SOLUTION BRIEF

Continuous device protection and identity management for Industrial IoT using STMicroelectronics STSAFE-TPM

How EnactTrust, Keyfactor, and STMicroelectronics STSAFE-TPM
deliver end-to-end device security for IoT operators

To protect connected devices against compromise, ensuring the boot process is secured is critical. Secure Boot is an effective security method to ensure that the operating system boot images and code are authenticated against hardware before they are authorized to be used in the boot process.

However, Secure Boot only ensures that device health is checked once — at system startup. Afterward, an IoT device can operate for months and even years without undergoing system integrity checks. This leaves IoT operators at substantial risk of running compromised IoT systems.

To solve this, ***EnactTrust*** provides continuous device health checks using the new ***STMicroelectronics*** STSAFE Trusted Platform Module 2.0 (TPM) for industrial applications, available with an SPI (ST33GTPMISPI) or I²C interface (ST33GTPMII2C). ***EnactTrust*** also provides device identity and certificate management, thanks to an integration with ***Keyfactor's PKI and machine identity automation platform***. Leveraging the STSAFE-TPM secure key generation and storage, ***EnactTrust*** can protect the device identity from being altered and used for malicious activity. The result is a trusted network of IoT systems.

Use cases

- Tamper-proofing Industrial IoT systems, including Edge gateways.
- Maintaining device health and identity by only allowing genuine firmware and configuration.
- Establishing a network of trusted IoT devices using hardware root-of-trust and PKI.
- Tracking and renewing certificates before they expire.
- First use device provisioning in a Zero Trust manner.

Requirements

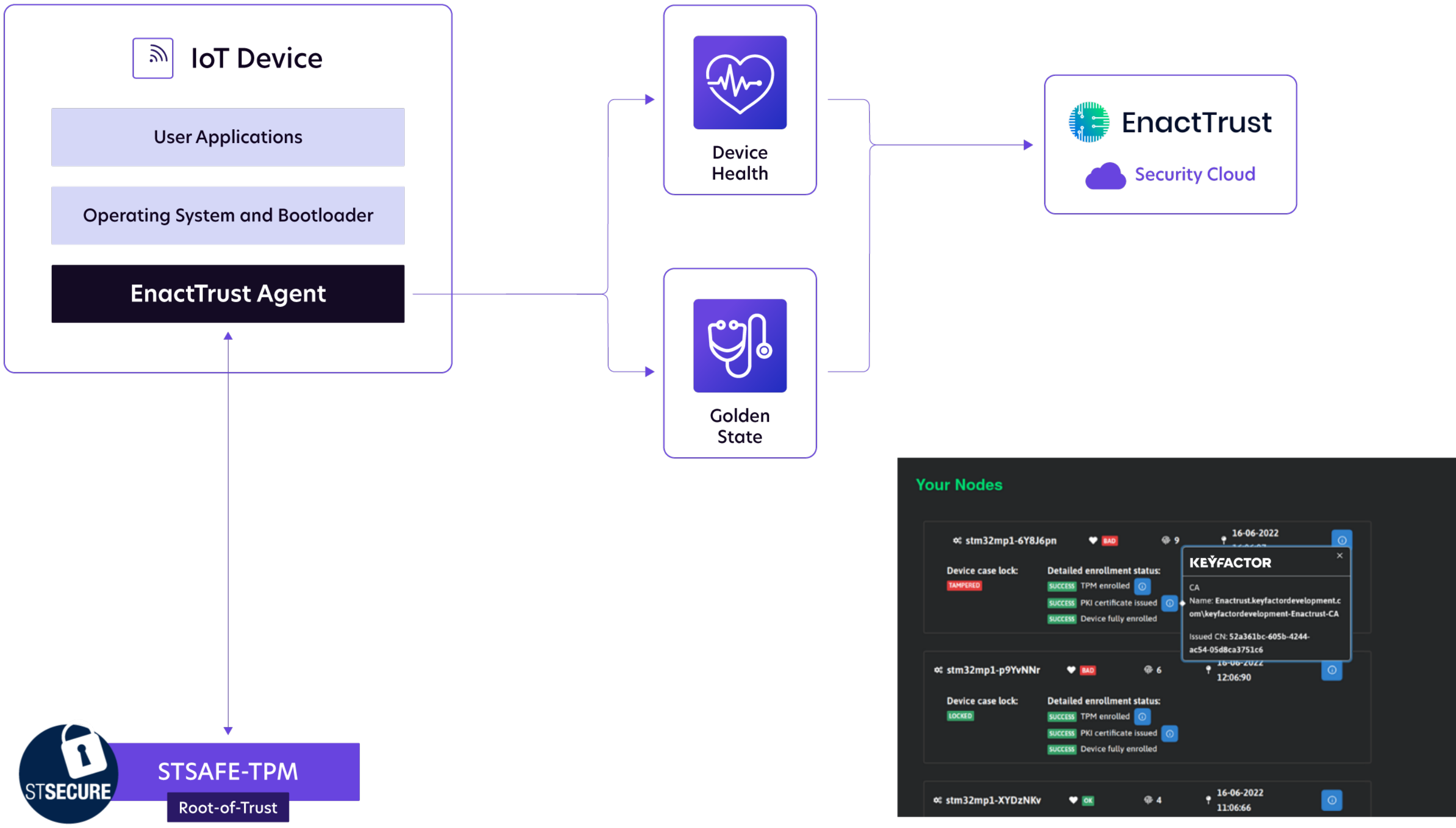
- Firmware ownership — to leverage the benefits of EnactTrust, the system owner must be able to deploy the EnactTrust firmware agent.
- Trusted Platform Module 2.0 (TPM) — device health checks and identity guarantees are provided using the hardware root-of-trust for reporting and storage of the Industrial STSAFE-TPM.

