

Security aspects for IoT devices connected via mobile networks

Architecture and validation

Heinfried Cznotka -

Director Business Development

security

health

mobility

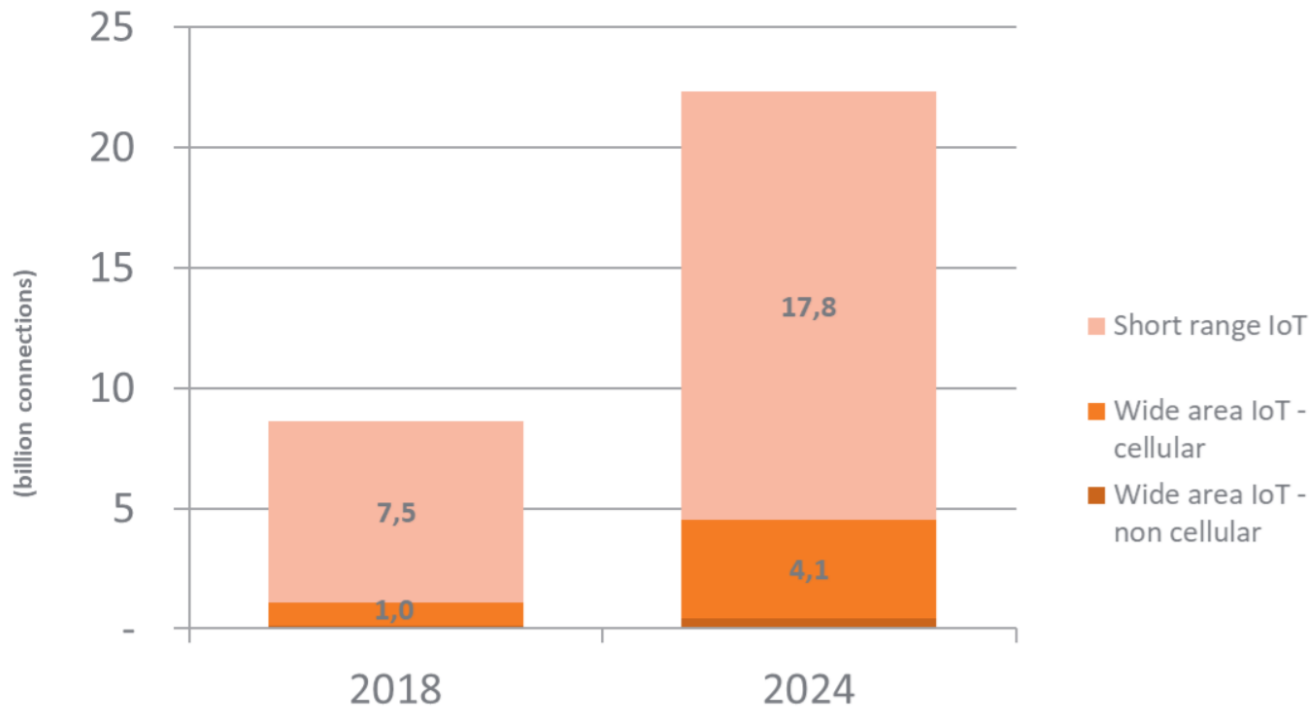
public

IoT

Agenda

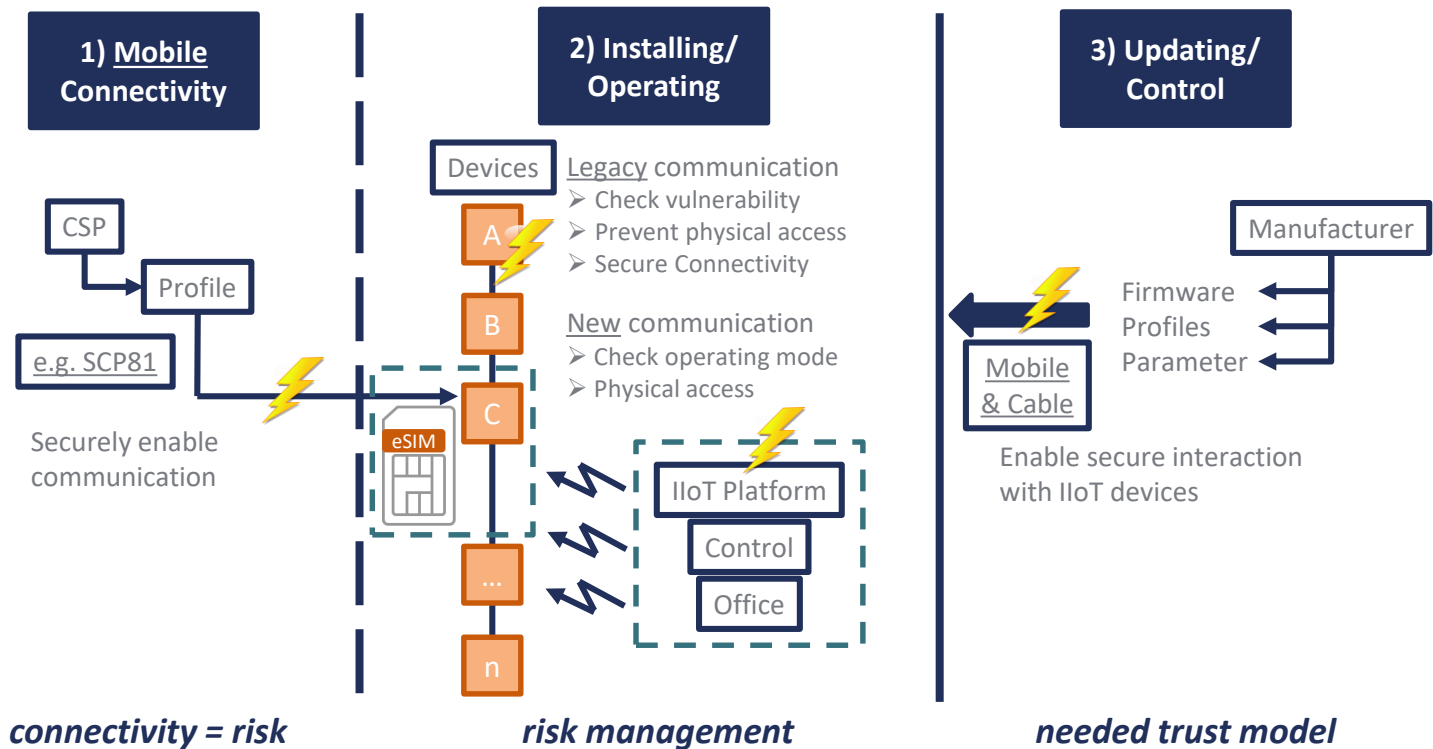
- 1 IIoT security challenges
- 2 eSIM life cycle & subscription management
- 3 Security architecture
- 4 Secure element management service
- 5 Wrap up

