Intel® Platform Protection Services

Outsource Assembly and Test (OSAT) Factory Device Identity Certificate Flow

White Paper

By

Masud Chowdhury
CPS Director
Pravin Chaudhari
Security Architect
Tom Dodson
Supply Chain Security Architect
Joesph Friel
Security Researcher
Avani Patel
Security Software Developer

intel

In the semiconductor manufacturing industry, ensuring the security and authenticity of devices is paramount. The OSAT (Outsourced Semiconductor Assembly and Test) Factory Certificate Flow is a critical process designed to manage and secure device identification through the generation and distribution of Device ID Certificates. With the expansion of data centers, cloud computing, and the Internet of Things, ensuring trust in the supply chain has become more important than ever. A hardware root of trust (HRoT), utilizing trusted hardware and standards like TPM, DICE, SPDM, and CoRIMs, can strengthen security throughout the entire process, from sourcing components to distributing the final product.

OSAT Flow in reference to the Generic Manufacturing Process and work with the IFS

> Verifying and documenting the integrity and provenance of devices and components is particularly crucial in today's complex, globally distributed supply chain ecosystem, where risks such as counterfeiting, unauthorized production, tampering, and insertion of unexpected software and hardware are prevalent.
>
> — National Institute of Standards and Technology (NIST)

INCENTIVES FOR SUPPLY CHAIN TRUST

The use of technology to compromise supply chains is not a new phenomenon; one article in *Supply Chain 24/7* provides a history of supply chain cyberattacks dating back to the Cold War.[1] Before end users even turn on their new equipment, malicious actors have numerous opportunities to disrupt and compromise the supply chain tasked with delivering new devices into end users' hands. Such attacks should concern every company regardless of size or market focus. The U.S. government is aware of the significance of the problem. There are existing regulations and emerging standards and guidelines being published by organizations like NIST and CISA to address cybersecurity supply chain risk management (C-SCRM):

NIST 1800-34, titled "Validating the Integrity of Computing Devices," is a comprehensive guide that addresses the critical issue of supply chain security. [2]

NIST SP 800-161: "Organizations should assess the risk of counterfeit or compromised components and implement controls to prevent, detect, and respond to such risks." [3]

Cybersecurity and Infrastructure Security Agency (CISA): "Supply chain risk management is critical to preventing the introduction of counterfeit or compromised components that could compromise the security and integrity of systems." [4]

Executive Order 14028: "The Federal Government must take action to prevent the introduction of counterfeit or compromised components into the supply chain." [5]

DFARS 252.246-7007: "Contractors shall inspect and test items, including electronic components, to ensure authenticity and detect counterfeits."[6]

Content Protection Service OSAT Factory Flow

Using Figure 4 we will go through each of the steps 1-4 and how they relate to the OSAT Factory Certificate Flow, highlighting the importance of each stage in maintaining device integrity and security.

