IAR Secure Deploy

Complementary tools to secure manufacturing processes.

Security Made Simple

The IAR Secure Deploy (SD) tools extend the concept of Root of Trust (RoT) to the deployment and manufacturing environment.

Key Highlight Features

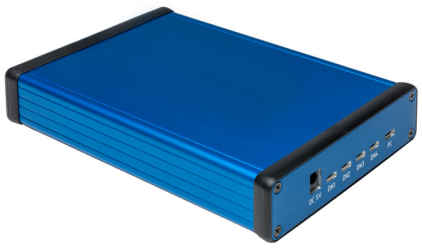
- Secure Provisioning within hostile environment
- Inhibit malware injection at production and in the field
- Inhibit Cloning and counterfeiting: Utilizing the unique device identity or feature, the anti-cloning protects the IPR and eliminates any unauthorized copy of the device.
- Secure infrastructure flow across global stakeholders
- Maintaining OEM key & data sovereignty
- Minimal impact on existing production flow
- Secure update & patching of constrained devices

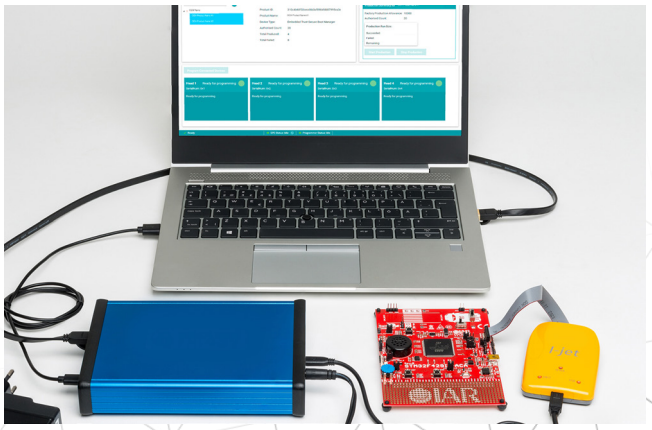
In embedded security, the RoT is considered to be an immutable boot process within the system based on unique identifiers (Unique ID), cryptographic keys and on-chip memory, to protect the device from being compromised at the most fundamental level. The SD is extending that protection while the chip is being provisioned in the assembly lane. Using the same technique and rooting security on the fundamental hardware anchors as before, the SD offers the ultimate solution to:

- Secure distribution of the application Software to the Manufacturing facilities in an encrypted form.
- Global control of high-value Intellectual Property (IP) at the manufacturing.
- Inhibit malware injection production and in the field.
- Anti-cloning protection.

Thanks to an easy and intuitive two steps approach, our customer can now rely on IAR Embedded Security basic infrastructure without compromising on quality and/or security standards. The SD family is coming in two variants:

- Secure Deploy – Prototyping (SD-P): Ideal for small production sample and/or validation quantity. Even from the development environment it is possible to sample how the real chipset provisioning will take place.
- Secure Deploy – Manufacturing (SD-M): Ideal for volume production. Fully integrated with the provisioning machine in the manufactory facility





Products SKUs and configuration

Two steps approach to secure deploy and provisioning

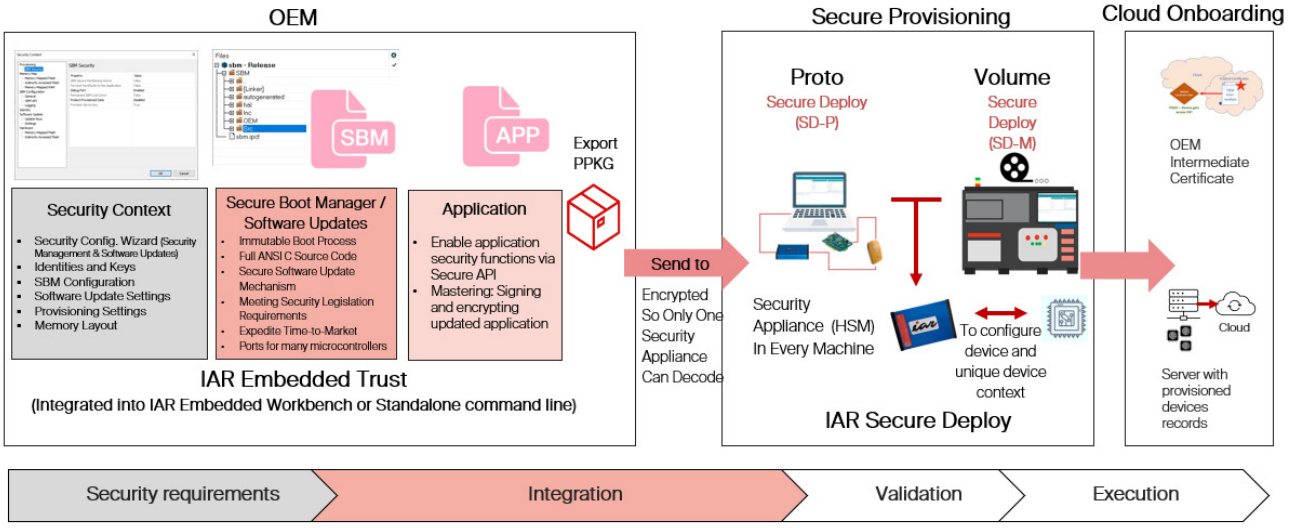
Either configurations, the SD-P and the SD-M, has two very simple step to complete in order to successfully provision one or multiple chipsets at the same time.