Connectivity for IoT

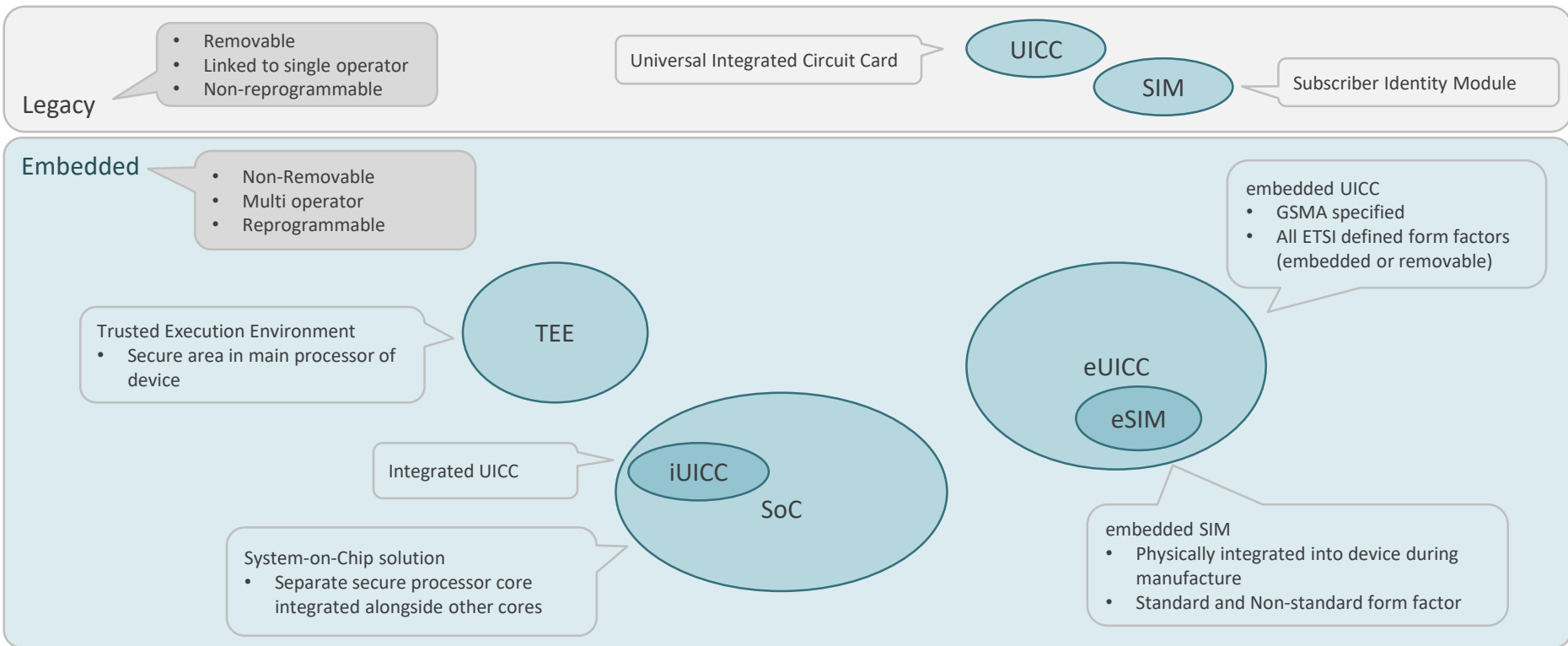


Source: Ericsson - Mobility Report - November 2018

IloT security challenges



Technology terms



SIM form factors – a little history



