Azure Sphere

Device Authentication and Attestation Service

Version 1.0.3 – 02 October 2018

Table of Contents

Introduction: Device authentication and attestation

The Device Authentication and Attestation (DAA) service is the primary point of contact with the Azure Sphere Security Service for Azure Sphere devices to authenticate their identity, ensure the integrity and trust of the system software, and certify that they are running a trusted code base. In addition, the DAA service provides Azure Sphere devices with a device authentication certificate, which can be used in downstream authentication flows to services such as the Azure Device Provisioning Service or directly to an Azure IoT Hub.

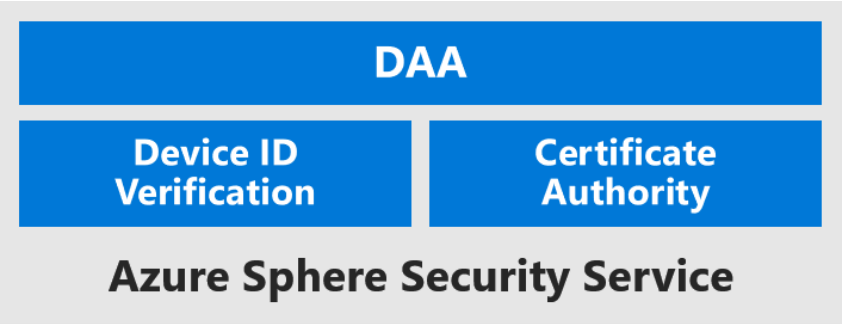


Figure 1 DAA service

The DAA service has three main components, shown in Figure 1:

- The DAA front-end service for direct device communication.
- The device ID verification component, which verifies that a device is a valid Azure Sphere device and is running trusted software.
- The certificate authority engine, which manages certificate issuance.

Device ID generation for Azure Sphere devices

Every Azure Sphere device has a unique device identification ID, which is generated by the device during the silicon manufacturing process and registered with Azure Sphere cloud services, as Figure 2 shows. The device ID is immutable throughout the lifetime of the device.

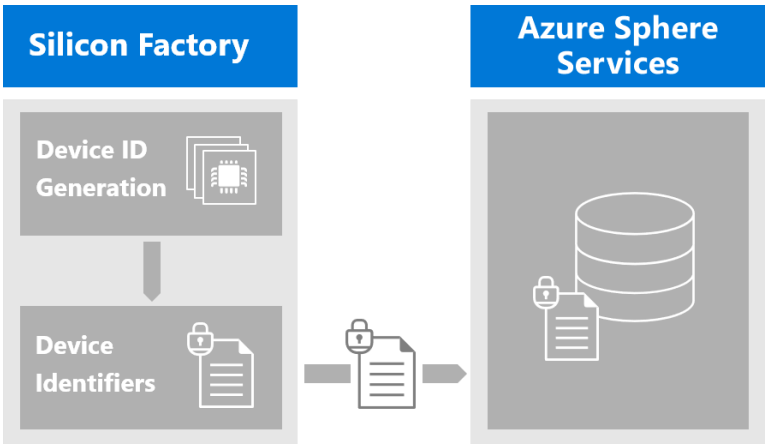


Figure 2 Device ID

Remote attestation

Remote attestation is the process by which a client proves its configuration to a remote server. The purpose of this attestation is to provide the remote server the capability to determine the level of trust and integrity of the client.

Azure Sphere devices adhere to the seven properties outlined in "The Seven Properties of Highly Secure Devices"[1] and support a Hardware Root of Trust. The Hardware Root of Trust enables an Azure Sphere device to securely sign the attestation data to prove that the device is the originator of the request and to send the remote attestation data to the DAA service.

