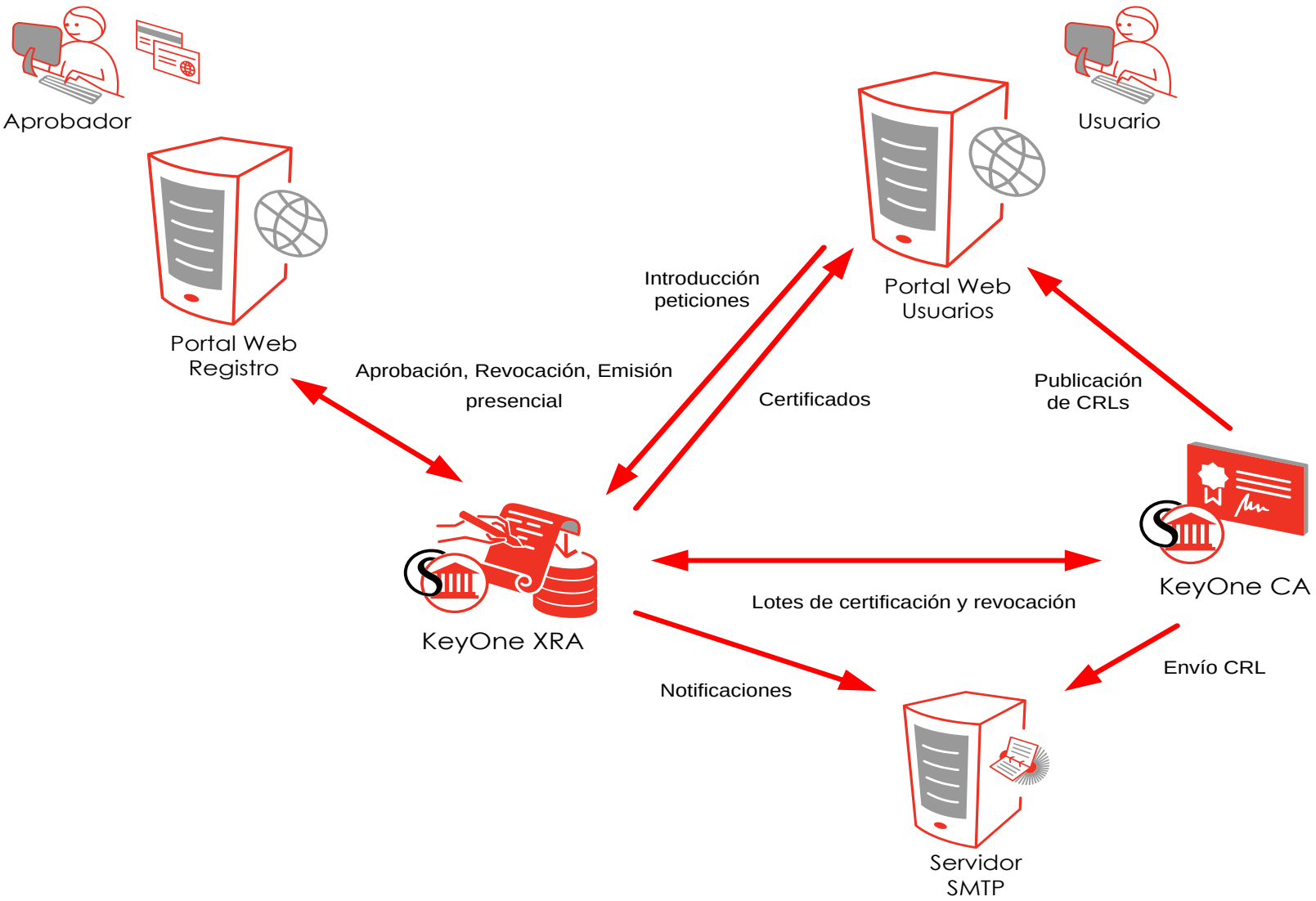
(*) Nivel de garantía ISO/IEC 15408 EAL4+ (ALC_FLR.2) www.oc.ccn.cni.es/certificacion_es.html y conforme al Perfil de Protección CIMC Security Level 3 (Certificate Issuing and Management Component, NIST, 31 de Octubre de 2001).

(**) Military Committee Communications and Information Systems Security and Evaluation Agency (NATO)

Topología PKI (basada en KeyOne)



