Using Certificate-based Authentication for Access Control

GLOBALSIGN WHITE PAPER

John Harris for GlobalSign

CONTENTS

INTRODUCTION

Organizations which for so long had only to focus on firewalls and virus scanners at the periphery of their network are now having to deal with customer data transiting to the cloud, employees bringing their mobile devices to work (and expecting them to be accepted) and hackers looking to score the next big information leak or credit card database.

All of these present significant challenges to the information security professional, who was already pressured into doing more with less. Information security demands answers to questions such as these:

- With so many threats and technologies being offered to address those threats, how do I know which I should prioritize and which solutions are best for my organization?
- How do I create a strategy that helps me meet my compliance goals, but also leaves my organization protected against unforeseen challenges?
- Can one product, or suite of products, help me comply with key regulations and also mitigate against a host of potential threats across my organization?
- What technologies do I need to invest in that are easy for my users to use, cost effective and also security-effective?

This white paper will assist organizations in crafting the right approach, beginning with a best practices-based information security strategy. The paper will then demonstrate how investing in certificate-based network authentication can be a powerful first step towards a safer, more agile business.

The paper will explain certificate-based network authentication, how it works and how it compares to other leading identity and access management solutions. This will be followed up with benefits to your organization and how you can take advantage of this technology.

FINDING THE RIGHT PATH

Achieving true information security for an organization has become a fluid target. Information security professionals must adapt to ever-changing conditions to meet client and business requirements like uptime and system stability, legal regulations for protecting potentially identifiable information (PII) and audit requirements for continuity in the face of natural disasters or terrorist attacks. Moreover, users and management need to be kept happy on a slimmer budget. It's not easy.

Facing this deluge of responsibilities, it's not surprising then that best practices get shoved aside in lieu of simply responding, firefighting-style, to needs as they present themselves. Rather than stepping back to get a bigger picture of how their work can benefit and protect the organization in the long run, information security professionals choose solutions that have immediate impact (or at least can be perceived to have an immediate impact) on a specific threat or compliance target. Problematically, these short-term fixes may fail to address broader problems or other regulations in the long run.

"Only 52% of information security executives have a documented security strategy."

-Global Information Security Survey 2011
Ernst & Young

The reactive approach can be appealing because (1) it's far easier to do and (2) shows responsiveness to management, who can at times, be focused on the short term in budgeting negotiations. However, pursuing information security in this fashion will force your organization to spend more money overall, wasting employee time and in the end, lowering potential revenues due to constant changes in infrastructure.

For example, a company faced with complying with the security provisions of the Health Insurance Portability and Accountability Act (HIPAA) may simply reach out to vendors claiming to have 'HIPAA-

compliant' products and then acquire and implement those technologies to meet the requirements imposed by HIPAA. What's missing in that discussion is how those technologies could be applied to the organization's other compliance requirements or how they address emerging dangers such as the Advanced Persistent Threat (APT).

It's possible the organization will need to throw out or completely retool that initial purchase because of a lack of vision for what was around the corner. This is borne out by Ernst & Young's Global Information Security Survey 2011 which showed that 31% of respondents invested in hardware or software in the past 18 months that had failed or under-delivered.

"31% of information security executives invested in hardware or software in the past 18 months that had failed or under-delivered."

- Global Information Security Survey 2011
Ernst & Young

This approach can also lead to a misplaced confidence in an organization's actual information security stance. According to Price Waterhouse Cooper's 2012 Global State of Information Security survey, over 70% of respondents marked themselves as confident in the effectiveness of their systems, but only 37% of those polled actually had a security strategy for mobile devices, arguably one of the most significant challenges facing IT departments. And when it came down to it, only 52% of those polled in the Ernst & Young survey actually had a documented security strategy.

If an organization's 'strategy' is to simply react to threats and requirements as they present themselves, that organization becomes a pinball, bouncing between threats and regulations. Organizations need to spend time developing and then implementing a security policy that relies on top level best practices, such as user authentication, network intrusion detection and prevention, business continuity and disaster preparedness, employee education and training, malware detection and prevention, data loss prevention (DLP) and encryption.

