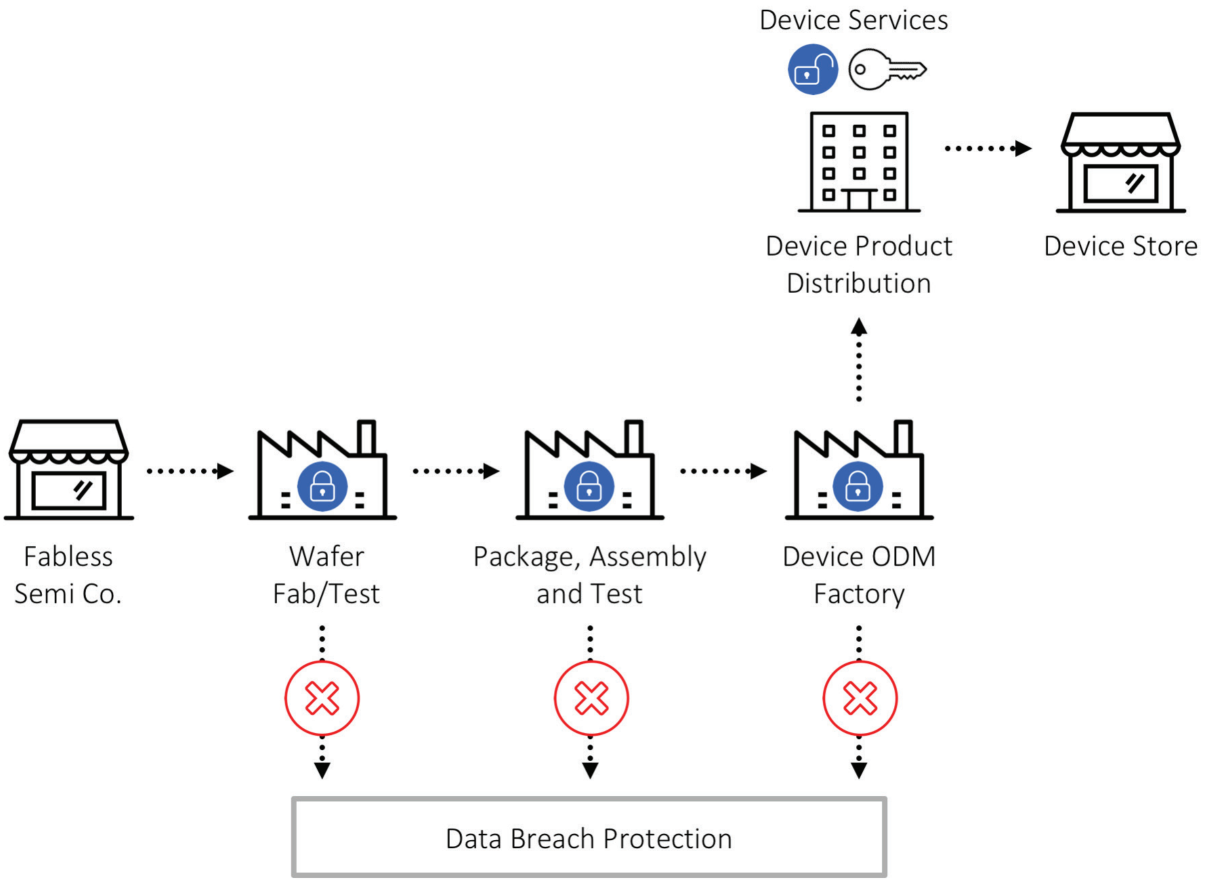
Secure Key Provisioning

With mobile devices housing more and more sensitive data that is utilized in a wide variety of applications, chip and device companies must meet the complex security requirements for each potential use case or capability. Most security measures require the injection of secret identity data and cryptographic keys. Currently, cryptographic keys are provisioned in the open without encryption on test equipment which is operated by third party contract manufacturers. These current provisioning methods expose chip manufacturers to liability and risks for any security breach that occurs within their supply chain.

Utilizing the CryptoManager Root of Trust hardware IP Core, SoC architects have a built-indesign for the secure provisioning of cryptographic keys during chip manufacturing. For OEM device manufacturing, this feature also enables remote secure key provisioning at the ODM (Original Device Manufacturer).

Figure 1: Secure Provisioning of Keys During Manufacturing



As illustrated in Figure 1, the CryptoManager solution provides the flexibility to provision keys and other sensitive data at any point in the manufacturing flow. More specifically, a key may be securely provisioned at any point in the chip manufacturer's supply chain. In cooperation with their OEM customer, the provisioning of keys may even be pushed to the ODM for downstream provisioning at board-level test or as a post-production provisioning step prior to shipping.

Since the communication channel is secured to a silicon root of trust provided by the CryptoManager Root of Trust (see Figure 2), robust provisioning is possible at the earliest stages of manufacturing. The CryptoManager solution has flexibility for highly specialized key management requirements such as the provisioning of key splits at different stages of manufacturing. For unique keys, there are also features to protect against key duplication in multiple devices. The uniqueness of such keys is checked at multiple locations during a provisioning event. This includes duplicate checking at the CryptoManager Service (see Figure 2) located in the datacenter of the chip or device manufacturer and at the CryptoManager Appliance located in the contract manufacturing location.

The CryptoManager platform helps solve challenging business use cases for manufacturing through the use of CryptoManager modules which specify device service transactions such as key provisioning. A module may provision one or multiple key types depending on the customer's requirement. Each module is authorized for the provisioning of key(s) at specified manufacturing locations.

