HOW TO FAST-TRACK COST-EFFECTIVE PKI-BASED 2FA IN A WINDOWS ENVIRONMENT

INTRODUCTION

The strength of Public Key Infrastructure (PKI) security principals are well established, but so too is the misconception that deploying them within a corporate environment is likely to be complex and costly.

Implementing PKI-based network logon security in an organisation can leverage the smartcard authentication infrastructure that has long been built-in to successive generations of Microsoft operating systems[2] and used by government agencies and large corporates world-wide to provide a cost effective, standardised and highly secure solution.

So, while the underlying cryptographic methods used are indeed complex, assembling the technical components needed into a secure, working system doesn't need to be. The challenge has been knowing just what additional software is and isn't required, where it can be found, and choosing the appropriate mix of off-the-shelf hardware.

To remove implementation barriers Dot Origin has put together a supported 'Proof of Concept' kit that enables IT professionals to try-out secure smartcard-based user authentication in their own Windows environment, at minimal cost and with typically just a few hours of set-up time. Once proven, it can be easily scaled to cover many users, and other related applications.

WHY SMARTCARDS

A fundamental benefit of the standards-based smartcard logon approach is that it relies on asymmetric cryptography, where the encryption algorithms use two different keys, one private and one public. The private key is generated by (and never leaves) the smartcard, so there is no risk of it being stolen.

Smartcard chips from manufacturers such as NXP and Infineon include tamper-proof countermeasures that prevent encryption keys and PINs from being accessed (even with the aid of an electron microscope!), thereby achieving certification to the highest security standards, such as Common Criteria EAL 5+ and FIPS 140-2.

Smartcards and the digital certificates stored on them can also very easily be used for a wide range of encryption applications, including email and file encryption, in addition to identity and access management functions.

By including RFID capabilities in the same card, smartcard use can be extended to contactless applications as well, such as secure print-release, cashless vending and building access. This provides users with a single convenient form of ID for just about everything, enterprise-wide, whilst rationalising identity management costs overall.

Whatever means of identity authentication is used, organisations commonly require their staff to carry a standard company ID card that bears a photo of the user and is worn to support site security. By their nature, smartcards lend themselves to this additional purpose and avoid burdening users with additional forms of identification.

OTHER ALTERNATIVES

Mobiles devices can host various app and cloud-based implementations of cryptographic algorithms to support 2FA, and depending on the device and OS these may be able to provide protection measures to defend private key information against acquisition by malware.

Like smartcards, mobile credentials can be used for other corporate identity and access applications; thanks to increasing numbers of solutions becoming available, although these may not always be possible to integrate together.

Perhaps the biggest barrier to mobile credential adoption currently is the far greater cost in comparison to well-established and reliable smartcard solutions. The complexity of managing and maintaining multiple apps and device platforms over time, as well as upgrading other systems such as security gateways and

door access readers can also detract from the financial viability of these solutions.

While there's nothing intrinsically wrong with one time password (OTP) technology, especially when based on the widely implemented OATH standards, there is a major weakness in most OTP systems, because they normally rely on sharing 'seed' encryption keys between multiple parties. This risk primarily stems from vulnerabilities in the manner by which these keys are stored and shared, such as via QR codes or email, and the fact that the producer and distributors may also have access to this critical information.

Virtual smartcards are a relatively recent development that enable the benefits of PKI-based authentication to be implemented using built-in TPM chips that are included in most PCs. Whilst technically effective, this removes the second factor benefit of having a removable hardware device (the smartcard) as well as the PIN, and can cause additional recovery issues if the PC is lost or stolen.

> ***81% of hacking-related breaches leverage either stolen, default, or weak passwords[1]***
>
> Protecting a company's network from unwanted access requires something far more secure than user names and passwords –
>
> 2-Factor Authentication

STRAIGHTFORWARD PKI-BASED LOGON IMPLEMENTATION

PKI implementations become complex when there is a need for legally-enforceable trust relationships to be established with third parties and external systems, because this adds onerous requirements for documented processes and policies to be put in place.

To protect a self-contained company network (even if the Windows domain controller is cloud hosted or operating across a hybrid environment) there is generally no need for such trust relationships with outside agents to be established. This makes setting-up the technical elements of a PKI-based solution very straightforward.

The security of the PKI environment that underpins smartcard logon relies on two things:

- The security of the smartcards

As outlined already, smartcards themselves provide superior protection of cryptographic keys by virtue of their secure chip hardware, leveraging the same protections used in payment and mobile SIM cards. Smartcards are also not capable of direct connection to the internet, and changes to their firmware or on-board applications are tightly controlled.