This strategy and security policy must also articulate those best practices in such a way that the needs of the business are foremost. This includes being sure that users are not overly burdened. Unhappy users, partners, or customers who have to contend with controls that are unsuited to the task at hand or are overly complex will tend to slow down the business, making an organization less agile and less productive.

Crafting a broad-reaching, best practices-based strategy is the first, most critical step. Organizations must next choose hardware and software that meet the strategy's goals. These technologies should be highly interoperable, mitigate a variety of threats, meet business needs across the organization, achieve compliance with existing and potential regulations and not place undue burden on users and systems already in place.

Access control and identity management is a key technology area within a best practices-based security regime. Certificate-based network authentication is a good example of a solution that's easy to implement, simple for users, meets requirements and can address challenges on the desktop, on mobile devices and even in the cloud.

CERTICATE-BASED NETWORK AUTHENTICATION

What is it?

Certificate-based network authentication is the use of a Digital Certificate (credential) to identify a user and often a device (or devices) employed by a known user on the network and is oftentimes deployed in coordination with traditional user authentication methods such as username and password.

By itself, certificate-based network authentication can verify that devices connected to the organization's network are those that are authorized. When combined with user authentication, organizations can clearly verify that user A logged on with laptop PC B and can make a determination if in fact that laptop is registered to

user A. If yes, the user can be granted access to the network on that device.

The Digital Certificates used are the same as any other Digital Certificate you might already be using within your organization for secure web services (SSL) or email/document signatures (digital signatures). However, in this case, as opposed to the certificates being assigned to a specific web server or person, they are assigned to a specific device.

How does it all work?

First, an administrator needs to generate and assign certificates to devices in their organization. This is typically done via a certificate management portal or web-based front end to a managed service.

The administrator configures his user directory and network security systems to trust specific users and devices for authentication by importing the Digital Certificates of the users and/or devices in question. The devices are also configured with the servers' certificates.

When a user wishes to log onto the network, an access request is sent from the device to the network. Messages are encrypted, sent, decrypted and sent back between device and server. This handshaking process continues between device and server until both are satisfied that the messages each sent have been correctly decrypted and the credentials are sound.

Mutual authentication ensures that the device is connecting to the server it expects (as only that server could decrypt the message with its credentials) and the server can also verify that the correct device is connecting (as only that device could decrypt the message with its credentials).

Once confirmed, the server could allow the device access, or request additional user authentication methods depending on the data being accessed or network being traversed.

What can users expect?

Impact on users is minimal to none. Certificate deployment is relatively mature in most operating systems today, so in general users will likely not need to do anything. They will continue to authenticate to the network as they always have, using logon credentials. Meanwhile, transparently, their identities and devices will be authenticated with strong certificate-based credentials.

Certificate-based network authentication does require that the device is kept secure so that the credential cannot be removed or copied.

How does it stack up to other authentication methods?

Authentication is typically described in 'factors': something you know (a password), something you have (a physical token), or something you are (your fingerprint). Single factor authentication tends to be the norm, but relying on only one factor provides a single point of failure for your network and systems that can at times be easily defeated by phishing and other attacks.

When various factors of authentication are combined, they provide multiple layers of defense that make a system much more difficult to breach. Tossing a bunch of factors together doesn't mean your organization will suddenly be more secure, however. Organizations need to consider user impact, the risks involved and other aspects.

Since certificate-based network authentication can be implemented with no burden on users, multifactor authentication is as easy as your users logging in with their own usernames and passwords on their assigned devices. For example, device Digital Certificates represent 'something you have' and the device becomes part of the authentication alongside a user's name and password ('something you know').

This is not necessarily the case with other forms of authentication, which may require users to carry additional physical devices or require them to go through more steps. How do these other authentication methods stack up?