Implementación

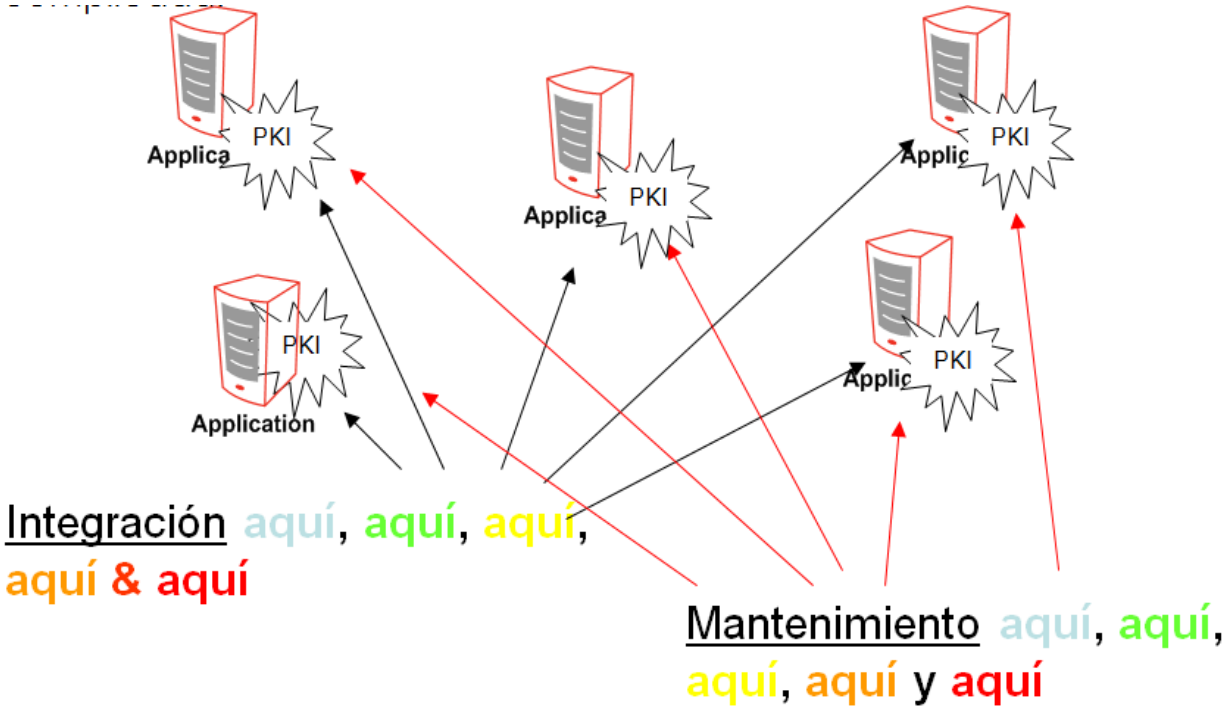


Plataformas de Servicios de Confianza

an atos company

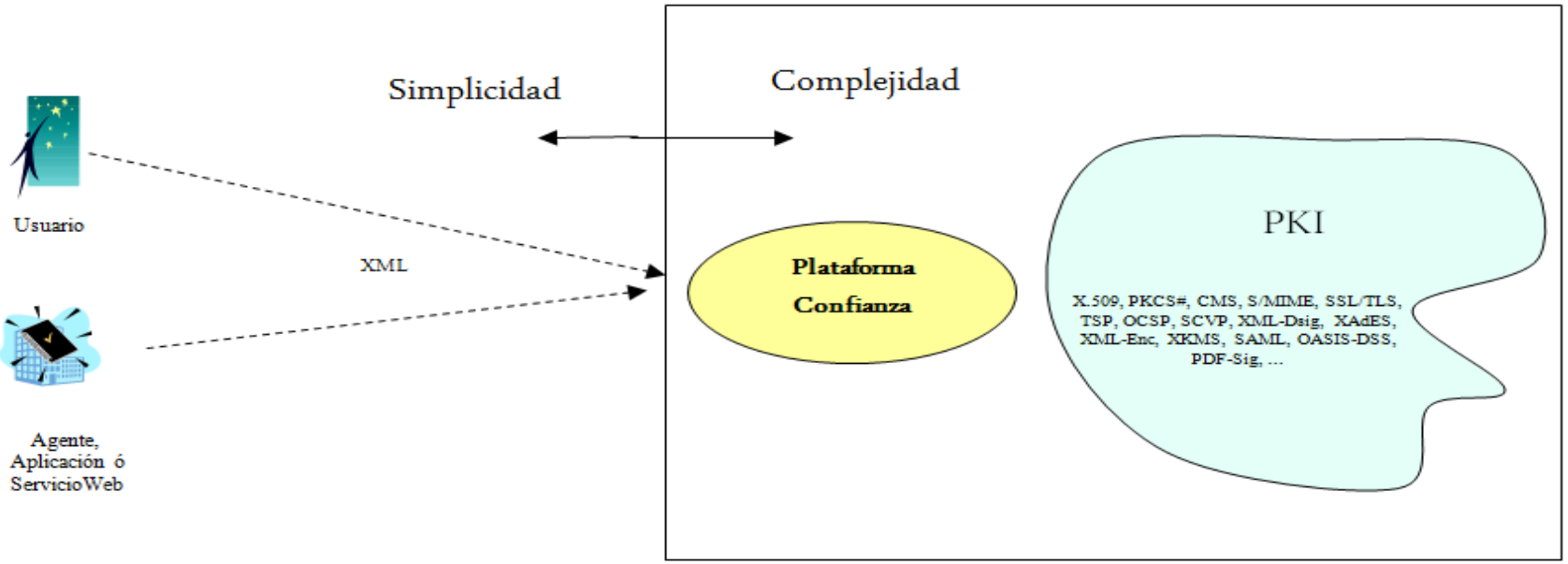
Desafíos

- La integración de mecanismos de seguridad puede resultar compleja.
- A su vez, la gestión de la interoperabilidad entre diferentes sistemas también es complicada.



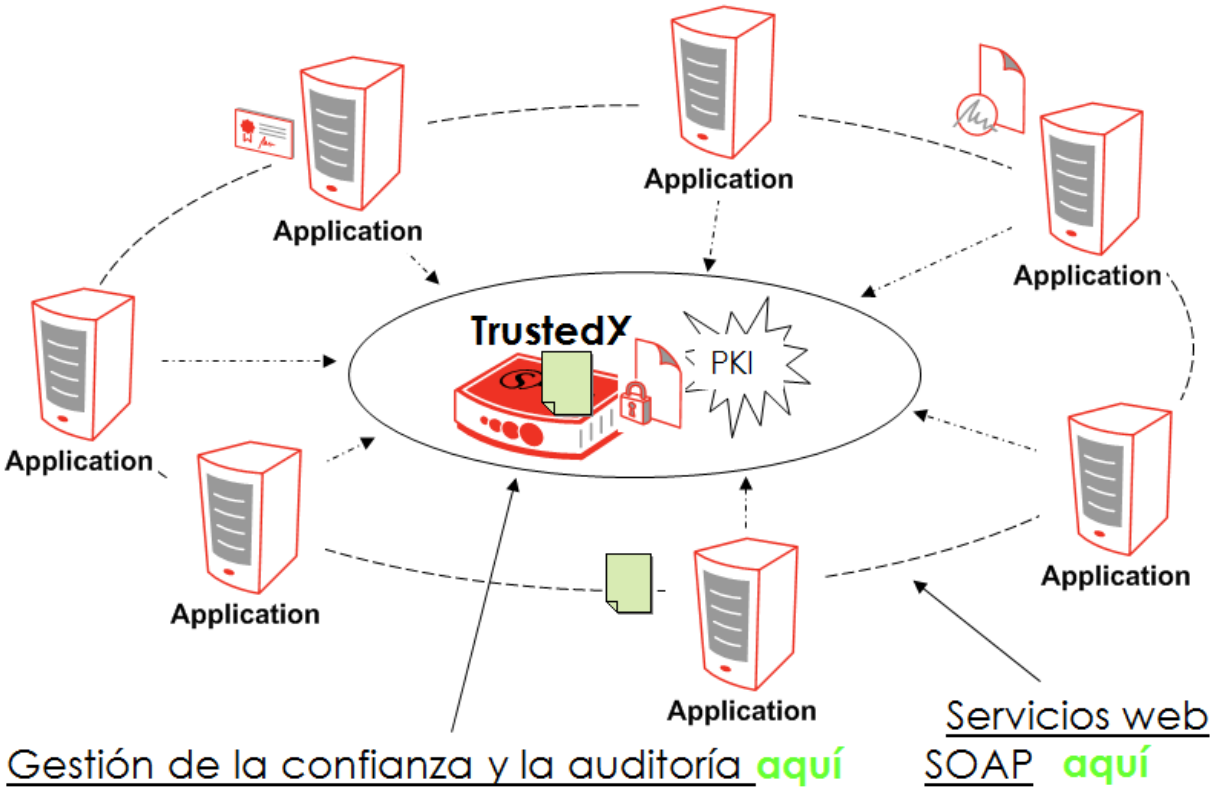
Objetivos

- Plataforma común que ofrece un conjunto completo de servicios de
  - Firma electrónica y protección de datos
  - Autenticación y control de acceso único
  - Gestión uniforme y centralizada de la información y su auditoria



