Softwareentwurf und Anwendungen verteilter Systeme

Digital Product Design and Development B.A.

Semester 3

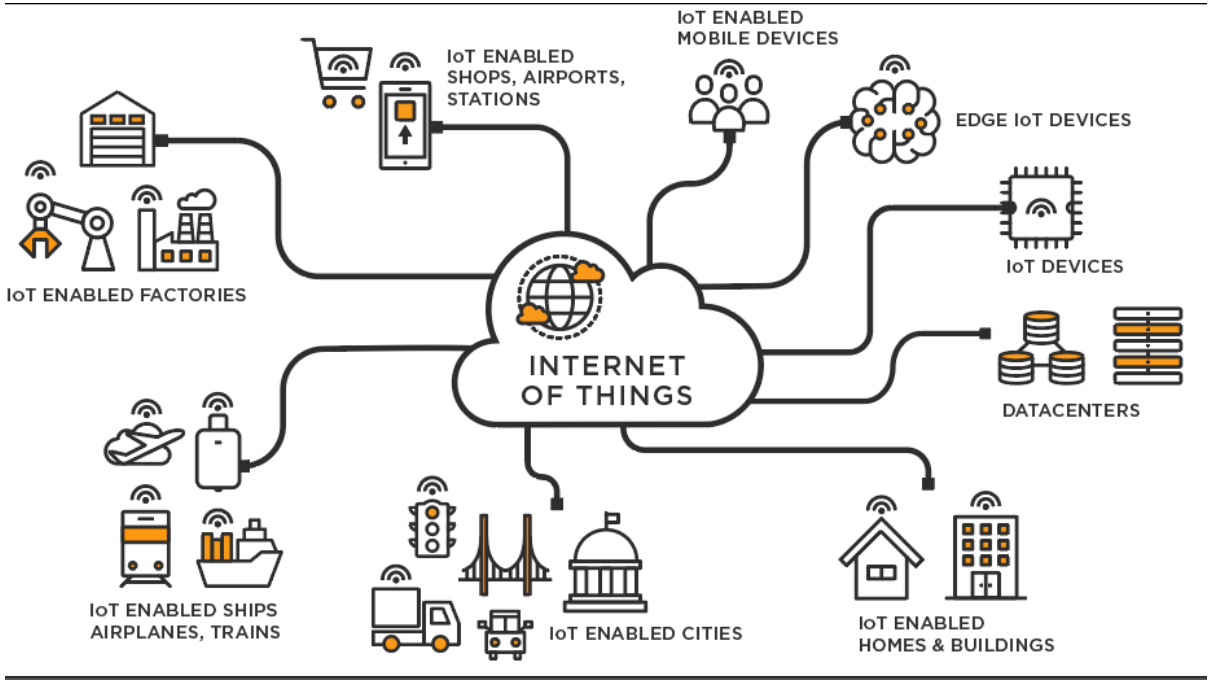
Hochschule für Gestaltung Schwäbisch Gmünd

Dozent: Yannick Schiele

H f G

Hochschule für Gestaltung
Schwäbisch Gmünd

Präsentation 1. Projekt



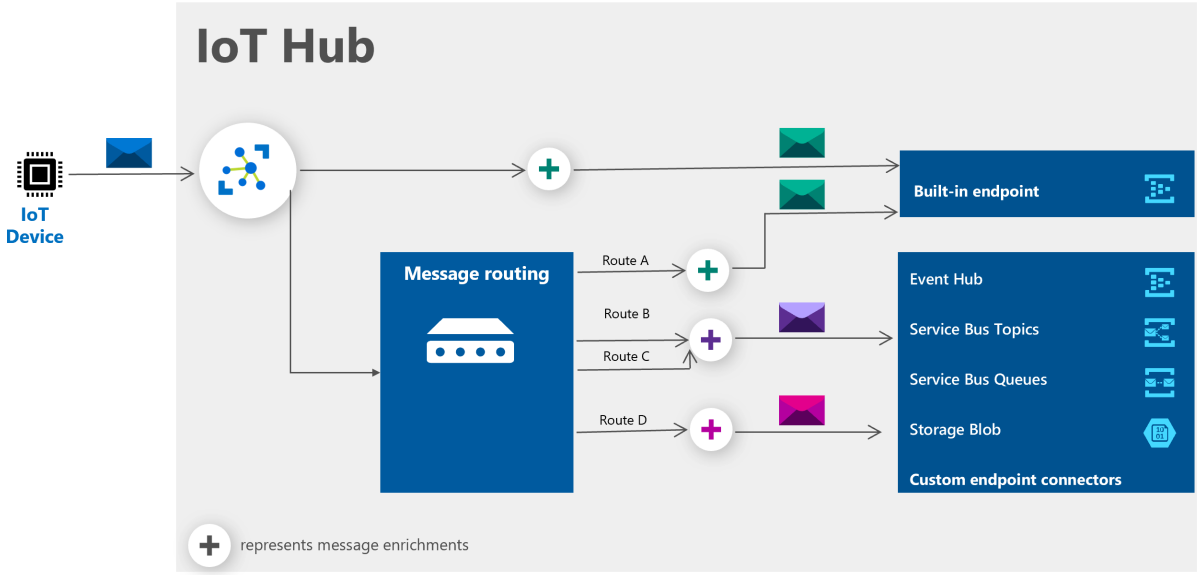
https://learn.microsoft.com/de-de/training/modules/introduction-iot-solution-architecture/2-subsystems-iot-architecture

„Definition“

Das Internet der Dinge (IoT) ist ein Netzwerk aus mit dem Internet verbundenen Geräten, die eingebettete Sensordaten für die zentrale Verarbeitung an die Cloud übermitteln.

