XXVIII Congreso Latinoamericano de Seguridad Bancaria - CELAES

Lima, 25 - 26 de Noviembre, 2013

Organizado por

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

Soluciones Tecnológicas para La Banca Virtual

Fabian Martins, M.Sc.

Gerente de Desarrollo de Productos y Ethical Hacking

SCOPUS

SCOPUS

1975 – Fundación.
1989 – Adquisición por Bradesco.
1996 – La primera banca por internet del América Latina y quinta en el mundo.
1997 – Browser 128 bits.
1998 – Moneda virtual.
2000 – Solución para transacciones de banca por móviles (WAP).
2001 – Participación directa en la implantación de la infraestructura de claves publicas de Brasil.
2004 – Solución de One-Time Password (OTP) para Bradesco.
2009 – ID de dispositivo.
2013 – Soluciones móviles (Autenticación, Virtualización de Tarjetas, Realidad aumentada…)

3600 empleados
140 mil horas de desarrollo/mes
+150 puntos de servicios en Brasil
Cifra de negocios anual (2012): US$ 320 millones (aproximadamente)

Las amenazas mas comunes

- *Las fugas de las credenciales y de la información confidencial*
  - Monitoreo, Phishing, Compartir de manera intencional o no intencional
- *Cambio de información en tránsito*
  - Captura de datos en la máquina del usuario o en el tráfico a través de proxy https
- *Posibles fraudes gracias a las debilidades en la arquitectura y en los procesos – Fracaso en la..*
  - Identificación (captura de las credenciales en el acceso y en las sesiones)
  - Autorización (captura y manipulación de datos y credenciales en la aprobación)
  - Definición de las responsabilidades (debilidades en el registro de transacciones)
  - Autentificación (debilidades en la autenticación de la información y los documentos)
  - Gestión de la seguridad de la infraestructura
- *Personas (Insiders y no insiders)*

Espacio de las soluciones

Protección en el ámbito de la sumisión de las transacciones	▪ Diseñar mecanismos que mejoren la confiabilidad de las operaciones (fuente de los datos, el comportamiento del cliente)
Gestión del acceso	▪ Utilisar mecanismos fuertes para la identificación y autenticación. ▪ Trazabilidad.
Autenticación de las transacciones por medio de canales distintos	▪ Ofrecer mecanismos que permitan la verification de la autenticidad de las transacciones por medio de canales y dispositivos distintos.
Privacidad en las operaciones	▪ Reducir la exposición de datos confidenciales del cliente.
Gobernancia	▪ Gestión de la configuración y seguridad del perímetro. ▪ Auditorias independientes y educación en seguridad de la información (ISO 27000+).

Plataforma de Seguridad – *Para los portales transaccionales*

La identificación del usuario, identificación del dispositivo, medida de seguridad de dispositivo, la identificación de origen de acceso y la prevención de la redirección

Mecanismos para la evaluación de las transacciones y detección del uso indebido de los sistemas.

Gestión de la IDM y el BMS

Trabajo constante en la detección de nuevas amenazas

1

2

BMS / IDM
Componentes para la identificación del dispositivo y el bloqueo de la monitoración

Organización

Software Web/Transacional

3

MSEG
Módulo de gestión de componentes de seguridad

4

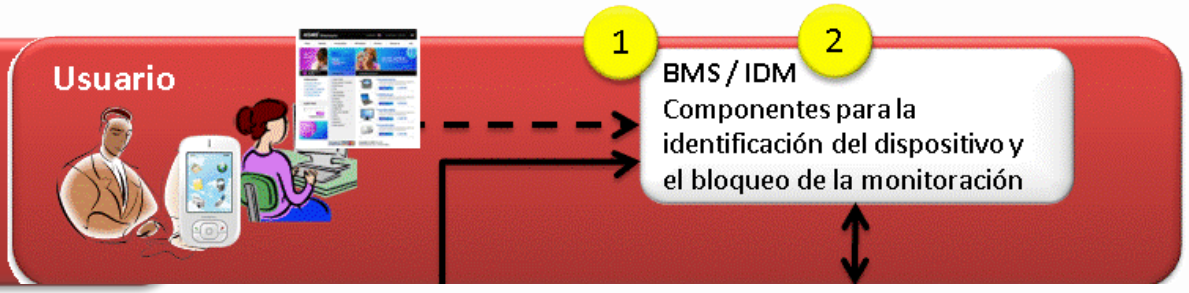
ANTI-FRAUDE
Módulo para la Prevención y detección del fraude

