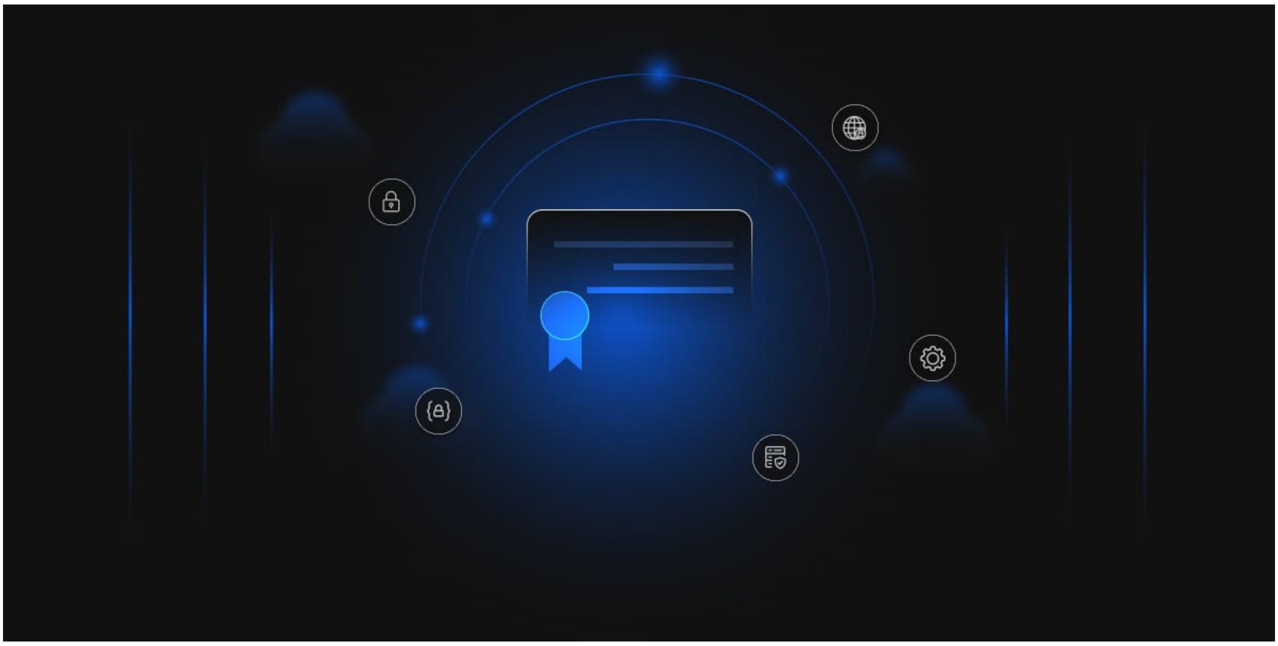
Microsoft’s Strong Certificate Mapping Enforcement — What It Means for Your PKI and How to Prepare

encryptionconsulting.com/strong-certificate-mapping

Manimit Haldar

March 3, 2025



Microsoft’s **February 2025 security update** introduces a critical change in certificate-based authentication by enforcing Strong Certificate Mapping on Active Directory Domain Controllers (DCs). This enforcement, aimed at mitigating privilege escalation risks, ensures that certificates used for authentication contain a Security Identifier (SID) extension, properly mapping them to users and devices in Active Directory (AD).

Organizations relying on certificate-based authentication for user logins, VPN access, and device management must act swiftly. Starting February 2025**,** authentication requests using weak mappings are set to be denied by default, and by September 2025, Compatibility Mode will be permanently removed. To avoid service disruptions, businesses should audit their PKI infrastructure, update certificate templates, and reissue non-compliant certificates ahead of these deadlines.

Understanding Strong Certificate Mapping Enforcement

Microsoft introduced Strong Certificate Mapping Enforcementin the May 2022 KB5014754 update to address vulnerabilities (CVE-2022-34691, CVE-2022-26931, and CVE-2022-26923) in Active Directory certificate-based authentication. These vulnerabilities allowed attackers to bypass authentication and escalate privileges. To counter this, Microsoft mandated the inclusion of a Security Identifier (SID) extension in issued certificates, ensuring accurate identity mapping.

Initially, domain controllers operated inCompatibility Mode, permitting authentication with non-compliant certificates while logging warnings. However, starting February 2025, Full Enforcement Mode has already been enabled by default, meaning authentication attempts with weak mappings will fail. By September 10, 2025, Compatibility Mode will be completely phased out, making **SID-based certificate mapping mandatory** for all authentication scenarios.

This enforcement affects various authentication mechanisms, including user logins, VPN access, MDM-enrolled devices, and certificates issued viaMicrosoft NDES or offline templates. Organizations must assess their PKI configurations, update certificate templates, and ensure compliance to prevent authentication failures.

