BlackBerry | certicom

CASE STUDY

DEVICE MANUFACTURING, BLACKBERRY CERTICOM SECURED TO MITIGATE SUPPLY CHAIN RISKS

A major smartphone Original Equipment Manufacturer (OEM) had successfully built a loyal customer base but as the business scaled, visibility across its supply chain decreased. This resulted in counterfeiting via remanufacturing of its products, which created significant risk to its brand – as non-genuine devices being passed off as genuine could suffer from quality and safety issues, threatening consumer confidence and putting commercial relationships with the OEM's key partners at risk. The lack of supply chain visibility also increased the risk of Intellectual Property (IP) theft and possible cybersecurity threats to both the OEM and its end customers.

This case study describes how BlackBerry® Certicom® key management and managed PKI solutions were used to secure this OEM's outsourced, contract manufacturing supply chain and establish a zero-trust device activation processes, mitigating the risks of device counterfeiting and trojan devices in its ecosystem. The smartphone OEM market is not unique in facing such risks – the same Certicom key management, provisioning and PKI technology and techniques used to secure this customer's environment apply to nearly any IoT-connected device.

FOUR TYPES OF SUPPLY CHAIN RISK CONSIDERED

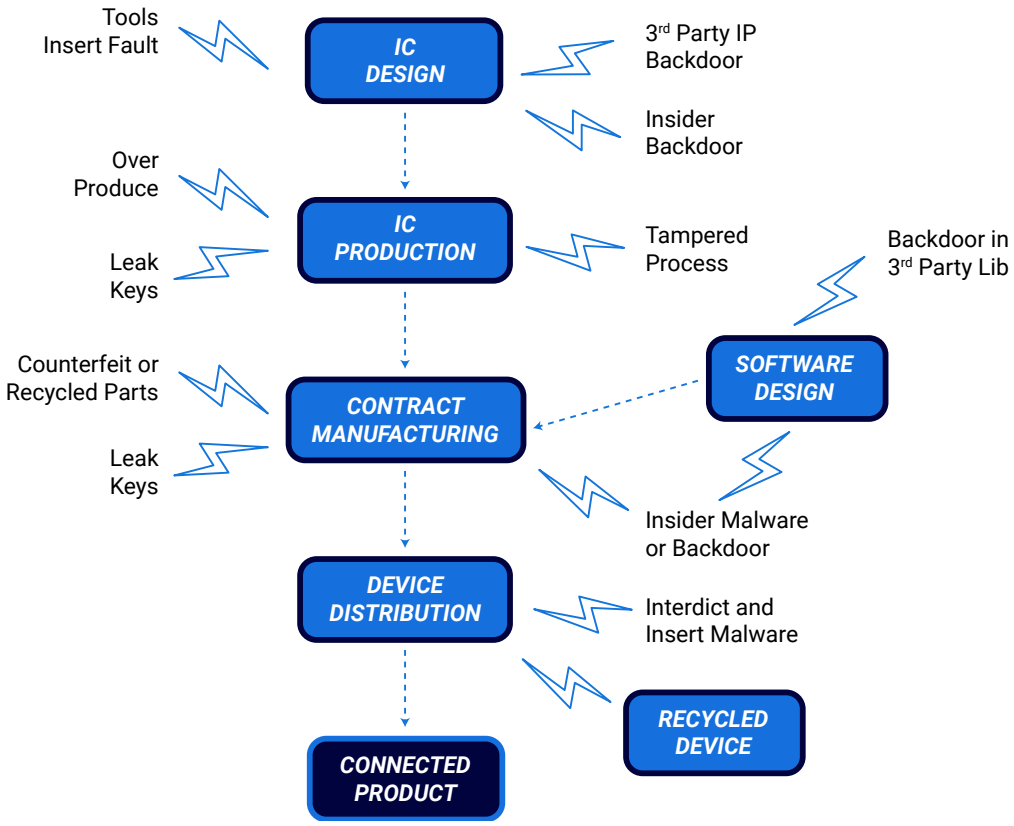
First, outsourced manufacturing tends to reduce supply chain visibility and creates the opportunity for counterfeiting to occur. This OEM outsourced its manufacturing to offshore locations and it became difficult to precisely detect and block these kinds of supply chain risks from happening. They decided to mitigate the risks by introducing traceability and control of offshore production, putting mechanisms in place to ensure that all its devices were manufactured with the OEM's authorization and strictly to the mandated specifications.

The risks faced were not just theoretical. Other device manufacturers had seen similar problems. Counterfeit production of mobile phone batteries had begun to plague the industry. They and other OEMs found counterfeit batteries in their phones catching fire and had uncovered cases of unscrupulous device resellers installing fake batteries while provisioning their customers' new phones.