ID Card Size
1FF



Mini SIM
2FF



Micro SIM
3FF

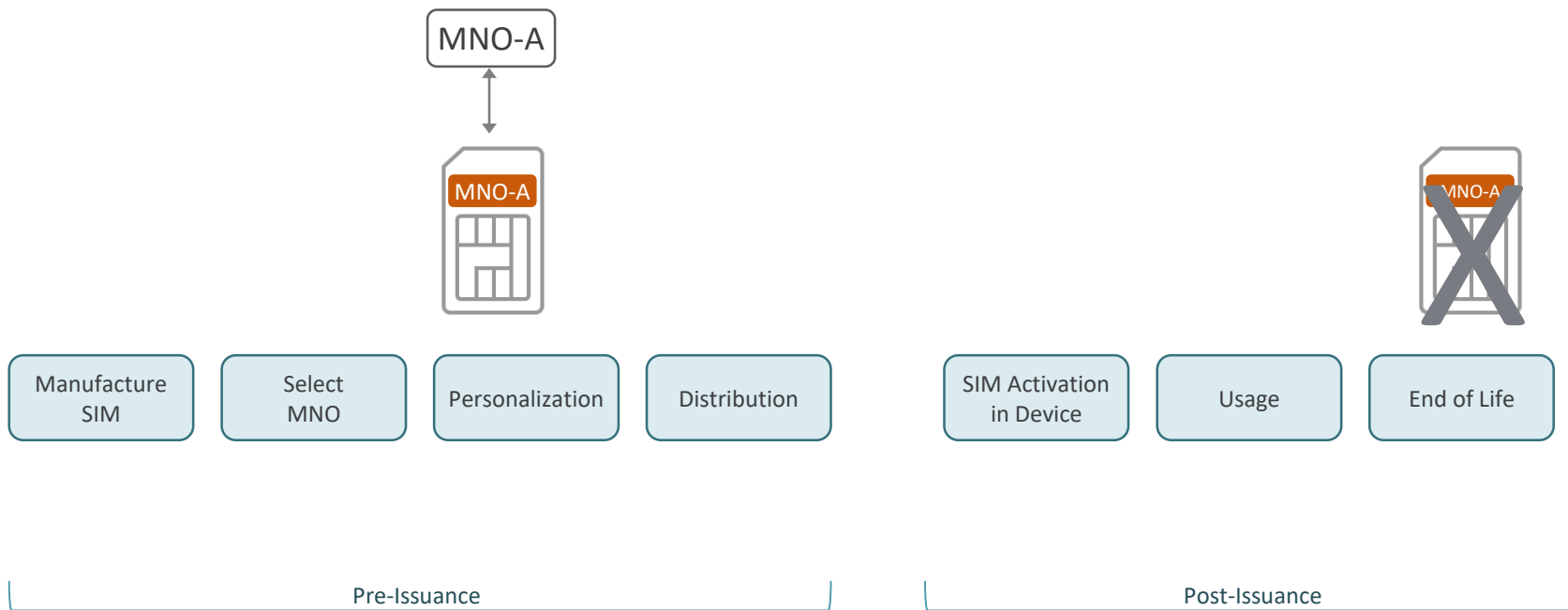


Nano SIM
4FF

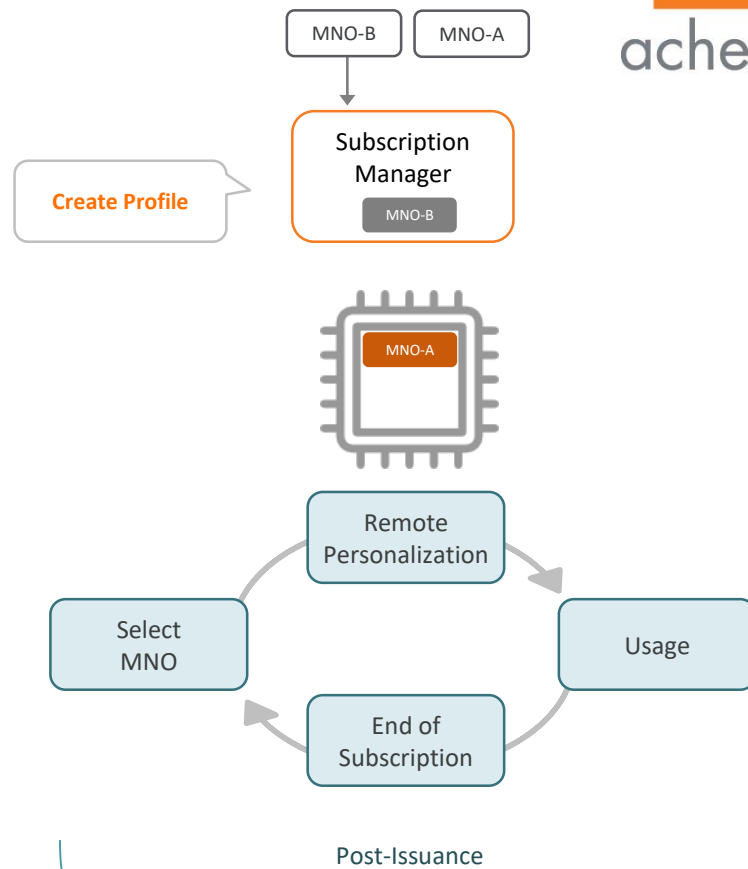
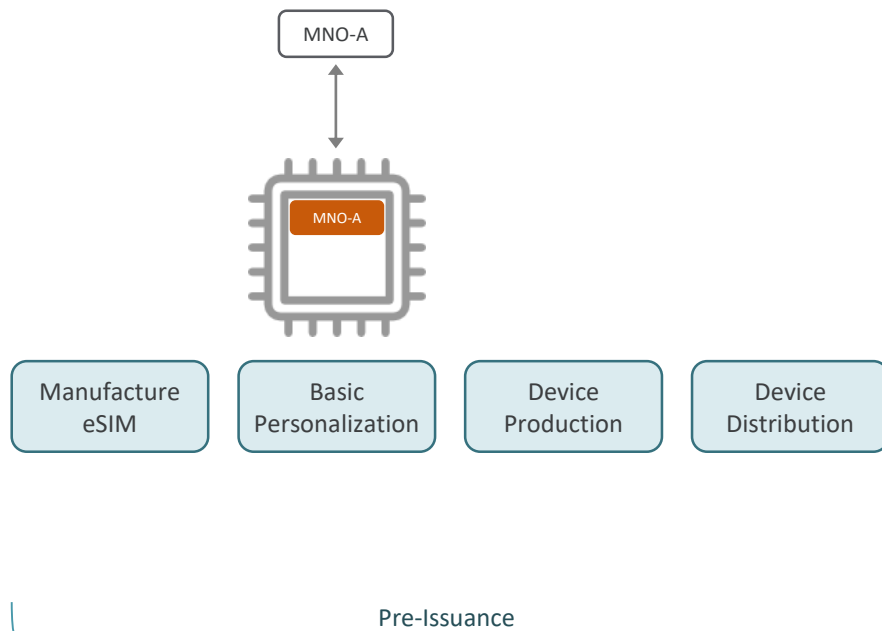


