KEYFACTOR MICROCHIP

SOLUTION BRIEF

Securing Embedded Devices with Microchip and Keyfactor

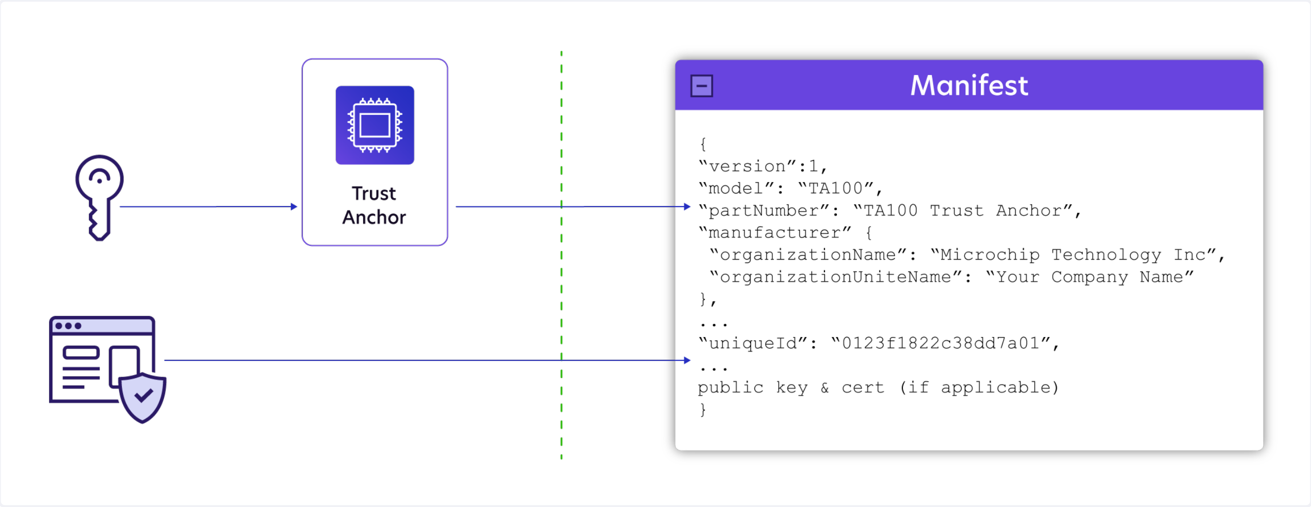
How to secure IoT devices in a zero-trust world with
Microchip Trust Anchor security ICs and Keyfactor Command

Securing Embedded IoT devices throughout the supply chain is essential to prevent fraudulent devices from accessing the OEM or Intellectual Property (IP) owner's integrated IoT and cloud systems, such as Microsoft Azure IoT Hub. Using a secure authentication IC (such as Microchip's Trust Anchor TA100) with the Keyfactor Command platform allows manufacturers to support Zero-Trust First-Use device provisioning, severely reducing the risk of attack or device compromise. This best practice is also beneficial when OEMS are leveraging insecure manufacturing locations, or offline contract manufacturers.

Secure Key Provisioning for the Authentication IC

Figure 1.

Microchip Secure Provisioning Service



```
{
“version”:1,
“model”: “TA100”,
“partNumber”: “TA100 Trust Anchor”,
“manufacturer” {
 “organizationName”: “Microchip Technology Inc”,
 “organizationUniteName”: “Your Company Name”
},
...
“uniqueId”: “0123f1822c38dd7a01”,
...
public key & cert (if applicable)
}
```

Figure one shows Microchip secure key provisioning service in their factory manufacturing both the secure Trust Anchor and manifest file. A Trust Anchor is a definite purpose integrated circuit equipped with crypto-accelerators and common criteria JIL high secure key storage areas. All cryptography related functions are performed inside the device, and keys are physically isolated from code, users and 3rd party manufacturers. The device provisioning is performed by securely creating a keypair and a CSR (certificate signing request). The CSR can be signed by any OEM certificate authority.

The public details of each authentication IC manufactured for the OEM or IP owner is stored in a manifest. The manifest includes authentication IC details such as the device unique ID, the public key, the part number, etc. The manifest is only provided to the OEM, IP owner, and the parties they authorize. Then, the provisioned devices are provided to the contract manufacturer.

Security at Contract Manufacturers is Insecure

Figure 2.