A ***second*** supply chain risk was with re-manufactured devices — those built by unauthorized manufacturers using a mix of components including scrap parts from discarded devices. These were not built to original specifications and lacked consideration for cybersecurity protection. As such, remanufactured or cloned devices could potentially infect a customer with spyware, which was a major risk to the perceived security of the OEM's brand.

These counterfeit devices could have been otherwise compromised, for instance by bypassing secure boot and software validation protections to load malware onto insecure devices. This could turn a cloned device, appearing safe and trusted, into a potential spy phone. This cloned device could be strategically placed into distribution to target high-value organizations and individuals, putting their sensitive data and communications at risk.

Juniper Research estimates that, without a paradigm shift in software supply chain cybersecurity management, cyberattacks targeting software supply chains will cost organizations an estimated $80.6 billion in lost revenue and damages annually by 2026.



A ***third*** supply chain risk related to lost or stolen devices that R&D teams used as engineering samples. These authentic but insecure devices were a concern since they often had debug capabilities enabled. In the hands of a bad actor, pre-release product vulnerabilities would be easier to exploit if an engineering sample was lost or stolen. Additionally, the smartphone OEM needed to be able to block access to its global messaging network from any lost or stolen device as that too could become an attack vector.

A ***fourth*** supply chain risk related to the cybersecurity protections at the manufacturing sites and the threat of potential data breaches involving IP theft. Although the smartphone OEM signed its code, had tightly controlled production software in place, and managed device unique serial numbers, it had also seen attempts to penetrate manufacturing sites to steal secrets, or get access to sensitive code sign-in and key management systems and manufacturing tools.

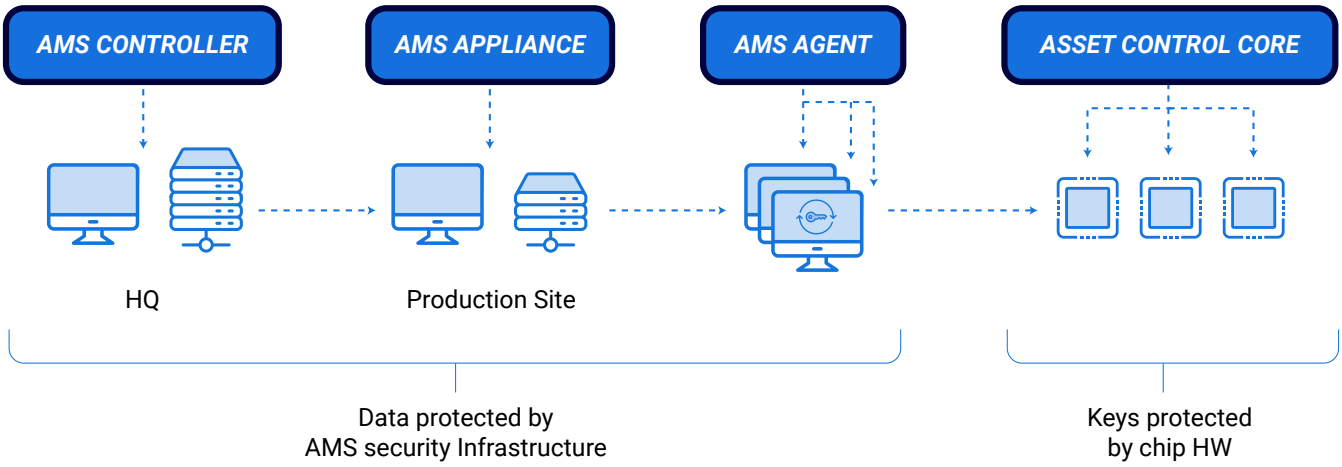
AN END-TO-END DIGITAL ASSET MANAGEMENT SOLUTION WOULD MITIGATE THESE RISKS

The smartphone OEM determined these were all security concerns to be addressed and turned to Certicom for help. Certicom provided end-to-end traceability and authentication – from chip to printed circuit boards (PCBs), to device onboarding and in-life operation – establishing a secure foundation for the customer's mobile application services.

Building very secure devices starts with knowing the chips being used to manufacture PCBs are trustworthy, fused and configured to your specifications, and in particular the security-specific bits. Chip serial numbers and secure identity artifacts can be used to track chips from wafer production to integrated circuit (IC) package and test, then to PCB manufacturing and device assembly. Each step is an opportunity to mitigate outsourced manufacturing and counterfeiting risks. Certicom's Asset Management System (AMS) capabilities such as device serialization, key injection and logging were used to automate these processes.

