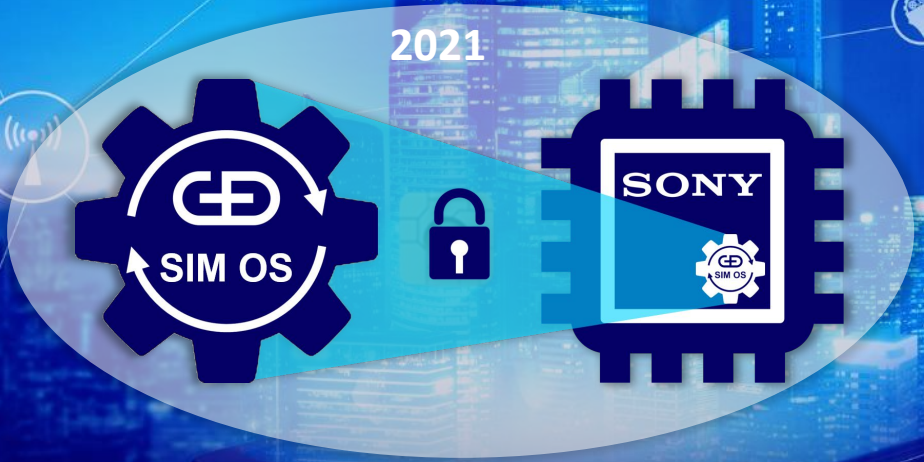
The World's First Secure Integrated SIM for IoT

2021



Giesecke+Devrient
Creating Confidence

SONY

Your Trusted Integrated SIM Solution for IoT

Giesecke+Devrient
Creating Confidence

+ SONY

Our Joint Integrated SIM Offering

ALL-IN-ONE

Accelerated deployment of IoT devices
Modem + Integrated SIM

PRODUCTION

Secure personalization process for IoT devices to meet supply chain requirements

BATTERY POWER

Optimized power consumption to support battery life requirements of beyond 10 years

SIZE REDUCTION

No need for embedded or pluggable SIM

SECURITY

Isolated tamper resistant hardware (secure element), Comparable carrier-grade security

FAST TIME TO MARKET

Provide generic and easy-to-integrate solution for all IoT verticals

FOR CONSTRAINT DEVICES

Efficient profile configuration built for IoT use cases.
Optimized compute resources including cryptography

COST REDUCTION

In comparison to legacy solutions

Contents

01

Introduction to **Sony Semiconductor IL and the Altair Solution**

About Sony Semiconductor IL

Sony is a $80B Multinational Corp. headquarters in Tokyo, Japan.

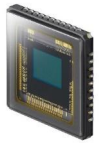
Sony Semiconductor Israel is part of Sony Semiconductor Solutions Corp. Sony Semiconductor Solutions produces imaging, display and IOT products.

Sony acquired Altair Semiconductor Ltd. in **2016**. Now named Sony Semiconductor Israel Ltd.

“Altair” is a trademark of cellular IoT chipsets by Sony Semiconductor Israel Ltd.

The Sony Group

Electronics

Mobile Communications	Game & Network services	Imaging Products & Solutions	Home entertainment & Sound	Semiconductors	Others
					
Internet Service	Mobile Phone	Network Service	Software	Entertainment System	Medical	Professional Solutions	Digital imaging Products	Video	Audio	Televisions	Semiconductors	Recording Media,Battery, Disk Manufacturing

Entertainment

Pictures	Music
	
Media Networks	Television Production	Motion Pictures	Visual Media and Platform	Music Publishing	Recorded Music