SOLUTION OVERVIEW:

Continuous device health protection and compliance

EnactTrust offers a unique combination of attestation technology and ease-of-use that helps vital industries adopt state-of-the-art security measures.

EnactTrust verifies the health of IoT devices continuously and renders entire classes of exploits useless. It consists of an easy-to-deploy firmware agent that runs as part of ARM's Trusted Execution Environment (TF-M/TF-A) and a cloud service.



Your Nodes

stm32mp1-6Y8J6pn ♥ BAD 9 16-06-2022

Device case lock: TAMPERED

Detailed enrollment status:
SUCCESS TPM enrolled
SUCCESS PKI certificate issued
SUCCESS Device fully enrolled

KEYFACTOR

CA
Name: Enactrust.keyfactordevelopment.com\keyfactordevelopment-Enactrust-CA

Issued CN: 52a361bc-605b-4244-ac54-05d8ca3751c6

stm32mp1-p9YvNNr ♥ BAD 6 16-06-2022 12:06:90

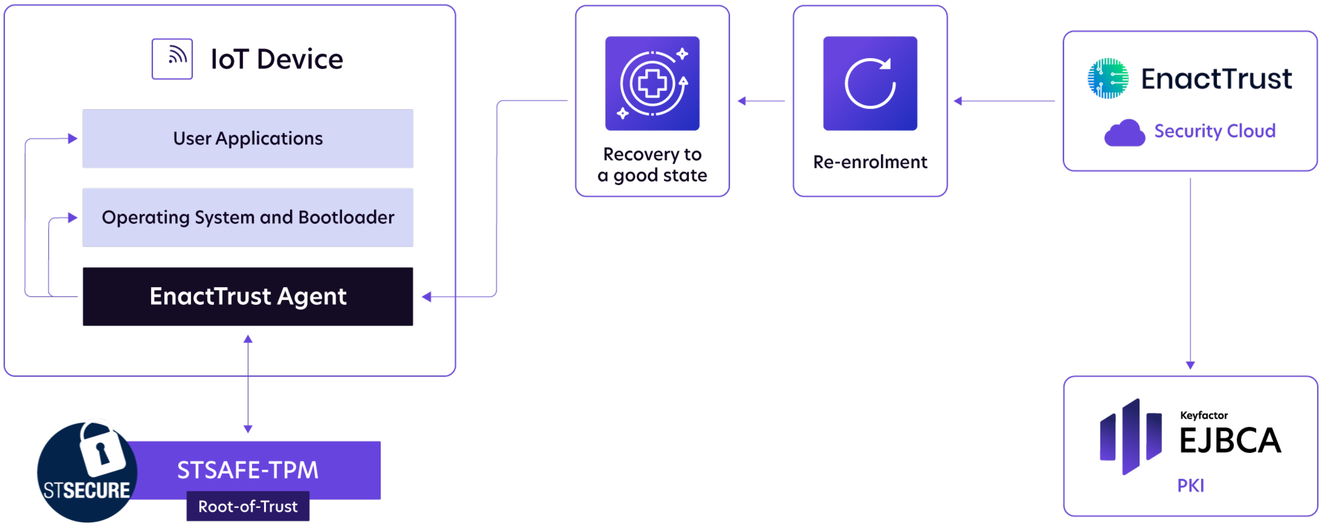
Device case lock: LOCKED

Detailed enrollment status:
SUCCESS TPM enrolled
SUCCESS PKI certificate issued
SUCCESS Device fully enrolled

stm32mp1-XYDzNKv ♥ OK 4 16-06-2022 11:06:66

Use the ***EnactTrust Security Cloud*** to get notified immediately when suspicious activity is detected. You can set up workflows that restore the device's firmware to a known good state, remotely wipe data, do OTA updates, or transform raw logs into structured data.

EnactTrust enables easy integration with ARM-based IoT devices and has no significant impact on the device performance and power consumption. The solution requires no changes to the software running on the protected device.



EnactTrust also provides compliance with upcoming IoT cybersecurity regulations in the US, UK, and EU, which mandate IoT devices possess critical cybersecurity capabilities, including *device identification, device configuration, data protection, and cybersecurity state awareness*.

Key features:

- Device identity and health protection backed by the STSAFE-TPM root-of-trust.
- Remote data wipe to be compliant with IoT regulations in US, UK, and EU markets.
- Secure Vault for storing sensitive data in the physically protected NVRAM of the STSAFE-TPM.

IoT Device Identity Management

Every device needs a trusted identity, and every identity must be managed. With Keyfactor, IoT operators get full lifecycle identity management for IoT devices at scale — so you can protect every device from manufacturing to end-of-life.