Secure manufacturing of PCBs includes validating the use of trustworthy application processors, a process that can vary from one processor vendor to another, or even between processor families. In this case, the OEM required that application processors could support a uniquely attestable identity – and to support a per-device key encryption key linked to the chip serial number. These characteristics were used to support a challenge response-style authentication of processors during the provisioning of PCB test and production software packages.

A custom module within Certicom's AMS Appliance Hardware Security Module (HSM) provided the functionality to generate each functionality to generate each application processor's device-unique Key Encryption Key (KEK) and attestation key pair. The HSM module then encrypted the private key with the KEK to securely provision the KEK into secure fuses in the IC's Root of Trust hardware fuses. AMS sent logs of the encrypted data bundles back to the chip manufacturer with the corresponding I serial numbers. The chip manufacturer transferred a block of encrypted data bundles to the OEM when a batch of ICs was ordered for device production.

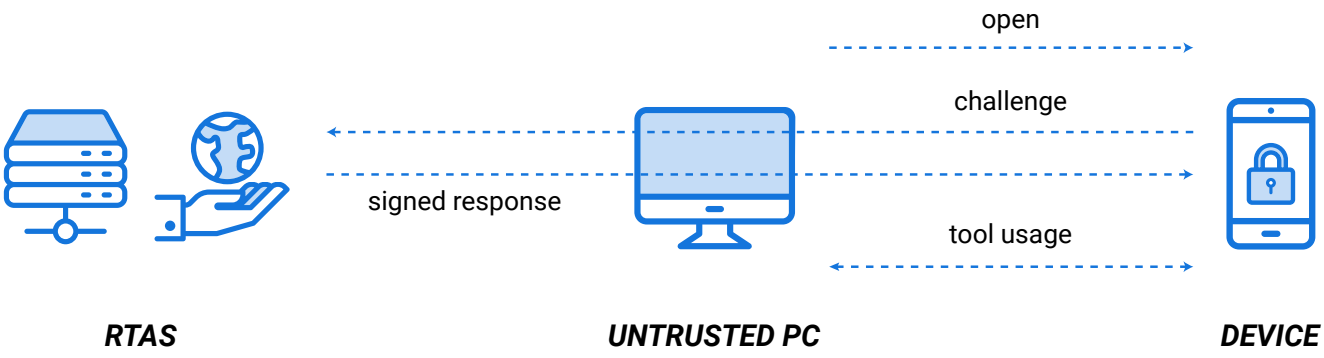


At the contract manufacturer, PCB manufacturing equipment received access to the unique per-chip KEK encrypted data. AMS's Addressable Key Injection module makes that chip provisioning process very straightforward, providing a pipeline of traceable data bundles to each manufacturing site. Loading the data for a specific IC into flash memory on the PCB running the corresponding application processor IC allowed the processor to use its KEK to decrypt the data inside the IC's secure enclave. This data included a device-unique key pair to be used for device attestation. No other processor could decrypt the processor-specific KEK-encrypted key bundle.

The OEM also determined it was important to control test tools that could be used during "board bring-up" and PCB production, ensuring only "trusted" tools could interact with a PCB during the manufacturing assembly and test or re-work process.

When making a connection to a device under test, a test tool needed to receive a permission token from a central OEM diagnostic server running a Remote Tool Authentication Service (RTAS). The diagnostic server signed challenges proxied by the test tool from a device under test using a protocol that included the use of the device's attestation key and a message encrypted using the central diagnostics server's public key.

Only testers that could both authenticate to the diagnostics server and provide the valid challenge response token to a device under test were able to establish a secure diagnostics or programming session with the device. This authenticated both the tester and device to the diagnostics token service – the tester with an X.509 certificate and the device with its attestation key pair. Controlling tools during the outsourced manufacturing process mitigated the risk of manufacturing test tools being stolen or misused, as well as from tools being used to build devices using untrusted application processors.



A custom AMS module was used to provide the RTAS diagnostic token service. The system authenticated testers making a request, looked up the requested device serial number, validated the signature using a stored attestation public key, and signed a device-encrypted challenge back to authenticated testers. Only a device with the corresponding private key could decrypt the corresponding diagnostic token.

MANUFACTURING GOVERNANCE AND CONTROL

Another critical requirement is the ability to govern contract manufacturers – monitor production and stop it if necessary – for whatever reason, e.g. due to a security breach, overproduction, or simply the termination of a business relationship. For the OEM, stopping production at a contract manufacturer was straightforward – simply stop providing encrypted key bundle assets and manufacturing tool diagnostic service tokens. Since the OEM monitored provisioning and supplied these assets, it could control how many smartphones a manufacturer could produce. It could also control test tool access to the devices to have visibility on Work in Progress (WIP) quality control issues and prevent unauthorized device rework.