TrustedX

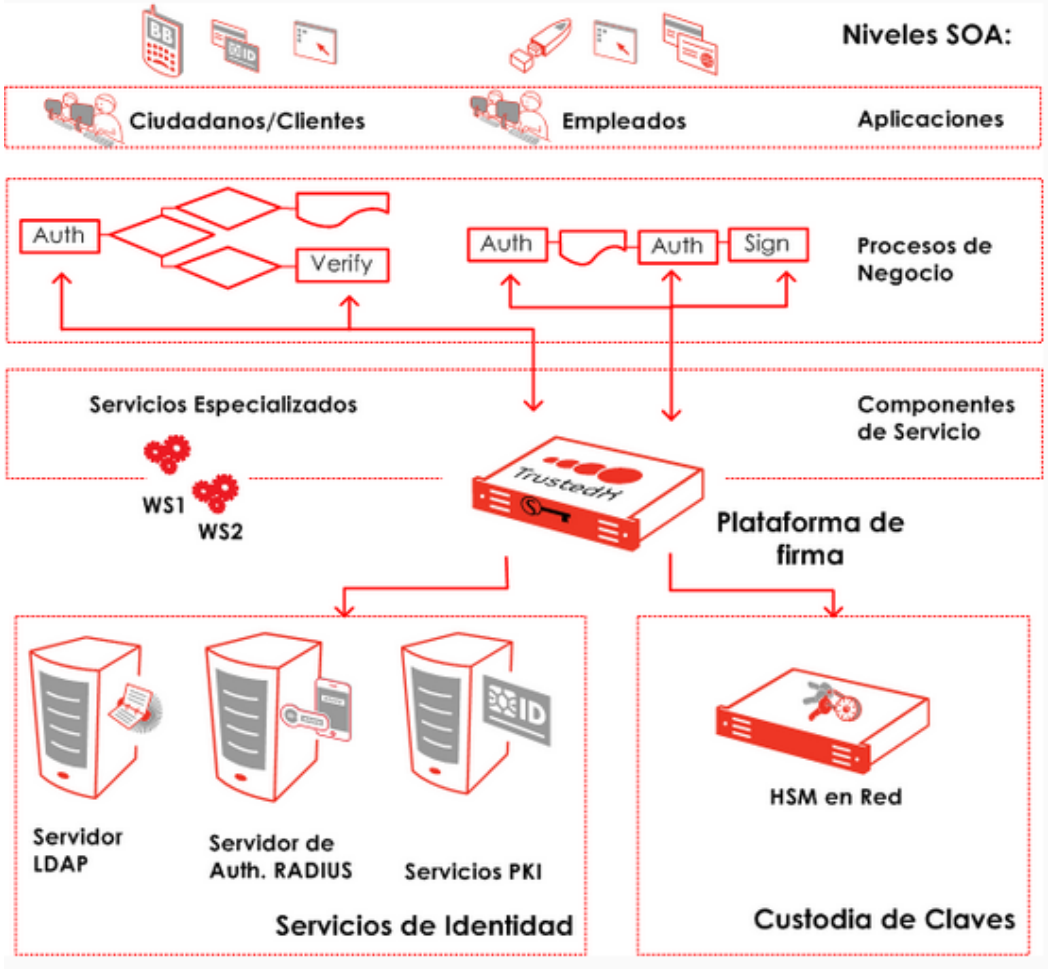
- Mecanismos de autenticación, federación y SSO adaptativos
- Generación de firmas electrónicas en diferentes formatos según los requerimientos de cada aplicación.
- Servicios de validación de firmas y certificados, utilizando los mecanismos ofrecidos por terceros o por otros componentes de la solución (KeyOne VA)



Caso de uso – firma electrónica

TrustedX Electronic Signature

- Firma electrónica de usuario del lado cliente
- Firma electrónica de usuario del lado servidor
- Firma electrónica corporativa del lado servidor



