CNG Key Storage Providers

- Article
- 11/21/2024

In this article

Unlike Cryptography API (CryptoAPI), Cryptography API: Next Generation (CNG) separates cryptographic providers from key storage providers (KSPs). KSPs can be used to create, delete, export, import, open and store keys. Depending on implementation, they can also be used for asymmetric encryption, secret agreement, and signing. Microsoft installs the following KSPs on Windows. However, vendors can create and install other providers.

Microsoft Software Key Storage Provider

The **Microsoft Software Key Storage Provider** supports software key creation and storage and the following algorithms.

Algorithm	Purpose	Key length (bits)
Diffie-Hellman (DH)	Secret agreement and key exchange	512 to 4096 in 64-bit increments
Digital Signature Algorithm (DSA)	Signatures	512 to 1024 in 64-bit increments
Elliptic Curve Diffie-Hellman (ECDH)	Secret agreement and key exchange	P256, P384, P521
Elliptic Curve Digital Signature Algorithm (ECDSA)	Signatures	P256, P384, P521
RSA	Asymmetric encryption and signing	512 to 16384 in 64-bit increments

Microsoft Smart Card Key Storage Provider

The **Microsoft Smart Card Key Storage Provider** supports smart card key creation and storage and the following algorithms.

Algorithm	Purpose	Key length (bits)

Algorithm	Purpose	Key length (bits)
Diffie-Hellman (DH)	Secret agreement and key exchange	512 to 4096 in 64-bit increments
Elliptic Curve Diffie-Hellman (ECDH)	Secret agreement and key exchange	P256, P384, P521
Elliptic Curve Digital Signature Algorithm (ECDSA)	Signatures	P256, P384, P521
RSA	Asymmetric encryption and signing	512 to 16384 in 64-bit increments

Related content

CNG Algorithm Identifiers

CNG Key Storage Functions

Understanding Cryptographic Providers

Additional resources

Training

Module

Azure Key and Certificate Management - Training

In this module, you learn about essential concepts for using encryption keys and digital certificates in Azure to help secure cloud workloads and ensure data sovereignty.