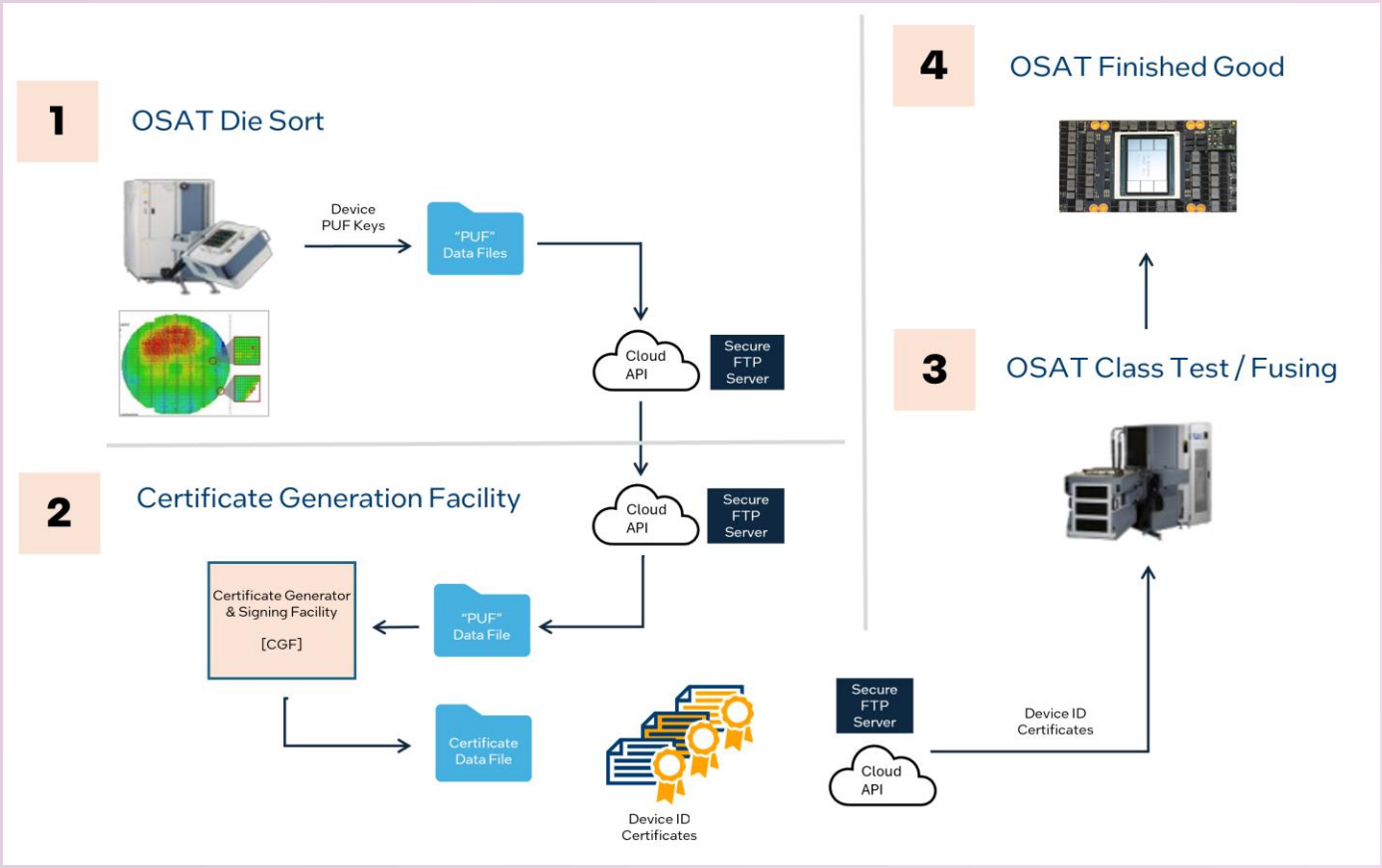

Figure 1: OSAT Factory Certificate Generation Flow

1. OSAT Die Sort

The process begins with the OSAT Die Sort, where individual semiconductor dies are sorted and tested. During the Sort Testing stage, unique device cryptographic keys are generated using PUF (Physically Unclonable Function) technology or other options like IKGF (Intel Key Generation Facility) pre-generated cryptographic keys. PUF is one of the most effective options, leveraging inherent physical variations in semiconductor devices to create unextractable Device ID keys. Other methods include using an internal silicon-based True Random Number Generator (TRNG) to create a seed and use this seed to derive a cryptographic keypair using a Cryptographically Secure Pseudorandom Number Generator (CSPRNG). The Keypair can also be pre-generated externally and injected into the device during manufacturing. Pre-generation of the keypair is cost-effective and provide customers with additional flexibility to meet diverse needs. These keys are essential for the subsequent steps in the certificate flow.

Once the public key is read from silicon, it is used to create a manifest containing metadata about the device such as unique identifier of the silicon. This manifest is then signed with a pre-trusted asymmetric key for integrity protection. These signed manifests are then transferred securely via a Secure FTP Server or via Secure Cloud mechanism to ensure confidentiality and integrity.

- Process: Read the public key from silicon, create signing manifest with integrity protection and transfer signed manifest to Certificate Generation Facility.
- Output: Integrity protected manifest received by Certificate Generation Facility containing cryptographic device public keys.
- Security: Data is transferred securely via a Secure FTP Server or via Secure Cloud mechanism (such as REST API’s or AWS S3 buckets) to ensure integrity.