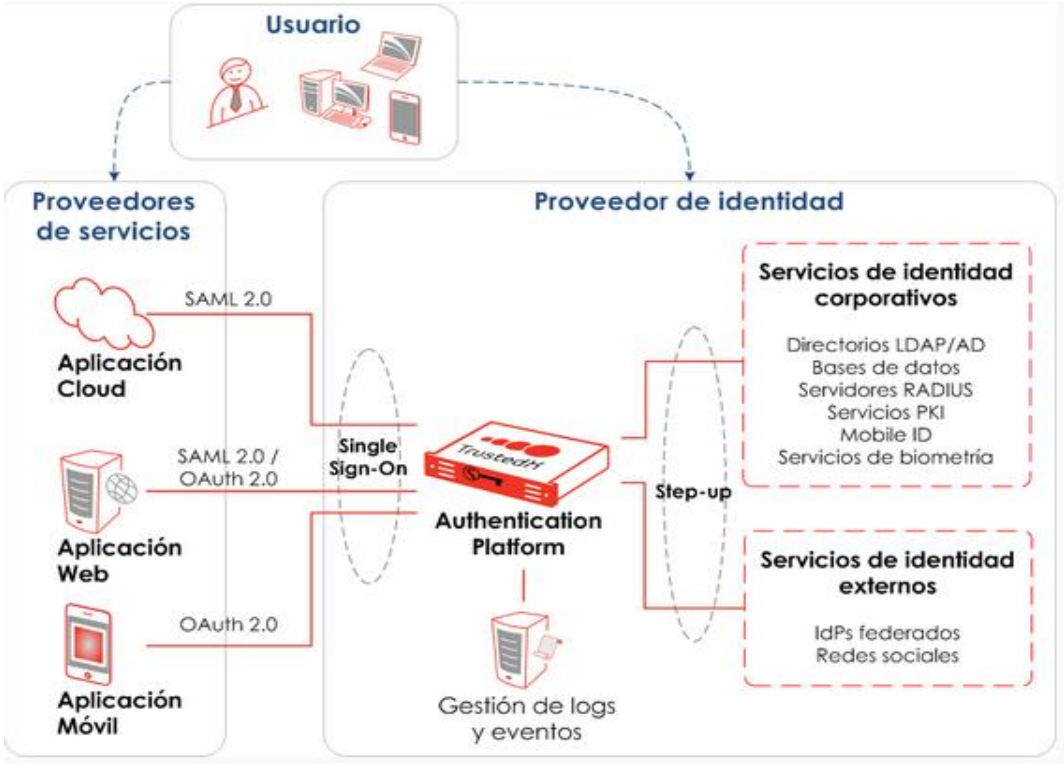
Caso de uso – Factura electrónica

- Automatización de la creación y verificación de facturas
- Creación y validación de firmas
  - PKCS#7/CMS, CAdES, PDF Signature, PAdES, XML-Dsig y XAdES para documentos
  - S/MIME para mensajería electrónica
  - WS-Security para la securización de los mensajes SOAP

Caso de uso – AuthN

TrustedX Authentication Platform

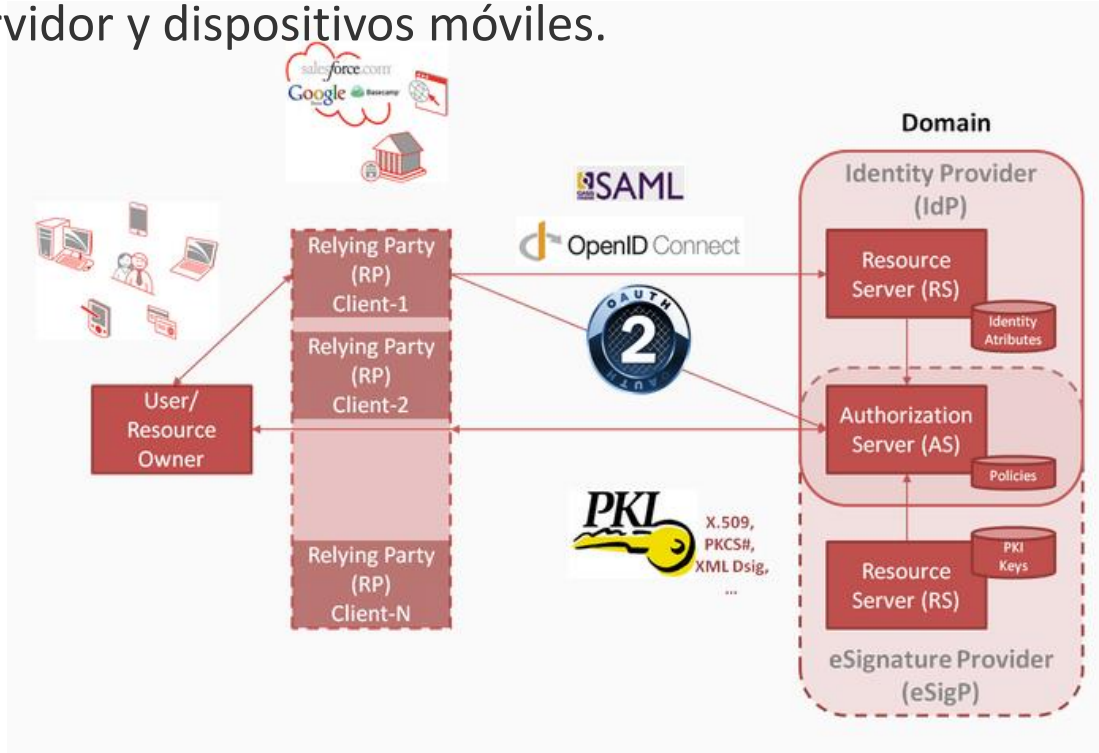
- Servidor de Autenticación Adaptativa para entornos Web y Cloud
  - Soporta varios mecanismos de autenticación
  - Autenticación acumulativa. Evalúa el nivel de confianza de la autenticación y lo eleva cuando la aplicación lo requiere
  - Análisis de información contextual. Mejora la seguridad de la autenticación sin alterar la experiencia del usuario



Caso de uso – Identificación, AuthN y firma

TrustedX eIDAS Platform

- Plataforma de identificación, autenticación y firma electrónica para entornos Web.
  - Autenticación, inicio de sesión único (SSO) y federación de identidades.
  - Servicios de firma en servidor y dispositivos móviles.



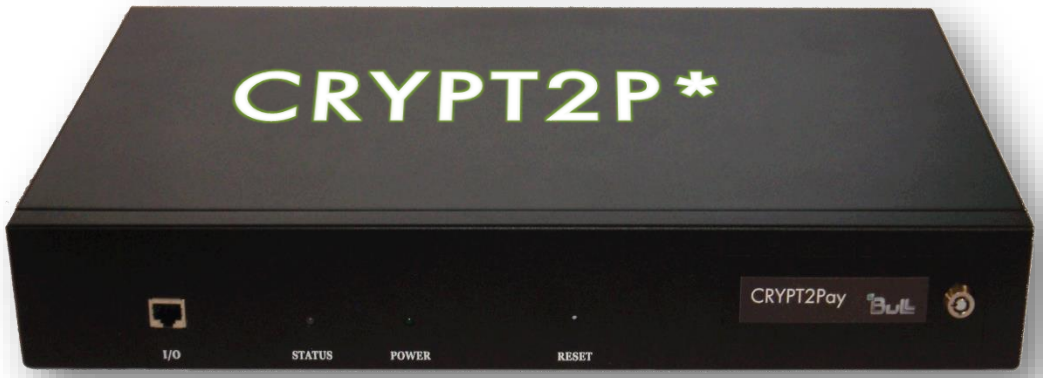
HSM – Hardware Security Module

Definición

Un HSM es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas y suele aportar aceleración hardware para operaciones criptográficas. Estos dispositivos pueden tener conectividad SCSI / IP u otras y aportar funcionalidad criptográfica de clave pública (PKI) de alto rendimiento que se efectúa dentro del propio hardware.