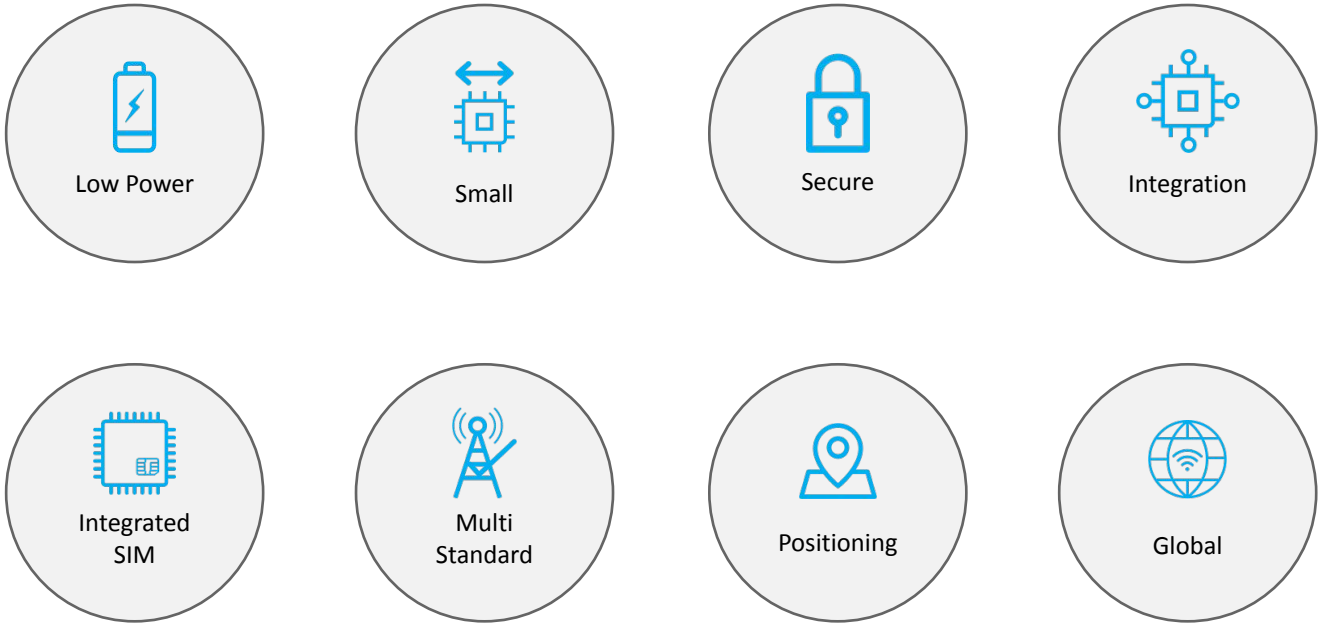
Finance

Finance Service
Sony Life
Bank	Non-life Insurance	Life Insurance

Consolidated Revenue ~$80B

Enabling a World of Cellular IoT Applications

Sony’s Altair Chipset Technology



ALT1250 – CAT-M/NB-IoT/2G Cellular IoT Chipset

Modem Optimized for IoT

- eMTC (CAT-M), NB-IoT (CAT-NB1/NB2)
- 2G/GPRS support
- Cellular and satellite positioning
  GPS, GLONASS, A-GPS, CGI, OTDOA
  (with SW update)
- Global coverage with OneSKU™
  technology
- Rich application layer
  IPV4/V6 IP stack, TLS/DTLS, MQTT,
  HTTP(s), Cloud Connectors
- LWM2M device management and
  differential FOTA
- Highly integrated: On-die BB, RF, memory,
  MCU, PMU and SE. No LPDRAM/PSRAM
- Voice over LTE
- Ultra low power design

Integrated User MCU

- ARM Cortex-M4 Based
- 128KB dedicated RAM + 128KB retention
- IoT optimized interfaces
- Code execution from Flash

Integrated SIM

- HW based integrated SIM
- Compatible with external USIM/eSIM

On-die Security Features

- 2 x integrated Secure Elements (App/SIM)
- HW crypto engines and TRNG
- Secure code execution

ALT1255 – CAT-M/NB-IoT/2G Cellular IoT Chipset

Modem Optimized for IoT

- Release 14 NB-IOT (CAT-NB1/NB2)
- 2G/GPRS support
- Global coverage with OneSKU™ technology
- Rich application layer
  IPV4/V6 IP stack, TLS/DTLS, MQTT, HTTP(s), Cloud Connectors
- LWM2M device management and differential FOTA
- Highly integrated: On-die BB, RF, memory, MCU, PMU and SE.
- Ultra low power design
- Optional PSRAM interface for extended application memory

Integrated User MCU

- ARM Cortex-M4 Based
- 128KB dedicated RAM + 64KB retention
- IoT optimized interfaces
- Code execution from Flash

On-die Security Features

- HW based Integrated SIM
- Secure Boot
- HW separation between modem and MCU

02

Introduction to **G+D**

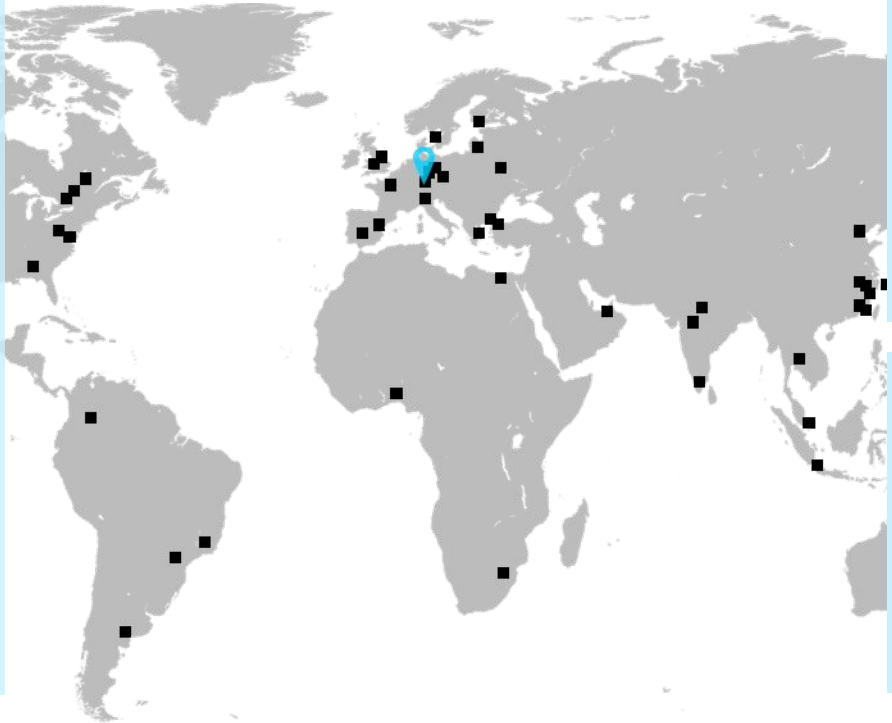
The G+D Group –
Our Global Footprint and Key Business Data for 2019

Founded in
1852
Headquarter in Munich

Presence in
33
countries

76
Subsidiaries
& joint ventures

11,500
Talents worldwide



Sales (2019)

2.45
billion Euro

Earnings (EBIT)

148
million Euro

Solution and Service Business

+33%
Sales

Digital Business

50%
of sales growth

G+D Secures Physical and Digital Values in Four Major Fields

For over 30 years, G+D has been a market leader in providing Trusted Connectivity for mobile devices and the Internet of Things

Enabling secure **Payment** transactions in physical, electronic, and digital form

Providing secure **Connectivity** solutions for mobile devices in the Internet of Things

Safeguarding **Identities** and authentication of persons and objects

Protecting **Digital Infrastructures** systems, networks, and confidential data

Security

Creating confidence through **physical security components** and hardening solutions with **digital security technology**

