

# maverick™

## 4-F™ Authentication in an EDUCATIONAL INSTITUTION



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



# maverick™

TOLL FREE / 888-266-1678 WEB / [www.MaverickSecure.com](http://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 sizes are 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

<b>Education Scenario</b>	<b>1</b>
<b>Welcome</b>	<b>2</b>
<b>Contents</b>	<b>3</b>
<b>Introduction</b>	<b>3</b>
<b>Case Scenario</b>	<b>5</b>
<b>The Challenge</b>	<b>5</b>
<b>Key Requirements</b>	<b>5</b>
<b>Maverick Solution</b>	<b>5</b>
<b>Implementation</b>	<b>6</b>
<b>Results</b>	<b>6</b>
<b>About Maverick Secure LLC</b>	<b>7</b>

### Introduction

Increasingly, online education makes network security more important than ever. Schools are an attractive target for cyber attackers because the culture of sharing in academic settings slows down the adaptation of a strong authentication system.

### Case Scenario

A private elementary establishment wanted to grant its teachers remote access to the school network for productivity, efficiency and cost reduction. The School's existing password system was deemed unacceptable by today's stricter network security standards. Accordingly, school management evaluated vendors and technologies most suited to their needs.

### The Challenge

Coming up with a simple, easy-to-use, and affordable authentication system, without impacting teachers' workflow and pupil performance, was a big challenge for the school

### Key Requirements

- Strong authentication – Depending on a teacher's access privileges, the authentication factors required could go from two to four; never username and password alone;
- Easy to use – Teachers' work shouldn't be impacted by the new authentication system;
- Easy to implement and manage

### Maverick Solution

The Maverick 4-F™ Authentication System fit the school's needs and also was able to assist in the financial bottomline by keeping budgetary costs under control.

### Implementation

Implementation was fast and non-intrusive, thanks to teacher cooperation and existing networking skills

### Results

- Data Protection and Peace of Mind
- No Impact on Faculty Workflow
- Easier IT Management

### 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.

## Making learning and school networks more secure with Maverick 4-F™ Authentication System

### At-A-Glance

#### Key Requirements

- Strong authentication – Depending on a teacher's access privileges, the authentication factors required could go from two to four; never username and password alone;
- Easy to use – Teachers' work shouldn't be impacted by the new authentication system;
- Easy to implement and manage – Deployment should be fast to avoid burdening the teachers further, since pupil examinations and performance evaluations were fast approaching.

#### Solution

- Maverick 4-F™, considered a breakthrough 4-factor password system. Combines smart Public Key Infrastructure (PKI) capabilities with one-time passwords (OTPs). Maverick 4-F™ is compatible with a wide range of encryption, authentication, and access gateway solutions that meet government requirements.

#### Results

- Data Protection and Peace of Mind
- No Impact on Faculty Workflow
- Easier IT Management

### Introduction

Like many institutions, schools have benefited from the Internet and the accompanying technologies associated with it. As a result of social networking, school staff have now a vast teaching resource at their fingertips. They also have the ability to connect to their school data remotely. This makes it easier to transmit grade computations, reports, lesson plans, assessments and even academic requirements from the comfort of their homes. On the administrators' part, they can easily manage enrollment, employee records and other administrative processes. This has spurred more demand for online connectivity in many educational institutions.

As schools increasingly become more wired and networked and their data migrates from paper records to electronic records, the more vulnerable—and valuable—the data becomes. These data includes sensitive personally identifiable information about parents, pupils/students, teachers, and school administrators—for example think of names, grades, salaries, loans, strategic business plans, addresses, workplaces, phone numbers, and school medical records. Exposure or theft of any of these would terribly damage a school's reputation and expose it to multiple legal ramifications.

Previously, the greatest enemy of school records were the elements, e.g. rodents, burglars, flood, etc. Nowadays, the danger is from fraudsters and hackers who profit from any information they can get from electronic records databases they manage to breach.

Consequently it should be a priority for schools to safeguard access to their records. School constituents can do this by creating a strongly protected e-records department, administered by vigilant IT staff that are aware that the key to keeping one step ahead of cyber-criminals is to acquire a strong, regularly updated data security and access authentication system.

Fortunately, governments have begun laying down data security regulations and technical standards to follow to keep everyone's data more secure.



In the UK., there is the Data Protection Act of 1998, while the U.S. and other countries also have legislated similar data protection requirements.

Not too long ago, a simple username and password combination was enough to secure a computer network from unauthorized access. This was called single-factor authentication. Now, with criminals organizing and continually developing newer and more sophisticated methods of attack, single-factor authentication is no longer enough. Depending on the severity of the consequences of security breaches, some network access and transactions may need two or more factors of authentication.

Traditionally, there were three recognition factors of authentication:

1. **Something You Know** – Username and password;
2. **Something You Have** – A physical object the presence of which is necessary for authentication—like ATM cards, security badges, or tokens; and
3. **Something You Are** – Natural characteristics of a person, like fingerprints, voice-prints, retina patterns, and the like.