Fuente: wikipedia

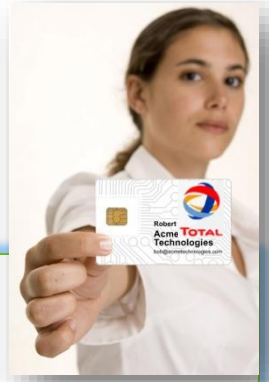
HSM – Hardware Security Module



iti

MEPS2

PCI Security Standards Council ™



CRYPT2Pay

HSM multipropósito para la gestión de tarjetas (banking, loyalty, identity)

CRYPT2Protect

HSM multipropósito
Ofrece funciones adicionales PKCS#11 y funciones de gestión de claves

Solución de gestión de claves

Seguridad y performance

Zeroización de clave secreta

Seguridad:

- Detección de apertura o degradación
- Sensor de movimiento / inclinación
- A prueba de temperatura
- Filme inalterable Molex
- Sensor de voltaje.
- Firmware firmado

Upgrade dinámico

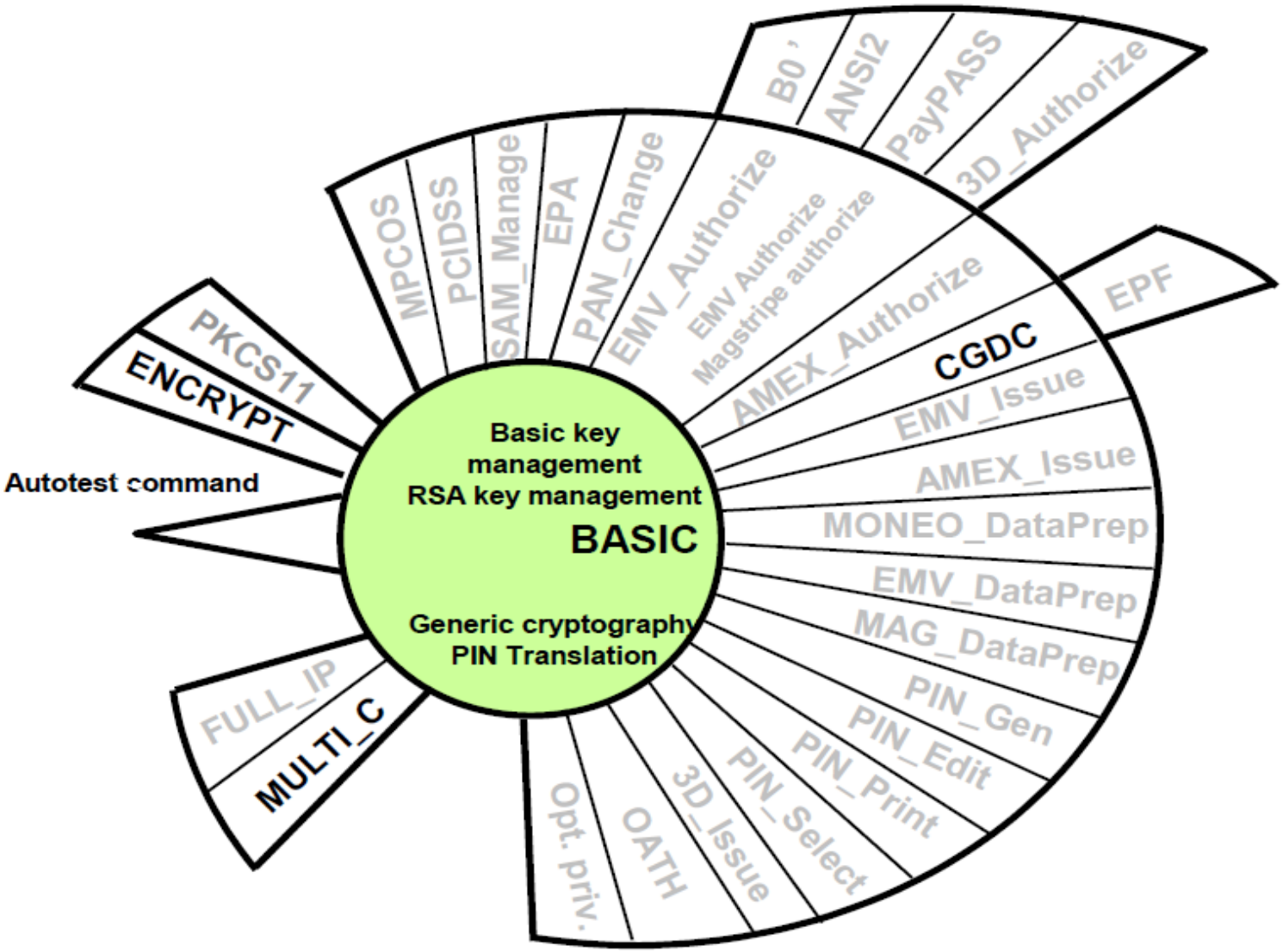
Performance (RSA2048):

- Modelo HR300 (30 fps)
- Modelo HR1000 (100 fps)
- Modelo HR1600 (400 fps)

El HSM multipropósito de BULL

3DES,
AES,
HMAC,
RSA,
ECC.

HSM Multiproposito



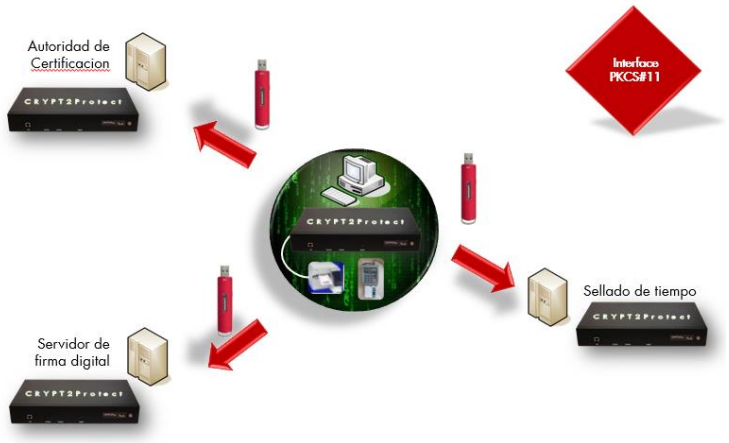
Sabia que…

la tecnología CRYPT2pay de BULL es utilizada por el 95% de los bancos Franceses, y por un gran número de los mayores bancos Europeos para sus transacciones.