IoT Lösung:

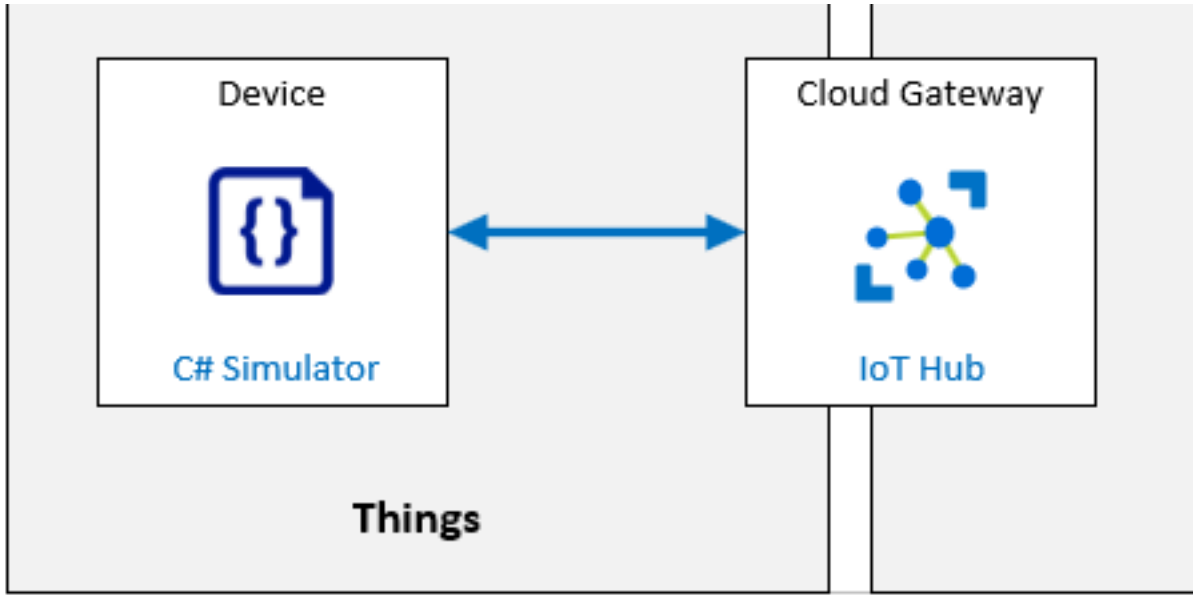
- Eine Geräteseite (bestehend aus einzelnen Geräten), die als Datenquelle fungiert
- Eine Cloudseite, die Daten sammelt und Ressourcen zum Analysieren und Verwalten der Daten bereitstellt



https://learn.microsoft.com/de-de/training/modules/explore-azure-iot-services/2-features-azure-iot-hub

Azure IoT Hub

- ein in der Cloud gehosteter, verwalteter Dienst, der als zentraler Nachrichtenhub für die bidirektionale Kommunikation zwischen IoT-Anwendungen und den Geräten dient
- unterstützt mehrere Messagingmuster wie z.B. Gerät-zu-Cloud-Telemetrie, Dateiuploads von Geräten und Request-Response-Methoden zum Steuern der Geräte über die Cloud



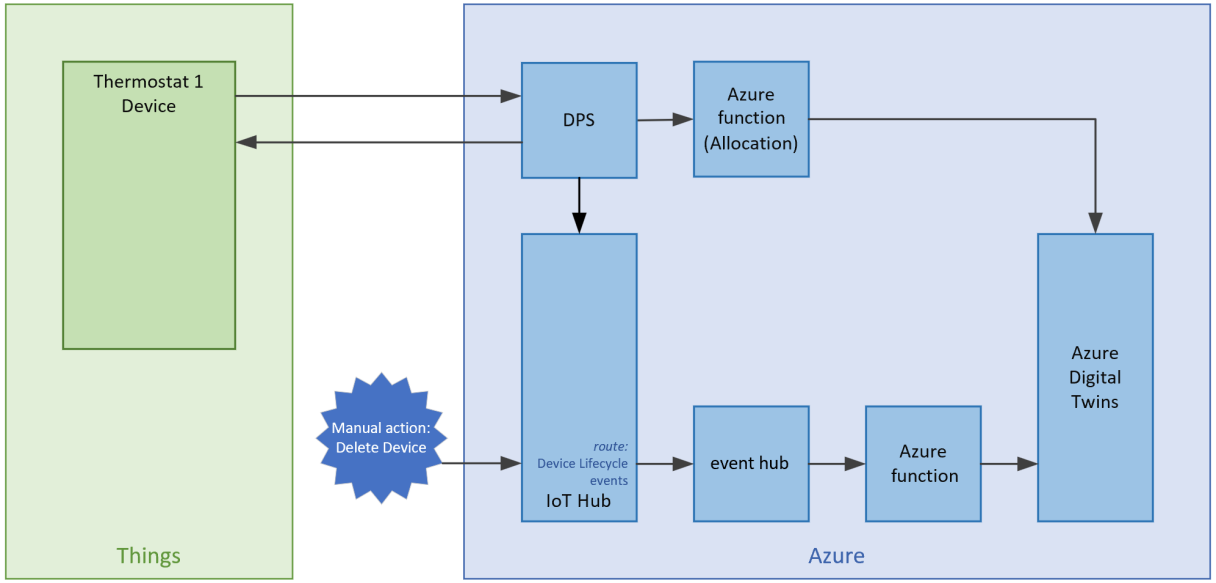
Lab 04: Connect an IoT Device to Azure - Module 2: Devices and Device Communication

