IoT Hub Device Provisioning Service device concepts

IoT Hub Device Provisioning Service is a helper service for IoT Hub that you use to configure zero-touch device provisioning to a specified IoT hub. With the Device Provisioning Service, you can provision millions of devices in a secure and scalable manner.

This article gives an overview of the *device* concepts involved in device provisioning. This article is most relevant to personas involved in the manufacturing step of getting a device ready for deployment.

Attestation mechanism

The attestation mechanism is the method used for confirming a device's identity. The attestation mechanism is also relevant to the enrollment list, which tells the provisioning service which method of attestation to use with a given device.

> [!NOTE] IoT Hub uses "authentication scheme" for a similar concept in that service.

The Device Provisioning Service supports the following forms of attestation:

- **X.509 certificates** based on the standard X.509 certificate authentication flow.
- **Trusted Platform Module (TPM)** based on a nonce challenge, using the TPM standard for keys to present a signed Shared Access Signature (SAS) token. This does not require a physical TPM on the device, but the service expects to attest using the endorsement key per the TPM spec.
- **Symmetric Key** based on shared access signature (SAS) Security tokens, which include a hashed signature and an embedded expiration. For more information, see Symmetric key attestation.

Hardware security module

The hardware security module, or HSM, is used for secure, hardware-based storage of device secrets, and is the most secure form of secret storage. Both X.509 certificates and SAS tokens can be stored in the HSM. HSMs can be used with both attestation mechanisms the provisioning service supports.

> [!TIP] We strongly recommend using an HSM with devices to securely store secrets on your devices.

Device secrets may also be stored in software (memory), but it is a less secure form of storage than an HSM.

Registration ID

The registration ID is used to uniquely identify a device in the Device Provisioning Service. The device ID must be unique in the provisioning service ID scope. Each device must have a registration ID. The registration ID is alphanumeric, case insensitive, and may contain special characters including colon, period, underscore and hyphen.

- In the case of TPM, the registration ID is provided by the TPM itself.
- In the case of X.509-based attestation, the registration ID is provided as the subject name of the certificate.

Device ID

The device ID is the ID as it appears in IoT Hub. The desired device ID may be set in the enrollment entry, but it is not required to be set. Setting the desired device ID is only supported in individual enrollments. If no desired device ID is specified in the enrollment list, the registration ID is used as the device ID when registering the device. Learn more about device IDs in IoT Hub.

ID scope

The ID scope is assigned to a Device Provisioning Service when it is created by the user and is used to uniquely identify the specific provisioning service the device will register through. The ID scope is generated by the service and is immutable, which guarantees uniqueness.

> [!NOTE] Uniqueness is important for long-running deployment operations and merger and acquisition scenarios.