Today G+D is Already Managing Billions of Things

1 billion
mobile devices
managed globally

> 3 billion
SIM cards
managed in over 80 countries

#1
in eSIM management

> 150
OTA customer Systems for M(v)NOs
globally

> 200
eSIM customer systems worldwide

67%
of consumer eSIM devices
are equipped and managed by G+D

#1
in eSIM for consumer IoT devices

99.99%
server availability for our best-in-class eSIM management solution

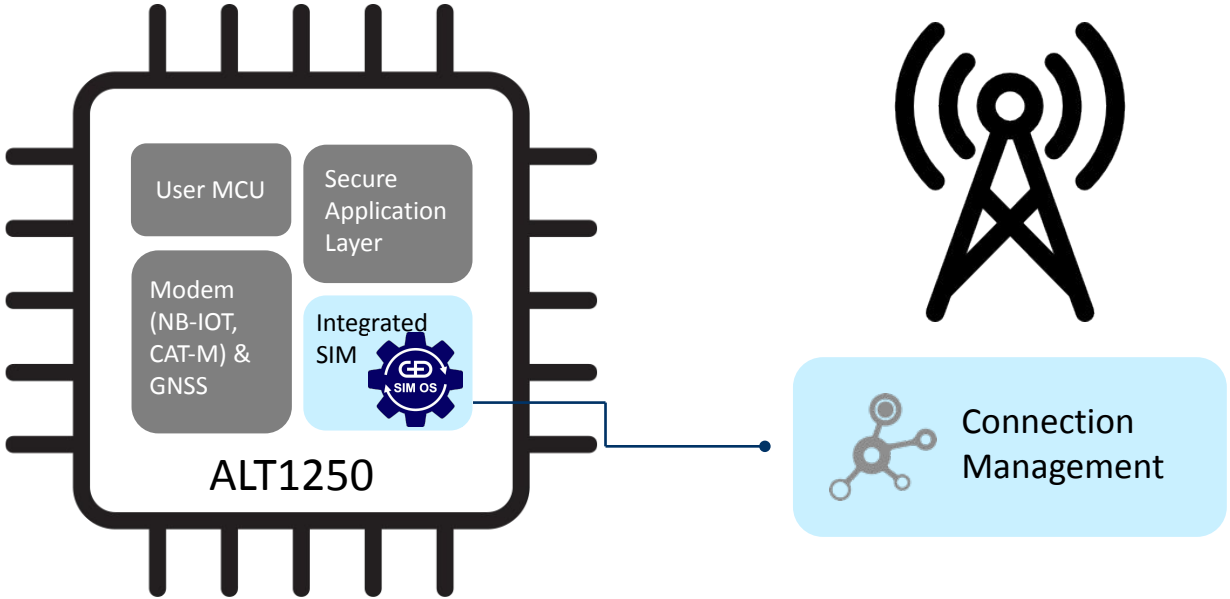
8 of the top **10**
car manufacturers
trust in G+D's connected car solutions

> 1/3
of all connected cars
are enabled by G+D

03

The Secure Integrated **SIM Solution**

ALT1250 Integrated Secure Element Used For Connectivity Management



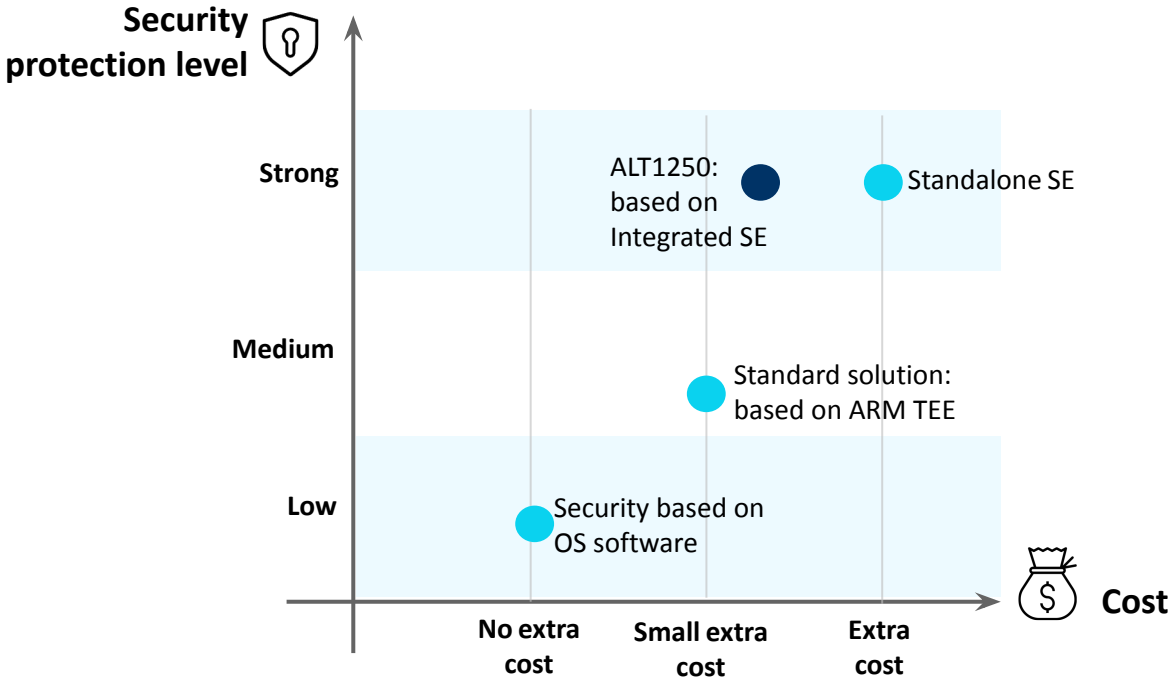
G+D’s Secure Integrated SIM OS

Optimized for IoT use cases

- LTE CAT-M, NB-IoT and 2G
- Integrated and security proven
- Power consumption optimized
- Intelligent memory management system
- Remote file management
- Secure provisioning of OS and Data
- Test profile to verify Integrated SIM in production
- One-time profile switch to operator profile (live environment)

