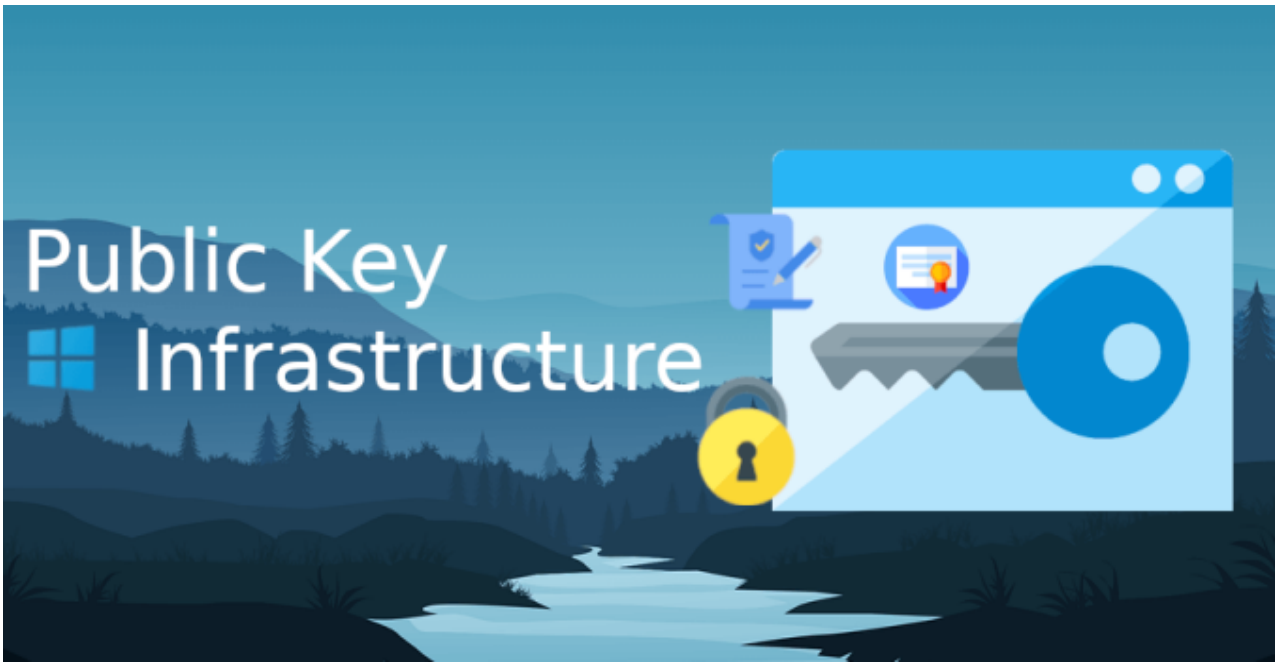
PKI – Part 4: Understanding Cryptographic Providers

michaelwaterman.nl/2023/10/13/pki-part-4-understanding-cryptographic-providers

Michael Waterman October 13, 2023



Introduction

In the realm of Public Key Infrastructure (PKI), where the keys to digital security are exchanged, stored, and safeguarded, cryptographic providers play a pivotal role. These providers are the guardians of cryptographic keys, ensuring the integrity, confidentiality, and authenticity of digital communications. They are the invisible sentinels that underpin the very foundation of trust in the digital world.

The choice of a cryptographic provider is no easy choice. It wields profound influence, not only over the security but also the performance of a PKI system. In this blog post, I will delve into the evolution and landscape of cryptographic providers in Microsoft PKI, understanding their significance, exploring the available options, and offering guidance on selecting the right provider for your unique requirements.

Historical perspective

The history of cryptographic providers within Microsoft PKI is a journey marked by continuous evolution and adaptation. In the early days, cryptographic services were primarily reliant on software-based solutions that were embedded in the operating system. However, as the digital landscape grew in complexity, the need for more robust and secure cryptographic mechanisms became evident.

Transition to Data Protection API (DPAPI)

A significant turning point in the evolution of cryptographic providers within Microsoft PKI was the transition to the Data Protection API (DPAPI). This transformation occurred with the release of Windows 2000 and later versions. DPAPI, introduced in these operating systems, offered a standardized and more secure way to protect sensitive data.

The significance of DPAPI lies in its ability to securely encrypt and store cryptographic keys and sensitive information using a user or system-specific key. This was a substantial improvement over previous methods, providing better protection against unauthorized access and key theft.