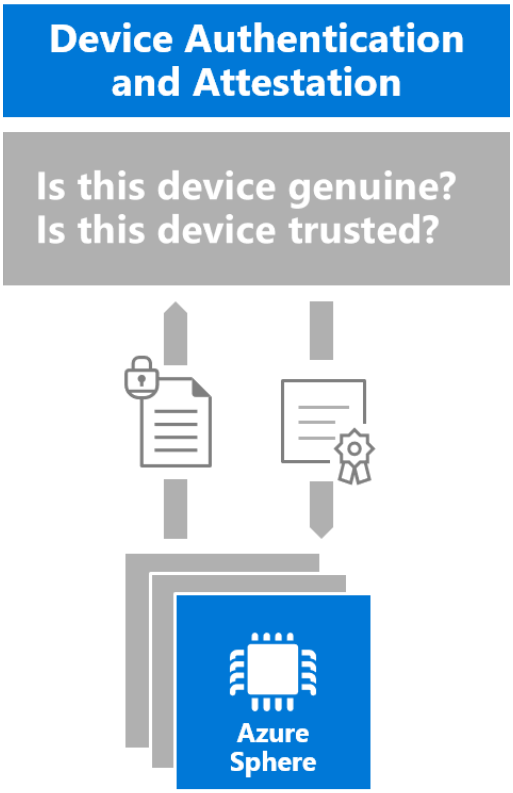


Figure 3 Remote attestation

Along with authentication, securely signed remote attestation data is a key component in the end-to-end security path for any IoT device. Authentication can prove that a device is a genuine Azure Sphere product, but it does not guarantee that the device is running an approved and trusted software stack. Securely signed remote attestation data attests to the Azure Sphere Security Service that the device's software is not compromised. After DAA has verified the identity and state of the device, it issues the device a short-lived authentication certificate.

If a device has not yet received a device authentication certificate, the DAA service requires remote attestation before the device and Azure Sphere Security Service exchange any additional messages, work, or other information.

Remote attestation, combined with authentication, is a powerful tool to guarantee the integrity and authenticity of each device that communicates with Azure IoT services.

[1] https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/SevenPropertiesofHighlySecureDevices.pdf

Azure Sphere tenant overview

In the Azure Sphere Security Service, an Azure Sphere tenant represents a group of devices. The tenant not only contains information about the devices, but also provides an isolation boundary for management of these devices.

Each Azure Sphere tenant typically represents the devices in a company or in one or more business divisions within a company, and provides the ability to manage these devices as a group. Each Azure Sphere tenant is distinct and separate from other Azure Sphere tenants. In addition, the tenant provides a security boundary for its devices due to the fact that the DAA device authentication certificates are unique to each tenant and cannot cross tenant boundaries.

Each Azure Sphere device must be "claimed" by an Azure Sphere tenant, so that the tenant knows about all its devices and can manage them as a group. A device cannot be claimed by multiple tenants. Please work with your SDM or CDS contact to onboard your devices to the Azure Sphere Security Service and create an Azure Sphere tenant.

PKI and device authentication certificates

A digital certificate is part of a public key infrastructure (PKI), which is a system of policies, certificate authorities, and certificates that verify and authenticate each party involved in an electronic transaction through the use of public key cryptography.

A certification authority issues certificates and each certificate has a set of fields that contain data, such as subject (the entity to which the certificate is issued), validity dates (when the certificate is valid), issuer (the entity that issued the certificate), and a public key.

A certificate chain is a hierarchal collection of certificates that leads from the end user or computer back to a root of trust, typically the root certification authority (CA). Because all parties presumably trust the root certificate, a party can gain trust in an end-entity certificate by verifying the certificate chain. Verification typically requires establishing that each certificate in the chain is signed by the public key in the preceding certificate, is not expired, and has not been revoked. The following figure represents the DAA certificate chain for an Azure Sphere tenant.

