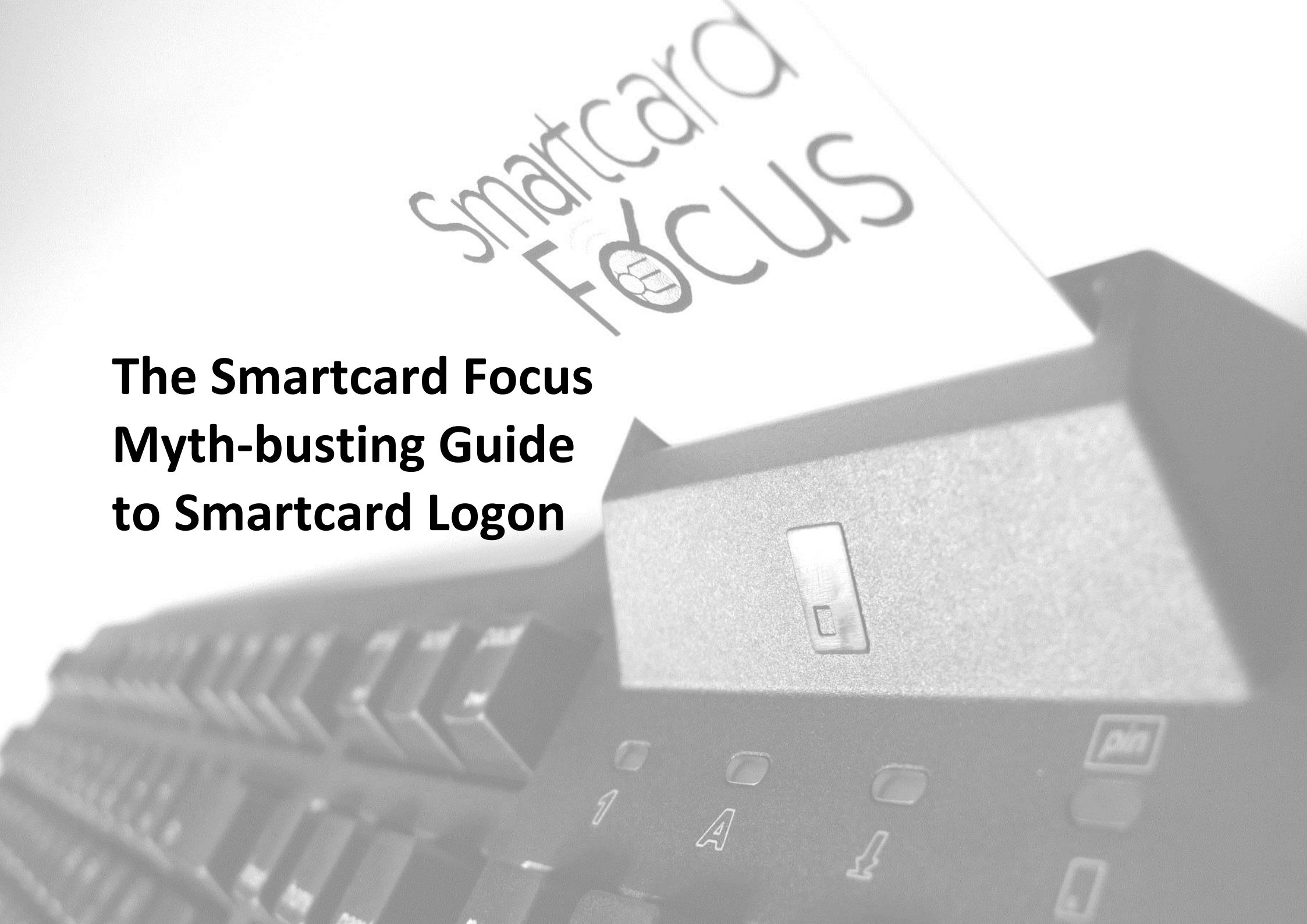

The Smartcard Focus Myth-busting Guide to Smartcard Logon

Introduction

Our customers often ask about using smartcards for secure logon to PCs and laptops. They may have heard about this as the preferred solution for secure two-factor logon, or perhaps seen it in action elsewhere and just want to know more about how it works and what it costs.

This guide sets out the key facts on this topic, and addresses some of the typical queries, misunderstandings and technical issues involved, as well as our recommended approach to implementation.