Windows Vista, introduced changes related to the Cryptographic Service Providers (CSPs) being replaced by the Cryptographic Next Generation (CNG) architecture. This transition further enhanced cryptographic capabilities and security in Microsoft operating systems.

Available cryptographic providers

The choice of cryptographic provider is an important decision. Microsoft PKI offers a diverse array of cryptographic providers, each tailored to different use cases and security needs. In this section, we will explore and demystify the major cryptographic providers available within the Microsoft PKI ecosystem. From software-based solutions to hardware security modules (HSMs) and specialized accelerators, each provider brings its unique strengths to the table. Whether you're safeguarding sensitive data, enhancing performance, or navigating compliance requirements, the right cryptographic provider can make all the difference in your PKI deployment.

Enumerate the list of cryptographic providers

Listing all the cryptographic providers on a system is an easy task, fire up a command-line shell and type the following:

```
certutil -csplist
```

The output of the providers on a Windows server 2022 are displayed below:

```
C:\Users\Administrator>certutil -csplist
Provider Name: Microsoft Base Cryptographic Provider v1.0
Provider Type: 1 - PROV_RSA_FULL

Provider Name: Microsoft Base DSS and Diffie-Hellman Cryptographic Provider
Provider Type: 13 - PROV_DSS_DH

Provider Name: Microsoft Base DSS Cryptographic Provider
Provider Type: 3 - PROV_DSS

Provider Name: Microsoft Base Smart Card Crypto Provider
Provider Type: 1 - PROV_RSA_FULL

Provider Name: Microsoft DH SChannel Cryptographic Provider
Provider Type: 18 - PROV_DH_SCHANNEL

Provider Name: Microsoft Enhanced Cryptographic Provider v1.0
Provider Type: 1 - PROV_RSA_FULL

Provider Name: Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider
Provider Type: 13 - PROV_DSS_DH

Provider Name: Microsoft Enhanced RSA and AES Cryptographic Provider
Provider Type: 24 - PROV_RSA_AES

Provider Name: Microsoft RSA SChannel Cryptographic Provider
Provider Type: 12 - PROV_RSA_SCHANNEL

Provider Name: Microsoft Strong Cryptographic Provider
Provider Type: 1 - PROV_RSA_FULL

Provider Name: Microsoft Software Key Storage Provider

Provider Name: Microsoft Passport Key Storage Provider

Provider Name: Microsoft Platform Crypto Provider

Provider Name: Microsoft Smart Card Key Storage Provider
CertUtil: -csplist command completed successfully.
```

In the upcoming sections, I will provide an explanation for all listed Cryptographic providers . These providers will be categorized into ‘Modern Providers,’ showcasing their capabilities, ‘Legacy Providers,’ which still serve specific purposes, and ‘Deprecated Providers,’ highlighting those you should steer clear of. I will delve into their functions, use cases, and help you make informed decisions on when to harness their cryptographic prowess for your PKI needs.

Modern Microsoft cryptographic providers

The term modern cryptographic providers refers to the providers that are recommended for use in modern systems. These providers are based on the Cryptography API: Next Generation (CNG) and are designed to replace the legacy Cryptography API (CAPI) providers. Below is a list of the most currently available cryptographic providers on Windows Server 2022.

Cryptographic provider that should be avoided

There exist certain cryptographic service providers that have outlived their utility and should be approached with caution, if not altogether avoided. In this section, I will shed a light on these deprecated or less secure providers. By staying informed about these outdated choices, you can ensure your cryptographic operations remain robust and resilient against emerging threats.

- Microsoft Base Cryptographic Provider v1.0
- Microsoft Base DSS and Diffie-Hellman Cryptographic Provider
- Microsoft Base DSS Cryptographic Provider
- Microsoft Base Smart Card Crypto Provider
- Microsoft DH SChannel Cryptographic Provider
- Microsoft Enhanced Cryptographic Provider v1.0
- Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider
- Microsoft Enhanced RSA and AES Cryptographic Provider
- Microsoft RSA SChannel Cryptographic Provide
- Microsoft Strong Cryptographic Provider

Note! The functionality of Key Storage Providers in a certificate template becomes accessible when both the certification authority and requesting clients are configured for compatibility with Windows Vista or later, such as Windows Server 2008. This upgrade elevates the certificate template to version 3, rendering it incompatible with older operating systems