ALT1250 Secure Element

ALT1250 iSE architecture provides comparable security to standalone SE, at fraction of the cost



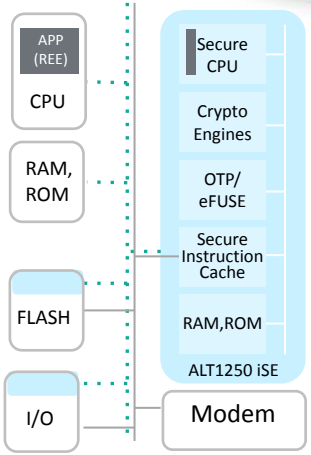
SE – Secure Element
TEE – Trusted Execution Environment
REE – Rich OS Execution Environment

Hardware Integrated Secure Element

Mandatory for enabling secure integrated SIM

ALT1250 Integrated SE-based solution

Static HW sub-system isolation –
very small attack surface

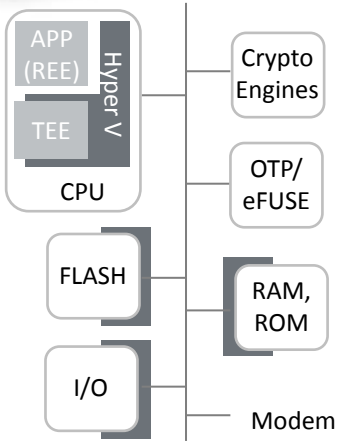


Architecture	Full Hardware
Isolation	**Strong** *Hardware enforced*
Side channel attacks on cache	**Full protection**

Software based on a rich-OS, e.g. TEE

Dynamic resource allocation by SW-attack surface

Architecture	Partially software
Isolation	**Weak** *Software enforced*
Side channel attacks on cache	**Proven vulnerable** ***(spectre & meltdown)***



Security Assessment of ALT1250 with Secure G+D OS

- ALT1250 architecture has been assessed according to standard smartcard security measures
- ALT1250 Integrated SE in combination with the G+D secure OS has been proven to achieve the security level comparable to high-end SIM cards

Giesecke+Devrient

3. Conclusion

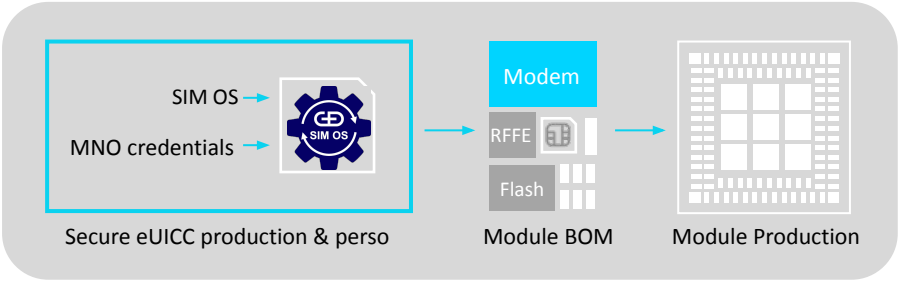
Together with an Operating System which realizes all requirements of the Security Guidance document, e.g. the G+D Operating System "Sm@rtSIM Aquarius iUICC Version 1.0", the achieved security level is comparable to the security level of traditional high-end G+D SIM cards.

Production & Personalization – Secure, Scalable, Low-cost

Trust Domain

LEGACY PRODUCTION MODEL

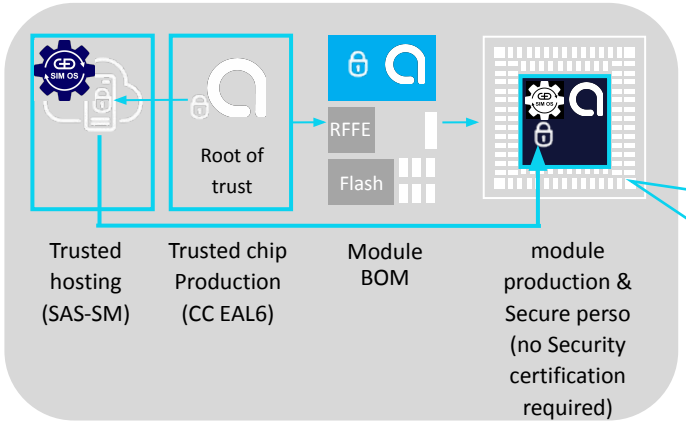
Module production is non-secure, thus low-cost and scalable



