**Automatically provision IoT devices securely and at scale with the Device Provisioning Service**

1. create an IoT Hub

CheeseCaveHub-01

1. add the DPS service

### Link the DPS resource to your IoT Hub

1. an X.509 root certificate, and multiple leaf certificates, are created to handle security
2. link all the pieces together

=========================\

**The process of validating the authenticity of a device** is known as **"provisioning"**

**Device Provisioning Service (DPS):** A service that enables the near-automatic provisioning of any number of devices.

**root certificate**: used to validate another certificate

**intermediate certificates**: validate other intermediate certificates, or validate leaf certificates

**leaf certificate:**  used to validate a device

All these certificates will be self-signed.

### **Individual and group enrollments**

An Azure DPS can contain a number of individual, or group, enrollments.

**Group Enrollments:** One enrollment group works with one root certificate, and any number of leaf certificates signed by this root. An enrollment maintains information on all the devices that have tried to register.

**Individual enrollments** are best used for devices that have a unique configuration, and require greater security than the connection strings you may have used in other Learn modules or Azure samples.

**allocation policy:** Allocation policies only apply when you've multiple IoT Hubs handling telemetry from a huge number of devices, and want to direct the incoming data to one of these hubs based on a policy.

### **Proof of possession**

When uploading certificates to Azure DPS, you'll be asked to generate a verification code.

Proof of Possession of a certificate is provided to DPS by uploading a verification certificate generated from the root certificate with this verification code. The verification certificate is chained to the root certificate.