Other authentication methods

- **One-time password (OTP) tokens** are traditionally physical tokens that are carried by a user and feature a small screen that displays a random number generated by the device. The user enters this number alongside a PIN code, often in addition to his or her password, when logging in. This additional PIN prevents someone from simply stealing the token itself. These devices satisfy the 'something you have' factor, but because they are another device the user has to account for, they can be lost, preventing a user from logging in at critical times. OTP solutions are now available as apps running on a user's mobile device, but this still requires that the user have that mobile device handy (and charged) whenever they need to log in. It's also not as easy to switch between apps when you're trying to log into another app on the same mobile device

- **SMS** authentication relies on the availability of a user's mobile device to add a second factor. SMS-based systems send a text message to the user's mobile phone after they log in with their username and password. The user then enters that SMS message when prompted. Like mobile- based OTP, however, this system requires the user have access to their mobile phone when logging in and may not be convenient for logging into other mobile apps

- **Out-of-Band** authentication relies on the proximity of a user to their mobile phone or another phone. In this approach, during authentication, the user receives a call on their mobile or landline and is asked to dial in a number or repeat a small, set phrase. Based on his or her response, the system allows access. Because out-of-band authentication requires the user to take a call, it may be disruptive to the workplace or impossible given the user's location (out of coverage area, etc.)

- **Smart card / USB tokens bearing Digital Certificates** that identify the user can provide multiple factors of authentication simultaneously, by requiring the possession of the card or token, the password to unlock the card's multiple certificates (often ones for both the card and the user) and even biometric authentication (see below). Smart cards can also be personalized to include a user's picture, name and affiliation, serving not only as logical authentication (network login), but also physical access to a building. This is one of the more secure forms of authentication available today, but it comes at a price. The user must physically carry this card or token with them and present it when they login. A smart card often requires an additional reader device. Both smart cards and tokens are difficult to use on mobile devices as they do not commonly feature a reader or full-size USB port, though there are some 'sleds' available that can plug into a mobile device and allow the user to plug in their card

- **Biometric** authentication represents the third factor of authentication: something you are, such as your fingerprint, face, iris or even handwritten signature. Even more exotic forms of biometrics exist, such as vein structure. Obviously, it's quite difficult (but not impossible) to replicate these features. However, there are three key problems with biometric authentication

    - Availability of sensors on devices the user needs to access – A user's laptop may have a built-in fingerprint sensor, but her tablet does not. Even when similar sensors do exist (i.e. webcams and front-facing cameras on mobile devices), they may not be sensitive enough for biometrics such as face recognition

    - Environment in which the user is capturing the biometric – The user's hand may be in a glove when he needs to scan his finger, or in a dark place when he needs to scan his face

    - Privacy - Users may not be comfortable providing their finger or face to these devices

Comparing authentication methods

Authentication Method	Requires Additional Physical Device	Requires User's Mobile Phone	Extra Step for User?	Security versus certificate-based network authentication
Certificate-based Network Authentication	NO	NO	NO	--
Username and password	NO	NO	NO	
One-time passwords[1]	YES	MAYBE	YES	=
SMS	NO	YES	YES	=
Out-of-band	NO	YES	YES	=
Smart card / USB tokens	YES	NO	YES	+
Biometrics[2]	MAYBE	NO	MAYBE	+

HOW CERTIFICATE-BASED NETWORK AUTHENTICATION MEETS ORGANIZATIONAL NEEDS

Organizations need to be focused on security strategies that meet their business requirements for agility and revenue, while at the same time properly securing their data, intellectual property and systems against the risks inherent in a dynamic environment. To implement that strategy, organizations must invest in technologies that can effectively address security needs across the company, mitigate broad risks and assist in complying with the variety of regulatory imperatives facing today's businesses. Certificate-based network authentication has been shown to provide multifactor authentication without imposing burdens on an organization's user population: more security doesn't have to mean less agility.