Integrated SIM personalization requires an operational module

SECURE INTEGRATED SIM PERSONALIZATION

Secure personalization in a non-Trusted site

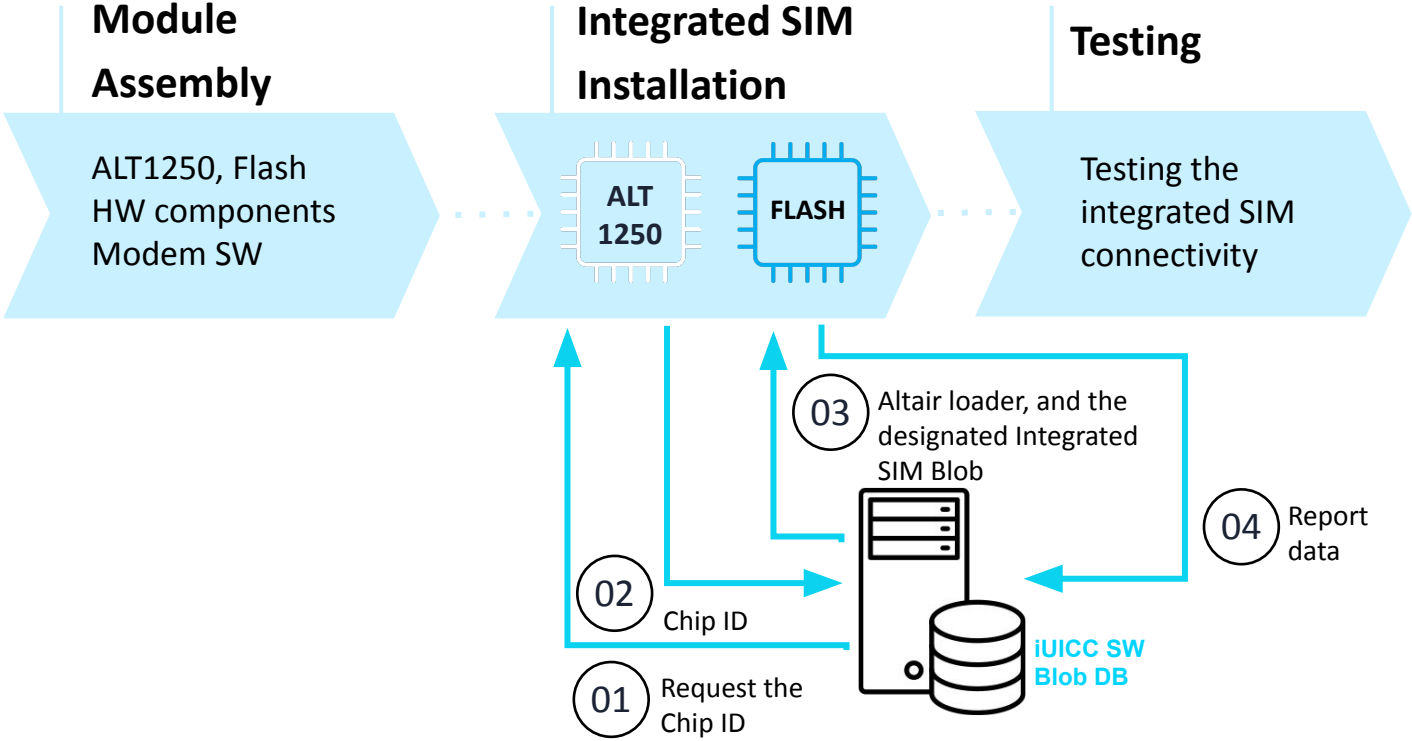


The Chip is the Root of Trust for Personalization
No security requirements for the ODM/OEM

Giesecke+Devrient
Creating Confidence

SONY

Assembly Production Flow for Integrated SIM



04

Integrated SIM **Eco-system**

Acknowledged Solution by Tier-1 MNOs

- AT&T and LG Uplus officially announced their collaboration with Sony and G+D to engage and commercially launch integrated SIM solutions
- Ongoing assessment for deployment of integrated SIM solutions by further Tier-1 MNOs globally

News Release

AT&T, G+D and Altair Team Up to Spur IoT Deployment

Next-Generation Integrated SIM Will Meet the Needs of an Expanding Global Internet of Things Market

DALLAS, Sept. 12, 2018 —An advanced SIM card promises to help usher a new chapter for the Internet of Things by making it easier for businesses to deploy IoT devices.

AT&T* is working with Giesecke+Devrient Mobile Security (G+D) and Altair Semiconductor to integrate a SIM into the modem chipset for deployment across licensed Low-Power Wide-Area cellular networks.

Right now, manufacturers purchase Subscriber Identity Modules (SIM) cards that identify the owner for the mobile network -- just like for your smartphone -- and provision them for IoT devices.

The integrated SIM securely embeds SIM functionality into the chipset, processor and other

LG Uplus' new cellular technology does away with SIM cards

LG Uplus is South Korea's third-largest mobile carrier.

Wednesday, September 9, 2020 2:42 PM UTC

LG Uplus Corp and its global partners have developed cellular module technology using Universal Integrated Circuit Card (iUICC) solutions that do away with Subscriber Identification Module (SIM) cards in mobile devices.

The partners include cellular chipset developer Sony Semiconductor Israel, German digital security solutions provider Giesecke+Devrient, and local communication module maker NTmore.

The latest technology will allow manufacturers to produce smaller devices with the space saved for a SIM card and related components.

The iUICC implements a communication chipset's SIM functionality that is responsible for voice and data connection.

Leading Module Maker Adoption of Integrated SIM on ALT1250

NTmore
Network Technology

WNC
Wistron NeWeb Corp.