We have organised this guide around the six most common myths that we hear in our industry:

Myth #1: You need to buy additional software to enable smartcard logon

Myth #2: You need to replicate your password policy for smartcard PINs

Myth #3: Using PKI is difficult, complicated and expensive

Myth #4: Once a card has been issued using the built-in Microsoft tools, it is secure

Myth #5: It is a good idea to use RFID/contactless technology for logon

Myth #6: One time passwords, tokens and mobile apps are just as good as smartcards

Myth #7: It is difficult and expensive to run a smartcard proof of concept

Please read on to get the true facts as we see them!

Myth #1: You need to buy additional software to enable smartcard logon

Fact: Smartcard logon is built into Windows!

Microsoft, along with the smartcard industry, already implemented a highly secure and standardised way to replace Windows usernames and passwords with two factor security based on PKI-capable smartcards. This has been available for many years and is built into Windows as standard.

This doesn't mean that there aren't other ways of doing logon with other types of smartcards, using added software, but the native Microsoft approach is well tested and generally regarded as the most cost-effective and secure solution. This is why it is used by government agencies and large corporates world-wide, and it also makes it pretty certain that it will be supported in future operating system updates.

The use of standardisation also results in lower total cost of ownership, and good interoperability between different systems. And the use of PKI technology means that you can also use the same infrastructure to implement disk encryption, digital signatures and email security, all based upon the same card. In fact, much of this functionality is also already embedded within other products from Microsoft and third parties.

For more technical information, the Microsoft smartcard environment is detailed further here:

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

There are effectively two types of PKI smartcard that can be used within this environment – those that also comply with the Microsoft smartcard 'minidriver' specifications, and those that have their own 'thick' middleware/drivers, known as a CSP. In both cases, additional drivers and tools may also be available from the card vendor, for instance to provide cross-platform PKCS#11 support, although this usually attracts an added cost. We cover this topic in more detail elsewhere.

Pre-requisites

To use the native approach you must be running Windows Server and thus be managing your users and PCs on a domain, via Active Directory. You also need to have a Certificate Authority running on the domain – usually the Microsoft CA that is included with Windows Server works fine, and this is easy to install if not already running.

The server infrastructure can be on-premise or in the cloud, but you will need a full Windows Server running somewhere as a domain controller, rather than just Azure AD, which doesn't yet support this logon method. For hybrid clouds you can link these two parts using Azure AD Connect.

How it works

The Microsoft solution follows best practices regarding the implementation of two-factor security. This results in usernames and passwords being effectively replaced by smartcards and PINs. The smartcard is something the user *has*, and the PIN is something the user *knows*. You cannot implement card-only logon (ie without a PIN) and nor can you implement card + password + PIN. These options are just not available as they don't fit with the technical architecture or the generally-accepted approach to security.

In a nutshell, when a smartcard is first issued to a user, the card itself generates a private key which is stored securely within the chip (only) and can never be accessed directly. The matching public key is sent to the CA, which creates a digital certificate for that user, and this certificate is also then stored on the smartcard. A PIN/passcode is also chosen by the user and stored within the card. Once set, this PIN cannot be read back under any circumstances, but must be submitted to enable access to encryption algorithms that use the private key.

When the user then wants to use the card for logon (or any other secure application) they insert the card into a smartcard reader, and the certificate is read by the PC, identifying them as a domain user. They must then enter their PIN, which is submitted to the card in order to 'unlock' their private key. If the PIN is incorrect, the card will reject the request, and, after a set number of attempts, the card will automatically block itself, just like a bank payment card, thus preventing 'brute force' attacks.

After a correct PIN submission, there is a unique exchange of encrypted data between the card and the server/CA, using Kerberos and PKI, which proves that the card is genuine, at which point the user is logged in to the workstation. Since only the user knows the PIN, and only the card has the private key, we now have a strong two-factor authentication. We can also now leverage the card and key for added functions such as email signing and encryption if desired.

If the card is removed from the reader, Windows can be configured using standard Microsoft Group Policy to either lock the workstation or log the user off completely. This is particularly useful if the card also has a separate RFID chip included for door access, so that the user must remove their card to move around the building.

Myth #2: You need to replicate your password policy for smartcard PINs

Fact: Implementing regular password or PIN change policies reduces security!

Firstly, note that the smartcard 'PIN' is a misnomer – most smartcards actually support alphanumeric PINs, so you can continue to use letters and other characters, rather than just numbers, if you want, and the PIN length can be variable too. Thus many users continue to use a favoured numeric or alphanumeric passcode, although clearly it should not be possible to guess this easily, and it should not be written on the back of the card!