MFF1
MFF2
Non-ETSI

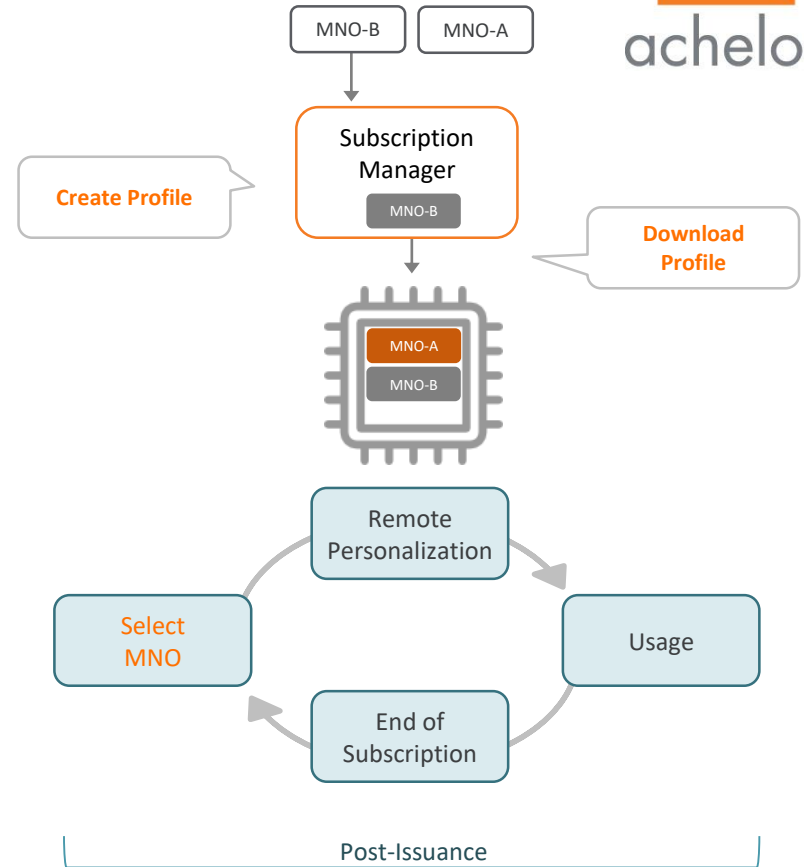
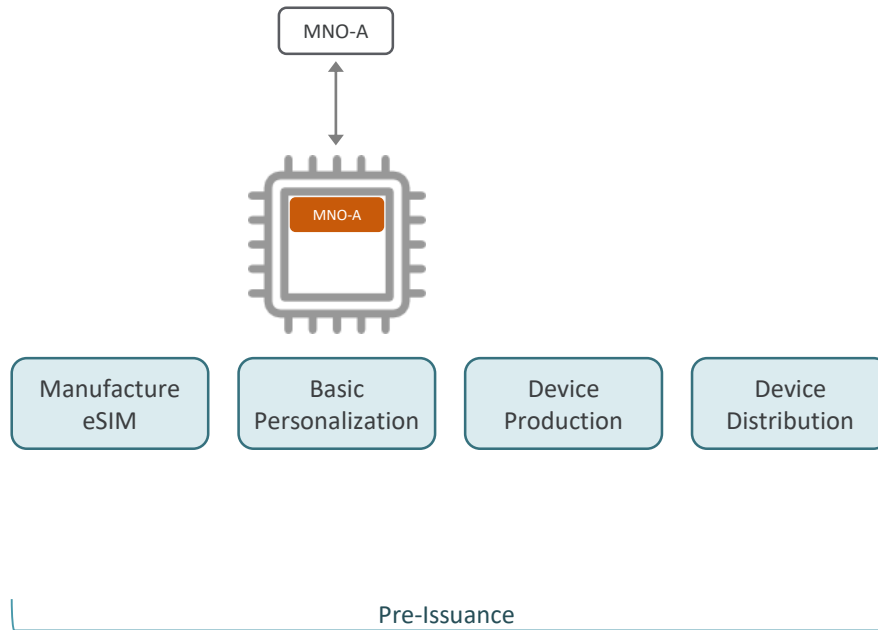
SIM life cycle



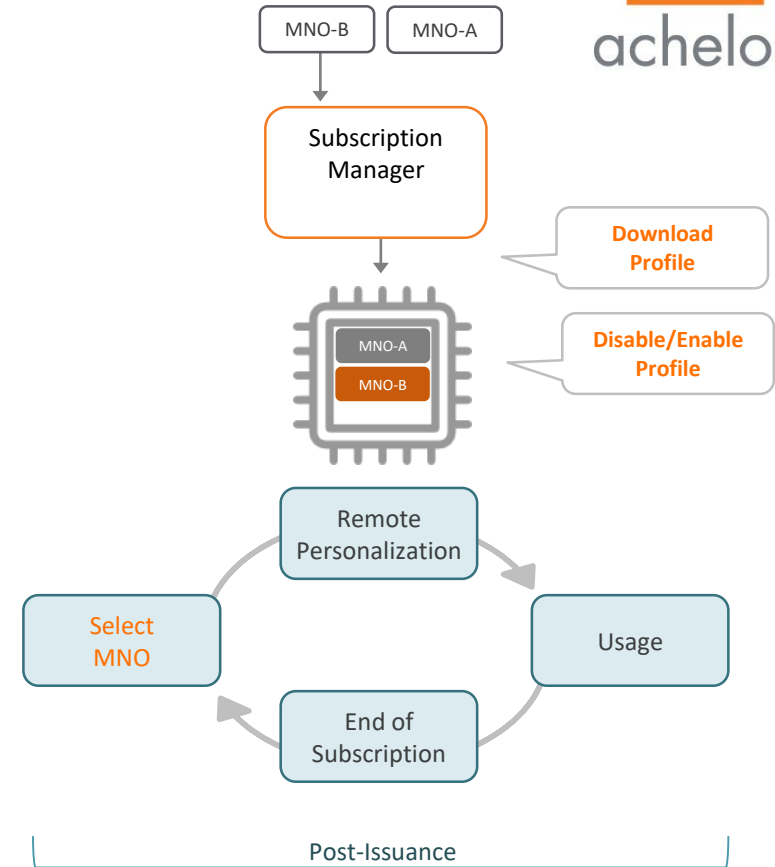
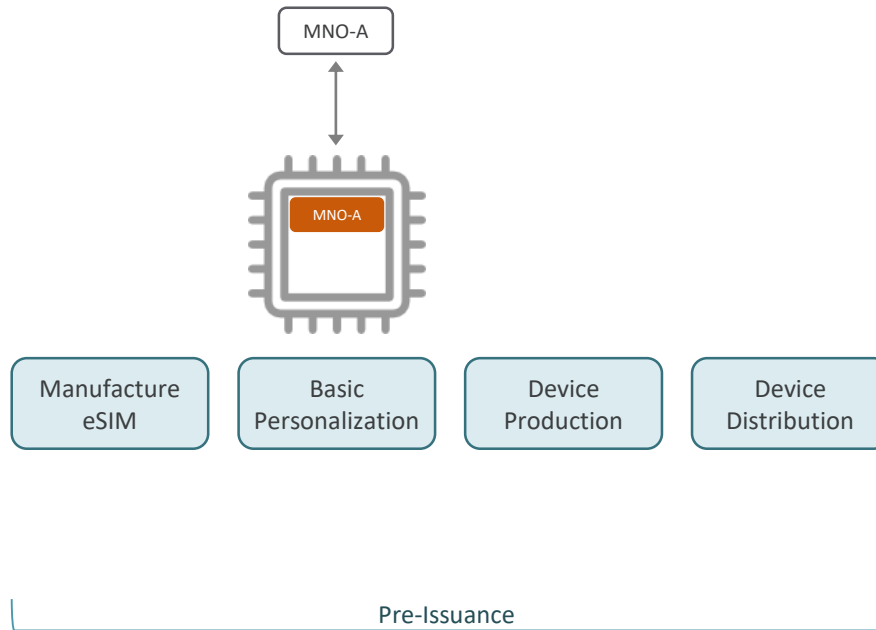
eSIM life cycle (M2M)



