maverick™

Multi-Factor Authentication Scenario:
A LARGE INTERNATIONAL BANK

*Scenario is for illustrative purposes only.
This is not a case study.

IBM Business Partner

maverick™

TOLL FREE / 888-266-1678 WEB / www.MaverickSecure.com

Hello and thank you for your interest in Maverick Secure.

In establishing Maverick I had a vision to build a company that everyone could be proud to work for, be associated with, and would want to conduct business. I believe we have achieved that goal and continue to aspire everyday to make that an on-going reality of continuous improvement. Here at Maverick Secure we are building a company that is run with integrity. Our ethos: SECURITY IS EVERYTHING. Our products, our service, and our mission will not be compromised. Our mission is to provide the most secure authentication process available on the market, and match that with the most affordable price point in the market.

The Maverick family is founded on several core principles:

- To stay ahead of hackers and rogue elements by providing the strongest, most secure, highly innovative and patented authentication processes available;
- To provide a great product at a reasonable price;
- To be responsible to our customers: your success is our success;
- To be responsible to our employees: we all work hard and so we should all share in our collective successes.
- To be responsible to this land that we all share: make every effort to create a sustainable product that will contribute to the health, vitality and industry of this planet;
- To invest in solutions that will enable the business community to grow and develop: businesses of all sizesare the backbone of our communities, our culture and our country.

Maverick Secure is fully invested in developing and protecting a work environment that rewards integrity and embraces diversity. We believe in quality service and support this with a strong work ethic. Here at Maverick Secure, we will not compromise integrity for profit. We will not discriminate on the basis of race, ethnicity, religious preference, sexual orientation or gender – rather, we will truly endeavor to embrace and elevate individuals who deliver on our core values. It's simple really: your success is our success. We believe in good honest work, and we will work hard to produce the tools, the solutions, and resources that make your task easier, more efficient, more profitable and most importantly, MORE SECURE.

On behalf of the Maverick family, I welcome you to learn more about our family of products, and to become our next Maverick Secure satisfied customer.

Thank you.

Patrick McNicholas
Managing Partner

Contents

Introduction

In a banking environment, the stronger and more varied the factors used to grant access to a user, the stronger the security level—a necessity in today's electronic banking systems where enormous fortunes flow between banks in the day-to-day operations of modern finance.

The Need for a Strong 2-Factor Authentication

A secure banking authentication system must meet the needs of all banking stakeholders, from the smallest client/employee to the biggest corporate account/banking executive. Without it, online banking will never be safe and secure enough to gain the banking clientele's trust.

Case Scenario

A large international bank sought to put up a unified online system of authentication usable for both central clearance and low-level transaction with the local branch management. Management wanted an authentication system that would adopt its required authentication factor with the level of the desired transaction and the channel used for the transaction, be it through the bank's web portal or just the intra-bank transaction system.

Maverick Solution

The Maverick 4-F™ security authentication system, with its four-factor authentication, PKI and OTP capabilities, was deemed able to meet the bank's requirements for a more robust authentication service for use at the bank's web portal.

Key Requirements

- Flexible and scalable
- Easy to use, deploy, and maintain
- Cost effective
- Secure

Results

- Increased customer confidence.
- Less maintenance expenditure
- Removed the need for extensive technical training.
- Maverick LLC's strong support position was an added bonus.

About Maverick Secure LLC

MAVERICK is dedicated to high-quality, affordable, user-friendly, scalable, and seamlessly-compatible technologies addressing the critical needs of the rapidly developing authentication market.

Banking security and management made more secure by Maverick 4-F™ Authentication System

At-A-Glance

Key Requirements

- Flexible and scalable for use in small or large organizations in a wide variety of channels and platforms.
- Easy to use, deploy, and maintain-Minimal learning curve and workflow impact.
- Cost effective – Minimal hardware and training costs.
- Secure – Strong authentication, transaction and data protection.

Solution

- A strong token access system featuring a versatile permissions level that can go from one-factor to four-factor authentication depending on the user, and the kind of transaction.

Results

- Secure transactions, communications and authentication anyplace, anywhere.
- Low total cost of ownership.
- Low workflow disruption.
- Robust after-sales support.

Introduction

Strong authentication depends on the quality and combination of factors brought into an authentication system. The stronger and more varied the factors used to grant access to a user, the stronger the security level.

In a banking environment, not all personnel are given the same security access to the system. Obviously, key management and administrative people are given the highest clearance, while ordinary rank-and-file employees are given regular system access that they need to carry out their day-to-day tasks.