Secondly, one of the reasons that regular password change policies have been adopted is that brute-force attacks on password-based systems are easy. This is not true of smartcards, because the card itself will lock after a small number of incorrect PIN attempts (usually 3 or 5). More recently, it has been established by security professionals that regular password change policies end up causing overall security to go down rather than up, due to human behaviour – people tend to forget, and thus write down, ever-changing passcodes:

https://www.ncsc.gov.uk/articles/problems-forcing-regular-password-expiry

Some smartcards do have useful PIN policy features on board, and this can be used to prevent more easily-guessed codes, such as sequential numbers or letters. They can also enforce minimum PIN lengths and other such requirements, but in general the users should be educated to choose a good PIN/passcode, and to change it whenever they want, to ensure best security. This matches the well-established approach of the banks, for chip-and-PIN cards, as well as the latest official guidance.

Myth #3: Using PKI is difficult, complicated and expensive

Fact: Implementing a trusted PKI that stands up to scrutiny in a court of law is difficult, but implementing the technical elements of a PKI to support smartcard logon is easy!

Strictly, a PKI (or Public Key Infrastructure) implementation involves setting up both the technology components and also complex policies and procedures that can be used to establish legally-binding trust relationships between the systems and people involved. This is why the technology is often involved in national ID cards, driving licenses and government/military ID systems, as well as for creating legally-binding digital signatures on contracts and other documents.

But the same popular PKI encryption algorithms are used every day in the technology world, for example in web server security (SSL/TLS), code signing, corporate WiFi and many other applications. Some of these involve trusted third parties, such as the public CAs that issue SSL certificates, but in other cases the technology can be used in a closed, self-contained environment, without the root of trust being needed.

The security of the PKI environment that underpins smartcard logon relies on two things – the security of the smartcard chips themselves, and the security of the Windows Server/domain architecture and particularly the Certificate Authority's own master private key. Unless you are trying to achieve trust between different organisations, you don't need to work outside of your network/servers, or implement a policy framework - you just need to use some common sense, and select appropriate products to build your solution.

On the chip side, PKI smartcards are manufactured using dedicated secure microcontrollers from well-established chip manufacturers such as NXP or Infineon who specialise in this area. With over 25 years' of past research and development, these chips have countermeasures to prevent the chip from being 'probed' or monitored, thus preventing the secret encryption keys or PINs from being accessed, even in extreme circumstances (such as under an electron microscope!) As such, they are often certified to very high international security standards such as EAL 5+ or FIPS 140-2.

At the server end, a 'proper' PKI implementation should include a hardware device called an HSM to hold the CA private key(s), plus an offline server to mitigate other attacks, but it is often deemed adequate to avoid these added costs in a corporate environment, depending on the other physical and practical protections used, and an assessment of the risks involved. Note that the cost of adding an HSM for 'ultimate' security has reduced from tens of thousands to a few thousand pounds/dollars in recent years, so this is now a viable option if required.

In reality, most of our customers find it easy to follow the available online documentation to set up the necessary server components, and get smartcard logon working within a couple of days. Specialist consultants are also available to advise in more security-conscious situations.

Myth #4: Once a card has been issued using the built-in Microsoft tools, it is secure

Fact: The Microsoft smartcard issuance process leaves the cards INSECURE!

NOTE: This is not a serious issue, unless you ignore it.

The standard tool for issuing a smartcard to a user is the Windows Server Certificates plug-in for MMC. This allows an IT administrator to request a certificate for another user, and to have this generated and installed on a blank smartcard, inserted into a smartcard reader. All of the necessary secure key generation and certificate loading is performed as needed, and the result is a card that can then be used immediately for logon, although the process does involve a lot of mouse clicks per card, and is not particularly well or widely documented.

The problem comes from the fact that blank smartcards generally have two default PINs – the user PIN (typically 0000) and the admin PIN, which is a longer authentication code (eg 48 digit hex for IDPrime cards, also defaulting to all zeros). While the user PIN can be set during issuance (and later changed by the user at logon time) there is no user interface for changing the admin PIN.

The admin PIN is very important though. It is used whenever a card has been blocked by the user, in order to calculate a code to unblock it, and can also be used to reset the user PIN to a new value, if the user PIN has been forgotten. Therefore, with an admin PIN of all zeros, someone can pick up another user's card, re-set their user PIN, and then log on as them!

