ENISE

INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

Procedimiento para la eliminación de fraudes en Mobile Banking

Seguridad en Mobile Banking

José D. Carrillo Verdún

Profesor Titular de Universidad

Facultad de Informática

Universidad Politécnica de Madrid

Índice

1 – Introducción

Nuevas tecnologías al servicio de la identificación y autenticación electrónica para banca on-line en movilidad

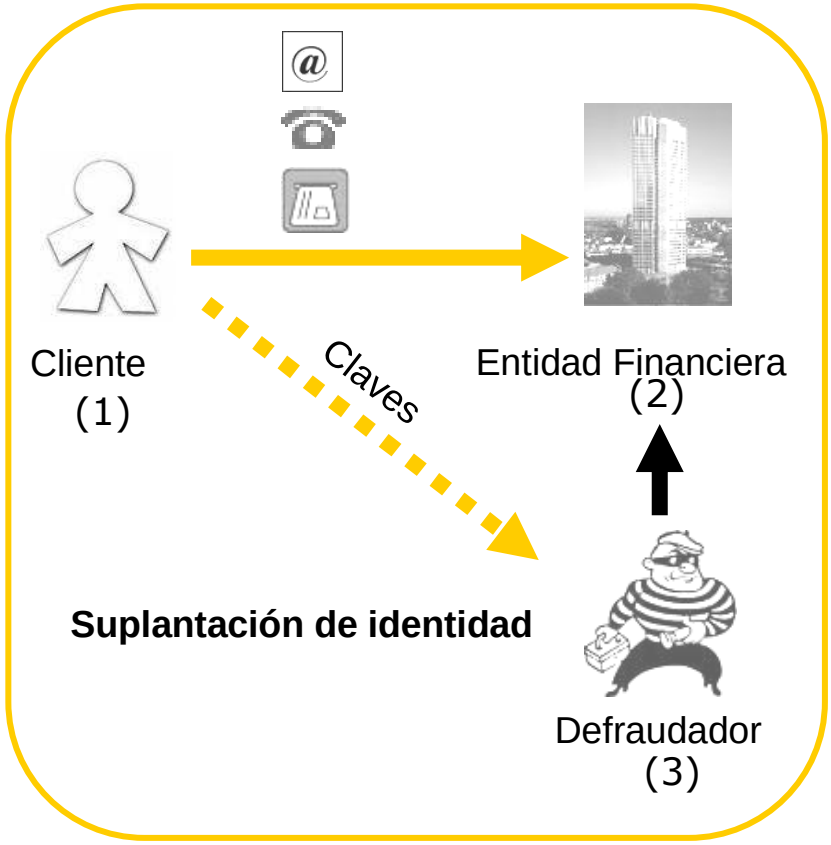
Uno de los riesgos principales en el entorno móvil bancario es el derivado de una **incorrecta identificación de los actores** que intervienen en las operaciones que se realizan y que puede **derivar en fraudes económicos y repudio de operaciones**.

Serán las entidades financieras, junto con la industria, las que deben implementar tecnologías y metodologías adecuadas que permitan ofrecer servicios de identificación y autenticación para banca on-line en movilidad con el nivel de seguridad necesario.

Existen nuevas tecnologías al servicio de la identificación y autenticación electrónica en la banca on-line que deben ser aplicadas para conseguir mejorar el nivel de seguridad de nuestras transacciones electrónicas y evitar los fraudes.

En esta ponencia se pretende dar a conocer el procedimiento de autenticación que se describe en una reciente Patente Europea que emplea la autenticación mutua, con intercambio de claves OTP almacenadas, como medio para asegurar la identificación y autenticación en nuestras transacciones electrónicas de banca on-line. Con ello se conseguirá la eliminación de fraudes como el Phishing y Man In The Middle.

El Phishing en banca on-line en movilidad



¿Por qué ocurre el phishing?

A. (2) es suplantado fácilmente por (3) ya que en la operativa entre ellos **no se exige el que (2) se identifique frente a (1)**

B. (1) **conoce sus datos para poder autenticarse** y operar con (2) y, con engaños, los entrega a (3)

C. los datos de autenticación que (1) entrega **pueden ser reutilizados en próximas operaciones** que realice (3) con (2) haciéndose pasar por (1)

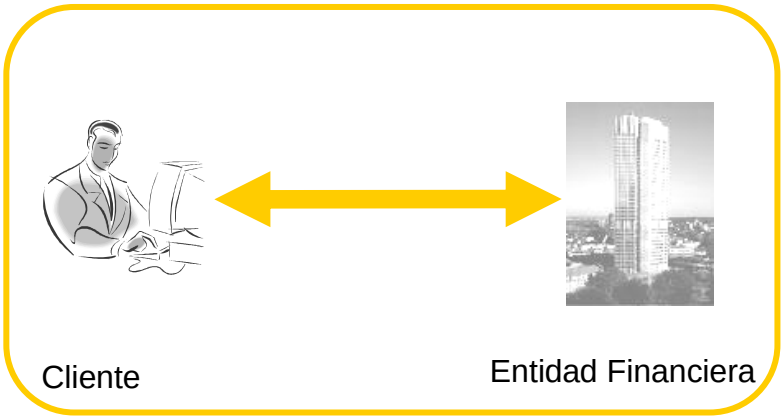
El Phishing: requerimientos de su solución