eSIM life cycle (M2M)



eSIM life cycle (M2M)



















A real-life example

DEVICE CONNECTIVITY MANAGEMENT

SHOW HISTORY

ICCID: 89462026041000009991 IMEI: STATUS: ACTIVE

VICCID	IMSI	MSISDN	POOL	DOWNLOADED	STATUS	ACTIONS
89462026041000009991	240076509509991	467191200019991		Jul 10, 2017, 1:35:41 PM	ENABLED	  
	89000000000000162				CREATED	  
	89462037051000000378				CREATED	  
	89462038023000000178				CREATED	  
	89000000000000106				CREATED	  



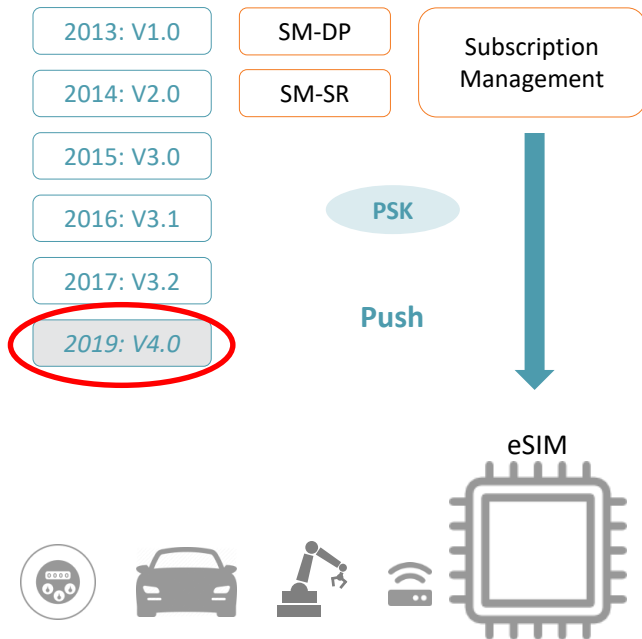
LOAD NEW

AUDIT

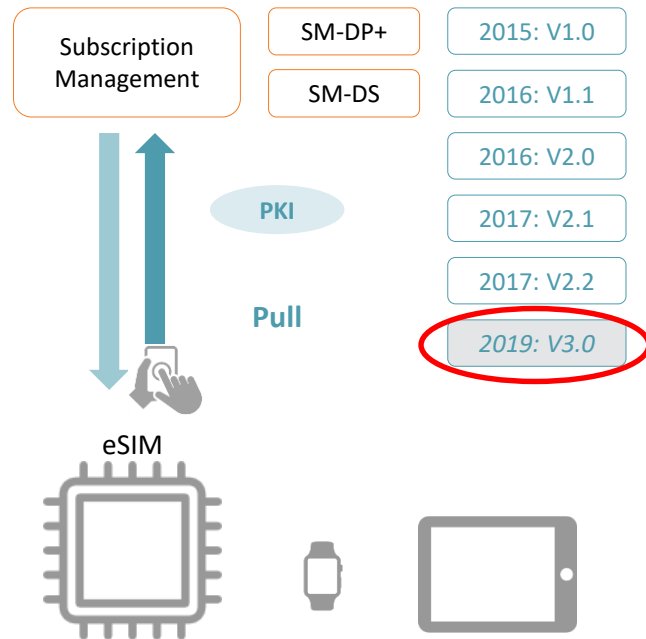
CLOSE

GSMA technical specification for eSIM handling






SGP 02 (M2M)