Key Changes in Strong Certificate Mapping Enforcement

1. **SID Extension Requirement**
2. **Domain Controller Behavior Modifications**
   - DCs will enforce SID-based certificate mappings and reject non-compliant authentication attempts.
   - Event logs will indicate authentication failures due to missing or incorrect SID extensions.
3. **Phased Enforcement Modes**
   - **Compatibility Mode (Current Default Mode):** Weak certificate mappings are allowed, but events are logged for administrative review.
   - **Full Enforcement Mode (Mandatory from February 2025):** Authentication requests using weak mappings are now denied by default.
   - **Final Deadline (September 10, 2025):** Compatibility Mode will be removed, enforcing strict SID-based mappings across all authentication requests.

Key Affected Areas

Organizations relying on certificate-based authentication must assess their environments to prevent disruptions in the following areas:

1. **User Logins and Wi-Fi Authentication** – Certificates used for **user and device authentication** must include the correct SID extension.

2. **VPN Access (e.g., Always On VPN)** – Certificates used for VPN authentication must comply with the new mapping standards.

3. **MDM-Enrolled Devices (Microsoft Intune PKCS/SCEP)** – Certificates issued via Intune's PKCS or SCEP connectors need **SID extension updates** to remain valid.

4. **Certificates Issued via Offline Templates or Microsoft NDES** – Organizations issuing certificates through offline templates or Network Device Enrollment Service (NDES) must update their configurations.

Impact on Different Environments

1. **On-premises Active Directory Environments**
    - If patches since May 2022 (KB5014754) have been applied consistently, existing certificates may already comply with the SID requirement.
    - Organizations must manually verify whether their Certificate Authority (CA) templates are configured to include OID 1.3.6.1.4.1.311.25.2 in newly issued certificates.
      How to track these Templates?
2. **Hybrid Environments (On-Prem AD + Intune or AAD Sync)**
    - Organizations using **Microsoft Intune** for certificate issuance must update their PKCS certificate connector to enable **SID-based mappings**.
    - Run the following command on the Intune Certificate Connector server to enable SID extensions:

      Set-ItemProperty -Path “HKLM:\SOFTWARE\Microsoft\MicrosoftIntune\PFXCertificateConnector” -Name EnableSidSecurityExtension -Value 1 -Force

    - SCEP Certificates: Ensure Subject Alternative Name (SAN) settings in Intune include the on-prem Security Identifier

      URI={{OnPremisesSecurityIdentifier}}

3. **Cloud-Only Environments (Azure AD with Certificate Authentication)**
    - Organizations using Azure-only authentication with certificates need to review their authentication flows.
    - Reissuing non-compliant certificates might be necessary if the authentication backend does not support SID extensions.

Identifying and Remediating At-Risk Certificates

1. **Strong vs. Weak Certificate Mappings**
   Microsoft supports six mapping types for associating certificates with Active Directory users via the `altSecurityIdentities` attribute.

   Organizations are recommended to migrate to strong mapping formats to comply with Microsoft’s enforcement.

2. **Auditing Certificate Templates**
   One of the major steps involves reviewing all active certificate templates to detect those missing the 1.3.6.1.4.1.311.25.2 extension. Use the following command to check template details:

   certutil -template | findstr “OID=1.3.6.1.4.1.311.25.2”

   Templates without this OID require updates to comply with Microsoft’s enforcement.

3. **Monitoring Event Logs for Compliance Issues**
   Keeping in mind the enforcement deadline, there should be a policy to regularly monitor domain controller logs for authentication failures related to certificate mapping. Key **Event IDs to monitor** include:

   Use PowerShell to filter relevant logs:

   Get-EventLog -LogName Security | Where-Object { $_.EventID -in @(39,40,41) }

   This can help identify and remediate non-compliant certificates before enforcement deadlines.

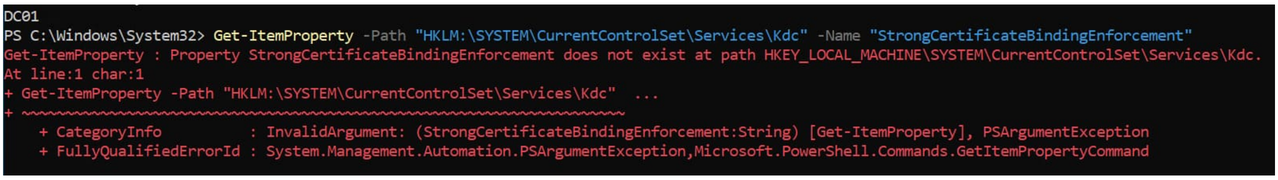
Temporary Mitigation with Compatibility Mode

Organizations unprepared for enforcement mode can opt for temporary mitigation by switching domain controllers back to Compatibility Mode until September 2025.