LAB_AK_04-connect-iot-device-to-azure.html

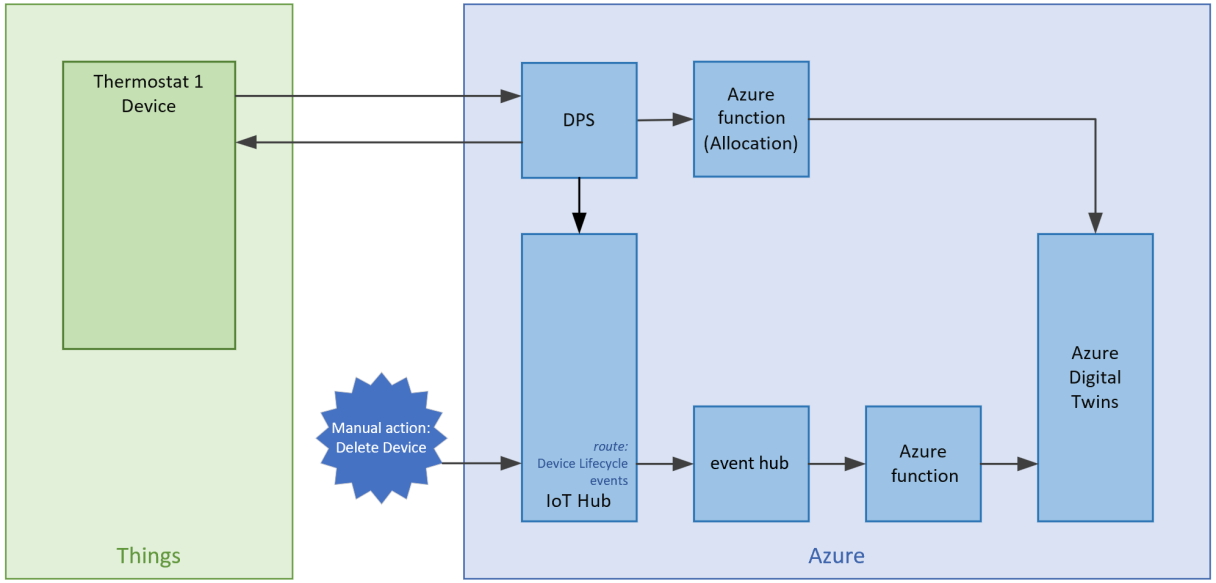
Azure IoT Hub Device Provisioning Service

Der Azure IoT Hub Device Provisioning Service ermöglicht die Bereitstellung von IoT-Geräten mithilfe einer Kombination aus Registrierungs-, Bereitstellungs- und Nachweisfunktionen

Der IoT Hub Device Provisioning-Dienst ist ein Hilfsdienst für IoT Hub, der die JIT-Bereitstellung im richtigen IoT-Hub ohne manuelles Eingreifen ermöglicht



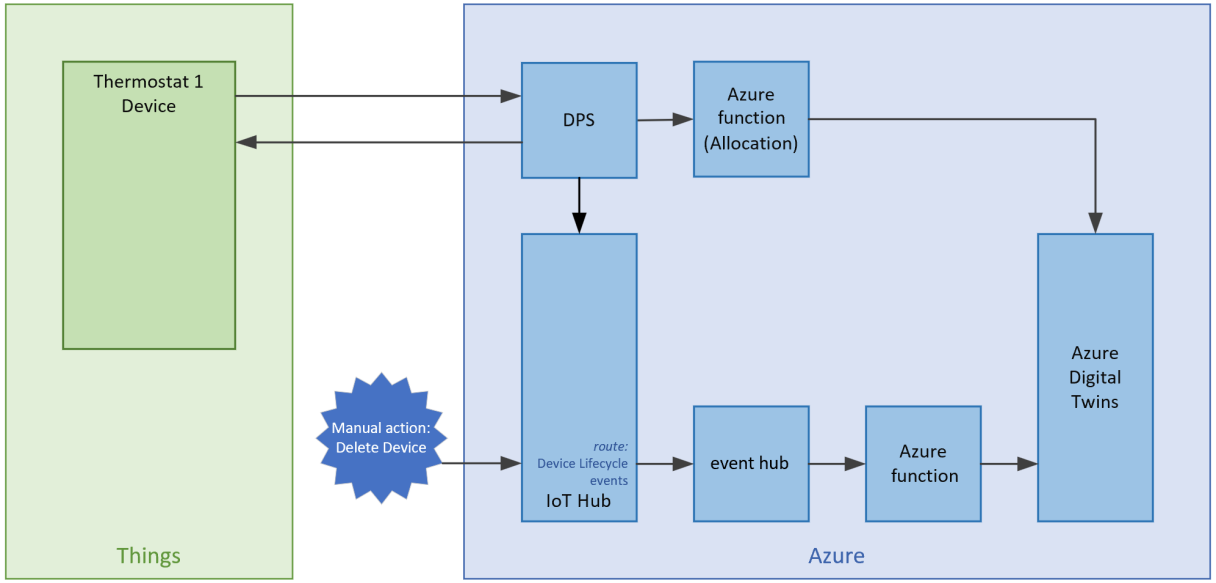
https://learn.microsoft.com/de-de/training/modules/examine-device-provisioning-service-terms-concepts/3-device-provisioning-service



https://learn.microsoft.com/de-de/training/modules/examine-device-provisioning-service-terms-concepts/3-device-provisioning-service