To prevent this, the admin PIN of every card should be changed to a secret value, and this value stored away securely, just in case it is ever needed for PIN unblock or reset. For a small system implementation, it may be ok to set all of the cards to the same admin PIN, but this does weaken the overall security of the system, especially if the information is leaked or stolen. Best practice, therefore, is to ensure that every card has a unique 'random' admin PIN, and that these are securely stored and managed somehow.

Solutions

The typical solution to the admin PIN problem is to install a smartcard management system, or CMS. This is a third party software package that takes over the responsibility of securely managing the entire lifecycle of the card, from cradle to grave. A typical CMS will provide an easy-to-use alternative to the Microsoft plug-in interface for issuing cards, plus it will randomise the admin PINs, store these safely, and provide various PIN unblock and reset functions. Other CMS features typically include the automatic management of card replacements, certificate renewals, card printing, PIN mailers, self-service unblocking and many others.

Most CMS systems also allow IT administrators to delegate certain functions to non-admins, with secure workflow and audit trails, freeing up their time and enabling a wider deployment across multiple departments and/or sites. Some also provide integration with other systems, for example enabling the provisioning of an RFID-capable smartcard within a compatible physical access control system (PACS).

If the cost of a CMS is prohibitive, then the simple solution is to use vendor-supplied tools to change the admin PINs manually, and to store the data somewhere safe, such as in an encrypted spreadsheet or a PIN-protected memory stick. It is therefore important to ensure that such tools are readily available, and that the facility to change admin PINs and calculate unblock codes are provided as standard, without having to pay for additional software.

Another approach is to ask your supplier (ie Smartcard Focus!) to change the admin PIN on every card supplied. We are happy to do this, and have developed automated tools for this as well as setting custom PIN policies and loading custom applets onto cards, but you have to then bear in mind that we then know some critical information about your network, which you may not be happy about..!

Examples of available smartcard CMS solutions include Microsoft's own Identity Manager suite, which includes a smartcard certificate lifecycle management component, Intercede's MyID, and Versasec's vSEC:CMS.

Myth #5: It is a good idea to use RFID/contactless technology for logon

Fact: It is a bad idea to use RFID/contactless technology for this!

We agree that it would be very nice to use RFID, contactless and/or NFC technology to implement smartcard logon functionality, but the reality is that it either does not work reliably, or it relies on proprietary software and cards that can be very insecure. Let's break this down into a couple of different implementation options:

A. We use a PKI-capable smartcard, which also has a contactless interface. Adding this interface is similar to adding a contactless payment facility to a bank card, so the technology is certainly available. However, there are a number of drawbacks:
   - The number of different PKI-capable smartcards on the market that have this dual-interface facility is much lower, and so choice is reduced and costs are higher;
   - These kind of cards can't easily be combined with other RFID technologies that are used for door access control, follow-me printing and other such applications, so the overall utility of the card is generally reduced;
   - Contactless readers are more expensive than contact smartcard readers (typically 3-4 times), are less portable and use more power;
   - Detecting card removal is less reliable, since there is no physical switch to detect the card leaving, and the card can slide off the reader instead of being held securely;
   - Many laptops and tablets with built-in proximity readers are not actually capable of talking to PKI-capable cards, because they do not have sufficient radio power, and have been optimised for simple NFC tag reading applications only. Drivers for these devices are also notoriously difficult to obtain.
   - There are also other compatibility problems that can creep in between certain cards and readers, which don't occur when using contact smartcards.

B. We use a non-PKI-capable smartcard, such as an existing RFID or MIFARE card, plus a proprietary logon or single-sign-on 'solution':
   - This can be convenient, but these solutions are not designed to be truly secure, and do not use industry accepted approaches to prevent card cloning or replay attacks, unlike the Microsoft Kerberos/PKI solution. Some just use the card chip ID as a 'token' to represent the user and others store a username and password in the card memory;
   - Many RFID and MIFARE Classic cards can be copied and cloned easily. This includes the chip IDs and memory contents. This is a massive problem within the door access technology world, and low cost kits for copying RFID cards are freely available on eBay for £10/$20!

Need we say more?!

Myth #6: One time passwords, tokens and mobile apps are just as good as smartcards

Fact: Even hardware-based OTP tokens have a major weakness - you have to disclose and share the keys

Making this comparison between security technologies is like comparing a Ferrari and a Ford (but without the cost differential!) There is nothing intrinsically wrong with OTP technology, especially when based on the OATH standards, which are widely recognised and implemented across multiple platforms and manufacturers, as well as on mobile (for example in Google's Authenticator app).

