

**Business
case**

SIM card management for private 5G networks with Tornio IoT platform



**Hewlett Packard
Enterprise**

a Partner Ready service

Introduction

Securing the management of SIM cards in private 5G networks, from creation to activation, is delicate and involves several processes depending on the purpose of the SIM card – for users (business/personal) or devices.

New approaches and solutions, such as eSIM and activation processes using QR codes create new opportunities, but also new business and legal challenges.

The processed information might include personal information, the handling and involved processes must comply with General Data Protection Regulation (GDPR) and more.

Principles of the solution

We offer a solution based on the Lequinox[®] Distributed Ledger Technology (DLT) that will create irrefutable audit trails of all actions in the SIM card management.

This includes an enforced legal and policy driven validation process during the activation of the SIM card.

The validation process is determined by the network owner and can include validation components such as, national ID, employment ID, biometrics and more.

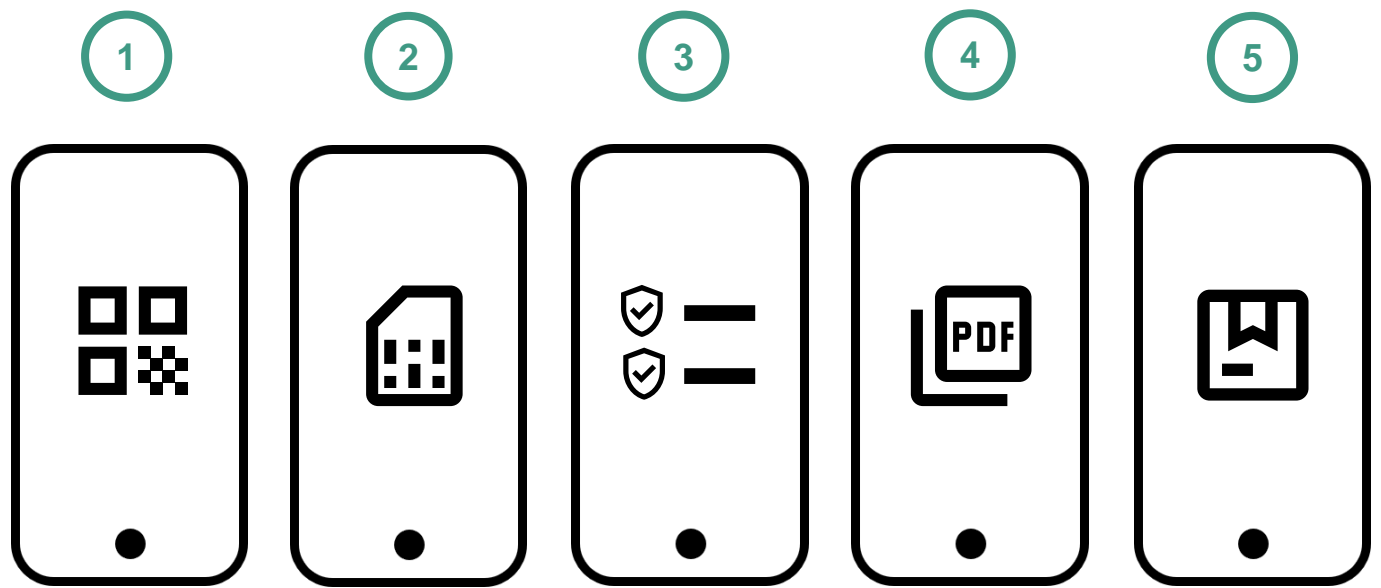
All in compliance with GDPR.

Administration



1. Create of a batch of SIM cards.
 2. Identify the activation validation components for the batch of SIM cards and enter user credentials and selected services.
 3. Sign and Seal the complete process.
- The *Signed and Sealed* information is automatically *encrypted, protected and stored* in an own digital archive, including the *irrefutable audit trail* (who did what and when).

Validation and activation



1. Scan the QR code, initiating the SIM card validation.
 2. Confirm eSIM user credentials and assigned services.
 3. Fulfil the validation process.
 4. Application creates validation documentation.
 5. Sign and Seal the complete validation documentation.
- The *Signed and Sealed* validation information, including the validation document, is automatically *encrypted, protected and stored* in an own digital archive, including the *irrefutable audit trail* (who did what and when).

Improved user experience

The policy driven validation and activation process lowers the risk and increases security and trust for network owners, users (business and personal) and devices within the private 5G network.

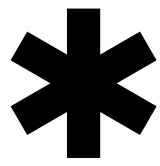
The user can if applicable, have an exact copy of the validation information.



**Hewlett Packard
Enterprise**

a Partner Ready service

Your business outcomes



Risk

- Reduced risk in private 5G network operations by the enforcement of set policies for validation and activation processes in compliance to GDPR and more.
- The Lequinox DLT platform ensures that all information is encrypted and protected with an irrefutable audit trail.



Safety

- Improved safety for both network owner and users, due to the policy enforcement and streamlined processes.
- The Lequinox DLT platform executes set policies, in the validation process.



Efficiency

- Improved efficiency in SIM card validation and activation.
- The Lequinox DLT platform ensures that all information is protected in an own digital archive.



Community

- Improved usability and clarified legal responsibilities in the work environment.
- The Lequinox DLT platform ensures distribution of the validation information to both network owner and users in an encrypted and protected format.



Environment

- Improved environmental footprint, due to the policy enforced and irrefutable processes.
- The Lequinox DLT platform creates the foundations to optimise existing or create new processes and services in compliance with regulation.



**Hewlett Packard
Enterprise**

a Partner Ready service