GAPFRUIT

REALIZATION

Step 1: Device Authenticity via Birth Certificate Provisioning Service

Hardware-Rooted Device Identity for OEM Mass-Manufacturing

Why it matters

Many devices still authenticate using serial numbers or MAC addresses—values that can be copied or spoofed, enabling attackers to impersonate devices without exploiting a single software vulnerability.
Each device leaves production with a tamper-resistant certificate that provides cryptographic proof of origin, which can be verified at any time.
The provisioning step runs on existing manufacturing equipment and requires no modifications to the production line.

TRUSTED® COMPUTING GROUP | digicert®

Gapfruit is a Contributor Member of the Trusted Computing Group (TCG), actively shaping future standards for trustworthy device manufacturing.

Our partner DigiCert is the world's leading PKI and digital trust solutions provider, securing billions of connections, devices, and identities worldwide.

The New Standard for Device Trust

The Birth Certificate Provisioning Service is built in alignment with Trusted Computing Group (TCG) specifications and operates in conjunction with DigiCert, a globally recognized provider of PKI-based trust infrastructure. This foundation ensures that device identities follow widely accepted and independently validated industry practices.

Each device generates and stores a TPM-attested, hardware-rooted certificate during its initial boot, establishing a verifiable chain of device identity that supports secure operation and long-term lifecycle verification. Modern cloud platforms such as Azure IoT Hub and AWS IoT Core already rely on certificate-based authentication, reinforcing the need for hardware-rooted identity at the device level.

Benefits

Authenticity that protects your business

Hardware-rooted Birth Certificates provide legally defensible proof that a device is genuine and produced under your control. They eliminate weak identifiers, such as serial numbers or MAC addresses, as trust anchors, thereby reducing the risk of counterfeit hardware, unauthorized replacements, and the associated financial and reputational consequences.

Regulatory Protection

Hardware-anchored identity supports compliance with authenticity and integrity requirements in regulations such as the CRA or NIS2, strengthening the OEM's position in regulated safety- and security-critical markets where provable device authenticity is becoming mandatory.

Seamless and scalable Integration

Verifiable device identity can be added during manufacturing within seconds, using existing equipment and workflows, enabling large-scale provisioning of birth certificates without new infrastructure, additional operational burden, or adjustments to the production line.

Take the First Step Toward Trustworthy Devices

Please discuss with our experts how birth certificates can be integrated into your manufacturing workflow.