SIERRA
WIRELESS

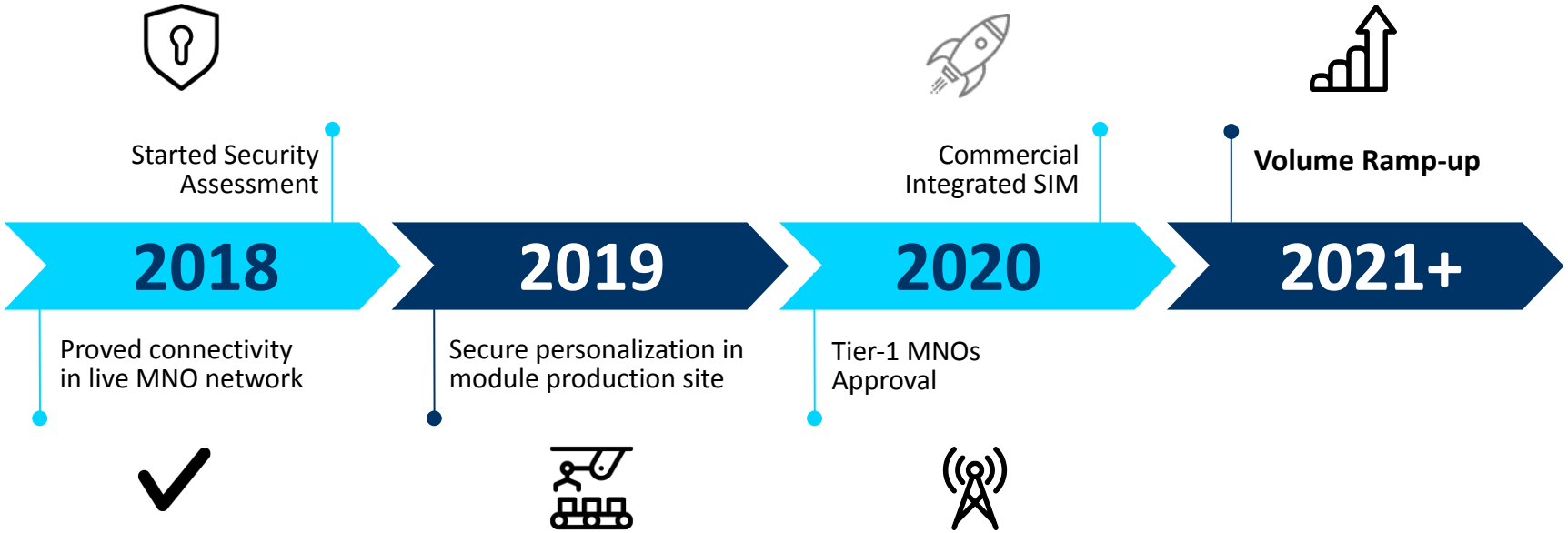
SERCOM

muRata
INNOVATOR IN ELECTRONICS

05

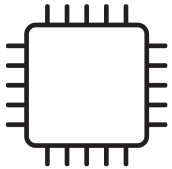
Timeline
and Next Steps

Integrated SIM Program Timeline



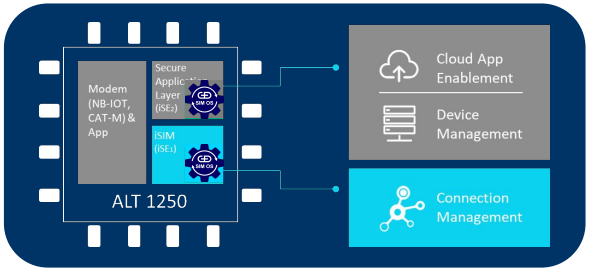
Next Phase Developments

01



All chipsets starting from ALT1250 will support Integrated SIM

02



Enabling the iSE2 as the security foundation for a variety of additional use-cases