Access management, auditing and forensic analysis of access history are improved, as data and network access can be tied not only to a user, but also to a specific device at a specific time.

Mobile devices are redefining the way in which consumers and employees are accessing content.

The demand to use smart phones and tablets in the office and on the road imposes challenges on security. While many authentication methods do not easily traverse the 'platform barrier,' certificates can be easily deployed to both desktop PCs and mobile devices, allowing a single investment to be used across multiple platforms.

Certificate-based network authentication can also be an effective tool in helping organizations comply with the authentication and access management requirements of key regulatory regimes.

Key regulations

Health Insurance Portability and Accountability Act (HIPAA)

Signed into law in 1996, HIPAA provided new rules for health insurance and electronic health records. The security and privacy of those records was a key provision, published as the 'Security Rule' in 2003.

HIPAA prescribes a wide variety of administrative, technical and physical controls to be implemented by any organization storing health care information including health care providers and insurance companies. While these controls are described at a

[1] OTP 'software' tokens can run on a mobile device, eliminating the need for users to carry a 3rd device.

[2] Biometrics may require an additional reader device (i.e. fingerprint scanner). They can also be used as the sole authentication method, but this still brings the authentication process down to a single factor. Biometrics can be substantially more secure, but should still be used as part of a layered process.

technology-agnostic level, the range and type of controls fit well into the best- practices model described earlier in this paper.

In regards to authentication, the Security Rule specifically requires organizations to implement authentication to access protected health information. Certificate-based network authentication can easily meet this requirement.

Access authorization is also required. Organizations must "implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism."[3] Certificates could be leveraged to ensure authorized users access patient records from specific PCs in protected areas, or within restricted parts of the network, as opposed to just any workstation in the building.

Payment Card Industry Data Security Standard (PCI DSS)

The payment card industry responded to credit card fraud risk and losses by authoring a highly detailed list of data security requirements for merchants, financial institutions, card vendors and other associated firms. First published in 2004, the PCI Data Security Standard has now been updated to version 2.0.

PCI DSS includes specific provisions regarding strong access control procedures. Organizations must use at least one factor of authentication (something you know, have or are) for general access and use two-factor authentication for remote access to networks. The transparent nature of certificate-based network authentication makes it well-suited to assisting in compliance with this aspect of PCI DSS.

Federal Finance Institutions Examination Council (FFIEC) Authentication Guidance

The FFIEC published rules in 2001 to better protect online banking customers against internet-based threats by requiring financial institutions to implement stronger user authentication measures. In 2005, it followed up with an updated guidance, "Authentication in an Internet Banking Environment." This document clearly stated that the FFIEC "consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties." Specifically, the FFIEC suggests "financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate assessed risks." In line with what this paper has presented as a best practice, the FFIEC continues:

> *The success of a particular authentication method depends on more than the technology. It also depends on appropriate policies, procedures and controls. An effective authentication method should have customer acceptance, reliable performance, scalability to accommodate growth and interoperability with existing systems and future plans.*

Because certificate-based network authentication imposes no burden on users and can be used on desktop PCs as well as mobile devices, it meets these tests of customer acceptance, scalability and interoperability.

In fact, the Appendix to the guidance praises "Digital Certificate authentication as generally being considered one of the stronger authentication technologies, because mutual authentication between the client and the server provides a defense against phishing and similar attacks."

CONCLUSION

IT departments face innumerable challenges in their mission to protect their organization, its data and its customers, while also achieving compliance with multiple regulations. The optimal approach requires an organization to step back from day-to-day reactive actions and assess the needs of the business and the broader, longer-term security goals of the organization. Following formal documentation and periodic review of those requirements, the

[3] HIPAA, 45 CFR Part 164.308(a)(4)(2)(B).

organization should choose technologies that can best be leveraged to meet those goals. A best practices-based model guarantees that an organization can remain agile and secure simultaneously. Certificate-based network authentication is a technology investment that keeps users productive while also improving security posture. This solution is easy to deploy and can enhance authentication practices on desktops and mobile devices. It is also superior to other authentication methods as it provides multifactor security without requiring users to carry an additional device or restrict their logins to specific locations.