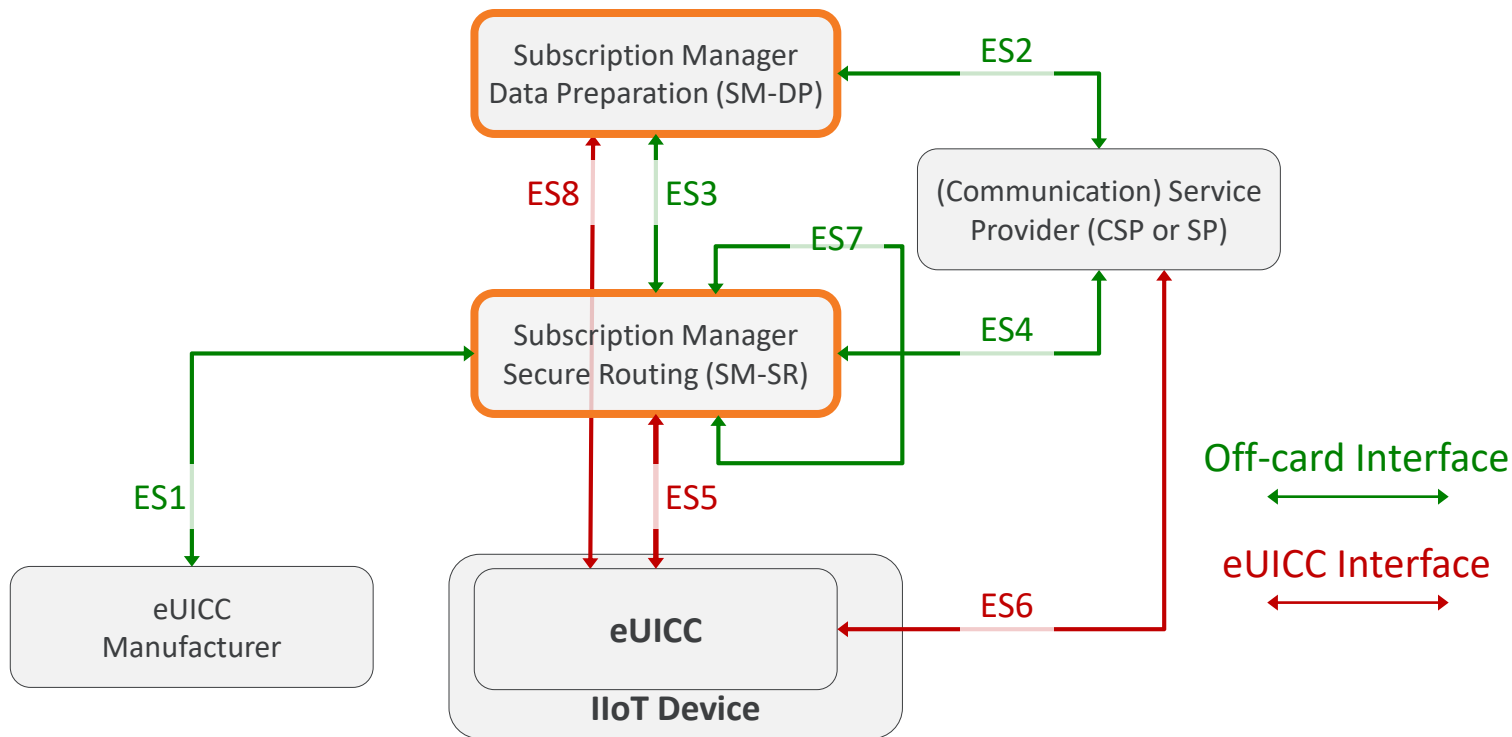
SGP 22 (Consumer)