Features des Device Provisioning-Diensts

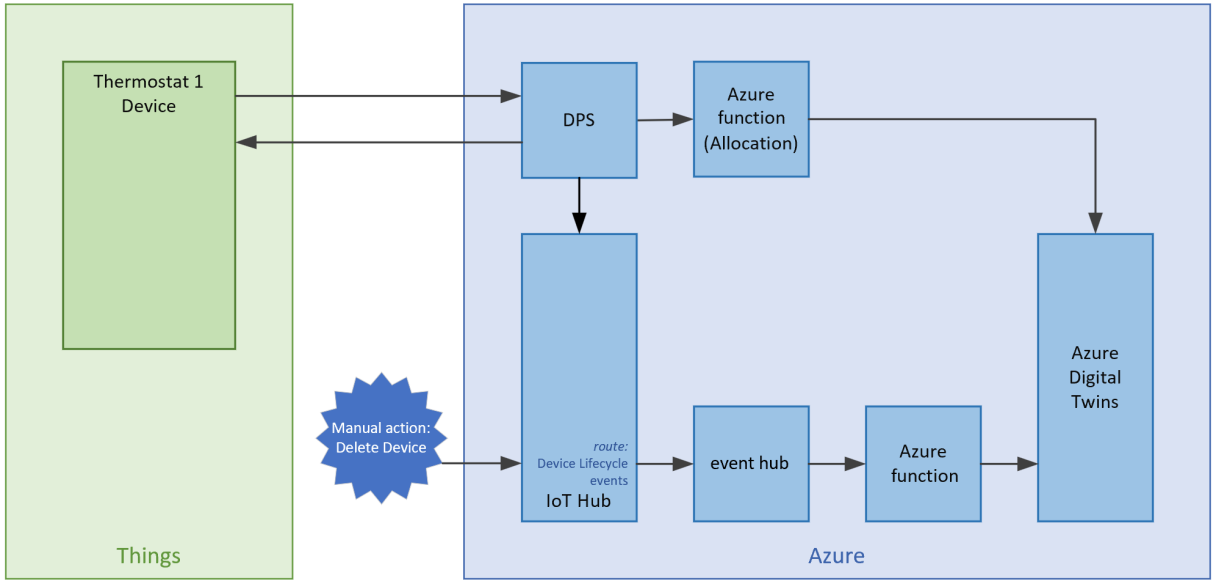
- Unterstützung des sicheren Nachweises für Identitäten
- Eine Registrierungsliste mit der vollständigen Aufzeichnung von Geräten/Gerätegruppen, die sich zu einem beliebigen Zeitpunkt registrieren könnten
- Verwenden mehrerer Zuordnungsrichtlinien für die Steuerung, wie Geräte von Device Provisioning Service den IoT-Hubs zugewiesen werden
- Überwachungs- und Diagnoseprotokolle, um sicherzustellen, dass alles ordnungsgemäß funktioniert
- Unterstützung für mehrere Hubs, sodass der Device Provisioning-Dienst Geräte mehreren IoT Hubs zuweisen kann
- Regionsübergreifende Unterstützung



https://learn.microsoft.com/de-de/training/modules/examine-device-provisioning-service-terms-concepts/3-device-provisioning-service

Anwendungsszenarien des DPS

- Bereitstellung ohne manuelles Eingreifen für eine einzelne IoT-Lösung ohne werkseitige Hartcodierung von IoT Hub-Verbindungsinformationen (Anfangssetup)
- Hubübergreifender Lastenausgleich für Geräte
- Herstellen der Verbindung eines Geräts mit IoT Hub mit der geringsten Wartezeit (Geo-Sharding)
- Erneute Bereitstellung basierend auf einer Änderung im Gerät
- Wechseln der Schlüssel, die vom Gerät verwendet werden, um eine Verbindung mit IoT Hub herzustellen

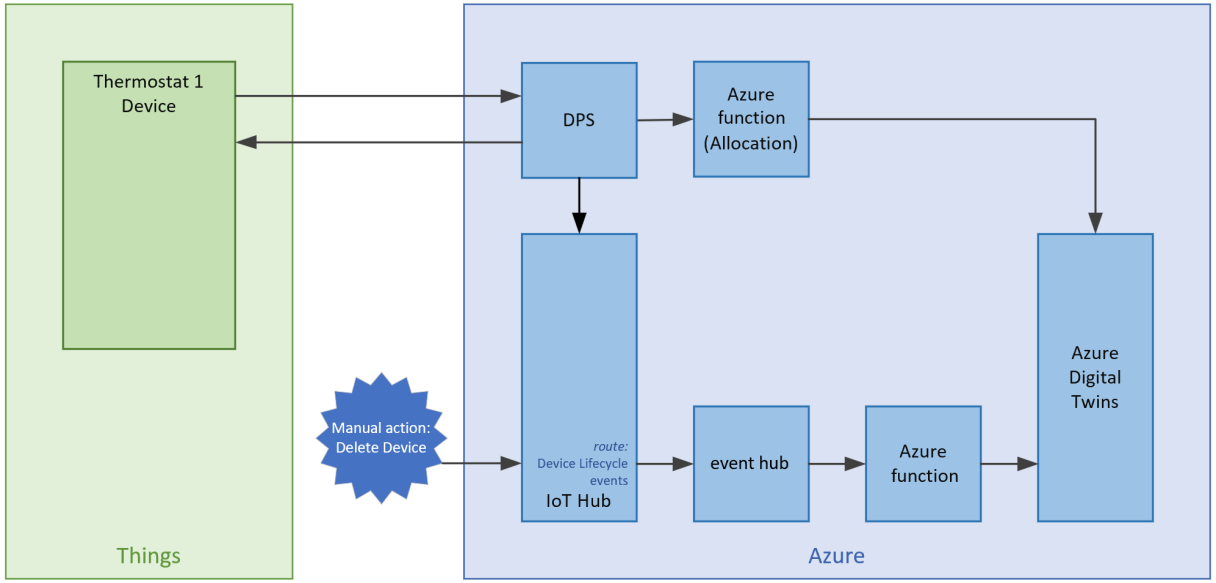


https://learn.microsoft.com/de-de/training/modules/examine-device-provisioning-service-terms-concepts/3-device-provisioning-service

Konzept des DPS

Die Gerätebereitstellung mit dem Device Provisioning Service ist ein zweiteiliger Vorgang:

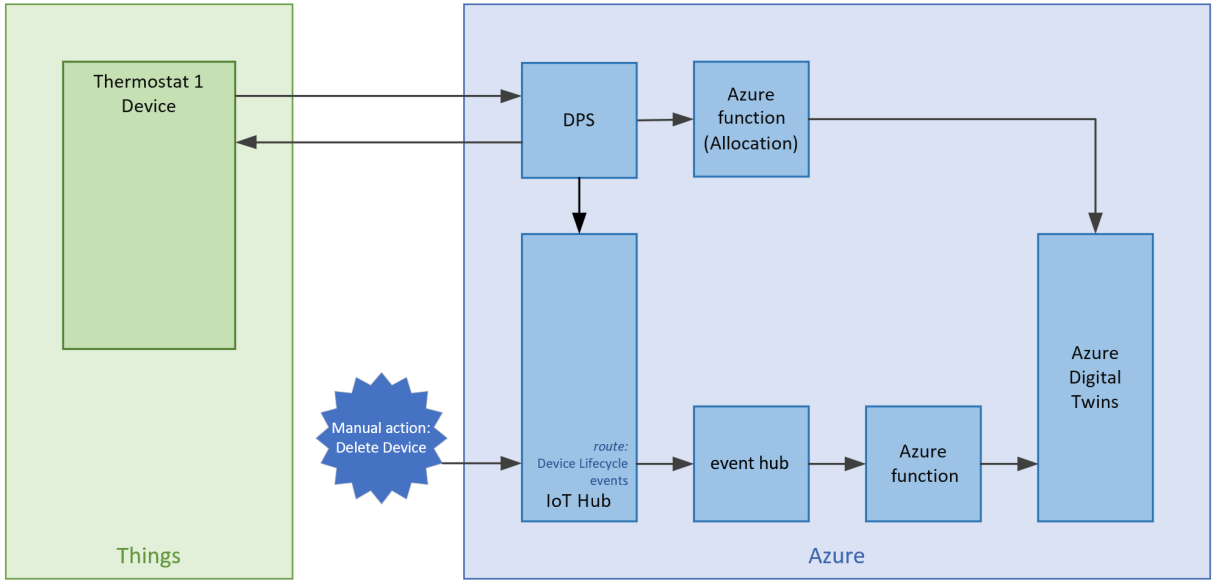
- Im ersten Teil wird durch Registrieren des Geräts eine erstmalige Verbindung des Geräts mit der IoT-Lösung hergestellt
- Im zweiten Schritt wird basierend auf den spezifischen Anforderungen der Lösung die geeignete Konfiguration auf das Gerät angewendet
- Nach Ausführung beider Schritte ist das Gerät vollständig bereitgestellt. Mit dem DPS werden beide Schritte automatisiert, sodass das Gerät nahtlos bereitgestellt wird.



https://learn.microsoft.com/de-de/training/modules/examine-device-provisioning-service-terms-concepts/3-device-provisioning-service

Zuordnungsrichtlinie

- Gleichmäßig gewichtete Verteilung: Bei verknüpften IoT Hubs ist die Wahrscheinlichkeit gleich hoch, dass Geräte für sie bereitgestellt werden (Standardeinstellung)
- Niedrigste Latenz: Geräte werden für einen IoT Hub mit der geringsten Latenz für das Gerät bereitgestellt.
- Statische Konfiguration über die Registrierungsliste: Die Angabe des gewünschten IoT Hub in der Registrierungsliste hat gegenüber der Zuordnungsrichtlinie auf Dienstebene Vorrang.
- Benutzerdefiniert (Azure Functions): Mit einer Zuweisungsrichtlinie kann genauer gesteuert werden, wie Geräte einem IoT-Hub zugewiesen werden.



https://learn.microsoft.com/de-de/training/modules/examine-device-provisioning-service-terms-concepts/3-device-provisioning-service

Registrierung

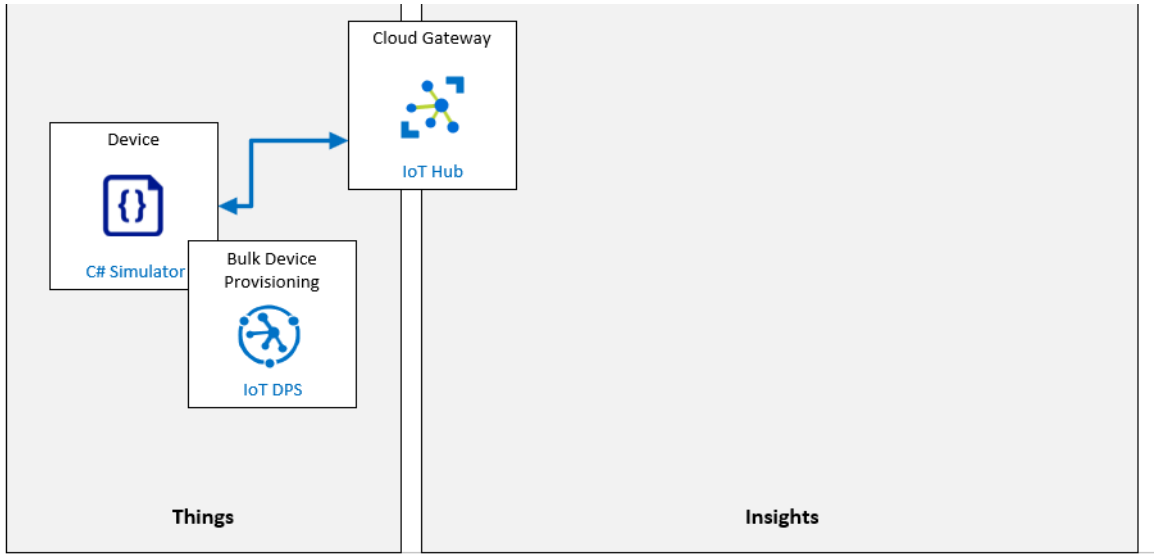
Eine Registrierung ist der Datensatz von Geräten, die sich über die automatische Bereitstellung registrieren können

- Gruppenregistrierung:

Eine Registrierungsgruppe wird für eine große Anzahl von Geräten, die eine gewünschte Erstkonfiguration gemeinsam nutzen

