Whitepaper

Seal SQ
Digital identity provisioning and zero-touch onboarding for IoT

In IoT digital transformation, it's getting more and more critical to design and implement solutions by combining technologies to onboard the IoT devices to the IoT cloud platform, establish a secure connection, publish the workload and process the workload in the cloud application without compromising on security. Apart from the technology stack that is applied in the IoT solution, the secure deployment of the IoT solution in the field is also a critical task to consider for every IoT solution provider/ integrator.

Zero-touch onboarding for IoT devices has been proposed and applied to different industries for years, but the way to implement it is various and is not secure enough. The best practice of implementing the secure zero-touch onboarding is using a digital identity, which must be unique per device, hard to fake and steal, as the device attestation, rather than a pre-shared key or hard-coded passphrase in the code. Once one can establish a complete trust chain for device authenticity, integrity and security of communication, then the data trustworthiness is verified.

What is needed to obtain a trusted digital identity of a device?

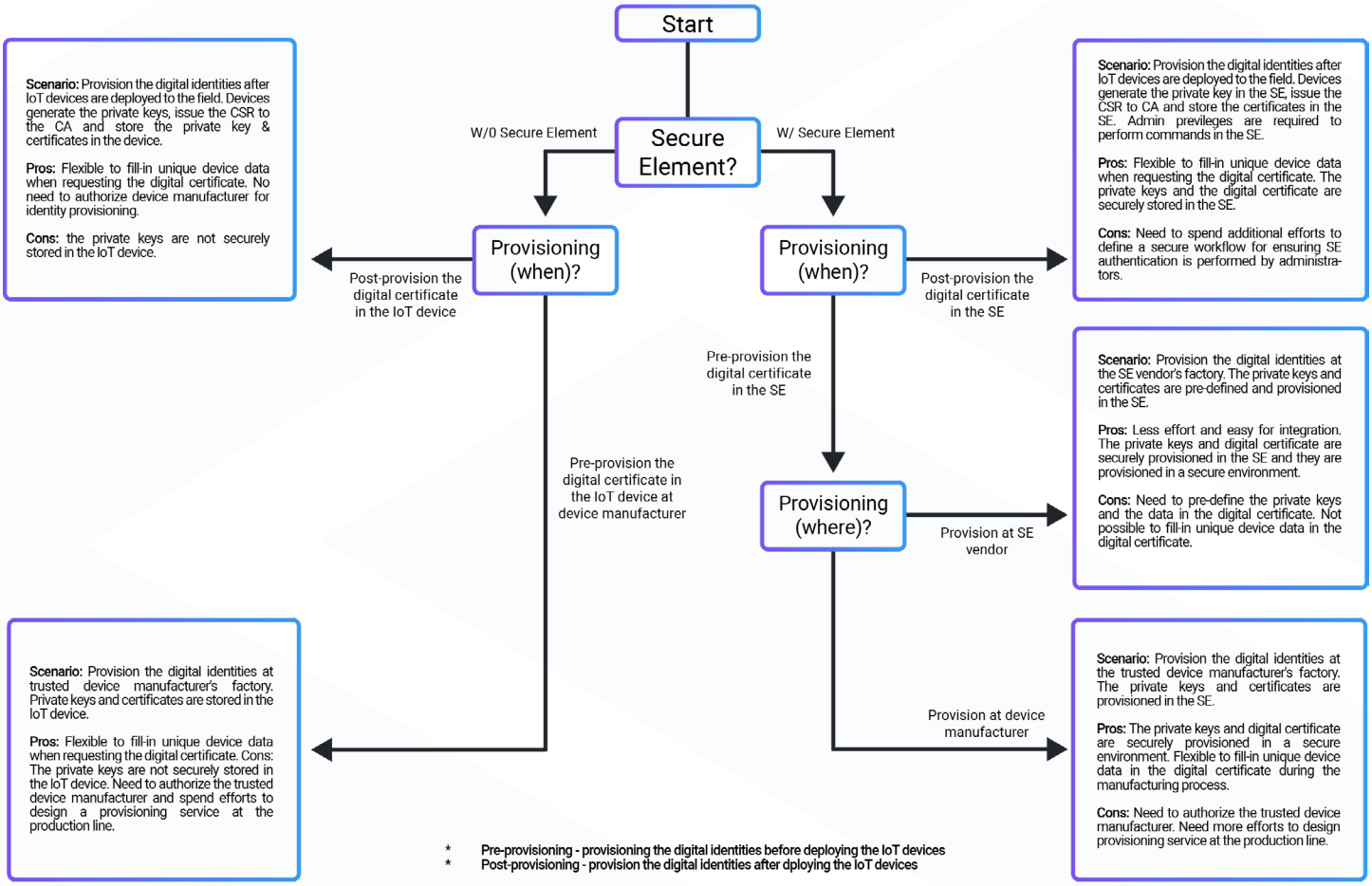
- A Certificate Authority (CA) – It's a well-protected environment and a trusted entity that issues digital certificates. These digital certificates are data files used to cryptographically link an entity with a public key where the link between this entity and the public key is asserted and certified by means of digital signature of this link.