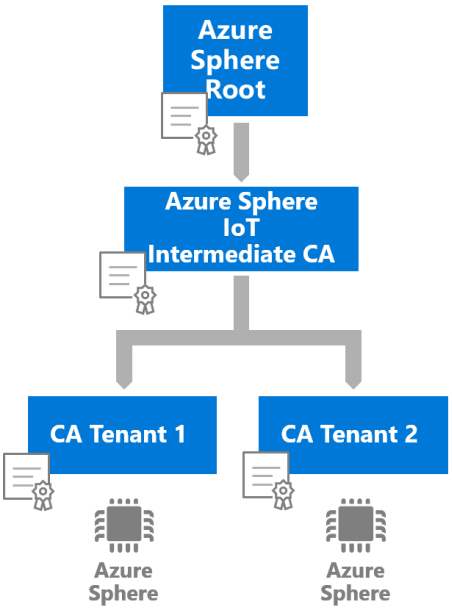


Figure 4 DAA certificate chain

From top to bottom in Figure 4, the following are the elements of the certificate chain:

- The Azure Sphere Root is a self-signed certificate that initializes the PKI chain.
- The Azure Sphere IoT Intermediate CA is signed by the Azure Sphere Root.
- The CA Tenant level is where each Azure Sphere tenant has a unique CA. This tenant-specific CA is signed by the Azure Sphere IoT Intermediate CA.
- The tenant-specific CA issues a unique, short-lived, device authentication certificate to each Azure Sphere device.

The DAA certificate services operate on a per-tenant basis, so that each device that is registered to an Azure Sphere tenant receives a certificate that is valid only within the tenant-specific chain. In Figure 4, CA Tenant1 represents the certificate authority that is unique to tenant one, and CA Tenant2 represents the certificate authority that is unique to tenant two. There is a 1 to 1 mapping between tenants and certificate authorities.

The DAA certificate authority service issues an x509 certificate to a device after confirming the device's integrity via remote attestation.

The certificate is valid for only 24 hours. The short life of the certificate ensures that each device must verify its state on a regular basis. Upon expiration of the certificate, the device will renew its certificate with DAA if the device passes the remote attestation process.

The x509 certificate contains the following information:

Certificate Fields

Field	Value
Subject Name	Device ID
Key Usage	Digital signature
Enhanced Key Usage	Client authentication
OID: 1.3.6.1.4.1.311.98.1	Remote attestation data

Azure IoT services integration

Azure IoT services securely connect millions of devices, support a broad set of protocols, and enable business owners to analyze and visualize large quantities of operational data.[2]

Azure Sphere devices integrate with two key Azure IoT services: the Azure IoT Hub and the IoT Hub Device Provisioning Service (DPS). These services are separate from the Azure Sphere Security Service and are managed by the DPS or IoT Administror, which is an Azure user identity that has permissions to manage these services.

Azure IoT Hub is a fully managed service in the cloud that securely connects, monitors, and manages IoT devices. The Azure Hub Device Provisioning Service (DPS) is a helper service for IoT Hub that enables zero-touch, just-in-time provisioning to the right IoT hub without requiring human intervention, enabling customers to provision millions of devices in a secure and scalable manner.

[2] Please see https://azure.microsoft.com/en-us/suites/iot-suite/ for more details.

DPS and IoT hubs

At the silicon factory, the manufacturer registers all devices and device IDs with the Azure Sphere service. When a device connects to the DAA service these identifiers are used to ensure the device is a known Azure Sphere device. Figure 5 shows the data flow between the device, the DAA services, and the Azure IoT services.