2. Certificate Generation Facility (CGF)

The Certificate Generation Facility (CGF) is responsible for generating and signing Device ID Certificates. Using the Device public keys received from the OSAT Die Sort or the customer via the signed manifest, the CGF creates a PKCS#10 Certificate Signing Request (CSR). Each of these CSR is then sent to a pre-configured trusted Certificate Authority (CA). This trusted CA creates a Device ID X509 Certificate and signs it, creating a verifiable digital identifier for the device. This trusted signing CA can be rooted in a Global DICE Root CA backed by Hardware Security Modules (HSMs) hosted in an air-gapped secure facility by CGF or can be provided by the customer to create an easily verifiable trust chain. This step is essential for establishing device authenticity and enabling secure communication and operation. No manufacturing secrets are handled by the CGF during this process. After issuing the device certificates, the CGF can then publish to a public distribution point or deliver directly to the customer.

- Process: Device ID Certificate Generator & Signing System.
- Output: Device ID Certificate Files.
- Security: Data is securely transferred back to the OSAT facility via a Secure FTP Server or via Secure Cloud
- Certificate Revocation: Revocation of Certificate

3. OSAT Processor Platform Validation or Board Manufacturing Fusing

Once the Device ID Certificates are generated and published, they are sent to the OSAT Class Test/Fusing stage. Here, the certificates are provisioned into the devices, most commonly via fusing (e.g. eFUSE, One-Time Programmable memory) or flashing. This provisioning ensures that each device is equipped with a unique, verifiable identity, enhancing security and traceability throughout its lifecycle. Because the Device ID certificates do not contain manufacturing secrets, there is no additional risk of exposure if this step is performed in a third-party facility.

- Input: Device ID Certificates, possibly including the complete Security Protocol and Data Model (SPDM) Trust Chain, onto the device.
- Process: Class testing and provisioning to embed certificates into devices.

4. OSAT Finished Good

The final stage of the OSAT Factory Certificate Flow is the production of the OSAT Finished Good. At this point, devices are fully assembled, tested, and equipped with their respective Device ID Certificates. The read/write access certificate storage is physically disabled. Now firmware running on the device can use the certificate to provide evidence of the device's identity to a Root of Trust or attestation service. These finished goods are ready for distribution, with their authenticity and security assured through the certificate flow process.

- Output: Secure, authenticated semiconductor devices ready for market.

Conclusion

The OSAT Factory Certificate Flow is a comprehensive process that ensures the security and authenticity of semiconductor devices. By leveraging industry standard public-key cryptography and secure data transfer protocols, this flow provides a robust framework for device identification and certification. As the semiconductor industry continues to evolve, maintaining the integrity of devices through processes like the OSAT Factory Certificate Flow will remain crucial for safeguarding technology and data.

Future Considerations

The OSAT Factory Certificate Flow is compatible with industry-standard, interoperable technologies like SPDM-based attestation and DICE x509 certificates. This process establishes a trusted identity for devices that can underpin a zero-trust hardware architecture, enabling features such as attestation and secure communication, as well as unlocking access to an ecosystem of complimentary secure services, like CoRIM management services to support a trusted supply chain. As the zero-trust ecosystem continues to evolve, continuous innovation and adaptation will be key to addressing emerging security challenges in the semiconductor industry.

References

1. http://www.supplychain247.com/article/the_supply_chain_silent_threat_cyber_attack/security
2. https://csrc.nist.gov/pubs/sp/1800/34/final
3. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-161.pdf
4. https://www.eventtracker.com/campaigns/nist-800-171-compliance
5. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity
6. https://www.acq.osd.mil/dpap/dars/dfars/html/current/252246.htm#252.246-7007

- Physically Unclonable Functions (PUF) Technology Overview

  https://www.osti.gov/servlets/purl/1184579

- Security Protocol and Data Model (SPDM)Specification Version: 1.4.0

  https://www.dmtf.org/sites/default/files/standards/documents/DSP0274_1.4.0.pdf

Contact Information

- Masud Chowdhury, Director, Intel masud.r.chowdhury@intel.com
- Pravin Chaudhari, Security Architect, Intel pravin.chaudhari@intel.com
- Tom Dodson, Security Architect, Intel tom.dodson@intel.com
- Joe Friel, Security Researcher, Intel joseph.friel@intel.com
- Avani Patel, Security Software Development Engineer, Intel avani.patel@intel.com