Scopus 5

Investigación y desarrollo de componentes y informaciones para la detección de troyanos y de redirección de DNS

Plataforma de Seguridad – Para los portales transaccionales

La identificación del usuario, identificación del dispositivo, medida de seguridad de dispositivo, la identificación de origen de acceso y la prevención de la redirección



En esta capa – en el dispositivo del cliente - están instalados componentes con dos objetivos:

(1) **BMS**: Hace la identificación de malwares. Cuando posible, hace la desactivación y desinstalación, especialmente para aquellos que hacen captura de datos (clics de ratón, las pulsaciones de teclado). Detecta y corrige la redirección de DNS.

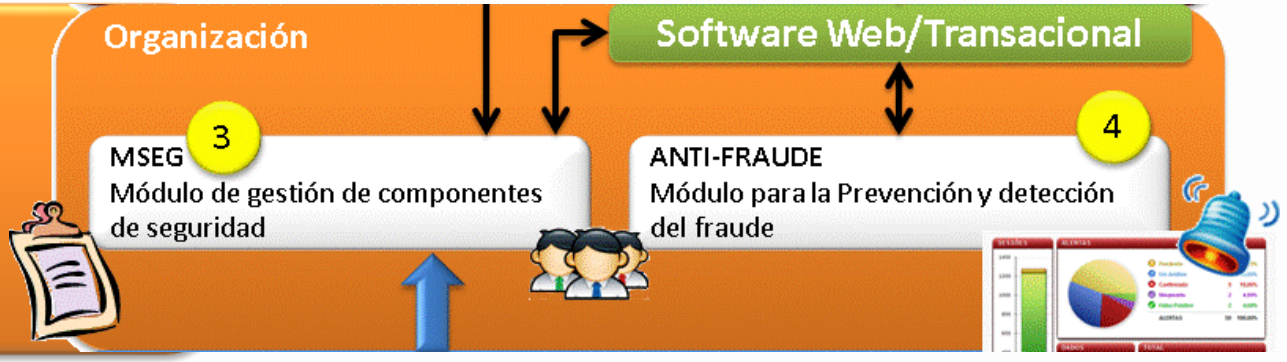
(2) **IDM**: Combina información de hardware y software por medio de funciones criptográficas para crear una identificación para los dispositivos..

- Diseñado para respetar la privacidad del usuario: las funciones son activadas solamente cuando se utiliza la URL del banco.

Plataforma de Seguridad – Para los portales transaccionales

Mecanismos para la evaluación de las transacciones y detección del uso indebido de los sistemas.

Gestión de la IDM y el BMS



En esta capa – en la organización- están los componentes de gestión:

(3) **MSEG**: Tiene los recursos para la gestión de los componentes en la capa del cliente y ofrece una primera oportunidad para la evaluación de fraudes potenciales. También indica la integridad del dispositivo, su identificación y la origen de acceso.

(4) **ANTI-FRAUDE**: Utiliza mecanismos de evaluación del comportamiento para la detección de fraudes en tiempo real. Necesita un vínculo con los sistemas transaccionales. Eficiencia de 7x1 (1 arbitrada para 7 transacciones avaluadas).

Plataforma de Seguridad – *Para los portales transaccionales*

Trabajo constante en la detección de nuevas amenazas

Scopus 5

Investigación y desarrollo de componentes y informaciones para la detección de troyanos y de redirección de DNS

Un equipo en SCOPUS en régimen 24x7x365 para:

- Actualizar los componentes de la capa-cliente:
  - Más de 70 nuevos *malwares* son evaluados diariamente.
  - La solución cuenta con más de 90% de efectividad para nuevos *malwares*.
- Identificar sitios clon.
- Detectar contaminación en los servidores DNS.