Now a fourth factor is being proposed, **Somewhere You Are** i.e., location. This means, if you are using your credit card in a certain location, a bank will make sure you are really there through the use of high-tech processes. This serves to facilitate cross-country processing and decrease the incidence of fraud. A transaction level of security is directly proportional to the quality and quantity of factors used in authentication. It is also linked with cost and administrative overhead but not all transactions require such heavily armored authentication.

Ideally, a security authentication system will adjust the number of its authentication requirements depending on the assessed severity of consequences and the access level of the one being authenticated. In the U.S., the National Institute of Standards and Technology (NIST) define four "Assurance Levels" in authentication. The higher the Assurance Level required for a transaction, the more stringent are the authentication requirements (and the more threats the authentication can prevent). In Europe, the European Network and Information Security Agency (ENISA) also has a four-level assurance scheme.

### The Challenge

The challenge was the deployment of the new authentication system which needed to be simple and seamless as the teachers were starting to get busier with the annual examinations, performance evaluations and assessments. Any further toll on their time could impact the school's standing and rating.

### Key Requirements

- **Strong authentication** – Depending on a teacher's access privileges, the authentication factors required could go from two to four; never just the username and password alone;
- **Easy to use** – Teachers' work could not be impacted by the new authentication system;
- **Easy to implement and manage** – Deployment needed to be fast to avoid burdening the teachers further, since pupil examinations and performance evaluations were fast approaching.

### Case Scenario

A high-end private elementary establishment wanted to provide its teachers remote access to the school network. The primary purpose was to allow the teachers the capability to work on marking pupil submissions, reports, and assessments etc., from the convenience of their homes or anywhere they had an Internet connection. This was aimed to increase teacher productivity and efficiency, and ultimately, lower school costs.

However, the school's IT-department convinced management that they should first implement a stronger authentication system before allowing teachers the capability to remote access into the school's LAN. They realized that just assigning usernames and passwords for these teachers was insufficient and security against unauthorized access was required.

The school management then evaluated vendor solutions that would meet their requirements for a stronger authentication solution.

### Maverick Solution

After reviewing solutions offered by several well-respected vendors in the rapidly developing authentication market, the school management chose the solution by **Maverick Secure LLC**, the **Maverick 4-F™**, considered a **breakthrough 4-factor password system**.

The **Maverick 4-F™** is a hybrid security token solution that combines driverless smart Public Key Infrastructure capabilities with short-lived (30 to 60-second) one-time passwords (OTPs) automatically generated at regular intervals.

To protect important data, the security token is compatible with a wide range of encryption, authentication, and access gateway solutions—meeting government requirements. The **Maverick 4-F™**'s PKI capabilities ensure encrypted certificates continuously validate the identity of the user (and the server) while on the department LAN or VPN during a remote session.



## Implementation

With 3 months to go before pupil examinations, the school IT staff had to deploy the new authentication solution within record time. Fortunately, all that was needed for deployment was to have the teachers sign off for their individually registered **Maverick 4-F™** authenticator at the faculty room and activate it through the school's LAN. The faculty could then start using the new authenticator remotely from their homes. The sign off took just two weeks. The IT staff formed a small team to handle any issues called in by the teachers. **There were none.** The calls they received were mostly how to access the school's portal to initiate the remote connection.

Overall, the deployment went without a hitch. The school was rewarded three months later when the results of the pupil examinations and faculty performance evaluations went beyond their expectations.

## Results

### 1. Data Protection and Peace of Mind

The school was directly able to benefit from the added productivity and efficiency of their remotely connected faculty who were secured from intrusion due to their new **Maverick 4-F™** authentication system.

### 2. No Impact on Faculty Workflow

Since the authentication system was easy to set-up and integrate with the school's current LAN, keying in the OTP after the username and password was just a breeze for the faculty. And, since the **Maverick 4-F™** had PKI capabilities, the identities of both user and server were both verified and continuously checked while the faculty was remotely connected to the school via VPN.

### 3. Easier IT Management

Through the web-based configuration and management tool, the school's IT staff were able to deploy access policies and permissions to each authenticator, revoking or changing permissions as and when required. This easily integrated with their anomaly detection systems so they could monitor for unusual access activities and patterns. Authentication requirements could also be changed on the fly, depending on the remotely connected faculty's level of access and operation he or she was trying to do.

## Summary

The school was pleased with their decision to go for the **Maverick 4-F™** hybrid authenticator solution in solving their network security authentication needs. Not only did the **Maverick 4-F™** satisfy every requirement, it's competitive price was well within the school's budget, plus the level of professional support was on par with the bigger players in the fast growing security authentication market.

Maverick LLC in 2007 reached an agreement with IBM in 2009 for extending and developing IBM-powered Maverick SMART Servers with accompanying business productivity software. Now the newly formed Maverick Secure, LLC addresses the critical needs of the rapidly developing authentication market.

## 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 please contact your local representative or authorized reseller.

### **Patrick McNicholas**

President

Maverick Secure, LLC.

[Patrick@MaverickSecure.com](mailto:Patrick@MaverickSecure.com)

[www.MaverickSecure.com](http://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](http://MaverickSecure.com)  
All rights reserved.