The selection of a cryptographic provider relies not solely on its cryptographic prowess but also on its compatibility with the intended application. To illustrate, operating systems predating Windows Vista lack the capability to harness key storage providers, rendering them incompatible with such legacy systems. Additionally, consider the Microsoft Platform Crypto Provider, which, as an example, does not encompass support for all cryptographic algorithms

Tip! Use PowerShell to list all the CSP

```
$CSP=New-Object-ComObject 'X509Enrollment.CCspInformations'
$CSP.AddAvailableCsps()
$CSP|Select-Object-Property Name
```

Tip! List all the modern Key Storage Providers

```
$CSP|where LegacyCsp -like False | select Name
```

Hardware Security Modules

Hardware Security Modules (HSMs) stand as hardware guardians of sensitive data and cryptographic keys. These specialized, tamper-resistant devices play an important role in fortifying the defenses of modern organizations against a myriad of threats. Their significance lies not only in their ability to protect cryptographic assets but also in the peace of mind they offer to businesses, governments, and institutions in the face of increasingly sophisticated cyberattacks. HSMs are not mere security peripherals; they are the bastions of trust in the digital realm. Their primary role is to enhance security by safeguarding cryptographic keys and executing critical cryptographic operations in a secure, isolated environment. Unlike software-based solutions, which may be susceptible to various forms of attacks, HSMs are designed with a specific focus on hardware-based security.

Pro tip! If you have the option available, always use a hardware HSM as this enhances security dramatically.

Choosing the right cryptographic provider

The choice of the right provider can significantly impact the security, performance, and functionality of your digital ecosystem. As I conclude this comprehensive blog post of cryptographic providers in the Microsoft environment, it's essential to bring our focus to the pivotal task of selecting the most suitable provider for your unique needs.

While an array of providers caters to various scenarios and requirements, there's one that often serves as the default choice within the Microsoft ecosystem – the Microsoft Software Key Storage Provider.

Rationale for default usage of the Microsoft software key storage provider

The Microsoft Software Key Storage Provider stands as the default choice for cryptographic operations within the Microsoft ecosystem for several reasons:

1. **Ubiquity and compatibility:** The Microsoft Software Key Storage Provider is natively integrated into the Windows operating system, making it universally available across Windows-based environments. This ubiquity ensures compatibility with a wide range of applications and services without the need for additional installations or configurations.
2. **Seamless integration:** It seamlessly integrates with Microsoft's cryptographic framework, offering a straightforward and consistent interface for cryptographic operations. This ease of integration simplifies development, deployment, and maintenance efforts for software applications.
3. **Versatile functionality:** The provider supports a comprehensive range of cryptographic algorithms, enabling it to handle various encryption, decryption, digital signature, and hashing requirements. This versatility makes it suitable for a wide array of use cases.

4. **Adaptability to changing needs:** For many organizations, the Microsoft Software Key Storage Provider strikes a balance between security and ease of use. It serves as a pragmatic choice for general cryptographic tasks, allowing organizations to adapt to evolving security needs while maintaining operational efficiency.
5. **Ideal for development and testing:** When developing and testing applications, the Microsoft Software Key Storage Provider offers an accessible environment for cryptographic operations without the complexities associated with hardware-based providers.
6. **Cost-efficiency:** As a software-based provider included with Windows, it does not require additional hardware investments or licensing fees, making it a cost-effective choice for many organizations.

While the Microsoft Software Key Storage Provider is a robust choice for many scenarios, it's crucial to recognize that specific use cases may demand specialized providers, such as Hardware Security Modules (HSMs) for heightened security or Cryptographic Hardware Accelerators (CHAs) for enhanced performance. Organizations should carefully assess their security, performance, and compliance requirements when selecting the appropriate cryptographic provider, considering both the default Microsoft Software Key Storage Provider and alternative solutions to ensure the best fit for their unique needs.

Pro Tips for working with cryptographic providers

Dump all provider capabilities

```
certutil -csptest
```

Dump a specific provider capability

```
certutil -csp "Microsoft Software Key Storage Provider" -csptest
```