Equipo de consultores para el mapeo de procesos, la identificación de los perfiles de la fraude y de los estafadores y diseño de soluciones a medida.

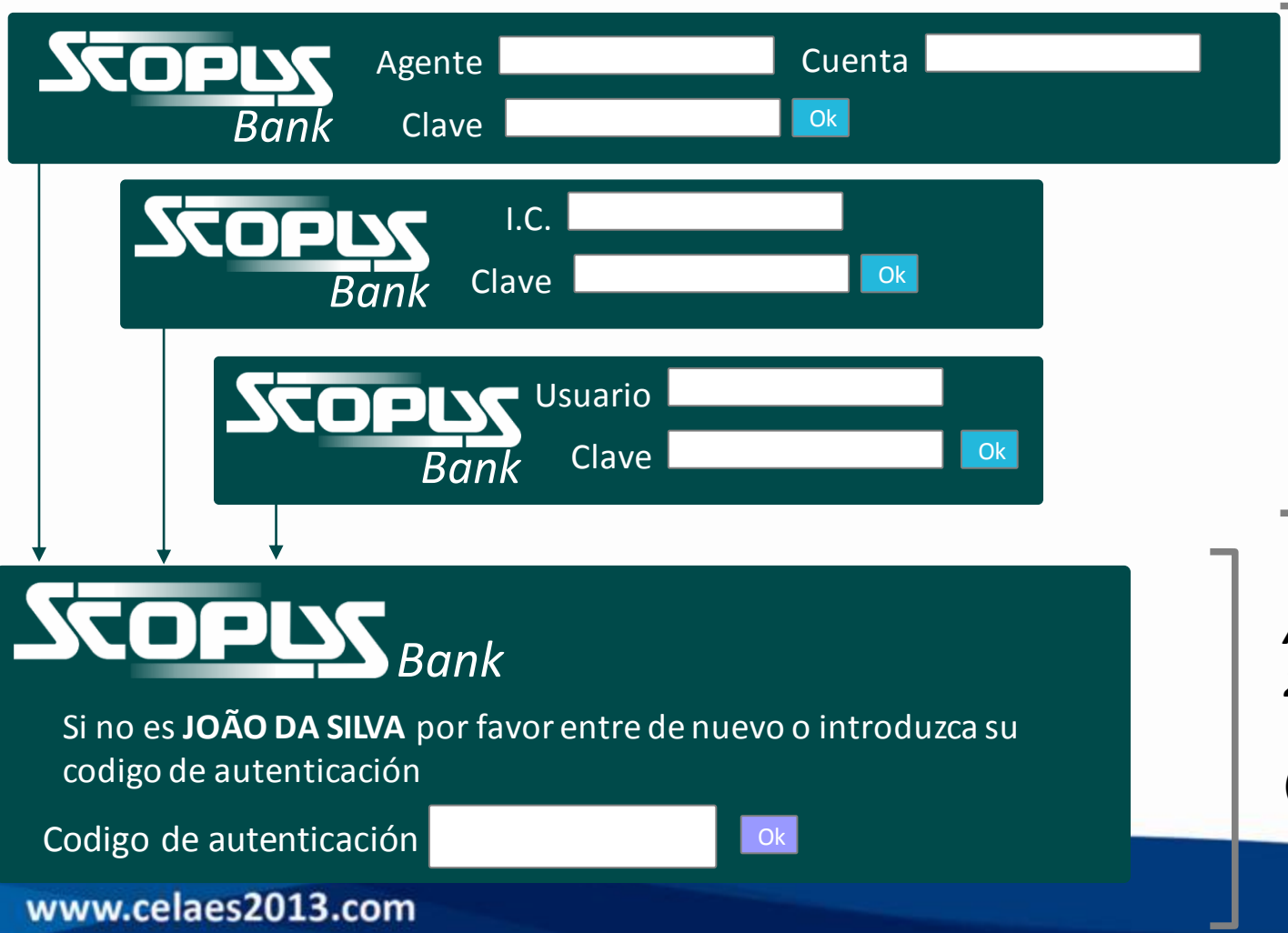
Gestión del acceso - Identificación y autenticación