A. La Entidad Financiera debe estar obligada a identificarse frente al Cliente para que el Defraudador, al no conocer como debe identificarse, no pueda suplantarla

B. El Cliente no conocerá **la información completa** que necesita para llevar a cabo una operación de autenticación mutua hasta que la Entidad Financiera quede autenticada frente a él. De esta forma un Defraudador, aunque consiga engañarle, no dispondrá de toda la información necesaria para llevar a cabo la suplantación de personalidad

C. Los datos que sean utilizados para una autenticación no podrán ser reutilizados para otras

Características principales de la Solución



Intuitivo y sencillo
Totalmente eficaz y fácil de implementar

- **Autenticación mutua:**
  - Se autentica el Cliente frente a la Entidad Financiera y también la Entidad Financiera frente al Usuario
  - El Cliente no conoce su clave final hasta que la Entidad Financiera se le ha autenticado. Hasta entonces sólo conoce la primera clave de las tres que va a necesitar
- **¿Qué tiene que llevar el Cliente ?**
  - Su dispositivo móvil, o un token específico para la autenticación, que contenga las claves a intercambiar en el proceso de autenticación
- **Claves**
  - De Un Solo Uso (OTP)
  - Almacenadas (no se calculan) en grupos de tres claves
  - Aleatorias generadas en un proceso de carga previo
  - La Entidad Financiera tiene una copia de las claves almacenadas en cada uno de los token de sus Clientes

Solución: procedimiento para la Autenticación Mutua en Banca on-line

Cliente con Token (soft o hard)

Servidor de la Entidad Financiera

PIN 

1. El Cliente inicia el token con su PIN y visualiza la Clave 1

2. Desafío_usr (Clave 1)

3. Con la Clave 1 y el identificador del token se obtiene la respuesta Clave 2

4. Se envía la respuesta Clave 2

Se marca la Clave 1 como ya usada

5. Respuesta_srv (Clave 2)

6. Se teclea Clave 2 para verificación y se muestra la Clave 3

Se enseña la Clave 3 y se marca la tripleta como usada sólo si la Clave 2 es la correcta

7. El Cliente responde con Clave 3

El Cliente sabe que se la está enviando a su Entidad Financiera y no a otro

8. Respuesta_usr (Clave 3)

9. Se valida la respuesta Clave 3

10. Se acepta o rechaza la entrada a la operativa

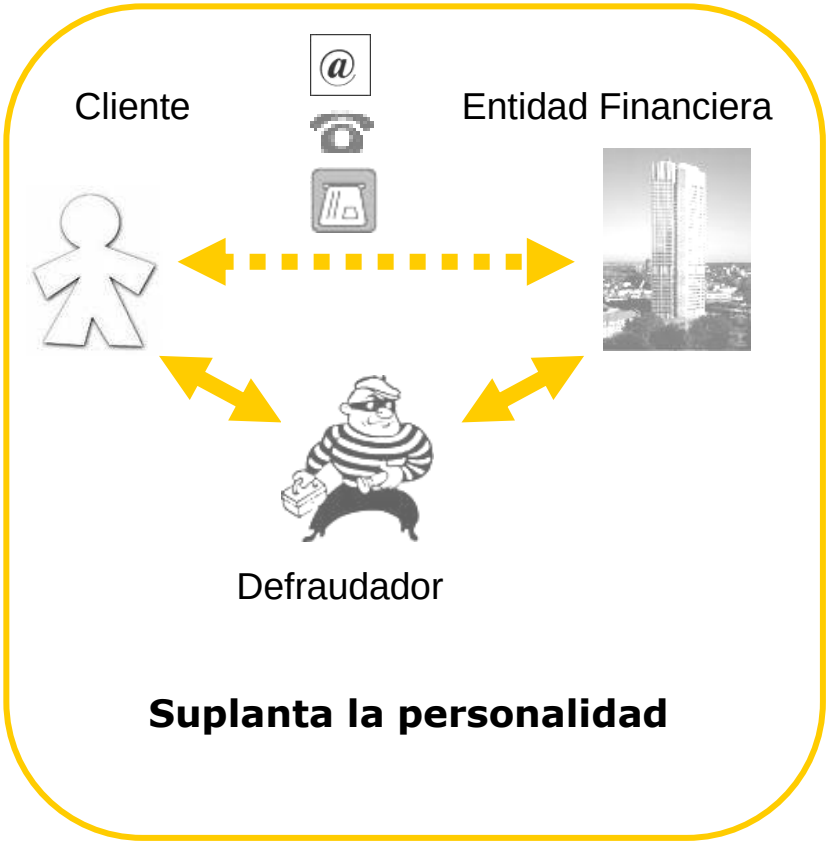
11. Acepta / Rechaza

Puntos fuertes de la Solución

1. **Si alguien se hace con el Token * (o aplicación de autenticación en el teléfono móvil) y quiere usarlo tendrá que conocer el PIN de entrada y si, además, quiere entrar a la Entidad Financiera tendrá que conocer también el código de Cliente y éste no consta en el Token**
2. **Cuando la Entidad Financiera envía la Clave 2 marca como ya usada la Clave 1 de forma que si la vuelve a recibir rechazará la solicitud de autenticación (si alguien ha llegado a conocerla ya no podrá reutilizarla)**
3. **Será el Token el que verifique la validez de la Clave 2 que recibe el Cliente y sólo presentará la Clave 3 al Cliente cuando la Clave 2 sea la correcta. Así:**
   - ✓ se evita que el Cliente pueda realizar una incorrecta validación de la Clave 2
   - ✓ si alguien se ha hecho con la Clave 2 pero no tiene el token no podrá conocer la Clave 3 que requiere la Entidad Financiera para permitir la entrada a la operativa del Cliente
   - ✓ se impide que el Cliente sea engañado y pueda entregar todas sus claves a un defraudador
4. **Las claves que se utilizan en el proceso son aleatorias, generadas en un proceso previo y se encuentran almacenadas en el Token del Usuario y en el Servidor de la Entidad Financiera:**
   - ✓ no tienen el problema de caducidad temporal que si tienen las generadas on-line con semilla temporal
   - ✓ están almacenadas, lo que elimina los requerimientos de capacidad de procesamiento para su generación on-line, ampliándose así el tipo de dispositivos de usuario que pueden ser usados y se reduce la inversión a realizar por la Entidad Financiera tanto en los Token como en su Servidor de proceso
   - ✓ en comparación con los métodos que usan claves generadas on-line, se consigue que el sistema sea menos vulnerable a ataques de denegación de servicio gracias a su menor consumo en recursos de proceso

(*) cuando se habla de Token se debe tener en cuenta que el mismo dispositivo móvil del Usuario puede actuar como tal siempre que tenga instalada la aplicación que soporta el servicio de autenticación mutua

El Man In The Middle en banca on-line en movilidad



¿Qué es el fraude 'man in the middle'?

En el fraude “hombre interpuesto” un defraudador **suplanta la personalidad de los dos participantes** en una operación realizada de forma no presencial, y consigue tener acceso a toda la información que se intercambia, con la posibilidad de cambiarla antes de que llegue al receptor.

¿Cómo evitar que modifique información de una operación económica?

Una forma de evitar un posible fraude de éste tipo en la realización de una operación económica exige que la validación de la operación sea llevada a cabo en tres pasos y haciendo uso de dos canales de comunicación diferentes

Aplicación para solucionar el Man In The Middle

Autenticación Mutua para llevar a cabo una operación económica (firma) en la que se hace uso de un SMS como diferente canal de comunicación entre la Entidad Financiera y el Cliente

Transacción electrónica que se ejecuta en el dispositivo móvil del Cliente

Clave 1

Clave 3

Servidor del Banco

Servicio SMS en el teléfono móvil del Cliente

Clave 2 vía SMS

1- El Cliente, desde la aplicación operativa del Banco en su dispositivo móvil, envía al servidor del Banco su Clave 1 con el fin de firmar una operación económica

2- El servidor del Banco envía al teléfono móvil del Cliente, vía SMS, la Clave 2 autenticando los **datos de que dispone para la operación a confirmar. El Cliente verifica la exactitud de los datos de la operación.** La aplicación de autenticación del Token verifica que la Clave 2 es correcta y presenta al Cliente la Clave3

3- El Cliente teclea en su dispositivo móvil la Clave 3 aceptando la ejecución de la **operación cuyos datos le han sido comunicados en el SMS**

Nota: opcionalmente el Banco puede enviar al dispositivo móvil del Cliente una cuarta Clave 4 con el fin de autenticar la comunicación en la que le informa de la realización de la operación para asegurar el no repudio

Otras aplicaciones de la Solución presentada

Tiene aplicación en todos aquellos diálogos caracterizados por la distancia física de los participantes que hacen necesaria la autenticación de las dos partes. Por ejemplo:

- ✓Banca on-line
- ✓Banca telefónica y cajeros automáticos
- ✓e-commerce
- ✓Pagos en comercio con TPV
- ✓Accesos a intranet corporativas
- ✓Domótica
- ✓Correo electrónico autenticado

10 – Conclusiones

En el entorno de la banca on-line en movilidad

1. **Es posible evitar los fraudes más frecuentes** y con ello:
   - reducir los costes directos del fraude así como los de las pólizas de cobertura y la inversión en procesos preventivos
   - los delincuentes tendrán menor motivación para lanzar nuevo malware
   - aumentará la confianza de los Usuario en el uso de las transacciones electrónicas lo que repercutirá en un incremento del número de operaciones que se realicen

2. **Es necesario primar la Seguridad y Calidad de los Sistemas de Autenticación frente a la mal entendida "comodidad" del Cliente**

Muchas gracias