HSM – Casos de Uso

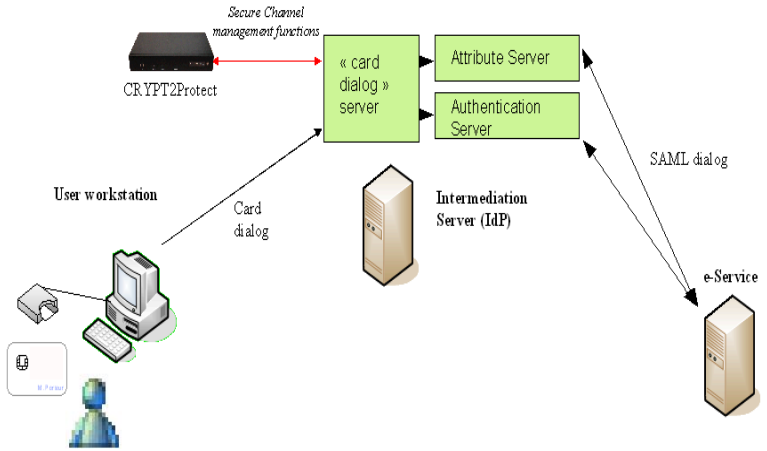
Casos de uso

- PKI
- Soluciones eGov
- Banca electrónica
- Cadenas de personalización
- eBussines
- AuthN de tarjetahabiente
- Sistemas de gestión de tarjetas
- Soluciones de cambio de PIN



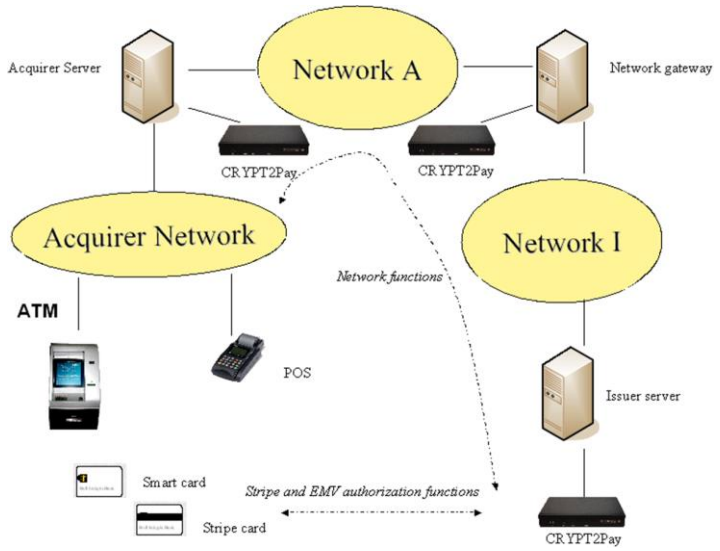
Casos de uso

- PKI
- Soluciones eGov
- Banca electrónica
- Cadenas de personalización
- eBussines
- AuthN de tarjetahabiente
- Sistemas de gestión de tarjetas
- Soluciones de cambio de PIN



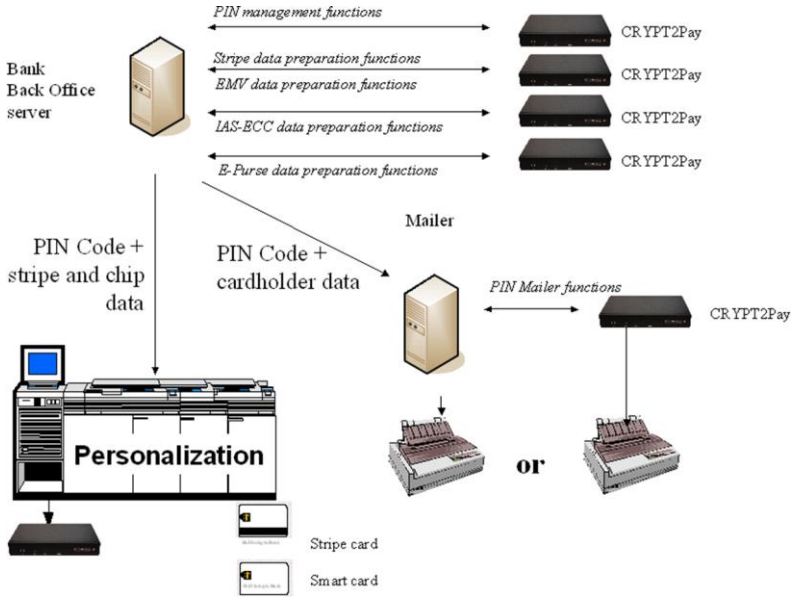
Casos de uso

- PKI
- Soluciones eGov
- Banca electrónica
- Cadenas de personalización
- eBussines
- AuthN de tarjetahabiente
- Sistemas de gestión de tarjetas
- Soluciones de cambio de PIN



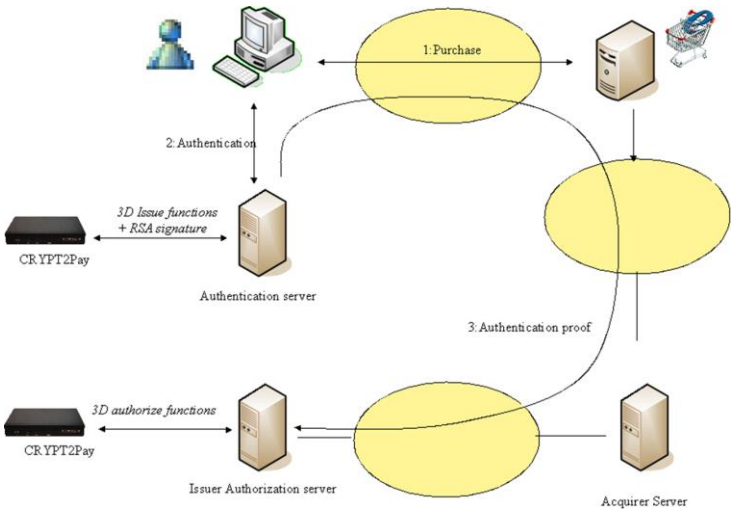
Casos de uso

- PKI
- Soluciones eGov
- Banca electrónica
- Cadenas de personalización
- eBussines
- AuthN de tarjetahabiente
- Sistemas de gestión de tarjetas
- Soluciones de cambio de PIN