EJBCA Enterprise is a flexible and powerful PKI that makes it easy to issue trusted and unique certificate-based identities for IoT devices at massive scale. The solution is available in the cloud, as a service (SaaS), and as a turnkey software or hardware appliance.

When combined with Keyfactor Control, an end-to-end IoT identity automation platform, IoT operators can rapidly issue, provision, renew, and revoke certificates and keys throughout the device lifecycle — all from a single console. They can also integrate with other private, public, or cloud-based certificate authorities (CAs).

Keyfactor provides first use device provisioning using birth certificates along with shared secrets known by the device and any backend enterprise system. The provisioning process adapts to individual business use cases.

Keyfactor provides automatic enrollment (ODKG with PKCS#10 CSR) for specific use case device identification certificates. For example, Azure hub identity, TLS certificates, and device-to-device identity certificates can all be managed through the Keyfactor platform.

With Keyfactor, IoT operators can be crypto-agile, such as moving from RSA2048 to ECC256 encryption on brownfield devices. This concept of crypto-agility also applies when root or issuing certificate authorities need to change or are compromised. The operator can quickly and remotely push a new root of trust to the devices, followed quickly by a new keypair generation/CSR request, followed finally by the removal of the old root of trust. This allows brownfield devices to stay relevant to shifting crypto requirements, such as changing from SHA-256 to SHA-384.

Secure Device Identity using STSAFE-TPM

Leveraging the secure key generation of a Trusted Platform Module 2.0, EnactTrust generates a secure device identity inside the physically tamper proofed STSAFE-TPM chip. This device identity cannot be spoofed, because it is anchored to the hardware root-of-trust of STSAFE-TPM.

Thanks to the integration between EnactTrust and Keyfactor IoT identity platform, the device identity can be provided to the device from a Keyfactor EJBCA Certificate Authority and anchored to the hardware root-of-trust for storage.