Identificación → **Autenticación** → **Autorización**

Auditoria

Alguien que el usuario dice que es	Asegúrese que es quien dice	Que permisiones tiene el usuario?
{nombre} , {identificación civil}, {usuario} , {cuenta}…	Algo que solo el Es – biometría Sabe – clave, *password* Tiene - dispositivo	Acceso a transacciones y servicios, los limites operacionales…

Gestión del acceso - Identificación y autenticación



IDENTIFICACIÓN

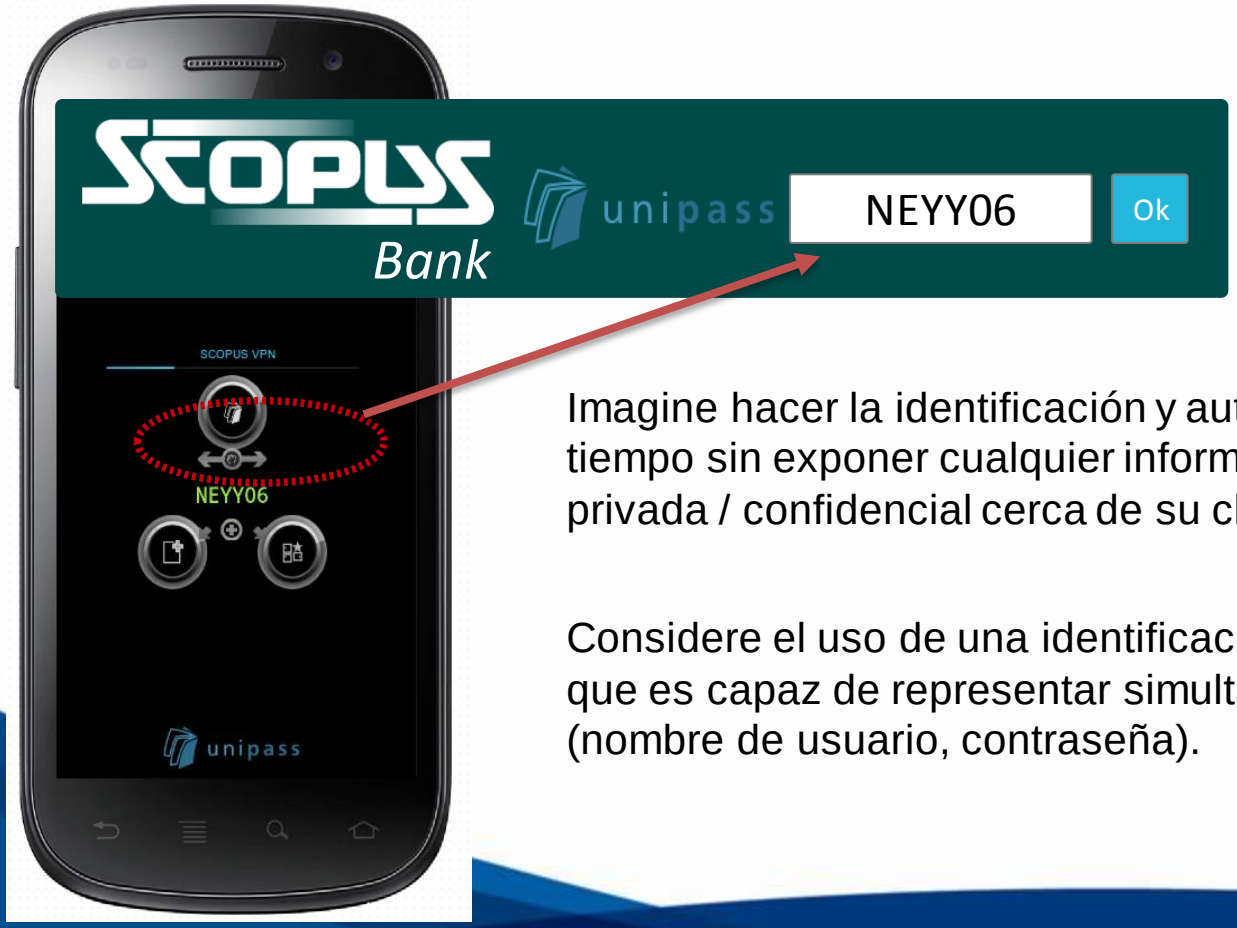
AUTENTICACIÓN 1º factor

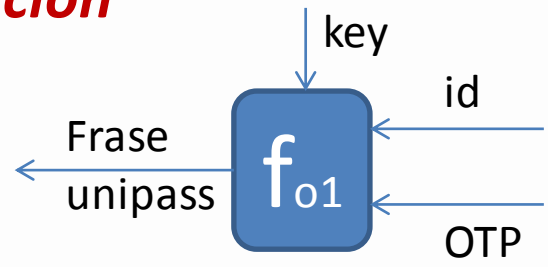
Información personal o privativas están expuestas a *malwares*

AUTENTICACIÓN 2º factor

(cuando disponible)

Gestión del acceso - Identificación y autenticación





Imagine hacer la identificación y autenticación al mismo tiempo sin exponer cualquier información sensible / privada / confidencial cerca de su cliente.

Considere el uso de una identificación variable en tiempo que es capaz de representar simultáneamente el par (nombre de usuario, contraseña).