To check if Compatibility Mode is enabled:

Get-ItemProperty -Path “HKLM:\SYSTEM\CurrentControlSet\Services\Kdc” -Name “StrongCertificateBindingEnforcement”

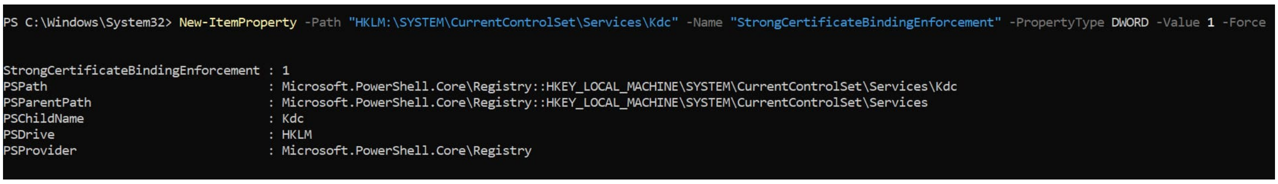
If the registry key **StrongCertificateBindingEnforcement** does not exist, then the domain controller is not configured. This means, the system is in full enforcement mode.



```
DC01
PS C:\Windows\System32> Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Kdc" -Name "StrongCertificateBindingEnforcement"
Get-ItemProperty : Property StrongCertificateBindingEnforcement does not exist at path HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc.
At line:1 char:1
+ Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Kdc"  ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidArgument: (StrongCertificateBindingEnforcement:String) [Get-ItemProperty], PSArgumentException
    + FullyQualifiedErrorId : System.Management.Automation.PSArgumentException,Microsoft.PowerShell.Commands.GetItemPropertyCommand
```

For enabling the Compatibility Mode, The **StrongCertificateBindingEnforcement** registrykeyshould be present. To manually add it and enable Compatibility Mode:

New-ItemProperty -Path “HKLM:\SYSTEM\CurrentControlSet\Services\Kdc” -Name “StrongCertificateBindingEnforcement” -PropertyType DWORD -Value 1 -Force



```
PS C:\Windows\System32> New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\Kdc" -Name "StrongCertificateBindingEnforcement" -PropertyType DWORD -Value 1 -Force


StrongCertificateBindingEnforcement : 1
PSPath                              : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc
PSParentPath                        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
PSChildName                         : Kdc
PSDrive                             : HKLM
PSProvider                          : Microsoft.PowerShell.Core\Registry
```

WARNING: This mitigation must be removed before September 2025 to comply with Microsoft’s final enforcement.

Enterprise Certificate Authorities (CA) Considerations

Enterprise Certificate Authorities (CAs) must adapt to these changes to avoid issuing non-compliant certificates.

New certificates issued using online templates will automatically include the **1.3.6.1.4.1.311.25.2** extension. If certain certificates should be excluded from receiving this extension, administrators can use the following command:

certutil -dstemplate user msPKI-Enrollment-Flag +0x00080000

This ensures that select templates do not enforce strong mappings.

CertSecure Manager: Your Compliance Partner in a Changing Cryptographic Landscape

CertSecure Manager has been at the forefront of supporting organizations in staying up-to-date with the latest cryptographic policy transitions. As compliance standards evolve—whether through NIST recommendations, PCI DSS updates, or new industry mandates—CertSecure Manager ensures businesses remain compliant without disruption.

How CertSecure Manager Keeps You Ahead

- **Proactive Compliance Adaptation**
  CertSecure Manager continuously updates its compliance framework to align with evolving regulations like HIPAA, PCI DSS, GDPR, and NIST 800-131A.

- **Automated Updates for Cryptographic Transitions**
  As cryptographic policies shift, such as the transition to stronger hashing algorithms, key sizes, and rotation intervals, CertSecure Manager automates certificate updates and renewals to ensure uninterrupted compliance.

- **Real-Time Monitoring and Policy Enforcement**
  Organizations receive instant alerts on expiring certificates and non-compliant cryptographic configurations, preventing security lapses and regulatory penalties.

- **Seamless Integration with New Standards**
  Whether it's post-quantum cryptography adoption, TLS certificate validity reductions, or emerging cryptographic best practices, CertSecure Manager is designed to integrate with new standards effortlessly. With extended reporting capabilities, your organization stays ahead of vulnerabilities and outages.

With CertSecure Manager, your organization significantly reduces the risk of service disruptions due to non-compliant certificates, saves time and resources in the transition to Strong Certificate Mapping, and ensures ongoing compliance with all evolving security requirements. Our solution not only addresses the immediate needs for the February 2025 enforcement but also provides a robust platform for long-term certificate lifecycle management.

In addition to CertSecure Manager, Encryption Consulting's PKI Assessment Service provides a comprehensive evaluation of your PKI infrastructure. Our service helps your organization identify security gaps and vulnerabilities in your PKI. Our expert team prepares a customized roadmap to help you optimize your cryptographic policies and ensure compliance with industry standards. Whether you are preparing for upcoming regulatory changes or strengthening your overall certificate management strategy, a PKI assessment delivers expert insights and actionable recommendations.

Conclusion

Microsoft’s Strong Certificate Mapping Enforcement is crucial in securing authentication processes. Organizations must act promptly to audit and update their PKI infrastructure before the **September 2025** deadline.

For expert guidance and automated certificate lifecycle management, consider contacting Encryption Consulting to explore how CertSecure Manager can support your organization’s compliance efforts.

Additional References:

KB5014754 – Microsoft Support

Windows Forum Discussion

Microsoft Tech Community – Intune Implementation