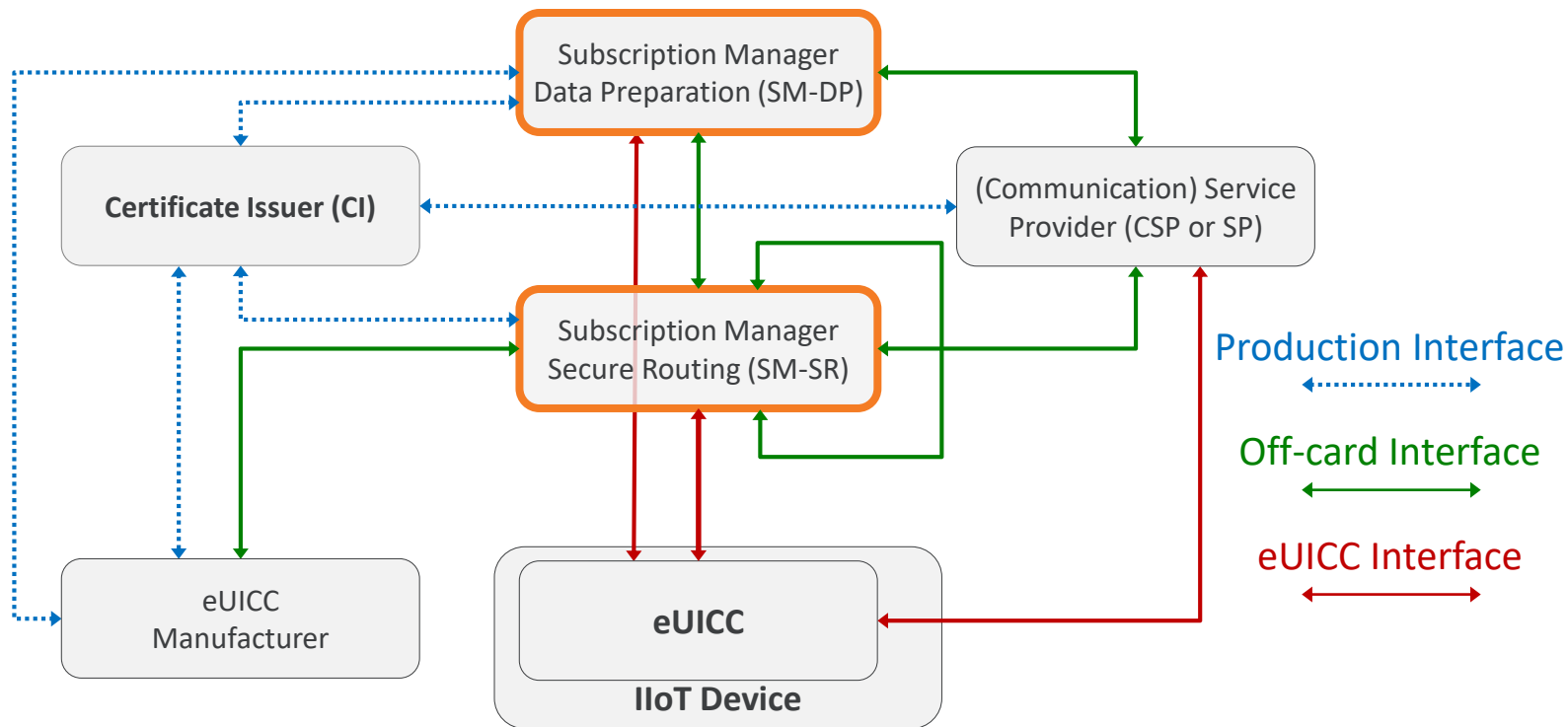
Participants in the eco system

Operator	<ul style="list-style-type: none"> Provides network connectivity to M2M SP or consumer Owens eUICC profile, including Network Access Credentials Connects to one or more SM-DP services 	
Device manufacturer	<ul style="list-style-type: none"> Manufactures M2M device, including embedding of eUICC Provides Provisioning Subscription (optional) 	
eUICC manufacturer	<ul style="list-style-type: none"> Delivers eUICC to Device Manufacturer or M2M SP Provides eUICC management credentials to SM-SR Provides Provisioning Subscription (optional) 	
M2M service provider	<ul style="list-style-type: none"> Owens eUICC (optional) Selects MNO for connectivity service Manages eUICC fleet directly or indirectly connecting to SM-SR service 	
Service consumer	<ul style="list-style-type: none"> Owens eUICC (optional) Receives connectivity service from MNO (directly or indirectly via M2M SP) Receives M2M service from M2M SP (optional) 	

System architecture (M2M)



System architecture (M2M)



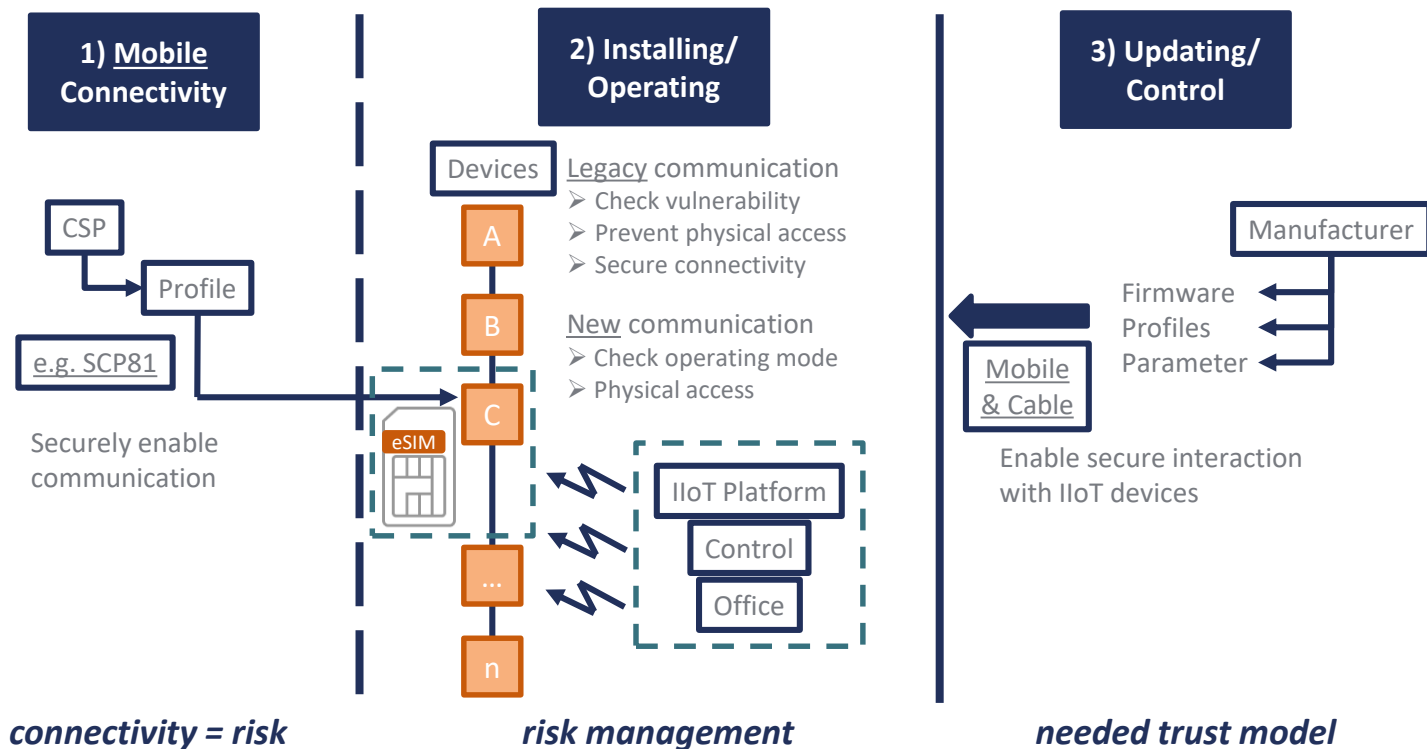
Security

Crypto server microservice	This service is called by any other microservice requiring crypto operations
SM-SR transport security	SCP80/81 - as defined by ETSI and 3GPP
SM-DP transport security	SCP03 and SCP03t - as defined by GP
Key establishment	ECC based – as defined by GSMA and GP SCP11a (ECKA based) – as defined by GSMA and GP
Sensitive data handling	Conform with GSMA SAS specification Crypto Server service interfaces with HSM
General security	CLP.12 for IoT Service Ecosystems - CLP.13 for IoT Endpoint Ecosystems - GSMA IoT Security Assessment Checklist CLP.17

Summary subscription manager

- The eSIM has many benefits for all stakeholders
- The market for eSIM will rapidly grow with the IoT market
- Subscription Manager enables secure, flexible and efficient handling of connectivity profiles

IloT security challenges – what next?