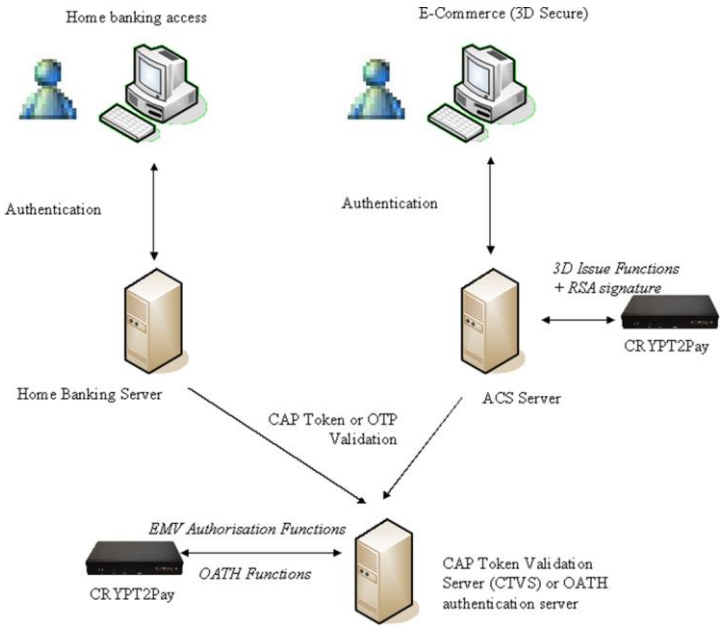
Casos de uso

- PKI
- Soluciones eGov
- Banca electrónica
- Cadenas de personalización
- eBussines
- AuthN de tarjetahabiente
- Sistemas de gestión de tarjetas
- Soluciones de cambio de PIN



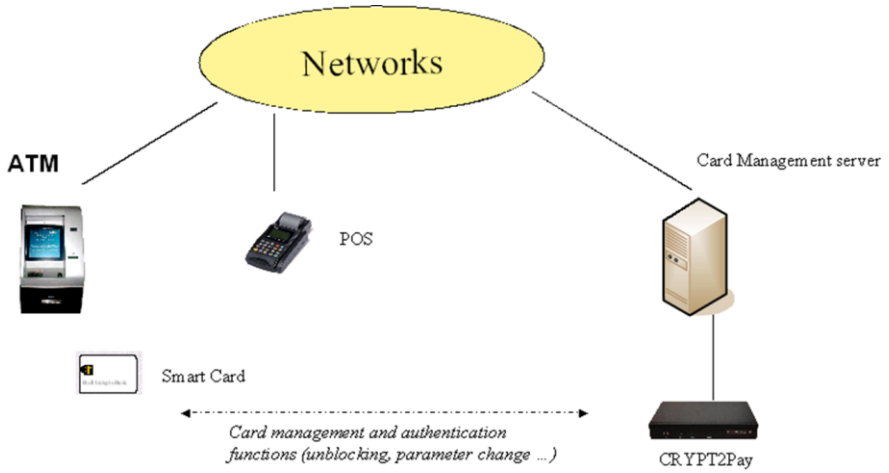
Casos de uso

- PKI
- Soluciones eGov
- Banca electrónica
- Cadenas de personalización
- eBussines
- AuthN de tarjetahabiente
- Sistemas de gestión de tarjetas
- Soluciones de cambio de PIN



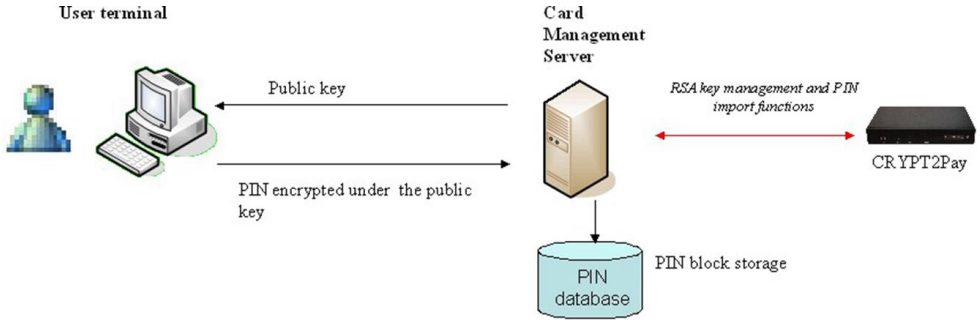
Casos de uso

- PKI
- Soluciones eGov
- Banca electrónica
- Cadenas de personalización
- eBussines
- AuthN de tarjetahabiente
- Sistemas de gestión de tarjetas
- Soluciones de cambio de PIN

