Device to Service Authentication

The Internet of Things (IoT) ecosystem requires an identity fabric for machine to machine (M2M) communication. For over 20 years, certificates have been a proven solution to identify entities and secure transactions over the Internet. In today's Internet, a person proves their identity (authenticates) to a website using passwords, certificates, and other multi-factor options. With M2M communications, Public Key Infrastructure (PKI) and digital certificates is an authentication method for devices that has proven to be highly secure. PKI and digital certificates in IoT is the identity fabric needed to ensure communications are both authentic and secure.

Certificates

For devices to authenticate to a service, each device must be equipped with a certificate used to identify itself (i.e., authenticate itself to the service). The service must also have a certificate for identifying itself (i.e., authenticating itself to the device) and for encrypting communications between the service and the device.

Validation Process

Before a device can establish a secure connection to the service, it must be validated by the service as follows:

1. The device reaches out to connect to your service.
2. The service requires the device to identify itself.
3. The device uses a certificate to perform a cryptographic authentication.
4. The service then compares the certificate presented by the device to a set of logic and rules set up to verify device authenticity.
5. The service validates designated certificate attributes. The specific attributes presented by the certificate and validated by a service vary, depending on the use case. Some common attributes used for validating the certificate are as follows:
    - Checking the certificate to see if it was issued by DigiCert's certificate services
    - Checking that the common name matches a list of accepted values for certificates issued to devices
    - Checking that the organization name on the certificate matches the acceptable value.
    - Checking a certificate's status, making sure it has not been revoked. Certificate status is often checked as part of the certificate authentication process.

Once a certificate has been checked and validated, the secure connection is allowed and data flow begins. If the certificate doesn't pass the authentication process, the connection is immediately terminated. *Diagram on following page.

digicert®

Certificate Revocation

Certificates issued to devices can also be revoked, meaning the device can no longer use that certificate to identify itself (authenticate itself to the service), even if that certificate had been used previously to identify the device to the service.

*Validation Process

The following diagram shows how a device securely authenticates to connect to a service. It is important to note that the same type of authentication can be used for machine to machine connections.