Secure element management service (SEMS)

- New GP specification, v1.0 published in March 2018
- Main objective: reduce card content management costs
- Main approach: managing groups of secure elements
 - enables broadcasted deployment and management
 - uses special certificates
 - transferable via any modern application store
- ➔ Disruptive change of traditional card content management model

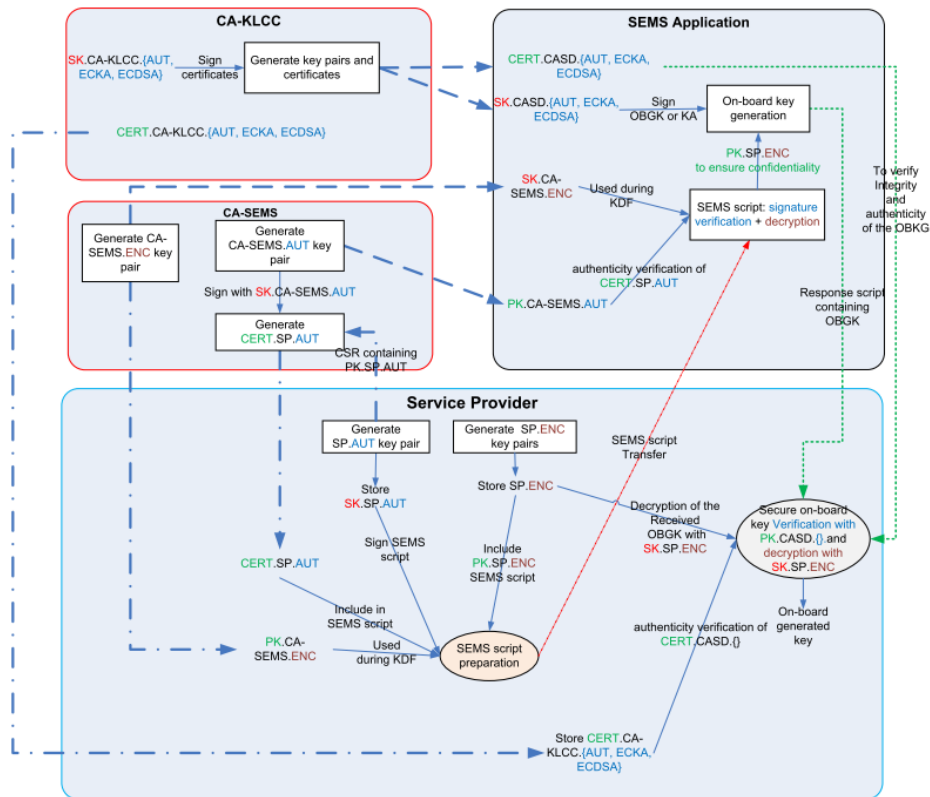
Content & service provision: model comparison

Reduced complexity, reduced costs by broadcasted CCM operations via SEMS

- Traditional CCM
- SE diversified keys
- 1:1 relation
- SE issuer centric
- Push model
- SE issuer TSM-centric model

- CCM with SEMS
- Groups of SEs with same keys
- 1:n relation
- SP centric
- Pull model
- SP TSM-centric model

Overview of keys and certificates



Source: Overview of Keys and Certificates [GPC_2.3.1_SEMS_v1.0, figure 4.1]

Summary: SEMS

- Card content provision easier than in traditional model but still complex, e.g. two CAs needed
 - Different prerequisites, e.g. device agent + personalized SEMS application
 - Enables broadcasted deployment and management of Java Card based services: management per groups of Ses
- ➔ The hurdle to download applications to the SE is clearly reduced

Summary – innovative approach

- Subscription manager enables flexible, secure and efficient choice of connectivity provider for IIoT devices
 - In combination with the newly specified secure element management service (SEMS) by Global Platform IIoT devices can be
 - Managed in groups using special certificates
 - Securely provisioned with new applications via app stores
 - Benefits:
 - Post-issuance remote control of IIoT device connectivity
 - Reduction of secure element content management costs
- ➔ Disruptive change of traditional management model

achelos product portfolio



**TLS test suite
IPsec/IKE test
suite**

**Smart card
simulation
(hard- and
software)**

**Java Card™
test suite**

**Interoperability
with the
telematics
infrastructure**

**Subscription and
connectivity
management**

**Online check of
a driving license
validity in real-
time**



Powerful test suites
to check the
security of network
connections



The virtual.card.kit
simulates the
German electronic
health card and the
digital tachograph



Testing of functional
security of Java
Cards and the
conformity to the
official Java card
specifications



„TI to go“ is a
vendor
independent test
environment for all
components and
interfaces of the
Telematics
infrastructure (TI)



Solution for the
M2M and IoT
market for remote
management of
MNO profiles and
network credentials



Complete process
from registration to
online check
concerning
government
regulations

achelos – security. connected. – for all segments



Security by design and as cross industry need – we test and develop products and customer specific solutions

Interoperability and coexistence of secure networks in eHealth

Mobile und digital – two trends with rapid growth need secure IT solutions

Cyber attacks on digital identities are growing – portfolio of security products for critical infrastructures

Security in a connected world – subscription and connectivity management solutions for IoT

Our references and networks

Close collaboration with the Federal Office for Information Security (BSI) in Germany for certification and approval procedures



Associate Member



Icons made by Freepik, Pixel perfect, Gregor Cresnar, Simpleicon and Those Icons from Flaticon [www.flaticon.com] are licensed by Creative Commons BY 3.0

Lock picture: Maksim Kabakou - Fotolia

Vielen Dank | Thank you

achelos GmbH

Vattmannstraße 1 | 33100 Paderborn | GERMANY

T +49 5251 14212-0 | info@achelos.de

achelos.de | IoT.achelos.com

security

health

mobility

public

IoT