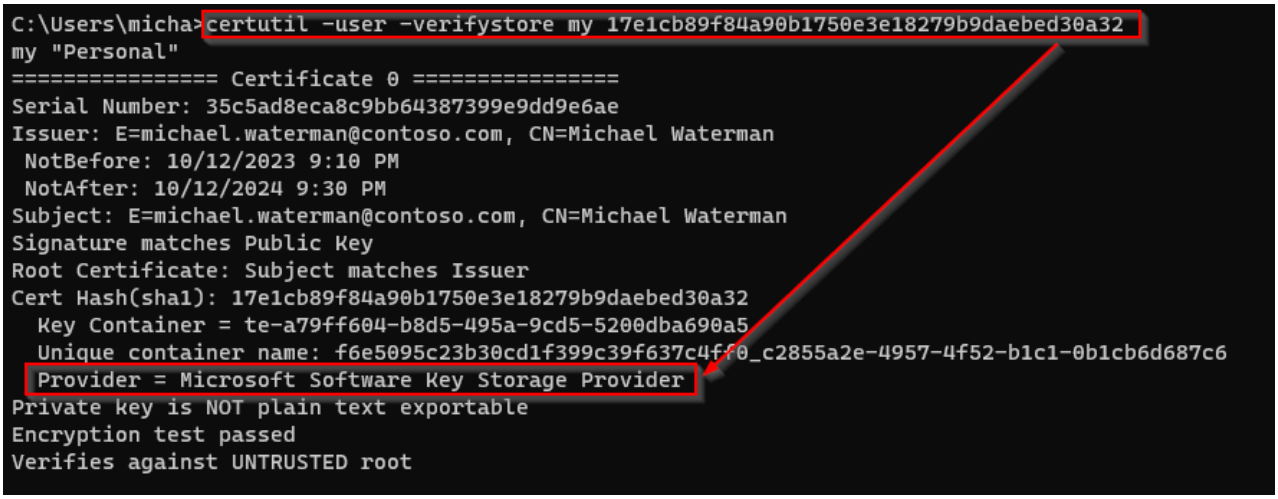
```
  NCryptCreatePersistedKey(Microsoft Software Key Storage Provider, RSA)
Algorithm Group: RSA
Algorithm Name: RSA
Length: 1024 (0x400)
Lengths:
  dwMinLength = 512 (0x200)
  dwMaxLength = 16384 (0x4000)
  dwIncrement = 8 (0x8)
  dwDefaultLength = 1024 (0x400)
Block Length: 128 (0x80)
Export Policy: 0 (0x0)
```

The cryptographic service provider exposes a comprehensive array of supported symmetric and asymmetric algorithms, hash algorithms, and key sizes. In the accompanying image, we observe the spectrum of key lengths, ranging from minimal to

maximal, with the upper limit reaching up to 16,384 bits. However, it's essential to exercise caution when using such extensive key lengths, particularly for RSA keys, as excessively large keys can introduce performance and compatibility challenges.

Get the provider per certificate

```
certutil -user -verifystore my
```

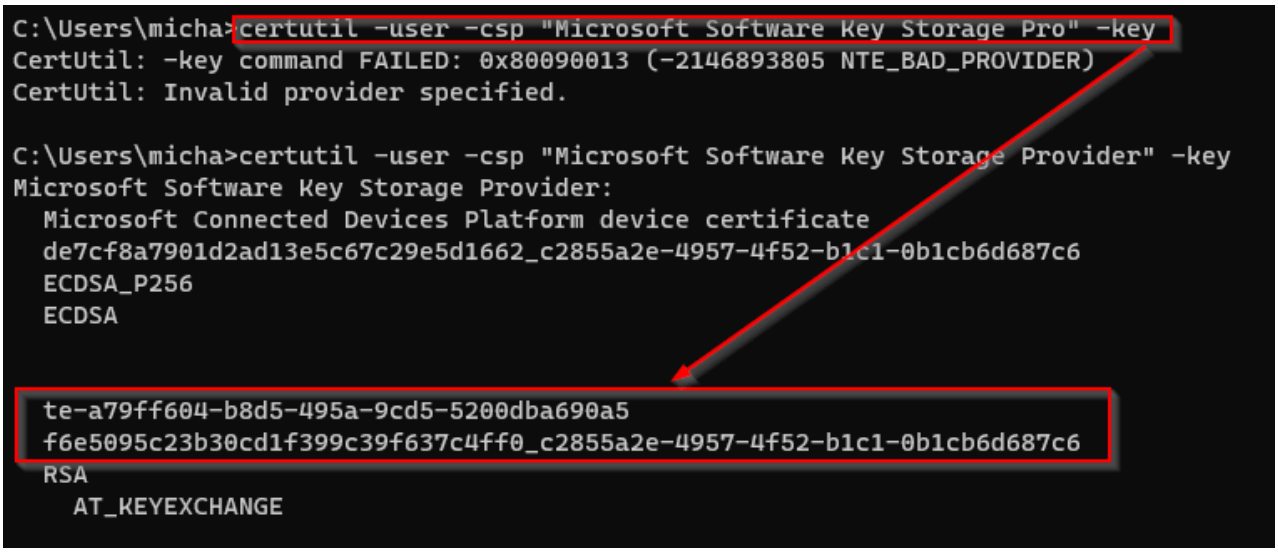


Pro Tip! Add the thumbprint from the certificate at the end of the command-line to get the specific certificate information.