unipass

HTTPS

Domain

TLS

NEYY06

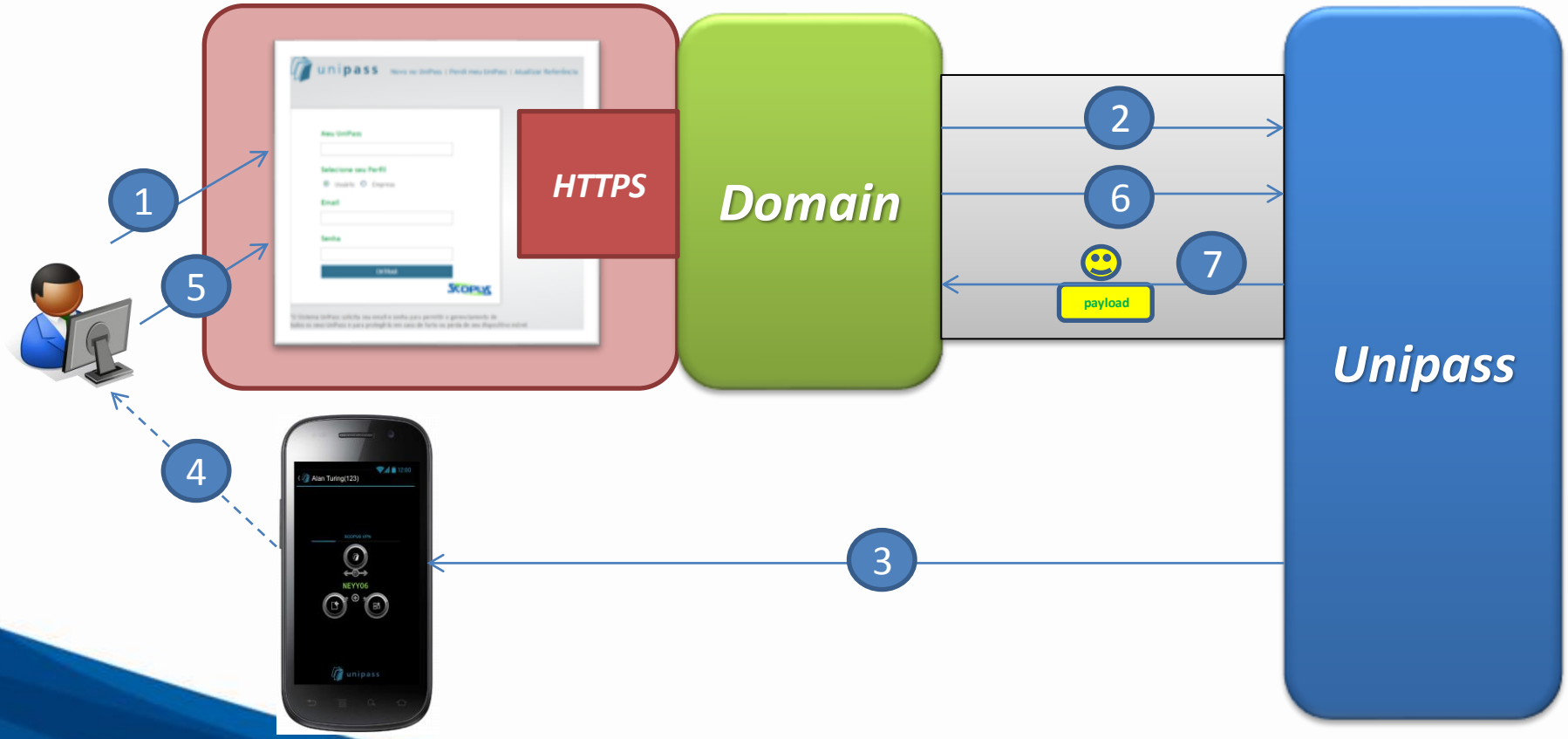
payload

Unipass

