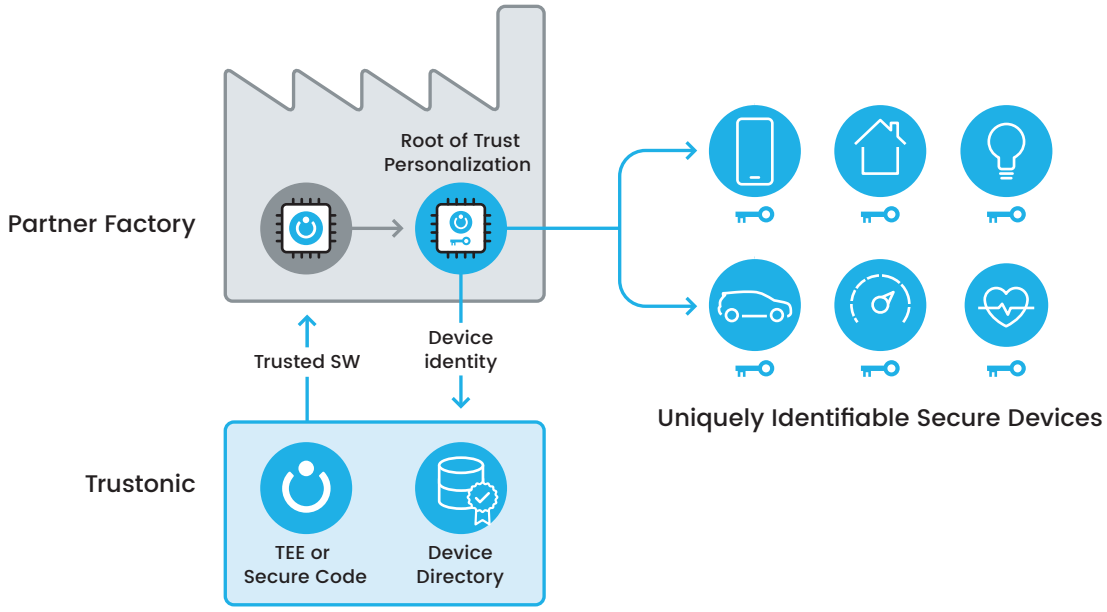
TRUSTONIC

Digital Holograms

Digital Holograms™ are an innovative mechanism which enable web services to securely determine the lifecycle of an IoT device. They are an extension of the key provisioning scheme that Trustonic has deployed into numerous factories worldwide and which has provisioned keys into over 1.2 billion devices to date. This key provisioning scheme securely embeds a “Root of Trust” into each device, enabling the secure attestation that a particular message originated from a specific device.



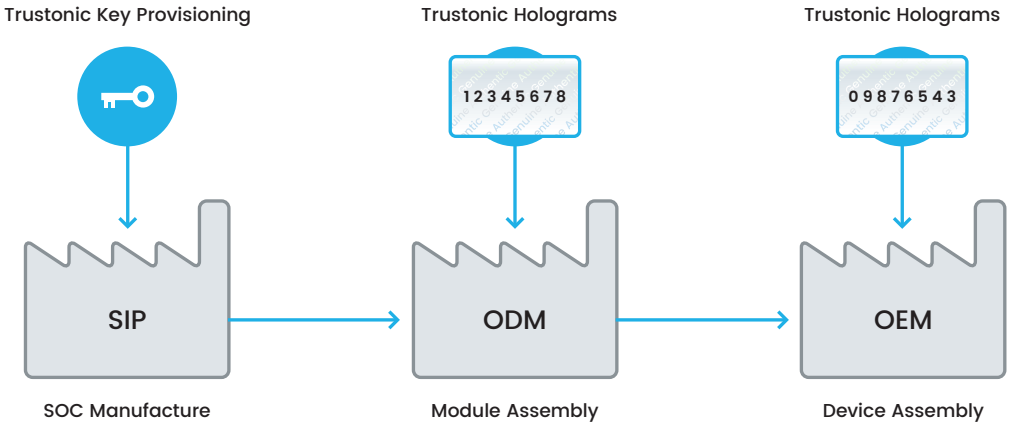
Whilst the Root of Trust and its associated X.509 certificate are sufficient to attest to a one-time event (that the device was in a trusted factory when the key was injected), due to the complexity of its value chain, IoT requires something more sophisticated. For IoT applications, the same basic chip design or low-level module may be used in countless different devices from different manufacturers. For IoT, attestation of a whole series of manufacturing events is required, not just attestation of a single event. Digital Holograms enable this.