RMA tool authentication was also critical for in-market devices returned for warranty repair. The RMA process was secure because a device and test tools once again needed to authenticate to our diagnostics token server. RMA re-work could thus be securely managed.

Once a PCB passed the test phase, it was provisioned with production software, assembled into a smartphone and configured for shipment. It was at this stage that the manufacturing system captured a snapshot of the as-built device configuration. The OEM kept these records for the next stage in the device lifecycle.

ATTESTED DEVICE ACTIVATION

The device attestation key pair remains a critical asset as devices entered the distribution chain and found their way into the hands of customers. At this point, the OEM required the device to prove its authenticity in order to register on its network. This process has been described as authenticated PKI enrollment, where device registration and policy enforcement are prescriptive. More recently in IoT circles, the process has been referred to as Zero Trust onboarding.

For this process, the OEM used a challenge response which included the device sending a fingerprint of the device's as-built configuration record, signed by the device's attestation key. This mechanism ensures that only expected devices from known manufacturers could register on the network. TPM-based device attestation that is more common today works in a similar manner.

In the process of device registration, the device also sent a Certificate Signing Request (CSR) to request a certificate for authenticating to OEM services. This CSR allowed a new device key, originating from within the device's secure trust zone enclave to be certified for use in a device identity certificate. The identity certificates issued were time-limited. This required a device to periodically certify a new device key pair prior to its identity certificate expiry. If a device failed to renew its certificate on time, it could be recertified on the network only after receiving additional authorization.

SCALING CERTICOM TECHNOLOGY

The OEM and its chip suppliers used Certicom's Asset Management System (AMS) platform to monitor remote device manufacturing and control device personalization, logging device as-built artifacts and encrypted key bundles as part of the manufacturing process.

To recap, IC fuses were the first place to establish down device security, first with a processor serial number. AMS can be used to provision unique serial numbers across a range of manufacturing sites.

AMS was also used to generate a device KEK and attestation key pair. Before the KEK was programmed into the device, the AMS HSM first KEK encrypted the device attestation private key. A data bundle consisting of the device serial number, the KEK-encrypted attestation private key and attestation public key were collected and sent to the chip manufacturer as part of a provisioning log when the KEK was fused into the chip. AMS then discarded the KEK so that only the application processor had a copy.

The link between AMS and the chip being provisioned with a KEK was secured by a link with the chip's root of trust. Even if a bad actor at the chip packaging and test stage obtained access to the KEK via a tester entry point and copied the serial number and KEK, the attacker would not have seen the encrypted attestation private key as it was not sent to the chip, but rather to the chip manufacturer. The chip manufacturer, likewise, was not sent the KEK so it could not decrypt the attestation private key for any chip. Had it been required for additional security, the OEM could further have encrypted the bundle and then later pre-decrypt it prior to distribution to a contract manufacturer.

