Avnet Silica Provisioning Service

STATEMENT

Securing the production and logistics side of connected embedded devices is essential to good security practices. These threat vectors can be addressed using a provisioning service.

WHY PROVISIONING?

Security is a rising concern in the embedded market and for good reasons. As adversaries become ever more capable and the economic gains from attacks increase, it is a common realization in the industry that security has to be implemented as a process - and not a feature.

Increased certification frameworks, such as the EU Cybersecurity Act, are not only helping to increase overall security in products, services and processes in the European single market; they are also providing a framework for implementation of a secure development process.

Such a process is not only concerned with the development of the product, but rather starts in the very initial idea phase and only ends as the very last of those products is decommissioned from the field.
As manufacturers realize this, it is clear that not only does security need to be applied to the product itself, but also to supply networks and distribution of the products.

It is becoming a growing risk that untrusted manufacturing can expose device credentials during manufacturing. This can result in counterfeit products, reliability issues, low performance and quality; further increasing warranty cost, and, in worst cases, undermining a company's entire business case.

A security process will provide guarantees to end customers and consumers that the unique credentials of the device are kept secret, thus securing data and future information-driven business models.
A well-documented process across the entire product flow is essential to good security and necessary to successfully implementing security by design. Infrastructure owners must provide proof that they control their assets and which HW devices are in use in the field. This includes proof of origin, HW/SW state, and history. All this must be available to users as proof of reliability and thus becomes an important part of the security process.

AVNET SILICA OFFERING

Avnet Silica has developed a highly secure solution for provisioning electronic components to cover security in the supply chain and distribution parts of electronic device manufacturers and OEMs.

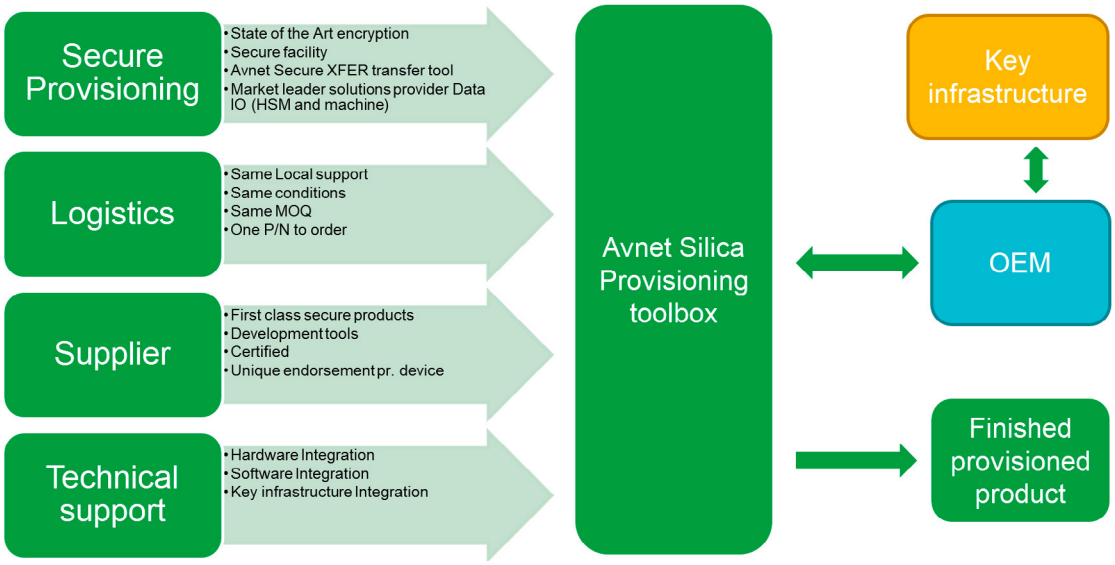
Avnet Silica is also a member of the European Cyber Security Organisation (ECSO) and, as such, we are involved directly in the development of the underlying frameworks for the EU Cybersecurity Act.
We strive to make sure our processes and offerings comply with industry standards, and of course with the Cybersecurity Act.

The service offers a toolbox including everything customers need to set up a supply network, where secret information is never exposed and always treated encrypted in a secure and documented process.

This service offers secure provisioning of devices through state-of-the-art encryption in a secure facility, taking advantage of Avnet Silica's flexible logistics setup.

We offer the service on the most trusted supplier's security parts implementing the most recent in security technology.

We support customers locally through hardware and software integration, as well as integration of customers' own key infrastructure into our provisioning facility to offer a seamless flow; all the way from the definition of the project into provisioning and final shipping of provisioned parts to the manufacturing site.



At this stage, the devices can be locked and cannot be further manipulated without providing appropriate security credentials. As these devices are strongly hardware secured, they offer both countermeasures against logical (software) and physical (hardware) attacks.

We offer both support for secure elements, TPMs, as well as many modern processors.

HOW TO GET STARTED

At Avnet Silica, we will provide a comprehensive overview of the provisioning options and solutions we offer. We will also help expand on the specific use case to understand the best implementation, expanding on hardware and software solutions, and how those play into the final security process flow.

By engaging with Avnet Silica, you will gain a framework for specifying your security credentials and mapping them to the specific slots in the secure component.

After defining the specification, we will provide a quote detailing the device cost and a timeline for the provisioning.

Our system will send your credential definitions to our secure programming centre, thus ensuring the integrity and secrecy of the data.

We will then provide a number of "first article" devices to test against the system requirements. This is to verify that the provisioning process has been completed successfully and according to specifications. Multiple iterations of this process can take place if required.

Avnet Silica is now ready to deliver components anywhere in the world, pre-provisioned to customers' specifications. Customers can order this with a single part number and the provisioning will happen according to the specifications agreed in the previous steps.

Contact

For more information, contact your local Avnet Silica sales office or Martin Milter, security specialist, directly.