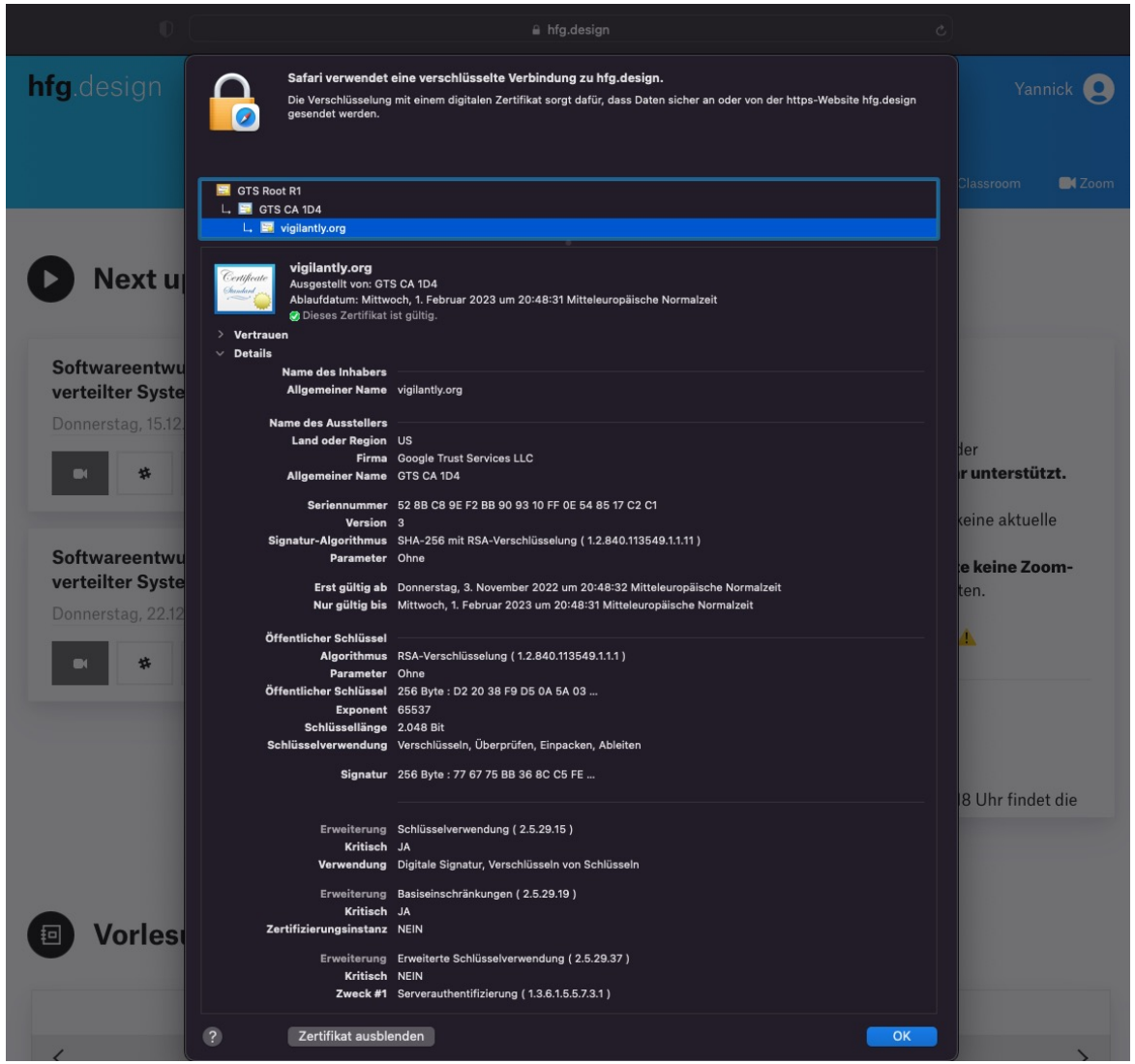
- Individuelle Registrierung:

Individuelle Registrierungen werden für Geräte, die einzigartige Erstkonfigurationen erfordern



Lab 05: Individual Enrollment of a Device in DPS - Module 3: Device Provisioning at Scale

LAB_AK_05-individual-enrollment-of-device-in-dps.html



X.509-Zertifikate

X.509 ist ein Standardformat für Public-Key-Zertifikate, digitale Dokumente, die kryptografische Schlüsselpaare sicher mit Identitäten wie Websites oder IoT Geräte verknüpfen

Certificate Summary

Subject

RDN	Value
Common Name (CN)	sensor-thl-2000

Properties

Property	Value
Issuer	CN = Azure IoT Hub CA Cert Test Only
Subject	CN = sensor-thl-2000
Valid From	14 Dec 2022, 4:40 p.m.
Valid To	13 Jan 2023, 4:40 p.m.
Serial Number	03 (3)
CA Cert	No
Key Size	4096 bits
Fingerprint (SHA-1)	79:E0:70:E1:FA:18:F8:D8:9F:27:4B:B6:22:3D:97:2A:44:CF:79:86
Fingerprint (MD5)	BD:0E:85:0E:73:0F:98:92:D8:8D:EB:94:5F:48:F3:00
SANS	

X.509-Zertifikate

Version: Welche X.509-Version für das Zertifikat verwendet wurde.

Seriennummer (CN): Die Identität, die das Zertifikat ausstellt, muss diesem eine Seriennummer zuweisen, damit man es von anderen Zertifikaten unterscheiden kann.