There is a management feature of PKI smartcards that must not be over-looked in order to ensure their overall security. In addition to a user configurable Passcode/PIN (the 'something they know') - used in conjunction with the smartcard (the 'something they posses') to fulfil both elements of 2-factor authentication – each card also has an admin PIN which can be used to reset the user Passcode/PIN or unblock it after several failed logon attempts.

Unfortunately the standard Microsoft tool (Windows Server Certificates plug-in for Microsoft Management Console) used for issuing a smartcard to a user does not include a feature for changing the default admin PIN on the card.

Guidance on several solutions to this issue are provided within the kit from Dot Origin, including free manufacturer tools as well as the use of a suggested Card Management System (CMS) that streamlines card issuance and management tasks, whilst also making it possible to delegate these administrative duties to HR or Security teams.

- The security of the Windows domain architecture

A Certificate Authority (CA) needs to be running on the domain in order generate a trusted digital certificate corresponding to each user's public key.

Usually the Microsoft CA included with Windows Server is perfectly adequate and is easy to install if that has not already been done. The CA uses its own private key(s) in the signing of the certificates that it issues, so these keys must be protected to prevent any false certificates from being created by others.

The best means of safeguarding the CA's private keys involves storing them in a hardware security module (HSM) with an additional offline server to mitigate attacks. While the cost of HSMs has reduced significantly over recent years it is often deemed sufficient to use other physical and practical protections in a corporate environment to avoid this added cost.

Dot Origin provides further advice and assistance on both approaches as needed.

> ***Once these issues are understood, implementation is straightforward, and the basic tools needed to start issuing and using smartcards for logon are all readily available.***

PROOF OF CONCEPT KIT

Pre-requisites

To make use of Microsoft's in-built smartcard logon functionality a full version of Windows Server is required with users and computers on the domain managed via Active Directory (for cloud and hybrid deployments Azure AD Connect is required). Additionally a Certificate Authority, such as Microsoft's free CA application must be running on the domain.

This native Microsoft solution also works in almost all virtualised and thin or zero client environments.

What's included

The kit provides everything needed to implement PKI-based smartcard logon to a Windows domain.

Products from industry leading manufacturers are included to enable different hardware and software options to be evaluated, along with various approaches to managing cards and users prior to a wider deployment.

Hardware includes PKI-enabled security-certified smartcards and a range of USB smartcard reader/writers in desktop and portable form factors, to suit different environmental and ergonomic needs.

Software includes tools to enable card PIN/Passcodes to be changed, certificates to be viewed and other basic tasks, plus documentation, links and suggested CMS software for which a fully-functional and easily-upgradable PoC license is included.

Expert support is on hand from the Dot Origin team to help where needed.

Extending application and integration

By making use of standards-based PKI technology, the same cards, digital certificates and infrastructure can be used for other applications in addition to logon, such as disk encryption, digital signatures and email security.

Additional paid-for software and drivers can be added to extend use to other operating systems (Linux and OSX) and to integrate with third-party applications (using standard PKCS#11 APIs).

Hybrid smartcards can also be supplied, which incorporate popular door access RFID technologies, such as HID Prox, iClass, MIFARE, DESFire, Paxton, EM among others.

CONCLUSION

Public Key Infrastructure defines the 'gold-standard' for identity driven security, with smartcards providing the most secure, reliable and cost-effective means of carrying keys and implementing 'chip and PIN' style 2-factor authentication.

The Dot Origin proof of concept kit has been put together by drawing from their experts' many years of experience in supporting customers through PKI logon implementation projects of all sizes, ranging from 20 users to 20,000. The kit allows IT professionals a fast-track route to evaluating this strong two-factor security solution in their own environment.

ABOUT US

Dot Origin is an independent supplier and developer of identity based security solutions - specialising in two-factor authentication, PKI, smart cards and other credentials, with unique capabilities in unifying and strengthening physical and IT-access controls.

Contact Dot Origin to find out more about Proof of Concept kits, and supply of a wide range of smartcards and readers.

DOT ORIGIN

www.dotorigin.com

Phone
Europe & Asia
+44 (0)1428 685 861
Northern and Latin America
Toll Free: +1 888-262-9642
Direct: +1 562-262-9642

E-mail
info@dotorigin.com

References:

[1] https://www.securityweek.com/compromised-credentials-primary-point-attack-data-breaches

[2] https://technet.microsoft.com/en-us/itpro/windows/keep-secure/smart-card-windows-smart-card-technical-reference