Likewise, not all clients are required to have the same level of authentication requirements in order for their transactions to be approved. Usually, the bigger the amounts and accounts involved in the transaction, the more complex the authentication requirements and protocols required. Personal savings accounts and transactions have different online access controls required compared to multi-billion dollar corporate accounts.

It is apparent that larger and more valuable accounts have a high degree of inbuilt security protocols but this is necessary in today's electronic banking systems where enormous fortunes in transactions are transferred from bank to bank as part of the daily flow of modern finance. It has been said that information is power. In the world of modern finance, data is money. That money should be protected by the best means possible—online access and authentication systems that are sophisticated enough to satisfy even the most stringent requirements of the military but scalable and simple enough to be used by even the smallest of businesses having an online banking presence.

In this context, a banking security authentication system must meet the requirements of the smallest client/employee to the sophisticated needs of the biggest corporate account/banking executive.

The Need for a Strong Multi-Factor Authentication

Authentication has always been associated with three factors: Something you know, something you have, and something you are. Using more than one kind of factor in authentication is usually more secure because it creates more barriers (layers of security) against fraud and electronic attacks. 'Something you know' is the usual username and password authentication. Many online banking systems require only this kind of authentication. Using only 'something you know' is not considered a reliable form of authentication.

Before we go any further, let us be clear on this: using more than two of only one kind of factor is not multi-factor authentication. For example, requiring a username, password and a specific piece of personal information or two valid IDs before one is authenticated, is not three-factor authentication; it is just one-factor authentication requiring more than one piece of the same kind of factor.

'Something you have,' the second factor, is something physical you have in your possession. The most common examples of the second factor are security tokens, smart cards, or USB dongles. Traditionally, two-factor authentication schemes use the first and the second factor, but using the first and the third factor, or the second and the third factor, are also forms of two-factor authentication.

'Something you are,' the third factor, is something uniquely your own, aka biometric—for example your voice, your fingerprints, or your retina patterns. The fact that these are physical features that can be lost or defaced (or which your twin might possess) makes some people say these are just more complex examples of 'something you have.' However, work is on the way to create a machine that can use one's brain wave patterns as a password—since brain wave patterns are considered unique to an individual and is not lost even when one loses his voice, fingers or eyes (and one who is not in his right mind is not the same person), the day will come when a true 'third factor' authentication system using brain waves will be commonly used—even if used alone (one factor), it would be a pretty secure authentication method. For now, three-factor authentications require username and password, a security token and a biometric input, commonly voice recognition or retina scan. Three-factor authentication is commonly reserved for high level access or transactions. In a bank, this means transactions requiring the approval of senior executives—involving huge amounts of money.

Then there is the so-called Four-factor authentication. The 'fourth' factor is commonly identified with 'somewhere you are'—in space (and/or time). The biggest argument against a fourth factor is that 'somewhere you are' does not meet the two main criteria for an authentication factor:

1. You can take it with you.
2. A factor can function as authentication by itself.

You cannot take a place with you, nor can you carry time around. And being automatically authenticated just because you are there defeats the purpose of authentication (not to mention the purpose of being online) so the fourth factor can be considered not an authentication factor at all but a window where an instance of authentication can take place—it doesn't make fraud any harder; it just limits the time and place where fraud can be done. Hair-splitting aside, the fourth factor (if it really is an authentication factor) still helps minimize the frequency of fraud at the expense of convenience.

Key Requirements

Not all transactions require the same kind and amount of authentication so a chosen banking e-security solution must be:

- Flexible and scalable – Can be used and tailored for small organizations or very large corporations with sites around the world. Should also be able to accommodate a wide variety of channels, operating systems, and platforms by which clients and bank personnel authenticate and transact.
- Easy to use, deploy, and maintain – Ease of use, speed of deployment, and simplicity of maintenance means workflows are not impacted much, if at all.
- Cost effective – A secure and simple system generally means not much is spent on procurement, distribution, installation of hardware, and training.
- Secure – must provide a transaction environment safe against online threats such as phishing, brute force attacks, replay attacks, shoulder-surfing, snooping and key-logging.

A system meeting all these requirements allows banking personnel to do what they do best—serving the needs of clients and acting in accordance with the bank's best interests.

Case Scenario

A large international bank is seeking to put up a unified online system of authentication that can be used both for central clearance or just to clear a transaction with the local branch management, the authentication requirements varying depending on the amounts and clients involved.