Digital Holograms are essentially secure serial numbers, which are distributed by Trustonic to OEMs, ODMs and others, to represent a specific manufacturing or lifecycle event. They are later associated with a particular device. For example, to record that a device has been assigned a specific model number, has passed through a QA process, or has been recalled or serviced, you could simply add a Digital Hologram.

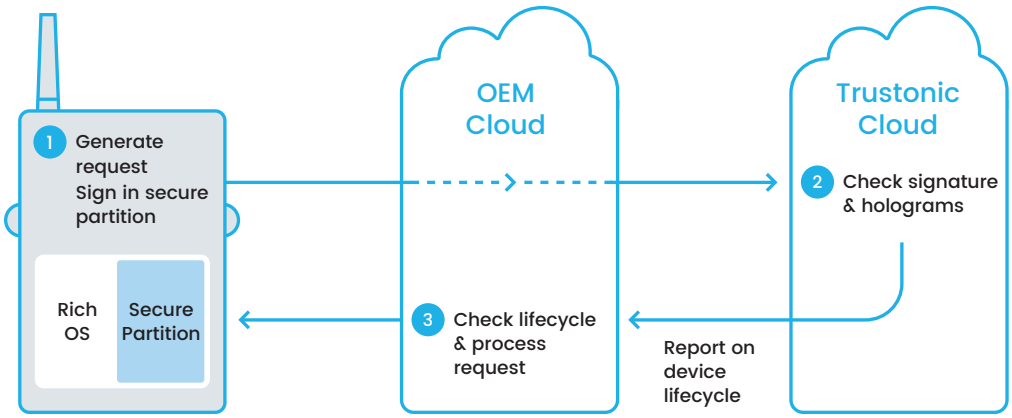
Hologram	12345678
Issued to	ABC Corp.
Tag	Model-X
Bound Device	87654

Digital Holograms are injected into the device during manufacturing and are stored securely. For example, on an ARMv8-M based device, they would typically be stored in a region of the flash protected by TrustZone. Digital Holograms are single use and, once they are bound to a specific device, they are cryptographically protected against re-use or theft.

During its manufacture, or subsequent lifecycle, a device may obtain several Digital Holograms, each representing individual events. If a step is missed, due to IP theft or overproduction, for example, then the faulty / counterfeit devices will miss one or more of the required Digital Holograms and the omission can easily be detected – either during a later stage of production or once the device is deployed in the field. The exact path a device takes from inception to the OEM is recorded when the Digital Holograms are installed, enabling manufacturing processes to be audited.



Trustonic software running on the device can collect all the injected Digital Holograms and prepare an attestation message that is underpinned by the device key provisioned by the silicon provider. A message sent to a web service can be forwarded to Trustonic for validation. Trustonic maintains meta data on all devices and Digital Holograms and can report back to the web service to confirm the series of manufacturing and lifecycle events that the device went through. The attestation message is cryptographically linked to a custom payload which enables the device to not only attest that it is genuine, but also that a specific message originated from it.



At ARM TechCon 2017, Trustonic demonstrated how devices can automatically enrol with an AWS web service, by using attestation to prove that an AWS Certificate Signing Request originated from a legitimate device, thus enabling the corresponding TLS certificate to be provisioned automatically. This was demonstrated on devices using both an ARM Cortex-A9 processor (the ARTIK 530) and an ARM Cortex-M23 processor (the Nuvoton M2351).

TRUSTONIC

For more information please email enquiries@trustonic.com

20 Station Road Cambridge CB1 2JD United Kingdom
trustonic.com