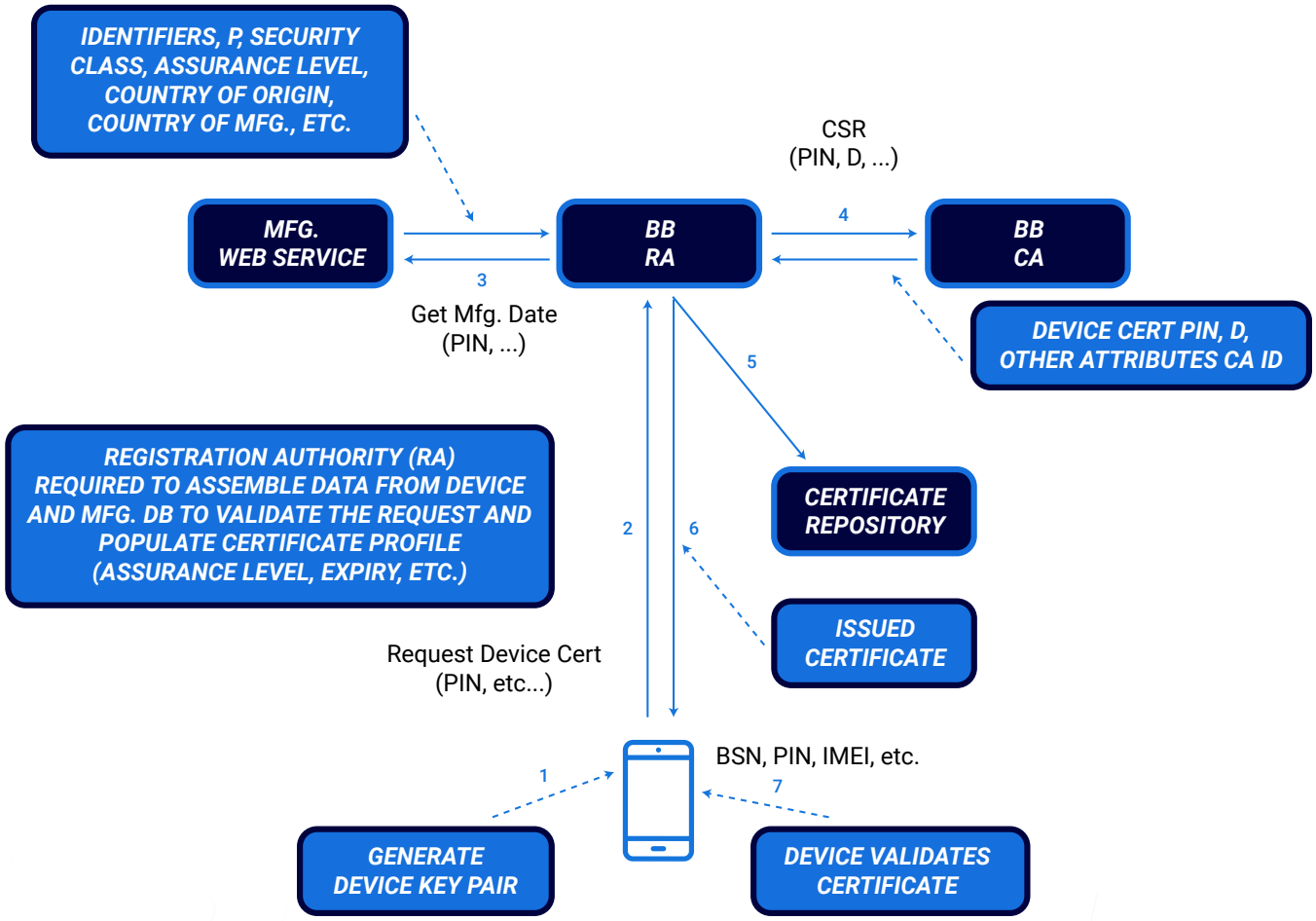
SEPARATION OF DUTIES AND SECURITY INTERLOCKS

AMS technology plus a separation of duties between the chip supplier, OEM and the contract manufacturer prevented the flow of unauthorized asset bundles to the contract manufacturer. Furthermore, the manufacturing equipment test tools needed diagnostic tokens to assemble and provision each device, so even if a chip supplier mistakenly sent the OEM's chips to a contract manufacturer, they could not be used to make smartphones. Only pre-registered processors were trusted, after they attested their identity to a test tool.

AMS technology was a fit because it had a number of ready-to-use modules such as static data injection, serialized key injection and addressable key injection that the OEM could leverage. It was also extensible to meet the OEM's specific requirements for key generation and wrapping, for RMA token generation, etc.

AMS's capability to operate on remote manufacturing lines with intermittent Internet connectivity for bulk provisioning applications made it ideal for offshore chip package and test operations. In contract manufacturing environments, the ability to support addressable key injection gave the OEM more fine-grained control over PCB production and diagnostic tools.

Certicom also provided the PKI that the OEM relied upon for attested device activation and secure network operation.



A comprehensive security solution, Certicom technology and interlocked operational techniques provided the OEM a means to detect and deter rogue and counterfeit devices:

- Control who manufactured its devices
- Control how many devices could be built
- Ensure devices could be manufactured only used trusted application processors
- Keep a record of each as-built device
- Ensure only authentic devices could access RMA tools
- Protect manufacturing and diagnostic tools from theft or misuse
- Activate only trusted devices on its network
- Certify devices for operation during a fixed time period, after which they would need to re-certify

If you are looking to improve the visibility and security of your device manufacturing supply chain, please contact:

sales@certicom.com

BlackBerry | certicom

As a leader in applied cryptography and key management, BlackBerry Certicom provides managed PKI, key management and provisioning technology that helps customers protect the integrity of their silicon chips and devices from the point of manufacturing through the device life cycle. Used to prevent product counterfeiting, re-manufacturing, and rogue network access, BlackBerry Certicom's secure key provisioning, code signing and identity management solutions are field-proven to protect next-generation connected cars, critical infrastructure and IoT deployments.

*For more information, visit **BlackBerry.com** and follow **@BlackBerry**.*

BB23 | 230807