Giesecke+Devrient

iUICC: From hype to realization

The integrated SIM is reality

Addressing the challenges of global adoption

What is an iUICC?

An integrated Universal Integrated Circuit Card (or iUICC) is the next stage in SIM solution technology. Traditional SIM cards are removable chips set into plastic surrounds, and eSIM are dedicated embedded chips on your device's circuit board, but an iUICC also named as integrated SIM is different.

An iUICC is an isolated hardware component or tamper-resistant element (TRE) that is physically incorporated to a device's system on a chip (SOC), a single chip which incorporates CPUs, memory, and in some cases even wireless transceivers, and is the heart of many connected devices. This means that security-critical code and data are still processed in an independent secure hardware unit, but at a much smaller size than an eSIM. So, you retain the security advantages of an eUICC while saving space on the device's circuit board.

The iUICC has the potential to completely revolutionize the connected device and technology market. It offers substantial efficiencies and improvements over previous generations of SIMs. However, it's important to remember that the technology is still in its infancy. The industry is working towards creating a standard definition for the solution, although some first pre-standardized iUICC solutions have been introduced.

SIM evolution towards an all-in-one connectivity solution

Reduction of:
- Cost, size, power consumption
- Process complexity, plastic / waste…

Increase of:
- Service, sustainability
- Flexibility, functionality…

Classical SIM card (plug-in)
- Pluggable SIM card
- Dedicated smartcard controller
- Typically, fixed and preconfigured MNO / connectivity profile
- Form factors are:
  - 2FF / ID000 / Mini SIM (25 x 15 mm)
  - 3FF / Micro SIM (15 x 12 mm)
  - 4FF / Nano SIM (12.3 x 8.8 mm)
- G+D provides complete product

Embedded SIM (eSIM)
- Solderable surface-mounted device (SMD)
- Dedicated smartcard controller
- Supports flexible connectivity via eSIM management
- Typical form factors are:
  - MFF2 (machine form factor 2 – 5 x 6mm)
  - VQFN-32 (very thin quad flat no leads package – 5 x 5 mm)
  - WLCSP (wafer level chip scale package)
- G+D provides an end-to-end solution incl. hardware, smartcard OS and eSIM management

Integrated SIM (iUICC)
- Tamper-resistant element (TRE) implemented within a system on chip (SoC)
- All-in-one connectivity solution for IoT baseband (e.g. NB-IoT) incl. integrated SIM
- No additional footprint required
- No specific form factor
- Enables power optimization
- Supports flexible connectivity via remote SIM management
- Secure production concept for IoT available
- G+D provides smartcard OS (license) + remote SIM management

Benefits

Reduced footprint
The iUICC solution is incorporated into the device's own hardware so there's no need to adjust your technology designs to make room for a dedicated eUICC. This means your devices can be smaller, lighter, and less expensive to produce.

Power optimization
As there's no need for dedicated SIM hardware, less power is needed for your connected device. So batteries last longer, and IoT devices can benefit from more efficient power requirements, a key benefit for devices in unmanned or remote locations.

More efficient production
As the iUICC will exist as an integrated part of the hardware of your own design, you can streamline your production and operations processes. You will no longer need to produce or use SIM housings or embedded chips built to someone else's standards.

Cost reduction and time to market
Provide a generic and easy-to-integrate solution for all IoT verticals as well as a smaller chip with less material, which leads to cost reduction.

Security
Isolated tamper-resistant hardware (secure element), comparable carrier-grade security.

Sustainability
The iUICC does not require any extra housing or plastic card material, nor does it need a plug-in slot, etc.

Taking the lead in integrated SIM technology

Developing trusted, tamper-resistant hardware

Challenge
In order for the market to adopt new standards and replace existing technologies, a high level of security is essential. G+D has already together with an international partner deployed a solution where the security is on the same level as traditional SIM cards, for the software as well as the underlying hardware. Robust physical mechanisms that help prevent intrusions and enable countermeasures against hardware and software attacks are in place.

Fact
G+D, mobile network operators (MNOs) and other technology partners have worked together to integrate the SIM into the modem chipset. This paves the way for the next generation of secure IoT connectivity especially for NB-IoT (Narrow-Band-IoT) and LP-WAN (Low Power Wide Area cellular networks). This is an industry first for iUICC partnerships, featuring both MNO and device maker buy-in. G+D is enabling both the MNO and the device maker portions of the solution.

Action
Although the iUICC doesn't rely on a standard hardware format, a set of design principles that are commonly agreed upon should be adopted to ensure that the device remains resistant to physical tampering. eUICC solutions already use sophisticated anti-tampering measures. The first commercially available iUICCs for Narrow-Band-IoT (NB-IoT) are on the market. They come with G+D's SIM OS, that enables the integrated SIM.

Agreeing upon approved specifications, standards, and processes

Challenge
The industry is in the process of defining the common standards and specifications for iUICC. To support device interoperability, developing these standards and specifications should become a priority. All the required functionalities, e.g. for enabling secure remote personalization, are in place.

Fact
Partnership is crucial to the successful worldwide acceptance of iUICC as standard IoT technology. That's why, thanks to our many years' experience and deep industry relationships, G+D is a key part of the effort to define these standards. We're working to ensure that the customers' needs are a fundamental factor in these deliberations.