03

Enhancing the integrated SIM OS to comply with upcoming GSMA standards

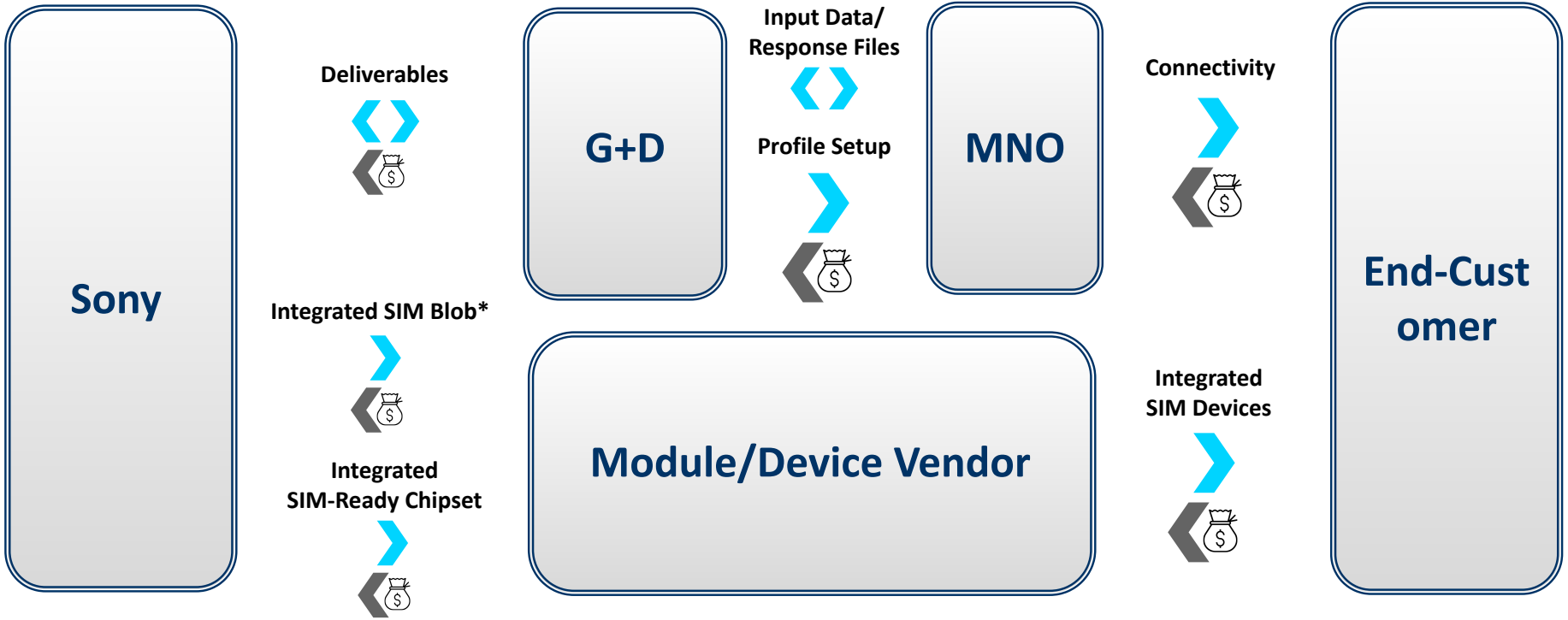
06

Business **Models**

Integrated SIM Business Model #1

Deliverable Cash Flow

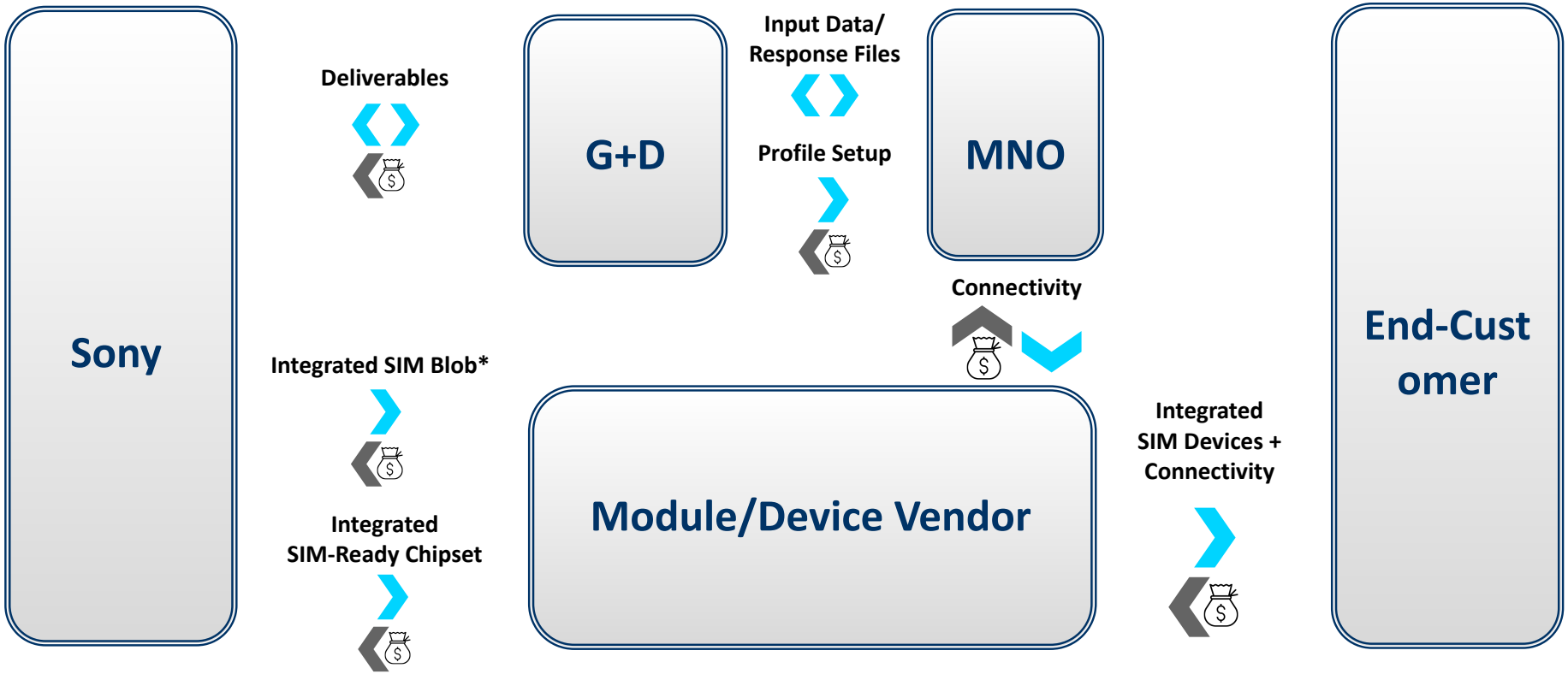
*Blobs = SIM OS and Data



Integrated SIM Business Model #2

Deliverable Cash Flow

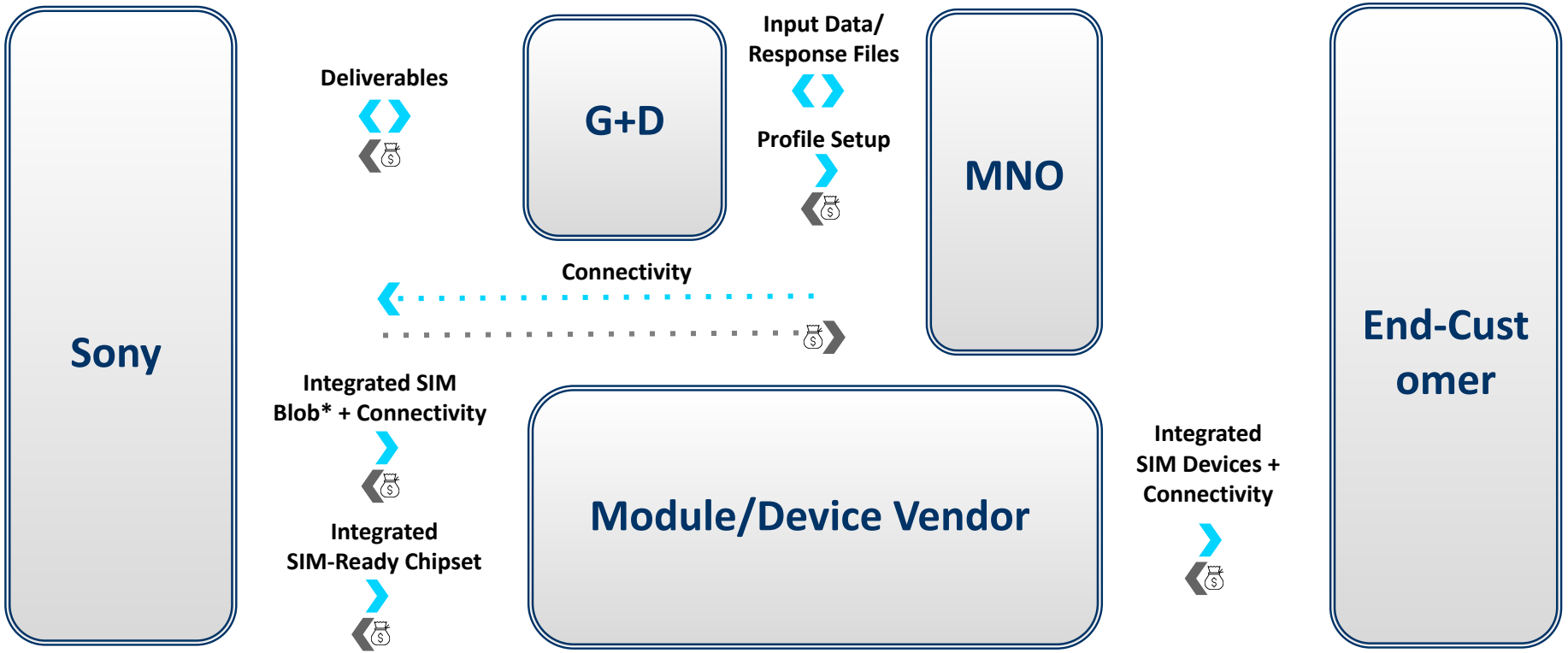
*Blobs = SIM OS and Data



Integrated SIM Business Model #3

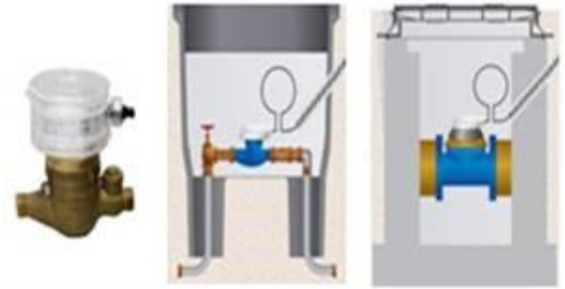
Deliverable Cash Flow

*Blobs = SIM OS and Data



Integrated SIM Reference Cases

Smart Label



Smart Water Meter

Wearable Device

(Not real product image)

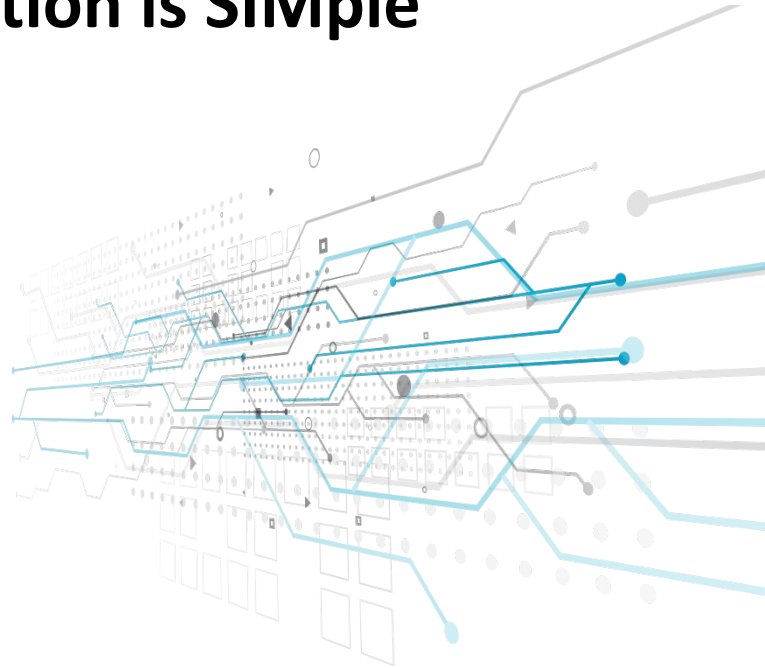
07

Summary

Using Integrated SIM in your Solution is SIMple

Simple business model for highly secured integrated SIM solution and trusted data management by G+D

- Established process for profile setup for integrated SIM between MNO and G+D
- Fast and easy verification of network connectivity by MNO
- Select your qualified Integrated SIM based module vendor for mass production



07

Q&A

Q&A The World's First Secure Integrated SIM for IoT

What is offered by G+D and Sony?

The world's first LTE IoT chip that fully integrates SIM functionality without compromising security.

Q&A The World's First Secure Integrated SIM for IoT

How does the system achieve this high level of security?

Q

A