Tip! remove the "-user" to list the certificates in the computer container.

List the provider protected keys

```
certutil -user -csp "Microsoft Software Key Storage Pro" -key
```



As you can see in the example, the key container name (te-a79ff604-b8d5-495a-9cd5-5200dba690a5) and the unique container name (f6e5095c23b30cd1f399c39f637c4ff0_c2855a2e-4957-4f52-b1c1-0b1cb6d687c6) match that of the certificate in the previous command. Also note that the key algorithm (RSA) is shown.

Needless to say that dropping the “-user” will default to the computer container.

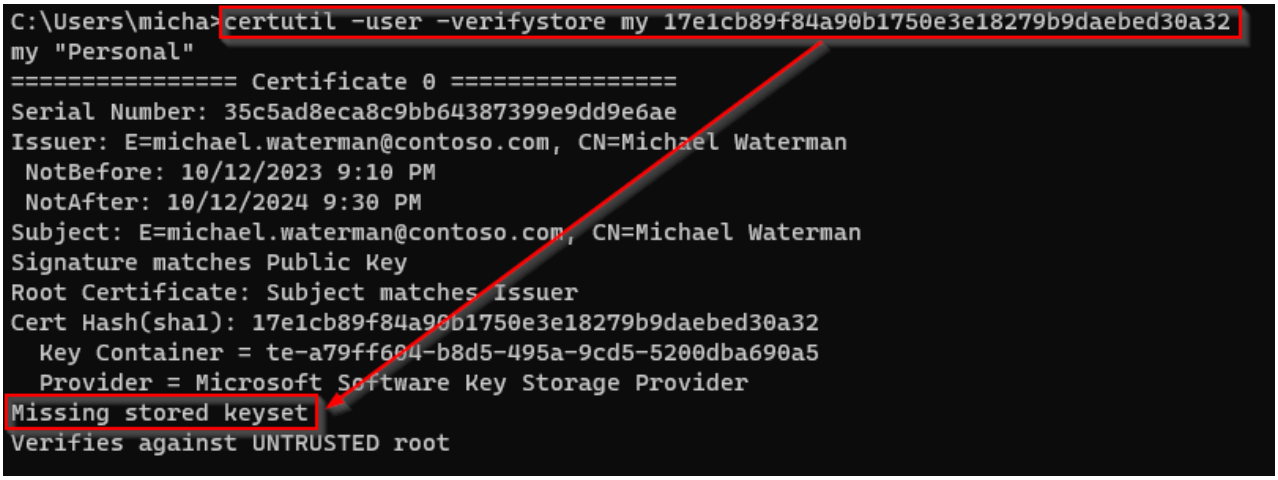
Tip! you can also add the “-v” to the command-line to get a more verbose output.

Destroying the key

There may arise a situation that you need to make sure your certificates and keys are securely deleted or otherwise made invalid. You can do that with the certutil tool as well. All you need to do is add the “-delkey” parameter.

```
certuti -user -csp "Microsoft Software Key Storage Provider" -delkey <key container name>
```

When I enumerate the specific certificate again I can now see that the private key material is effectively missing, rendering the certificate invalid.



Conclusion

The choice of a cryptographic service provider is far from arbitrary; it’s a pivotal decision that shapes the security and functionality of your digital ecosystem. Throughout this blog , I’ve navigated the landscape of cryptographic providers within the Microsoft ecosystem, from the default Microsoft Software Key Storage Provider to specialized Hardware Security Modules (HSMs).

It’s essential to emphasize that the selection of the right provider is a dynamic process, intimately tied to the unique needs and circumstances of your organization. Balancing security, performance, and compliance requirements is no small feat, but it’s a task that every security-conscious entity must undertake.

Remember, the default choice isn’t always the best choice, and sometimes the perfect provider for one scenario may not be suitable for another. Whether you’re safeguarding sensitive data, optimizing performance, or navigating the intricacies of regulatory compliance, making informed decisions about cryptographic providers is the linchpin of digital security.