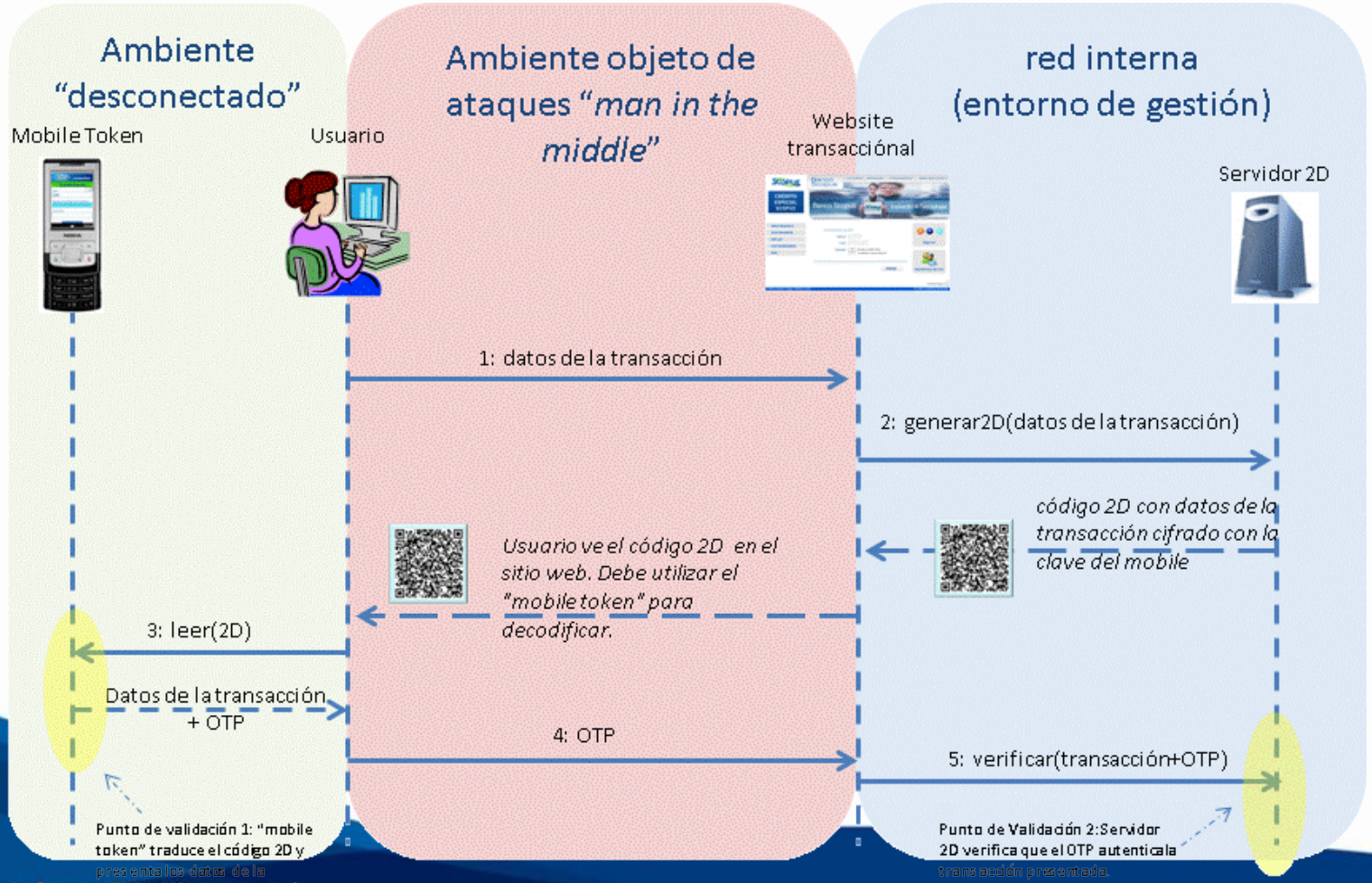
La etapa más critica es la habilitación

Autenticación de las transacciones (múltiplos canales)