As shown in Figure 2, the CryptoManager Infrastructure may handle third party keys or keys generated at the factory. All keys to be provisioned to devices are loaded into the Service in the host datacenter. The Infrastructure will automatically distribute keys to factory locations based on the module settings and inventory thresholds set by the system operator (see Figure 3). Key management requirements are specified by the module such that as new key provisioning requirements arise, new modules may be added.

Figure 2: Secure Key Provisioning Communications Channel

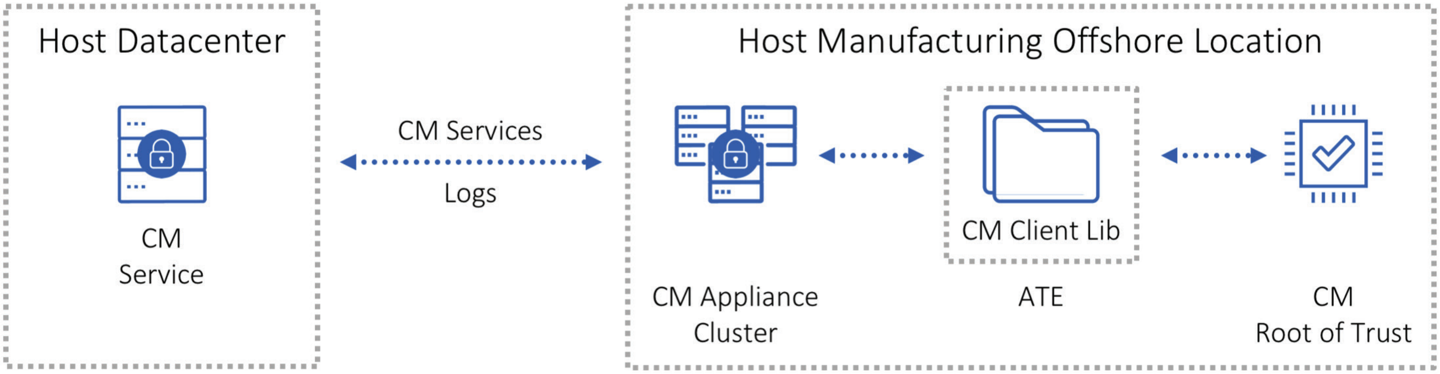
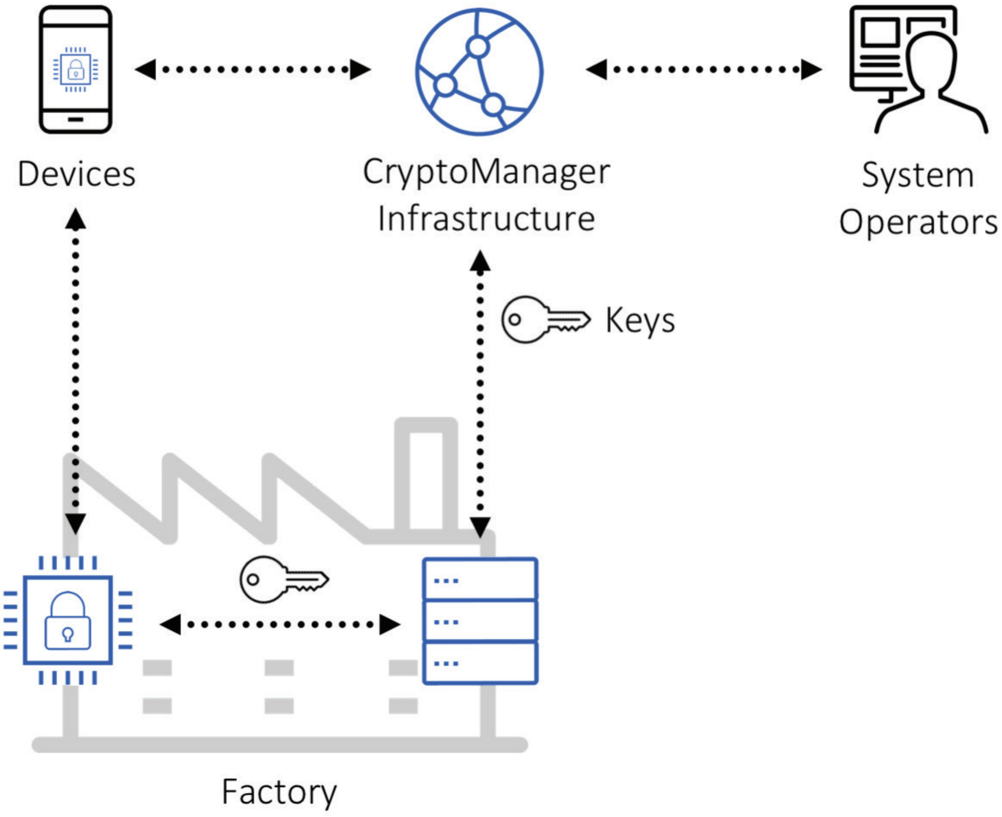


Figure 3: Key Inventory Threshholds Set by the Systems Operator



To enable forensics for secure key provisioning and management it is critical to have logging capabilities to assure an audit trail for each key provisioning event. The CryptoManager solution not only securely provisions keys down to the Root of Trust embedded in the SoC, but also securely acknowledges and logs each completed transaction.

The CryptoManager platform has been designed specifically for mission critical manufacturing applications. This provides manufacturers with the assurance that production will not be disrupted in the event of a component failure. The solution is scalable, it can be expanded to handle additional loading due to new key provisioning requirements or increased demand.

Using CryptoManager solution, manufacturers realize high returns on their investment in several ways. Risks and liabilities associated with data breaches are mitigated. New key provisioning requirements may be easily handled in manufacturing without disruption, providing a rapid time-to-market. Additionally, operations may be streamlined by provisioning keys at the appropriate stage of manufacturing, reducing the overall costs for key provisioning services.