However, there is a fundamental drawback with most OTP algorithms, which is that they rely on a single 'seed' key , which is different for each user/security device, and which is used both for generating the unique codes and also for validating them. This is because the algorithms are designed to be quick and easy to implement in hardware and software, and use a mathematical one-way encryption process that relies on both sides knowing this single key.

In reality, this means that the seed keys need to be shared, often between manufacturer and end user, and sometimes with resellers or service operators and often very insecurely, for example being sent by email or worse still encapsulated in a QR code for everyone to see..!

Yes, it's true, not everyone realises that those handy QR codes used for Authenticator-type apps simply contain the secure key that would normally be embedded in a hardware token, in the clear! Not good if someone takes a quick photo, and then logs in to your VPN!!

The fundamental benefit of the standards-based smartcard logon approach is that it relies on asymmetric (or public key) cryptography, where the algorithms use two different keys, one private and one public. The private key never leaves the smartcard and is therefore almost impossible to steal. This two-key encryption concept was first discovered in the 1970s by a pair of mathematicians Diffie and Hellman and commercialised shortly after by another group, Rivest, Shamir and Adleman, resulting in the well-known RSA algorithm and company. More recently, a second generation approach called ECC (elliptic curve cryptography) was discovered by Miller and Koblitz in the 1980s. Systems are slowly migrating to that, although RSA still remains popular.

Of course, you can do any kind of security in software, and any kind in hardware. Mobiles sit somewhere in-between, generally being software-based but with various facilities that try to protect key information from being stolen. This depends on the operating system, the generation of device and various other protections, which are very difficult to establish and measure for effectiveness. So although mobile solutions are convenient, our advice is always to protect the keys to your castle in a separate, secure piece of hardware, and one that is not directly connected to the internet and cannot have its secret key data stolen by any means – ie a smartcard..!

Myth #7: It is difficult and expensive to run a smartcard proof of concept

Fact: Smartcard Focus can help you do this for under £150/$200!

We can supply a simple kit of parts and software tools to help you implement smartcard logon on your own server and domain. We believe that this is the best way to understand the technology and to work out how it will benefit your organisation, rather than listening to a sales pitch or watching a video!

Our Smartcard Logon Proof of Concept kit includes the following items:

- Some recommended PKI-capable smartcards. We may supply just one type, or a mixture to try out. If you have a door access system and/or RFID-enabled printers, we will usually be able to provide additional hybrid cards that you can test on those systems too. You can also try SIM-sized cards that can be embedded in a USB 'token' reader.
- Various different smartcard readers. As an independent hardware distributor we have many makes and models to choose from. We will normally provide a mixture of desktop and portable readers to try out on your PCs and your users.
- Software tools and docs. We will provide various free-to-use tools to match the supplied smartcards, enabling simple 'offline' functions such as changing and unblocking PINs, viewing certificates etc..
- A free hardware-secured test license to vSEC:CMS S-Series, including getting-started support, documents and videos. We have a special arrangement with smartcard software specialists Versasec, and can supply a 5-user PoC system for just the cost of the (required) administrator token, licensed to your organisation. You can install this on your domain, link to your CA, and be issuing smartcards within a couple of hours. The benefit of using this hardware-secured license for evaluation purposes, rather than a standard demo, is that you don't have to recall and re-issue all of your cards when you choose to go ahead with the full software. You just need to purchase the full license when you are ready, and we will supply the necessary upgrade codes to enable the required number of users plus, of course, the full annual technical support and maintenance entitlement.

Many customers have purchased a Smartcard Focus PoC kit, and with a little help from the technical teams at Versasec and Dot Origin, have been up and running with smartcard logon, door access and other applications within a few days. Once they have validated the processes and requirements within their organisation they simply come back to us and purchase the necessary cards, readers and software licenses to enable a wider rollout.

Myths busted - problems solved!

For more info, please just drop us an email with details of your requirements – pki@smartcardfocus.com

Smartcard Focus is a trademark and trading style of Dot Origin Ltd.

Dot Origin is headquartered in the UK, with a subsidiary incorporated in California.

We are a specialist value-added distributor of smartcard related products and solutions, and hold significant stocks of cards and readers from multiple vendors for immediate shipment world-wide. You can purchase online from www.smartcardfocus.com, for world-wide shipping, or from www.smartcardfocus.us for USA, Canada and Mexico.

We also develop, sell and support our own software solutions, such as EdgeConnector – see www.edgeconnector.com

For reseller enquiries , please contact sales@dotdistribution.com

Our corporate web site is at www.dotorigin.com

Our privacy policy is at www.dotorigin.com/privacy