G+D's leading SIM software runs on an isolated hardware secure element integrated inside the Altair chip & adheres to G+D's strict security assessment standards.

Q&A The World's First Secure Integrated SIM for IoT

Which chip architecture is required in order to enable a security level identical to an external SIM?

The ALT1250 LTE IoT chip includes an integrated fully-hardware secure element comparable to an external SIM hardware architecture as opposed to other software or semi software architectures.

Q&A The World's First Secure Integrated SIM for IoT

What is the benefit for a cellular IoT device vendor?

This all-in-one technology breakthrough allows IoT device vendors to offer smaller and more power-efficient solutions to drive the predicted exponential growth in the IoT market.

Q&A The World's First Secure Integrated SIM for IoT

Which LTE IoT standards are supported by this solution?

NB-IoT & CAT-M 2G
is available in specific modules

Q&A The World's First Secure Integrated SIM for IoT

Is the integrated SIM interoperable with standard SIM ecosystem (3GPP, ETSI) ?

Q

Yes, the integrated SIM is fully interoperable, the same as any external SIM.

A

Q&A The World's First Secure Integrated SIM for IoT

Is the integrated SIM compliant with GSMA specifications?

Q

A

Our integrated SIM is well ahead of the GSMA activity, yet it is very much aligned with it. Once the standard will be fully defined our solution will be quickly adapted to be fully compliant with it.

Thank You