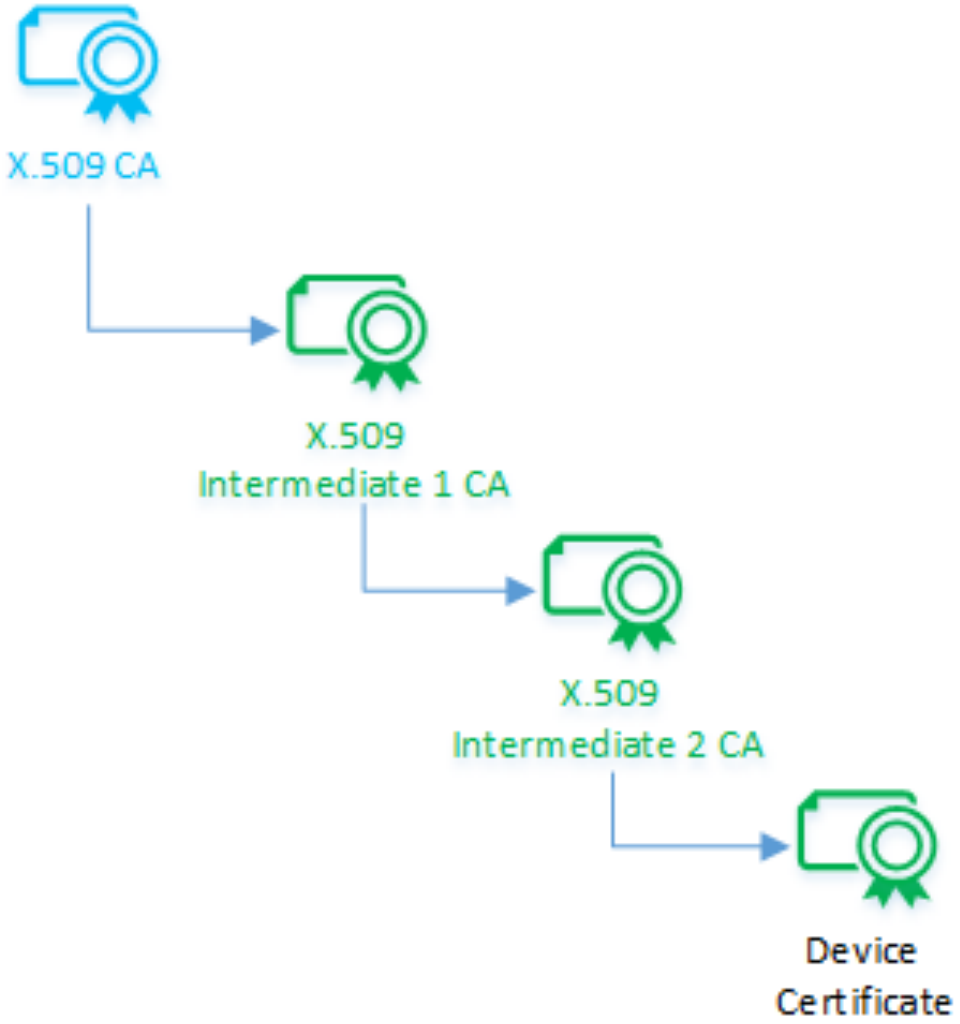
Algorithmus-Information: Das ist der vom Aussteller verwendete Algorithmus, um das Zertifikat zu unterzeichnen.

Eindeutiger Name des Ausstellers: Der Name der Instanz, die das Zertifikat ausgestellt hat. In der Regel ist das eine Zertifizierungsstelle (CA/Certificate Authority).

Gültigkeitsdauer des Zertifikats: Zeitrahmen der Gültigkeit des Zertifikats.

Eindeutiger Name des Subjekts: Der Name der Identität, für die das Zertifikat ausgestellt wurde.

Informationen über den öffentlichen Schlüssel (Public Key) des Subjekts: Der öffentliche Schlüssel, der mit der Identität assoziiert ist.

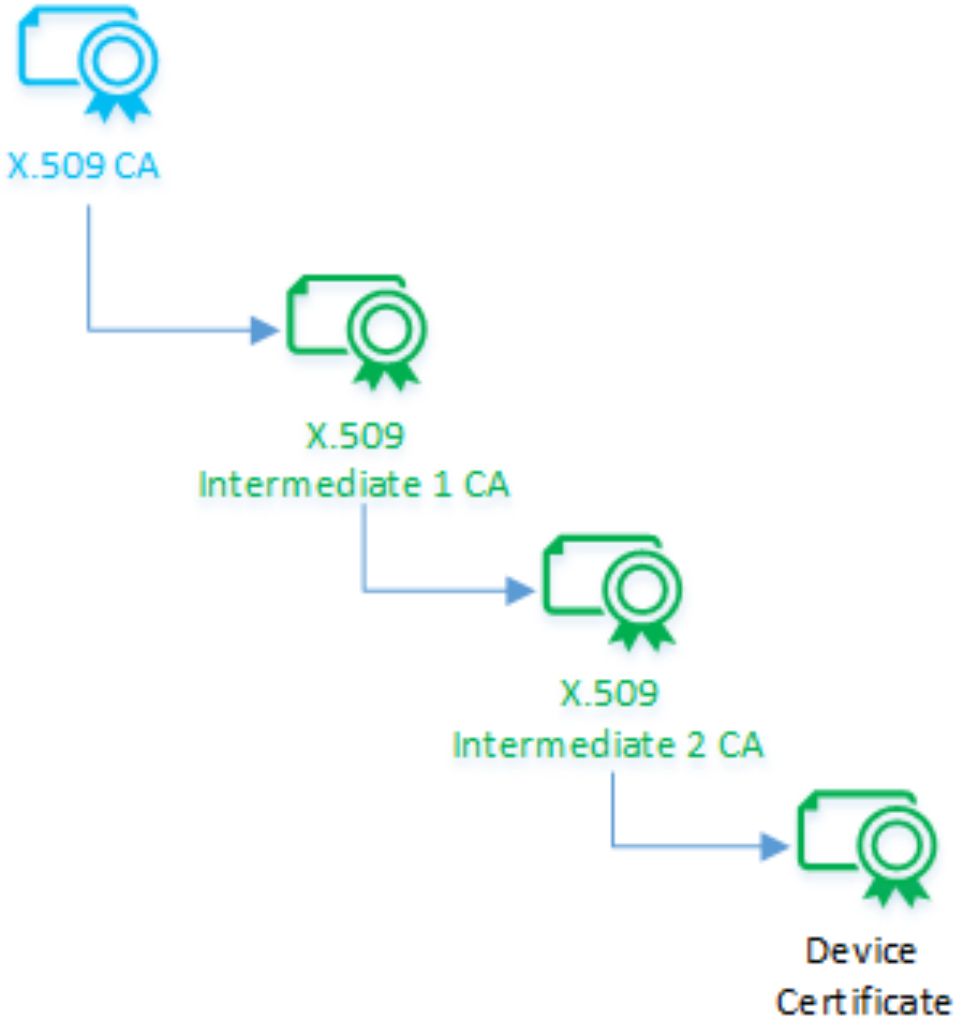


https://learn.microsoft.com/de-de/azure/iot-hub/iot-hub-x509ca-overview

Chain of Trust

Die Vertrauenskette bezieht sich auf das SSL-Zertifikat und wie es mit einer vertrauenswürdigen Zertifizierungsstelle verbunden ist.

Damit ein SSL-Zertifikat als vertrauenswürdig eingestuft werden kann, muss es bis zum Root-Zertifikat zurückverfolgt werden können, von dem es signiert wurde, d. h. alle Zertifikate in der Kette - Geräte-, Intermediate- und Root-Zertifikate - müssen ordnungsgemäß vertrauenswürdig sein.

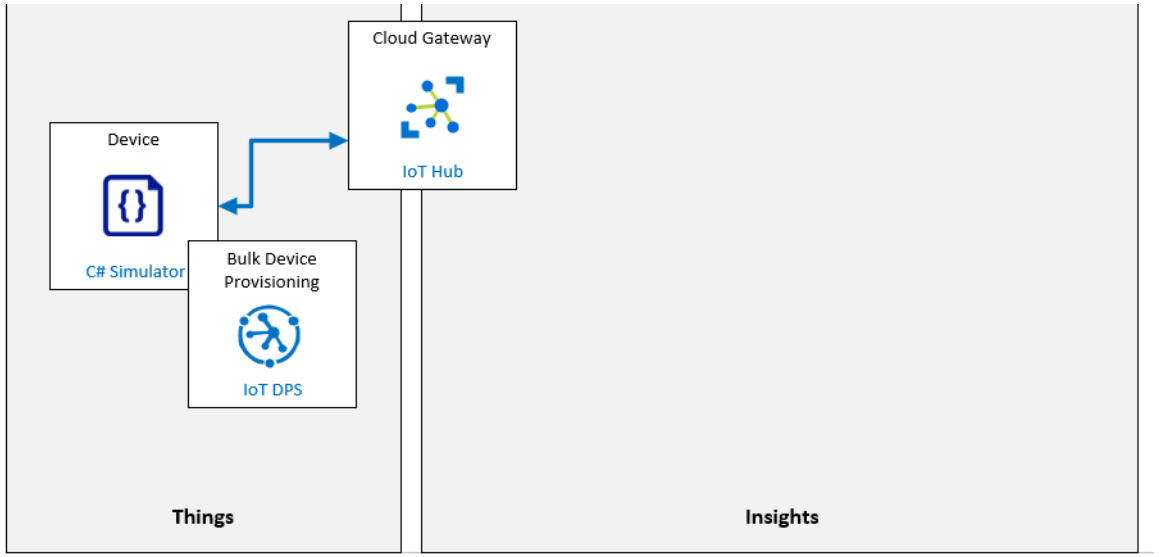


https://learn.microsoft.com/de-de/azure/iot-hub/iot-hub-x509ca-overview

Chain of Trust

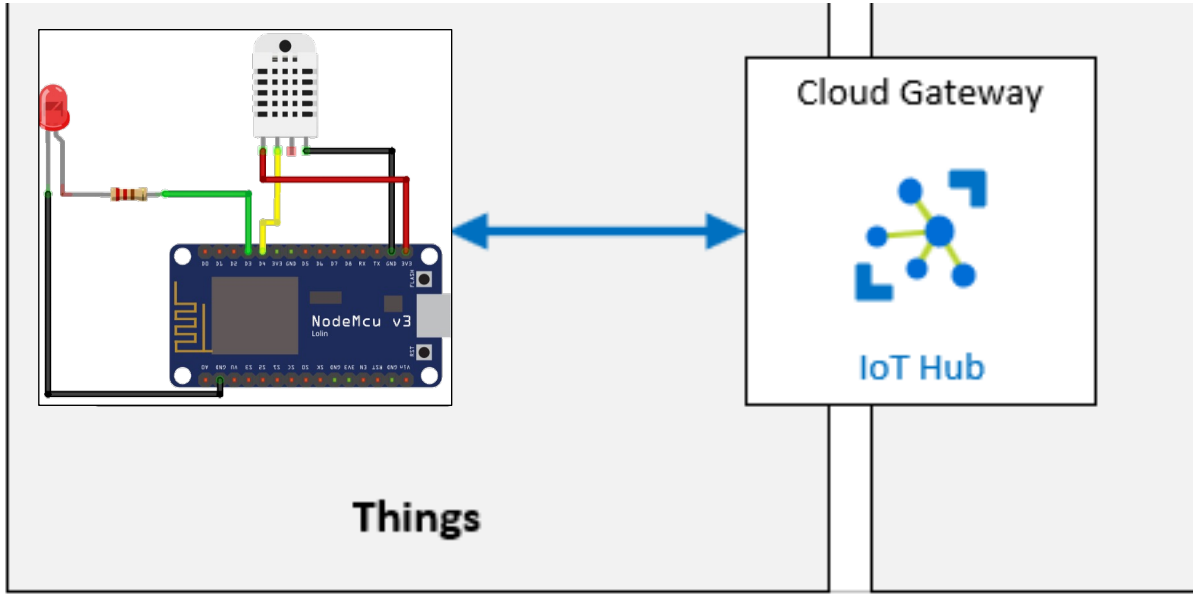
Die Vertrauenskette besteht aus 3 Teilen:

- Root-Zertifikat - Es ist ein digitales Zertifikat, das der ausstellenden Zertifizierungsstelle gehört.
- Intermediate Certificate – fungiert als Vermittler zwischen den geschützten Root-Zertifikaten und den öffentlich ausgestellten Server- oder Gerätezertifikaten.
- Gerätezertifikat - Das Gerätezertifikat ist das Zertifikat, das für die spezifische Geräte-ID ausgestellt wurde.



Lab 06: Automatically provision IoT devices securely and at scale with DPS - Module 3: Device Provisioning at Scale'

LAB_AK_06-automatic-enrollment-of-devices-in-dps.html



Aufgabe

Arduino mit dem Azure IoT Hub verknüpfen:

- Sensordaten per D2C Nachricht verschicken
  - Im JSON Datenformat
  - Als Telemetry Nachricht
  - Soll mit folgendem Command ausgelesen werden können:

az iot hub monitor-events --hub-name {IoTHubName} --device-id {deviceID}

- Aktor per C2D Nachricht steuern
  - IM JSON Datenformat
  - Kann im Portal oder VS Code PlugIn getriggert werden