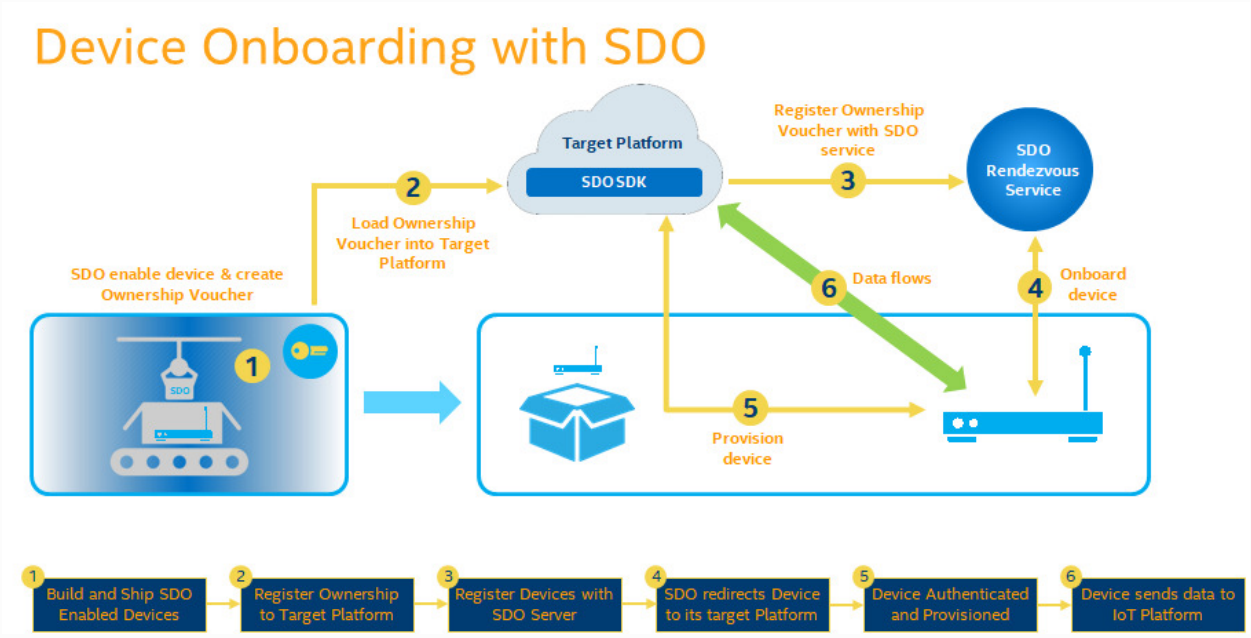
Secure Device Onboard (SDO)

What is SDO

SDO is a flexible software solution that simplifies and automates the process of onboarding edge devices. The term “onboard” here means the process by which a device establishes its first trusted connection with a device management service (DMS).

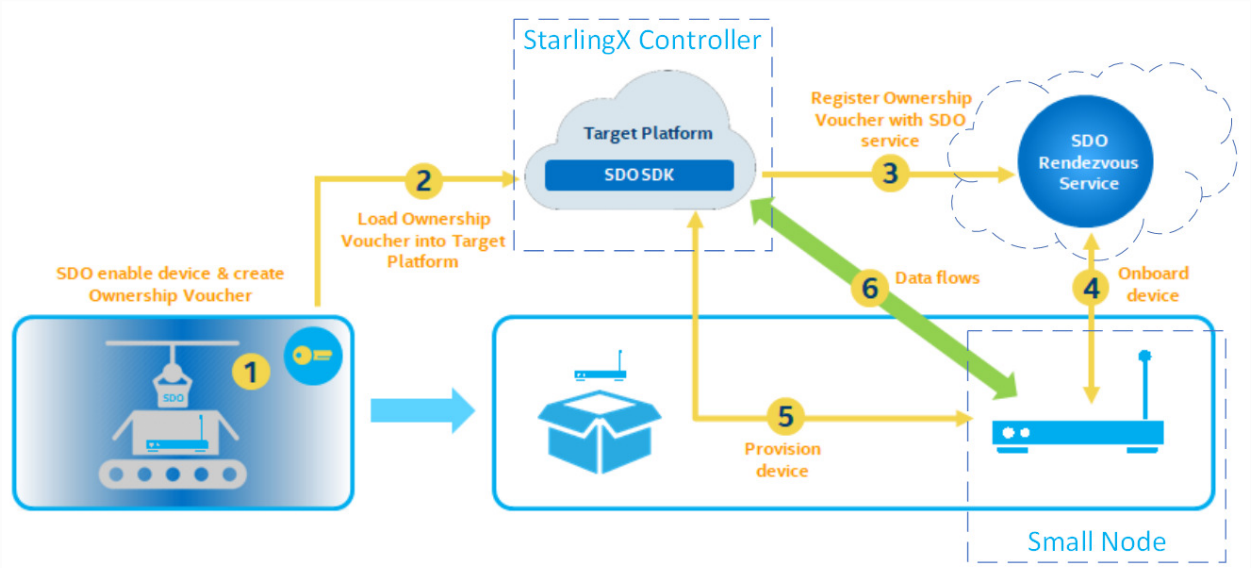


1. During the manufacturing process, an edge device is initialized with SDO client software and security credentials which contain the address of the SDO rendezvous service. Device initialization also creates an ownership voucher for the device. The ownership voucher is a digital document which contains secure information, for example, device GUID, rendezvous server location, manufacturer’s public key, etc.
2. The target platform with SDO platform SDK, i.e. DMS, loads the ownership voucher. It becomes the owner of the device.
3. The DMS registers the device to the SDO rendezvous service by the ownership voucher. This step is to declare the ownership of the edge device.
4. On the first time the edge device powers on, it will contact the SDO rendezvous service to authenticate itself and get redirected to the DMS. (The SDO rendezvous service got the address of the DMS in #3).
5. The edge device contacts the DMS to authenticate itself and establish a secure connection.

6. With the secure connection, the edge device and the DMS can securely exchange data.

How to integrate SDO with StarlingX

With the technology of SDO, we can automate the provision process of small nodes as shown in the figure below.



1. The DMS will be running in StarlingX's Kubernetes cluster, orchestrated to the active controller node.
2. The rendezvous service is not necessary to be running in StarlingX cluster. It could be running in public/private cloud. Only need to make sure it is reachable.
3. A small node will be initialized with SDO client software and security credentials by utilizing the supply chain tools provided by the SDO project. And its ownership vouchers will also be generated by the tool, and then be feed into the DMS before going through the SDO process.
4. Once the small node power on, it can establish a secure connection with the DMS through Standard SDO process. After that, the provision operation of the small node can be automatically performed. Finally, the small node will join StarlingX cluster and be managed by StarlingX platform. The whole process is true single-touch (plug the device in and power on).

References

1. Code: https://github.com/secure-device-onboard
2. Release: https://github.com/secure-device-onboard/release/releases/
3. Document: https://secure-device-onboard.github.io/docs/
4. SDO-support of Open-Horizon: https://github.com/open-horizon/SDO-support