Action
The only way to overcome this challenge is through cooperation to develop a joined-up ecosystem.
This requires input from many sources; network operators, manufacturers, testing and certification bodies, GSMA, and other organizations to name but a few.

Developing a secure embedded operating system

Challenge
Even once a set of standards for hardware design are agreed upon, an embedded operating system to manage the SIM profile and interact with the rest of the device must be produced. It is essential that this OS is at least as secure and resistant to intrusion as current eUICC operating systems.

Fact
G+D is engaged in activities to integrate its operating system directly in SoC for consumer devices. For example, we chair GlobalPlatform's Secure Element (SE) committee. The SE committee defines industry- and technology-neutral specifications for the secure and interoperable deployment and management of multiple embedded applications on SE technology. This includes both embedded and integrated SEs, SIMs, and UICCs.

Action
Again, this requires close cooperation between all sectors of the market to ensure a common approach and promote interoperability. This already forms part of discussions G+D is leading with all segments of the evolving iUICC ecosystem.

Link: https://globalplatform.org/technical-committees/secure-element-se-committee

Ensuring secure data preparation and provisioning

Challenge
New integrated technologies, such as eSIM, eUICC, and iUICC, absolutely require a trusted and secure environment, especially during the initial steps of the technology lifecycle. To be successful, the entire process and supply chain must be secure and protected so that data can be safely generated and processed, and service can be successfully delivered.

Fact
We are committed to the secure personalization of eUICC in consumer devices, phones, and tablets. G+D is working with multiple technology partners to commercialize the iUICC. The first solutions in the market have already been successfully delivered by G+D and partners.

Action
To ensure secure data preparation and provisioning, close collaboration across the entire ecosystem is needed. Chipset manufacturers establish Root of Trust – the physical foundation for security in a system on a chip environment. Then module and device makers need to help define a secure and efficient process for OS download and personalization.

Guaranteeing interoperability within the eSIM ecosystem

Challenge
Interoperability is crucial to the ongoing success of iUICC. Developing common approaches and standards to both hardware and software, as well as agreeing upon a shared definition of iUICC, will ensure that devices work smoothly with one another – a critical component of any IoT network.

Fact
The eSIM ecosystem has rapidly matured into a globally trusted, secure foundation for IoT connectivity. This maturity has been aided by G+D's commitment to industry standardization and proven interoperability, as evidenced by our 2019 win at GSMA's eSIM LITE interoperability TestFest. We foresee this commitment and dedication seamlessly moving forward into the world of iUICC. Since 2021 the iUICC is commercially available and has been proven in field.

Action
Partnerships with certification and testing labs to ensure interoperability as standard in testing protocols are crucial to success.

Implementation and security evaluation

Challenge
Can the new iUICC technology equal or beat the level of protection and security offered by existing secure elements and eUICC? The overall security of the device is dependent on this implementation of both hardware and software security.

Fact
In current eSIM-enabled IoT devices, the secure OS is the trusted anchor in a secure element which makes secure connectivity possible. With over 20 years of experience, G+D is a trusted provider, with manufacturers relying on its competence to securely deliver an eOS.

Action
Manufacturers, software developers, security labs, and network operators must all work together to implement and verify security. This level of security must be on a comparable level of trust and reliability to traditional SIM cards to keep customer trust and avoid external penetration.

Integrating and managing lifecycles

Challenge
Integrating and migrating secure OS on multiple chipsets, each potentially with its own architecture and security design, is complex and requires a high level of specialized expertise. Then, OS loading and updating with in-factory or in the field is equally complex with challenges across supply chain, processes and security. Manufacturers need to understand how they can navigate this complicated environment to take advantage of the benefits of iUICC.

Fact
G+D believes that standardization is the key to worldwide commercial success for the iUICC. We are working on several initiatives to define lifecycle management for integrated solutions concerning both operating systems and profile updates. These profiles are being developed in collaboration with trusted standards organizations such as ETSI, Trusted Connectivity Alliance, and GlobalPlatform.

Action
Lifecycle management solutions, such as that offered by G+D, can already remotely provision devices with SIM profiles to adapt to necessary network requirements, customer choice of MNO, and local network requirements. However, this capability should be expanded to include secure OS updates, either from an in-factory personalization perspective or remotely updated in the field over the air (OTA).

The future of integrated SIM

iUICC is a very exciting technology with massive amounts of potential, especially for the IoT. We pride ourselves on being at the forefront when it comes to bringing this to market together with our industrial partners.

If you are looking to leverage the benefits of evolving SIM technology now, we can help. We are the trusted market leader in eSIM solutions, with eSIMs numbering in the upper double-digit million range connected worldwide through G+D's solutions. Alongside enabling a complete eSIM solution for you today, our expertise and market position means we're ideally placed to help you prepare for the future of connectivity, and iUICC is definitely a part of that conversation. It is now available. Why not harness the eSIM opportunity today?
Talk to us!

Learn more about G+D solutions
www.gi-de.com

Giesecke+Devrient

Giesecke+Devrient Mobile Security GmbH
Prinzregentenstrasse 159
81677 Munich
Germany

www.gi-de.com
mobilesecurity@gi-de.com

Follow us on: