



La autenticación bancaria, revisada

En octubre del pasado año, la FFIEC¹ norteamericana publicó un documento titulado *"Authentication in an Internet Banking Environment"*, que es una renovación de otro publicado cuatro años antes, en agosto de 2001, titulado *"Authentication in an Electronic Banking Environment"*. La FFIEC es un ente colectivo puesto en marcha por la administración norteamericana para desarrollar los estándares utilizados en la auditoría federal que se realiza a todas las instituciones financieras por parte de organismos tales como la Reserva Federal o la Federal Deposit Insurance Corp. (FDIC). Este tipo de documentos, aunque no tienen rango de ley, sí son una declaración de buenas prácticas frente a las cuales los bancos e instituciones financieras norteamericanas serán auditados a finales del presente año.

Así pues, ya está en marcha el contador del tiempo en el que los bancos americanos tendrán que actualizarse y adaptar nuevas normas que llaman a una autenticación de usuario más robusta para poder permitir las transacciones online. Dado que las instituciones financieras no suelen ponerse en marcha hasta que es inevitable, ahora dicho colectivo vuelve su vista al mercado para ver cuáles son

A finales del año 2005 se hizo público un documento dirigido a las instituciones financieras de los EEUU, en el que se reconoce explícitamente la inseguridad de los actuales sistemas de autenticación de cliente que son utilizados en la banca y el comercio electrónico a través de Internet. A pesar de este reconocimiento sectorial, que siempre es un avance —de lo ya conocido por muchos otros—, el documento parece resolverlo todo con el uso de sistemas multifactoriales pero no aporta soluciones concretas y deja a los bancos a su libre albedrío ¿Qué harán éstos?

las diferentes opciones tecnológicas que, estando disponibles, satisfacen los requisitos

acceso a información del cliente o al movimiento de activos con valor. Según el



Para poder proteger los datos personales y privados de los clientes, para prevenir el lavado de capitales, la financiación de grupos terroristas y, en general, para reducir el fraude financiero, es necesario disponer de sistemas realmente efectivos en la autenticación de todos los agentes implicados.

de la nueva guía.

La FFIEC considera que, en solitario, la autenticación basada en un único factor

mencionado documento, las instituciones financieras que ofrezcan productos y servicios a través de Internet de-



La FFIEC públicamente reconoce que el fraude contable y el robo de identidad son el resultado frecuente de utilizar autenticaciones basadas en un solo factor y que las instituciones financieras deberán pasar a usar autenticaciones multifactoriales, a organizar la seguridad por niveles, y a adoptar otros controles que, correctamente calculados, puedan mitigar lo más posible esos riesgos.

es totalmente inadecuada para aquellas transacciones de riesgo que supongan el

berán emplear métodos más efectivos para autenticar la identidad de sus clientes y *"las técnicas de autenticación a utilizar deberán ser las apropiadas a la vista de los riesgos asociados con esos productos y servicios"*. La

FFIEC públicamente reconoce que el fraude contable y el robo de identidad, tan incesante en nuestros días, son el resultado frecuente de utilizar autenticaciones basadas en un solo factor (usuario/contraseña), y que las instituciones financieras deberán

pasar a usar autenticaciones multifactoriales, a organizar la seguridad por niveles, y a adoptar otros controles que, correctamente calculados, puedan mitigar lo más posible esos riesgos.

Sin embargo, a la vista de lo que hay en el mercado², es seguro que no existe una única tecnología que sea la apropiada para todas las necesidades actuales de autenticación y autorización y que, además, sea suficientemente cómoda como para que el cliente la acepte con cierto gusto y no con mera resignación. Como es fácil de entender, la solución o soluciones que se adopten deben ser, además, fácilmente escalables y esencialmente sencillas en su uso por parte de usuarios no técnicos.

Doble factor

La solución que propone la nueva guía de la FFIEC aboga por las tecnologías de doble factor para proteger todas las actividades de valor que se realicen en Internet, y la propuesta la hace con un fuerte carácter docente y divulgativo ya que en el amplio apéndice que acompaña a esta guía, se hace

¹ FFIEC = Federal Financial Institutions Examination Council

² Teclados gráficos virtuales, matrices de números o imágenes, tarjetas magnéticas, inteligentes y de memoria, OTPs, llaves criptográficas USB, lectores de huellas dactilares, certificados digitales de una PKI, etc.

una revisión de los métodos técnicos más conocidos para autenticar usuarios en entornos financieros.

Es en este apéndice donde se define lo que, en este contexto, se entiende como "factor" de autenticación y se proponen tres: lo que una persona sabe, lo que tiene, y lo que físicamente es.

El nivel de protección que se consigue con cada una de estas técnicas varía, y la selección de una u otra tecnología de autenticación siempre dependerá de los resultados obtenidos en la evaluación de los riesgos que haga, responsablemente, cada institución financiera.

Los métodos de autenticación dependientes de más de un factor son más difíciles de comprometer que los métodos de factor único, por lo que aquellos métodos que estén adecuadamente diseñados e implementados sobre principios multifactoriales son más resistentes y más disuasorios respecto al fraude.

Un mecanismo de autenticación mediante dos factores consiste en evaluar dos de los tres factores anteriormente citados, y exigir la correcta y simultánea verificación de ambos para dar por autenticado al sujeto.

Aunque al pasar a evaluar dos factores hemos complicado la tarea al atacante, algunas voces vaticinan que la autenticación por dos factores, por sí sola, no será suficiente para arreglar la situación actual, y que los bancos necesitan, además, instalar medidas específicas para combatir el fraude.

Para poder proteger los datos personales y privados de los clientes, para prevenir el lavado de capitales, la financiación de grupos terroristas y, en general, para reducir el fraude financiero, es necesario disponer de sistemas realmente efectivos en la autenticación

de todos los agentes implicados (bancos, clientes, productos, etc.); de no ser así, difícil será establecer la validez legal de los acuerdos y transacciones electrónicas que se realicen.

Hacer negocios con personas o instituciones



Aunque con un mecanismo de autenticación mediante dos factores hemos complicado la tarea al atacante, algunas voces vaticinan que esta opción, por sí sola, no será suficiente para arreglar la situación actual, y que los bancos necesitan, además, instalar medidas específicas para combatir el fraude.

incorrectamente identificadas en un entorno tan anónimo como es Internet ya se ha visto que conduce a pérdidas financieras muy graves y a daños difícilmente reparables en la reputación de entidades y personas.

Con todo, el problema que supone la propia guía del FFIEC es su excesiva confianza en que el paso



Dado el inexplicable alto precio que tienen los criptoartefactos transportables y tamper proof que hay disponibles en el mercado, y que la Administración española -e-, no sería de extrañar que las instituciones financieras dejaran el tiempo pasar hasta poder utilizar el e-DNI como segundo factor inalterable, que no se puede copiar.

a los sistemas con autenticación de doble factor va a resolver los serios problemas actuales.

Las cualidades de un sistema de doble factor depende de lo bien elegido y escrupulosamente bien implementado que esté, por lo que muchas soluciones podrían ser esencialmente inseguras debido a su incorrecto planteamiento y peor implementación.

Hay que recordar que el uso de los cajeros automáticos sigue un esquema de autenticación mediante doble factor (posesión de una tarjeta y conocimiento de un PIN) y, sin embargo, han sido varios los casos en los que, con simplemente poner

pseudo-cajeros automáticos a las puertas de un supermercado, los delincuentes se han hecho, en horas, con cientos de bandas magnéticas y sus correspondientes PINes. En estos casos, como en el del phishing actual, el error está en la falta de autenticación de la entidad financiera, de su equipamiento y de sus servicios.

transportables y tamper proof que hay disponibles en el mercado, y que la Administración española nos tiene prometidos para ya mismo un DNI electrónico con autenticación de usuario y firma electrónica, no sería de extrañar que las instituciones financieras dejaran el tiempo pasar hasta poder utilizar el e-DNI como segundo factor inalterable, que no se puede copiar. De este modo, habría sido el Estado el que le sacara las castañas del fuego a un gremio mercantil como es el financiero y, de paso, los ciudadanos de a pie volveríamos a utilizar frecuentemente un ya antiguo instrumento identificativo que realmente no usamos de forma cotidiana desde la segunda mitad de la década de los setenta.

El éxito de cualquier método de autenticación no sólo depende de la tecnología utilizada, sino también de las políticas, procedimientos y controles que la acompañan.

La solución no sólo consiste en distribuir llaves criptográficas "urbi et orbe", que ayuda bastante, sino además en ponerse en la piel del atacante y ver cuán débiles pueden llegar a ser los sistemas de seguridad concebidos dentro del secretismo empresarial o adoptados con la ciega fe en los estándares gremiales.

Cuanto más público sea un sistema, y lo sea por más tiempo, mayor es su seguridad y mayores sus méritos para confiar en él. ■

JORGE DÁVILA MUÑOZ
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS - Facultad
de Informática - UPM
jdavila@fi.upm.es