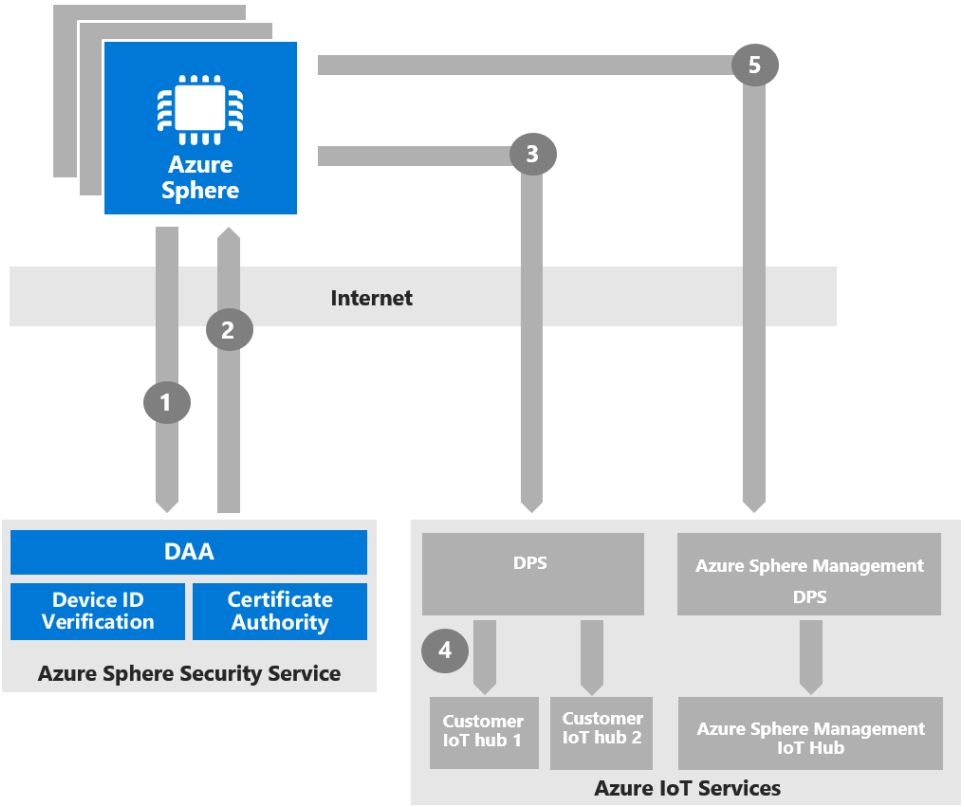


Figure 5 DAA and Azure IoT data flow

As the figure shows, the device connects as follows:

1. Device connects to the Device Authentication and Attestation services and validates the device identity and confirms the software running on the device is trusted.
2. The DAA certificate services issues a short lived certificate to the device based on the tenant to which the device belongs.
3. The Azure Sphere IoT device connects to the Azure Device Provisioning services in order to authenticate using the x509 device authentication certificate and register the device in the Customer IoT hub.
4. The device connects to the Customer IoT hub based on the DPS configuration and authenticates using the x509 device authentication certificate from DAA. It then proceeds to utilize the Azure IoT Hub services.
5. The device will regularly connect to the Microsoft Azure Sphere management services for OS updates and other management functions. Authentication to this service is outside the scope of customer boundaries.

DPS and IoT routing

Azure DPS supports several routing options for devices to connect to IoT hubs:

> **Evenly weighted distribution**: linked IoT hubs are equally likely to have devices provisioned to them. The default setting. If you are provisioning devices to only one IoT hub, you can keep this setting.

Lowest latency: devices are provisioned to an IoT hub with the lowest latency to the device. If multiple linked IoT hubs would provide the same lowest latency, the provisioning service hashes devices across those hubs

Static configuration via the enrollment list: specification of the desired IoT hub in the enrollment list takes priority over the service-level allocation policy

To route to an IoT hub based on the device authentication certificate, the DPS Administrator should choose the "Static configuration via the enrollment list" option and then configure the DPS Enrollment group to pair the Azure Sphere Tenant Certificate with the IoT Hub to which to direct devices.

DPS proof of possession

The DPS and Azure IoT services require that the DPS administrator—the person configuring DPS—to verify proof of possession of the signing certificate. The DPS service provides a random challenge to the DPS administrator, who then must sign a client certificate with the private key, where the subject name of the certificate is equal to the random value provided. This would prove that the DPS administrator has possession of the private key of the signing certificate.

However, the DAA service does not provide private keys outside of DAA for signing. Instead, the DPS administrator is required to generate the client certificate via the flow shown in Figure 6. In the figure, the Azure Sphere tenant Administrator and the DPS Administrator are the same individual, although this is not necessarily true.