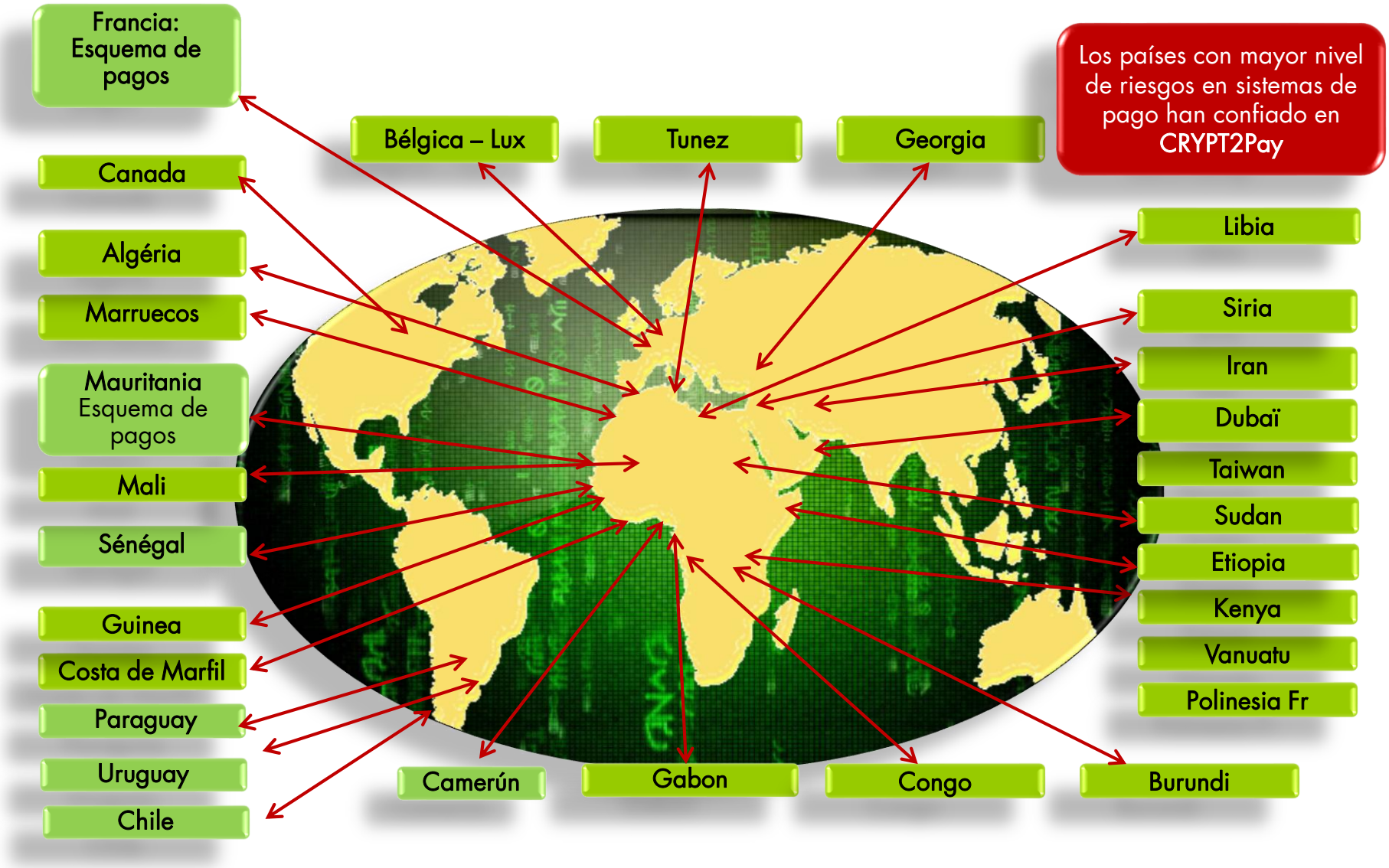


Casos de uso

- PKI
- Soluciones eGov
- Banca electrónica
- Cadenas de personalización
- eBussines
- AuthN de tarjetahabiente
- Sistemas de gestión de tarjetas
- Soluciones de cambio de PIN



Crypt2P* en el mundo



Referencias

Bancos

Agencias de Crédito

Sistemas de tarjetas

Servicios Outsourcing

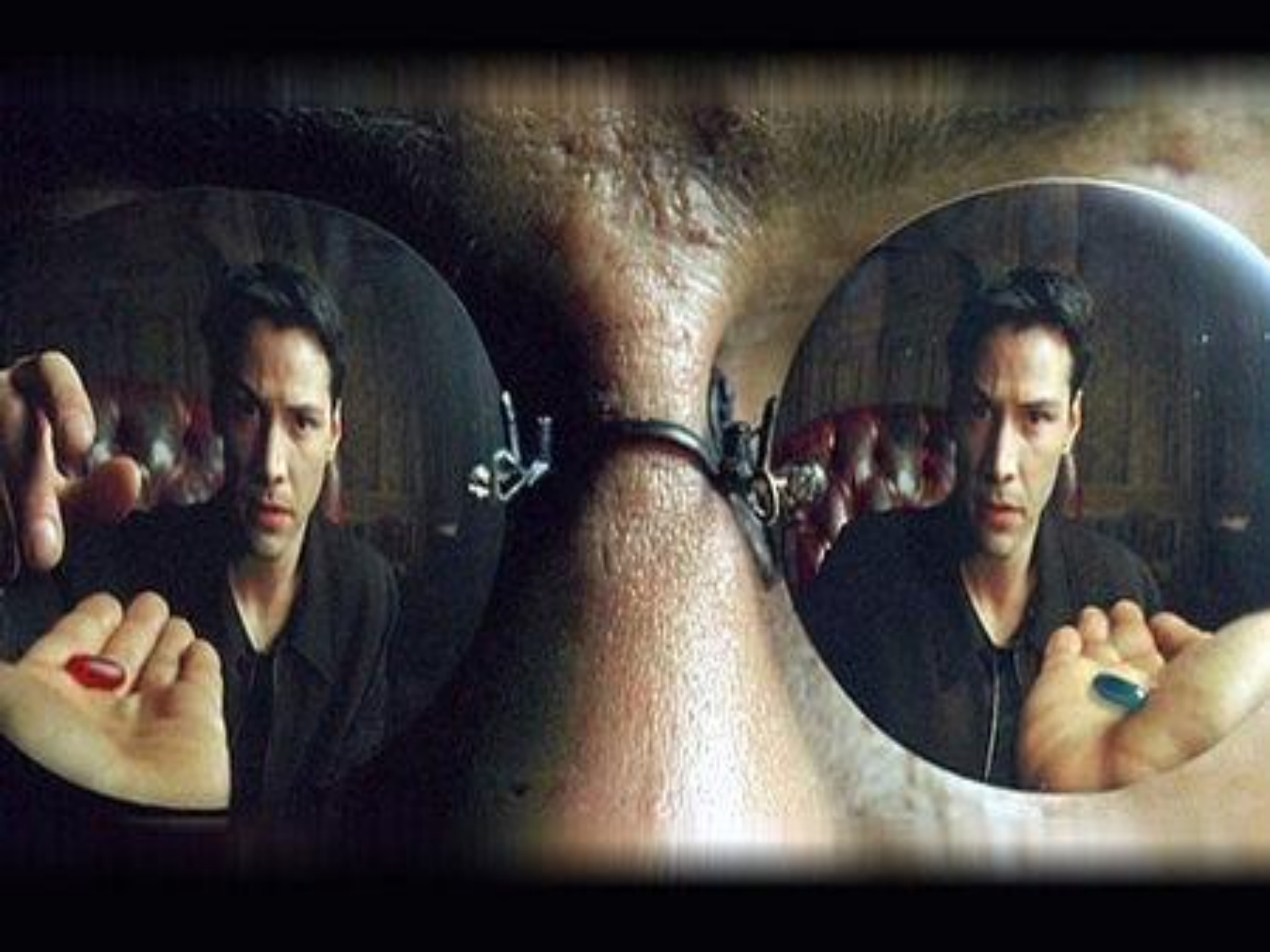
Referencias (cont.)

Referencias (cont.)

Regionales

- Sector construcción
- Sector retail
- Sector manufactura

Alianzas



Preguntas…

an atos company

Gracias !

americo.alonso@lam-bull.com


Bull
an atos company