1.) Import the encrypted software and data that must be provisioned. This is normally developed in the different environment, using either the IAR Embedded Trust or the IAR Embedded Secure IP. The file is in *.ppkg format and can openly and confidently shared with volume production and manufacturing.

2.) Use the Provisioning Hardware Security Module (HSM) box to retrieve unique information about the chipset that will be provisioned and produce that final image which is then used to program the image exclusively for that unique chipset. The procedure requires no more than few seconds and allow volume production to provision devices protected by possibility of cloning and counterfeit.

The SD-M product is designed to be integrated with provisioning machine and do require integration with the Graphical User Interface (GUI) of the machine itself. Thanks to our engineering design we have created a unique API which will ease that integration and allow communication with the Provisioning HSM. Normally the SD-M is subject to contract stipulation.

The SD-P is equipped with the same Provisioning HSM and drivers, but it does include a friendly GUI which can be used in a desktop computer. Furthermore, the SD-P comes equipped with a I-JET interface as final connection to the chipset. The SD-P can be ordered from catalogue and is subject to export control regulation, please contact our

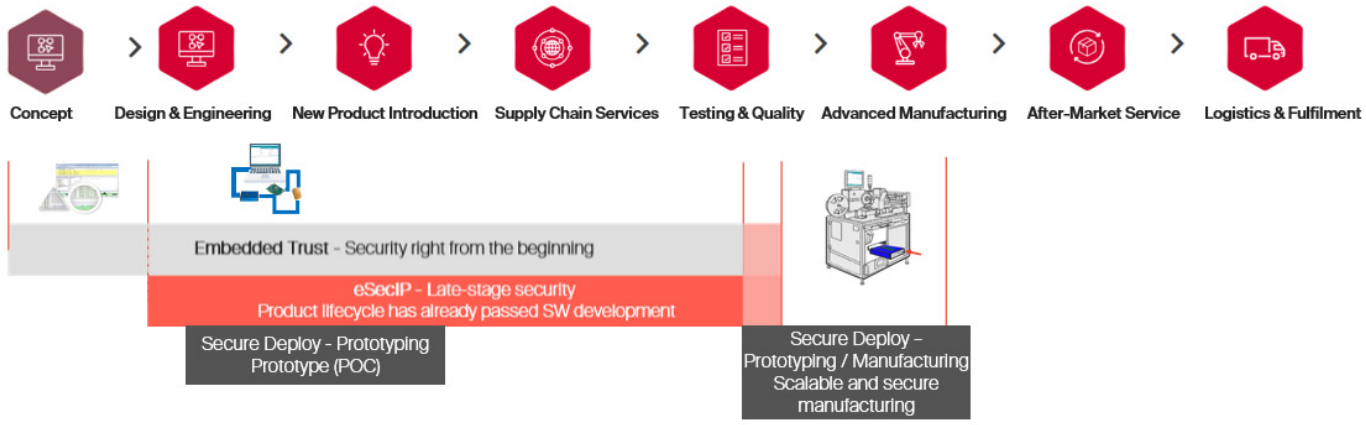


Fitting nicely in the IAR Embedded Security

Two steps approach to secure deploy and provisioning

IAR Secure Deploy are complementary tools to combine with IAR Embedded Trust and IAR Embedded Secure IP, and secure global production processes and flexible cost-saving at your terms.

The following picture highlights how the IAR Secure Deploy are working as complementary tools to secure manufacturing stage, protecting IP and devices.



Product SKUs, Features, and Ordering information

Orderable Part Number (P/N)	Notes
SDP	Secure Deploy - Prototyping solution, PC locked license, for secure prototyping, including: • Secure Desktop provisioning securee deploy prototyping software • Secure Provisioning Engine • Production HSM • I-jet • 1000 Tokens Support and Update Agreement for 12 months
SDP-SUA	Secure Deploy - Prototyping solution PC-locked License, Support and Update Agreement (SUA).
SDP-TOKENS(-3K/-10K)	additional 1000/3000/10,000 tokens for IAR Secure Deploy - Prototyping

Export Control Restrictions do apply

Products SKUs and configuration

Platform supported, device families and specific chipset can be found on
https://www.iar.com/products/security/secure-deploy-prototyping/