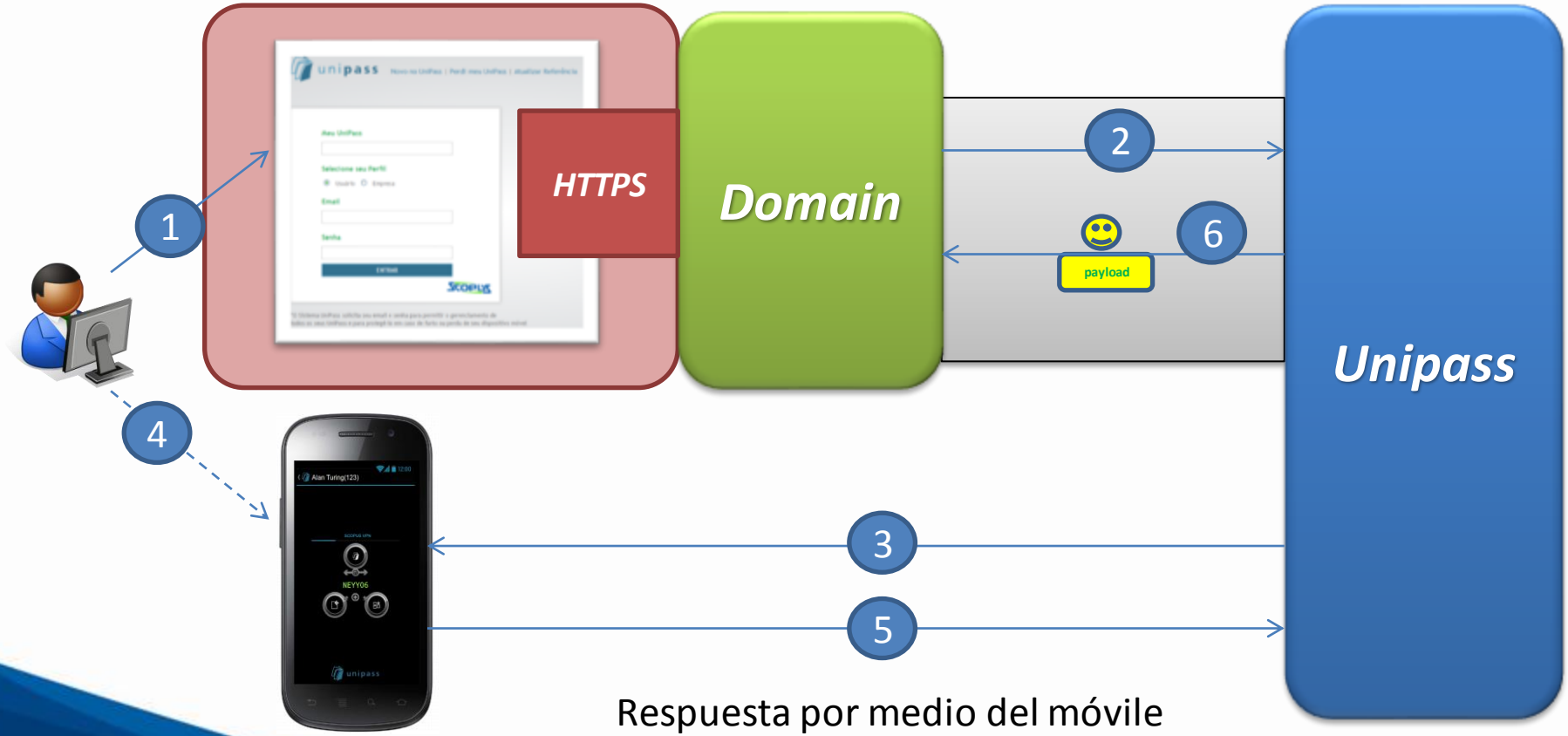
Autenticación de las transacciones (múltiplos canales)