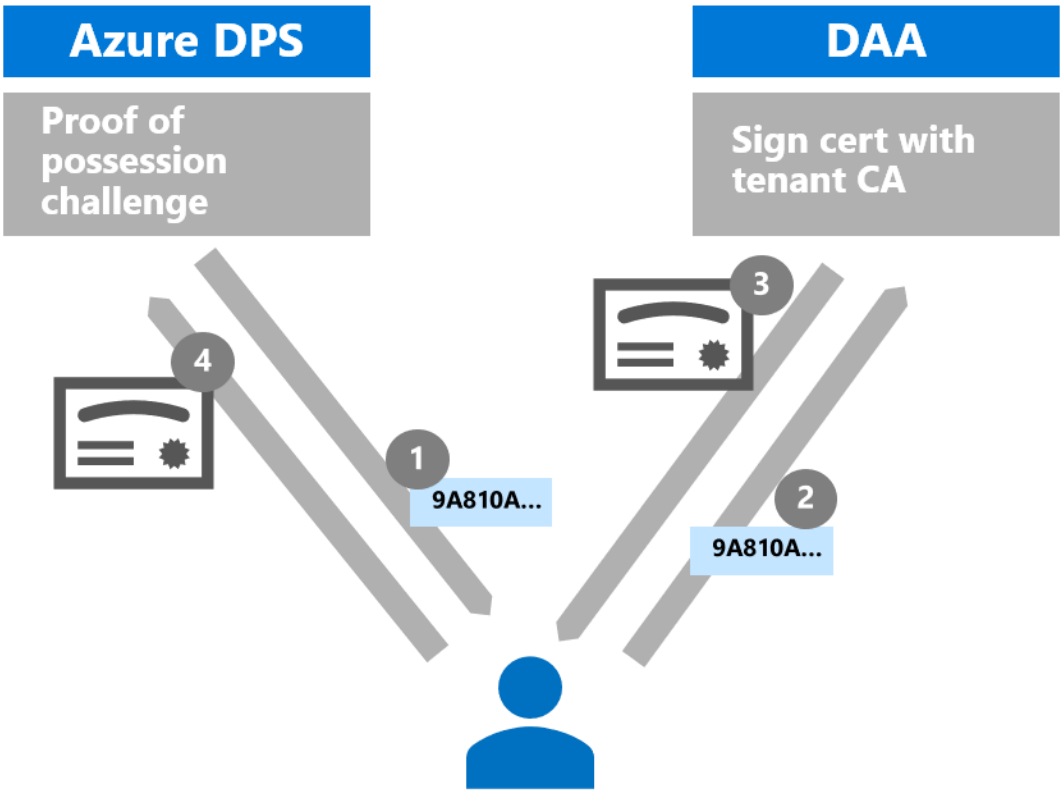
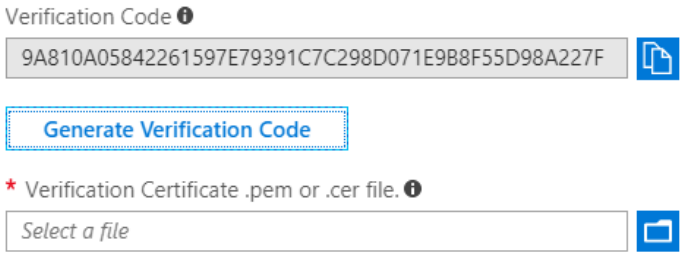


Figure 6 Proof of possession flow

Proof of possession proceeds in the following order, as the figure shows:

1. The DPS administrator registers the DAA tenant signing certificate and generates a random challenge value.



2. The Azure Sphere tenant administrator uploads the random challenge to the DAA service.
3. DAA retrieves the tenant-specific signing CA certificate and signs a certificate in which the subject name's value is the same random challenge value. DAA returns this certificate to the Azure Sphere tenant administrator.
4. The DPS tenant administrator uploads this certificate to complete the proof of possession flow with DPS/IoT hub.