- cryptographic techniques based in public/private key pairs—two keys with a unique mathematical relationship. Public-key cryptography works in such a way that a message encrypted with the public key can only be decrypted with the private key, and, conversely, a message signed with a private key can be verified with the public key. This technology is the foundation to build the four pillars of transaction security: confidentiality, authentication, integrity, and non-repudiation.

- Certificate Management Server (CMS) – A centralized platform that manages the lifecycle of all the digital certificates issued by the CA. At the same time, it also manages the lifecycle of the IoT devices, as their digital identities are these digital certificates.

Once the digital identities for IoT devices are created, other topics are needed to be considered. For instance, how/when/where do you provision those digital identities in your IoT devices? Do you use an additional hardware root of trust (i.e. Secure Element) in your IoT device? How many digital identities do you need for supporting the supply chain of your IoT device manufacturing? The answer would be various and it depends on each IoT application.

The flow chart below summarizes the pros and cons of different provisioning options, and it might help IoT solution providers to decide what could be the best option for each IoT application when considering the digital identity provisioning. In the flow chart below, the digital identity is the operational certificate that will be authenticated by the IoT application, the authenticity of IoT device for requesting the operational certificate from the CMS should have verified by using the pre-loaded birth certificate.



* Pre-provisioning - provisioning the digital identities before deploying the IoT devices
* Post-provisioning - provision the digital identities after dploying the IoT devices

Zero-touch onboarding - Certificate-based authentication through a secure Sales

The authentication of a device is done through industry-standard protocols, such as SSL/TLS. This protocol allows a back-end server or an IoT platform to check the validity of the digital identity and the status of the device certificate and its origin. From the digital identity verification, based on the secret information used therein, session keys are derived to protect the communication channel. Communication can be encrypted, authenticated and its integrity protected. If the digital identity passes verification, the device is considered authentic beyond doubt.

Therefore, the back-end server or your IoT platform needs to support certificate-based authentication through a secure communication protocol, i.e. MQTT/HTTP over TLS. WISeKey has a SaaS product called INeS CMS which has seamlessly integrated with commonly used IoT cloud platform (AWS IoT Core/Azure IoT hub & DPS). The device certificate issued by a CA defined in WISeKey and managed by INeS CMS will be authenticated by those IoT platforms to achieve the IoT device onboarding without touching. WISeKey has a complete solution that demonstrates the capabilities of implementing a secure zero-touch onboarding, please contact our sales representatives for more detail information.

Key features of INeS CMS

- Complete Certificate Management System for the needs of IoT. From certificate creation to lifecycle management, INeS CMS is agile, scalable, economical and easy to use.
- Advanced Web GUI (Graphic User Interface) with multi-tenant capabilities where multiple independent instances of one or multiple applications operate in a shared environment.
- Versatile REST APIs that allow easy integration with the business applications of the customer for device registration, certificate issuing, renewal and revocation. The REST API is available as an open API for easy back-end implementation for communications like HTTPS and MQTTS. Seamlessly integrated with AWS IoT and Azure IoT cloud services.
- Available as a service from WISeKey's secure data center or installed on premises.
- Certificate enrollment by the device through standard protocols (i.e. RESTful API, EST).

Conclusion and takeaways

- In the IoT application, authentication is one of the keys for each IoT device to be recognized as an authentic device to onboard before publishing the IoT workload to the cloud. Implementing a secure certificate-based authentication (based on PKI) is the best practice for every IoT application, it's more secure than pre-shared key and it minimizes the risk of the leakage of credentials if the private key is well-protected. Integrating a hardware root of trust (i.e. Secure Element) to store the private keys in the IoT device can be an even more secure solution working along with the PKI technology.
- WISeKey has a complete end-to-end solution that securely covers the credentials storage, managed PKI solution, certificate inventory and life-cycle management, flexible provisioning for digital identities and zero-touch onboarding for the IoT devices.
- Please contact our sales representatives below to know more about the best complementary security solution for each IoT application.

contact: **sales@wiskey.com**