Windows

Purpose of TPM Attestation

- TPM (Trusted Platform Module) provides hardware-based security functions. It's a secure crypto-processor designed to perform cryptographic operations.
- Windows has supported TPM-protected keys since Windows 8. However, there was no mechanism for Certificate Authorities (CAs) to cryptographically attest that a certificate requester's private key is genuinely protected by a TPM. This gap was addressed in later updates.
-

Key Components of TPM Attestation

- Endorsement Key (EK)
- : A unique asymmetric key inside the TPM, injected during manufacturing. It's unique for every TPM and can't be changed or removed. The EK is used to identify the TPM.
- EK Certificate (EKCert)
- : Some TPMs come with a manufacturer-issued certificate for the EK's public key.
- TPM Key Attestation
- : This is the process where the entity requesting a certificate proves to a CA that the RSA key in the certificate request is protected by a trusted TPM.
-

How TPM Key Attestation Works

- Every TPM comes with the unique Endorsement Key (EK).
- A CA establishes trust in the TPM either via the EK's public key (EKPub) or the EK Certificate (EKCert).
- The user proves to the CA that the RSA key for which the certificate is being requested is related to the EKPub and that they own the associated private key (EKPriv).
- The CA then issues a certificate with a specific policy OID to indicate that the key is protected by a TPM.
-

Deployment Overview

- TPM trust can be established in three ways:
-
    - Trust based on user credentials
-
    - : The CA trusts the user-provided EKPub as part of the certificate request.
-
    - Trust based on EKCert
-
    - : The CA validates the EKCert chain provided in the certificate request against an administrator-managed list of acceptable EK cert chains.
-
    - Trust based on EKPub
-
    - : The CA validates that the EKPub provided in the certificate request is in an administrator-managed list of allowed EKPub values.
- *
-

Importance of TPM Key Attestation

- A certificate with a TPM-attested key offers higher security assurance due to the TPM's features like non-exportability, anti-hammering, and key isolation.
- TPM key attestation allows administrators to define which devices users can use to access corporate resources, ensuring that only authorized devices can access them.
-

Windows Server Configuration for TPM Attestation

- Depending on the chosen TPM trust model, the CA might need to be configured to trust specific EKCert chains or a list of allowed EKPub values.
- For EKCert trust, the administrator must obtain the EKCert chain certificates from TPM manufacturers and import them into specific certificate stores on the CA.
- For EKPub trust, the administrator must obtain the EKPub for each device and add them to an allowed list.
-

In essence, TPM attestation in Windows involves a combination of hardware-based security from the TPM and software-based validation processes to ensure that cryptographic keys are securely stored and used. This provides a robust mechanism for ensuring the integrity and authenticity of cryptographic operations on Windows devices.

References

- WebAuthn TPM attestation
- Microsoft TPM Root Certificate Authority 2014
-

Previous Apple Next FIDO U2F Authenticator Last updated7 months ago On this page *Purpose of TPM Attestation * Key Components of TPM Attestation * How TPM Key Attestation Works * Deployment Overview * Importance of TPM Key Attestation * Windows Server Configuration for TPM Attestation * References

Was this helpful?