Autenticación de las transacciones (múltiplos canales - imagen)



Autenticación de las transacciones (múltiplos canales)



Respuesta por medio del móvile

Autenticación de las transacciones (múltiplos canales - imagen)

QRCode con datos de la transacción cifrados con la clave existente en el dispositivo

El cliente descifra el QRCode y puede comprobar los datos de transacción que tiene la banca.

El código de autorización es firmado por los datos de la transacción.

Mejora de privacidad y seguridad con tarjetas virtuales

- El modo tradicional de operación requiere que el cliente proporcione el número de la tarjeta, o la propia tarjeta, para el comerciante.
  - Uso de chip aumenta la seguridad, pero los riesgos aún existen
    - "*Chip and Pin is Broken*", Steven Murdoch, Ross Anderson, Mike Bond.
  - El acceso a datos de la tarjeta permiten la clonación o compras por internet.

- **Nuestra propuesta**
  - No permitir que el comerciante tenga acceso a los datos de la tarjeta.
  - Explícitamente insertar el cliente en el proceso de aprobación de la transacción (en presencia o por el comercio electrónico).

Infraestructura segura

Estándar del mercado de tarjetas de pago

Acquirer | **Brand** | **Issuer**

1 Cliente informa el número de móvil o apodo

2 pide a la aprobación de la transacción

3 Pide la selección de medio de pago (tarjeta, cupón)

4 cliente hace la selección de medio de pago e inserta la contraseña de aprobación

5 contraseña +
ID de la tarjeta +
ID del ordenador +
OTP firmado con datos de la transacción

6 confirmación de transacción + número de tarjeta

Scopus/IziPAY mWallet

* Cliente hace la aprobación directamente
* Unión segura entre entornos desconectados
* No se muestra el número de tarjeta
* Tecnología criptográfica para negar la clonación de dispositivos
* Tecnología criptográfica para negar fraude e ataques de hombre en medio

- ***Conclusiones***
  - Tener en cuenta que los dispositivos de los clientes ya están infectados.
  - Hacer verificación de la identidad y comportamiento de los clientes.
  - Utilizar canales distintos para sumisión y verificación de las transacciones.
  - Reducir la exposición de datos personales.
  - Fuerte gobernación.
  - *Insiders* siempre serán una grande preocupación.

- ***Tendencias***
  - BigData / Datos no estructurados.
  - Seguridad colaborativa (privacidad ←→ confiabilidad).