Isolate Manufacturing Backdoors with the Trust Anchor and Keyfactor

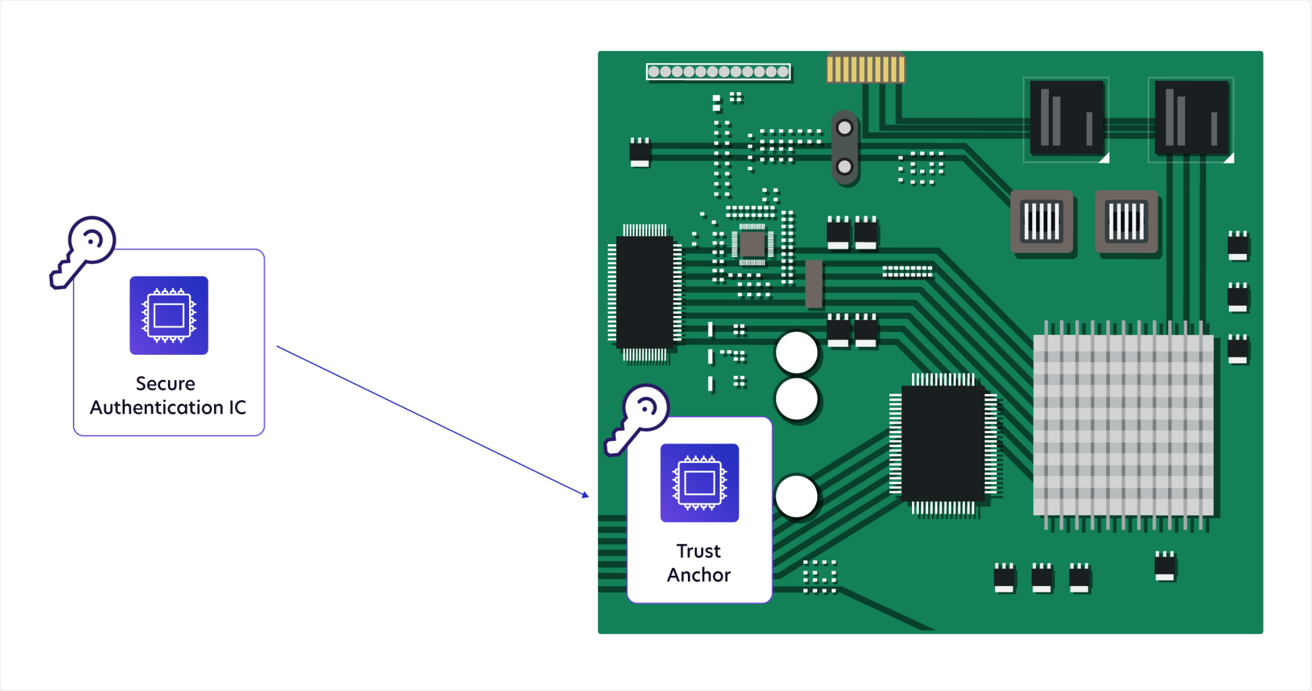
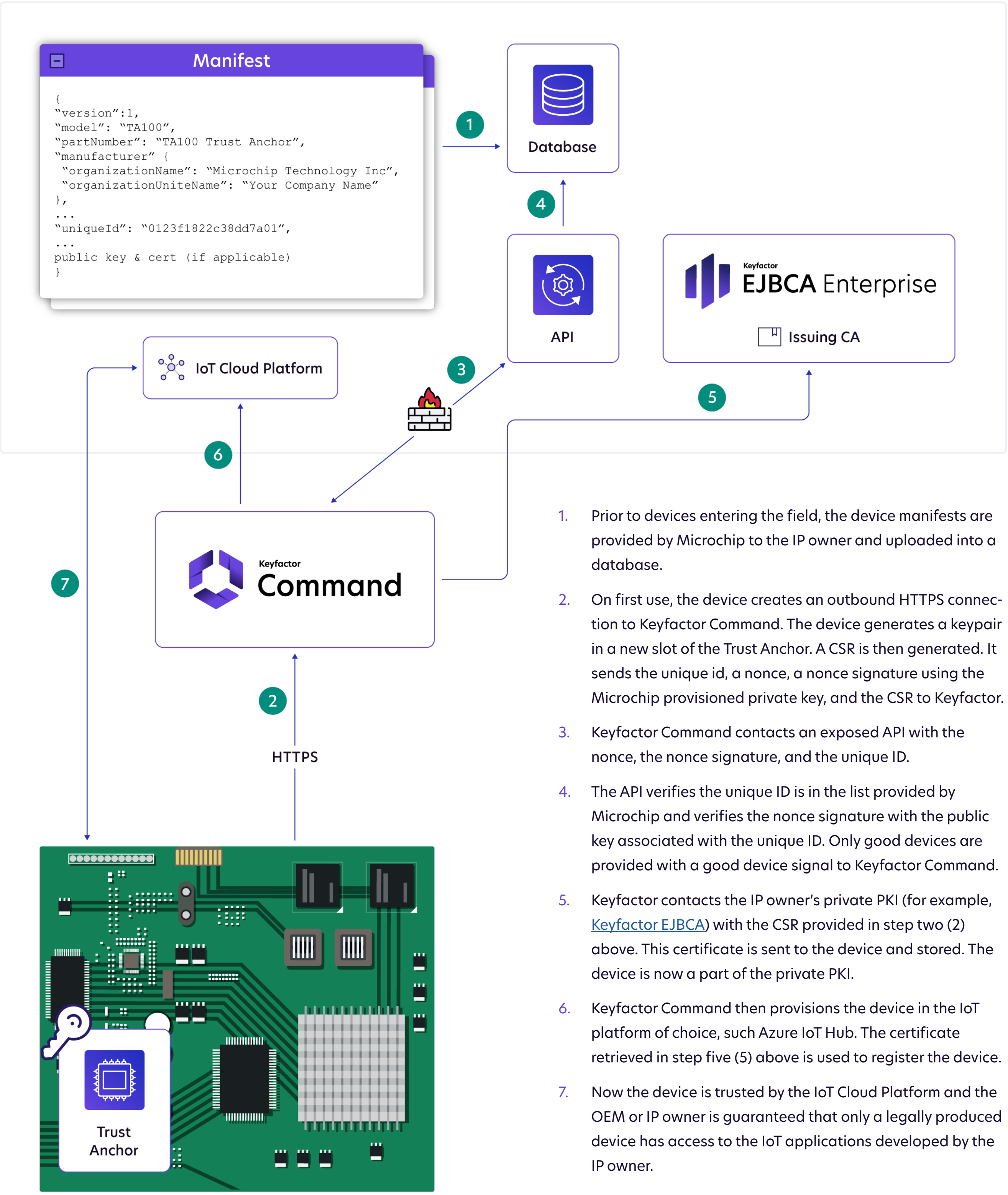