Maverick Solution

After reviewing several vendor solutions, the bank chose Maverick LLC's Maverick 4-FTM solution. The solution met the key requirements of ease of use, security, flexibility, scalability, and cost-effectiveness.

The key feature of this solution is the strong four-factor security token that has a seamless, driverless combination of PKI cryptographic APIs that support a wide range of authentication and access gateway solutions. The token is also an industrial-grade time-based OTP generator with the capability of strongly encrypting digital certificates for online and offline use.

Encased in tamper-evident hard molded plastic, the Maverick 4-FTM token is water and impact-resistant plus it is able to operate from 20°C to 70°C.

The token acts on three levels:

1. Authenticate using multi-factors, depending on the user's permissions level and the kind of transaction;
2. Secure the transaction against online attacks; and
3. Protect transaction data with a strong encryption algorithm.

Furthermore, the system is easy to setup and manage zero footprint authentication means there is no need to install any software or enter the OTP on the user's end. Maverick's central authentication coupled with a web-interfaced management tools allows the system to be used for remote management on different operating systems.

The bank also appreciated the way Maverick LLC had a reasonably priced advanced pre-sales and post-sales support service, a key requirement for customer support.

Results

- Bank customers and personnel were secure in the fact that they could conduct their transactions, communications and authentication with clients in a protected environment anywhere they wanted or needed to be.
- Since the system was simple, easy and convenient to deploy and use, the bank didn't spend a lot in integrating the chosen solution with its existing international network infrastructure. Easy maintenance also meant less calls to technical support.
- Scalability and simplicity also lessened the need for technical training that could otherwise impact the bank employee's workflow and performance.
- Maverick LLC's strong support position was an added bonus.

About Maverick Secure LLC

Maverick provides multi-factor authentication solutions to safeguard confidential digital records and data. It is applicable to industries including technology, Internet, healthcare, education, financial services, government, military and subscription services. Maverick's strong multi-factor authentication processes are your solution when passwords just aren't enough to protect your sensitive data from unauthorized users and hackers.

The Maverick brand is dedicated to providing the business community with a high quality and affordable alternative to the pre-existing/overpriced offerings currently available in the market. By providing user-friendly, scalable and seamless compatible technologies, our products match and very often exceed our competitors' products while remaining price sensitive, affordable and much greater offering value for money.

Maverick offers stronger security by leveraging the industry's leading multi-factor authentication processes in very unique and efficient out-of-band channel methods. By living up to its name, Maverick takes a unique "out of the box" strategic perspective in protecting our clients from the threats that surround us in this constantly evolving security-vulnerable world. Maverick provides an easy-to-use approach for users while providing the highest level of security as an overlay to existing business applications and systems.

The Maverick brand started out as Maverick Computers and was named as "One of the fastest growing computer companies in North America," "#1 Solution Provider" and the "#1 System Builder in North America based on growth (2004)," and "Server Innovation Award" by CRN Magazine for developing a virtually indestructible server. The company then launched a new sister company called Maverick Communications which was awarded "2005 North American System Builder Association – Business Innovation of the Year" for creating an integrated array of video, voice and data services that included what was then the world's fastest Internet access for consumers at 45mbps. Over the past five years a new division of the Maverick brand, Maverick Secure LLC., was launched to combat the ever-evolving and tenacious attacks of hackers such unauthorized access of data and the multitude of other security breaches have caused serious turmoil within the computer and associated industries. In 2009 Maverick partnered with IBM, the number one server company in the world for enterprise users, to develop the "Maverick SMART Server Powered by IBM." By utilizing the award winning hardware of Maverick Computers, the industry's leading authentication process of Maverick Secure and the online and business applications of IBM, Maverick is now positioned to deliver end-to-end solutions for businesses small and large. We believe we have brought together the perfect harmony of leading technologies to offer one of the most secure solutions that addresses issues related to password authentication.

Contact Us

To learn more about how 4-Factor Authentication products, services, and solutions help solve your business and IT challenges contact your local representative or authorized reseller

Patrick McNicholas
President
Maverick Secure, LLC.
Patrick@MaverickSecure.com
www.MaverickSecure.com
772-216-9535 (Cell)
888-266-1678 (Toll-Free)
305-600-0772 (Miami)
917-470-9469 (New York)
415-424-4245 (San Francisco)
020-337-174-11 (London)
888-219-0113 (Fax)
GoToMaverick (SKYPE)

Maverick helps organizations secure and manage their information-driven world with security management, endpoint security, messaging security, and application security solutions.

Copyright © 2012 MaverickSecure.com.
All rights reserved.