No matter the compliance target or industry, certificate- based network authentication meets the needs for multifactor, strong authentication while keeping the technology easily accessible, dynamic and mobile.

It's clear that certificate-based network authentication can be a valuable part of a comprehensive information security strategy and process.

HOW CAN GLOBALSIGN HELP?

Now that you've learned about the benefits and capabilities of certificate-based network authentication, why not implement it? GlobalSign, a worldwide leader in information security solutions, can provide your organization with the tools and talent to put this solution into place. Using their web-based management platform known as Enterprise PKI (EPKI), GlobalSign allows you to easily manage the lifecycle of multiple Digital Certificates for the entire organization. In fact, GlobalSign offers several products and services that can accelerate your company's implementation of a best practices-focused information security strategy.

GlobalSign's product portfolio

- SSL Certificates for protecting websites and promoting secure electronic commerce
- Authentication Certificates for accessing cloud services such as Google Apps and Microsoft SharePoint
- Individual and organizational Digital Certificates for protecting the integrity and authenticity of documents and email messages via digital signatures and certification
- Code Signing Certificates to protect the integrity of software code and applications distributed via the Internet

Why choose GlobalSign?

- History of security innovation and trust: Over 20 million certificates worldwide rely on the public trust provided by the GlobalSign Root Certificate. The company has been operating a trusted PKI since 1996 and has been WebTrust-compliant for over 12 years
- Commitment to customer support excellence: Talk to real people when you call GlobalSign
- Worldwide presence: With technical support offices located around the world, you can expect quicker response times and solutions tuned for your language, region and country

INQUIRE ABOUT OUR AUTHENTICATION SOLUTIONS

Call or email GlobalSign today to speak with a specialist who will help guide your organization towards a best practices-based strategy and provide you with the tools to implement it. Alternatively for more information visit: https://www.globalsign.com/authentication/

ABOUT GLOBALSIGN

GlobalSign was one of the first Certificate Authorities and has been providing digital credentialing services since 1996. It operates multi-lingual sales and technical support offices in London, Brussels, Boston, Tokyo and Shanghai.

GlobalSign has a rich history of investors, including ING Bank and Vodafone. Now part of a GMO Internet Inc. group company - a public company quoted on the prestigious Tokyo Stock Exchange (TSE: 9449) whose shareholders include Yahoo! Japan, Morgan Stanley and Credit Suisse First Boston.

As a leader in public trust services, GlobalSign Certificates are trusted by all popular Browsers, Operating Systems, Devices & Applications and include SSL, Code Signing, Document Signing, Email & Authentication, Enterprise Digital Solutions, Internal PKI and Microsoft Certificate Service Root Signing. It's trusted Root Certificates are recognised by all operating systems, all major web browsers, web servers, email clients and Internet applications; as well as all mobile devices.

Accredited to the highest standards

As a WebTrust accredited public Certificate Authority, our core solutions allow our thousands of enterprise customers to conduct secure online transactions and data submission and provide tamper-proof distributable code as well as being able to bind identities to Digital Certificates for S/MIME email encryption and remote two factor authentication, such as SSL VPNs.

GlobalSign Americas Tel: 1-877-775-4562 www.globalsign.com sales-us@globalsign.com	**GlobalSign EU** Tel: +32 16 891900 www.globalsign.eu sales@globalsign.com	**GlobalSign UK** Tel: +44 1622 766766 www.globalsign.co.uk sales@globalsign.com
GlobalSign FR Tel: +33 1 82 88 01 24 www.globalsign.fr ventes@globalsign.com	**GlobalSign DE** Tel: +49 30 8878 9310 www.globalsign.de verkauf@globalsign.com	**GlobalSign NL** Tel: +31 20 8908021 www.globalsign.nl verkoop@globalsign.com