Figure two shows the Trust Anchor TA100 being fitted onto the IoT embedded system. The TA100 placement into the full assembly can be performed in an insecure/untrusted environment at your oversea ODM without sharing the secured private key with the manufacturer. In this manner, only devices produced under contract with the contract manufacturer are permitted to receive Trust Anchors produced by Microchip for this manufacturer. If other Microchip Trust Anchors (procured outside of the correct supply chain) are used, later vetting provides assurance that these devices are not allowed to access the OEM or IP owner's IoT Cloud Platform.

First-Use Zero-Trust Provisioning

Figure 3.

IP Owner



```
{
"version":1,
"model": "TA100",
"partNumber": "TA100 Trust Anchor",
"manufacturer" {
 "organizationName": "Microchip Technology Inc",
 "organizationUniteName": "Your Company Name"
},
...
"uniqueId": "0123f1822c38dd7a01",
...
public key & cert (if applicable)
}
```

1. Prior to devices entering the field, the device manifests are provided by Microchip to the IP owner and uploaded into a database.
2. On first use, the device creates an outbound HTTPS connection to Keyfactor Command. The device generates a keypair in a new slot of the Trust Anchor. A CSR is then generated. It sends the unique id, a nonce, a nonce signature using the Microchip provisioned private key, and the CSR to Keyfactor.
3. Keyfactor Command contacts an exposed API with the nonce, the nonce signature, and the unique ID.
4. The API verifies the unique ID is in the list provided by Microchip and verifies the nonce signature with the public key associated with the unique ID. Only good devices are provided with a good device signal to Keyfactor Command.
5. Keyfactor contacts the IP owner's private PKI (for example, Keyfactor EJBCA) with the CSR provided in step two (2) above. This certificate is sent to the device and stored. The device is now a part of the private PKI.
6. Keyfactor Command then provisions the device in the IoT platform of choice, such Azure IoT Hub. The certificate retrieved in step five (5) above is used to register the device.
7. Now the device is trusted by the IoT Cloud Platform and the OEM or IP owner is guaranteed that only a legally produced device has access to the IoT applications developed by the IP owner.

From time to time, the device should check in with Keyfactor Command. Keyfactor Command is a powerful certificate lifecycle automation platform. The platform enables device certificate bulk management including:

- Certificate renewal before expiration
- Management of roots of trust on the devices
- Crypto-agility – changing the cryptography on devices from a central platform
    - Push the new root of trust
    - Generate a new keypair and CSR
    - Retrieve a new certificate from the new PKI chain
    - Deletion of the old root of trust
- Automatically updating device certificates in the IoT Cloud platform.

Designers and developers of IoT devices can leverage these concepts above to implement strong security best practices from the start. Leveraging Trust Anchor devices and unique device identity certificates along with a robust process for provisioning upon first use allows OEMs to produce devices that will be protected against unauthorized attacks or compromise. Robust and scalable Private PKI solutions (Keyfactor EJBCA) in combination with a robust Certificate Lifecycle Automation platform (Keyfactor Command) provide a simple way to manage risk from provisioning through lifecycle of IoT devices.