SECURITY RESEARCH

GSMA INQUIRY AROUND eUICC / eSA CERTIFICATION SCHEME

We inquired GSMA on the issues pertaining to eUICC / eSA certification process, its costs[1], mandatory status, liabilities and "privileged" parties (with a power to provision potentially malicious apps into eSIMs). This document contains our questions along the answers (in purple color) provided by GSMA staff members on Jun 27, 2025.

[Question 1]

I got information that no eSIM does bytecode verification (per eSIM protection profile described in SGP.25 and the JavaCard protection profile).

This implicates all eSIM are likely vulnerable. This also implicates the industry / ecosystem knew / was well aware of this in 2019.

Can GSMA confirm this (that all eSIMs are likely vulnerable in particular) ?

Currently, none of the GSMA RSP specifications require bytecode verification (although this is likely to change following your CVD). The GSMA is not aware of the implementation-specific details for the eUICCs so we cannot provide any market or proprietary implementation information.

However, this does not mean all eSIMs are potentially vulnerable to the attack as detailed in your CVD. It is possible that eUICCs have additional proprietary mechanisms within their JVM implementations that, while not a full on-card bytecode verification, would stop some attacks and as a minimum require further, highly complex work to be successfully attacked.

As mentioned, GSMA will publish an Application Note that recommends the use of bytecode verification along with guidance on the safe use of GSMA Specifications.

[1] in the context of the exploit presence and Kigen investments to ensure the company is building secure products

One thing not raised by your CVD, but worth mentioning, is that the access to the eUICC should be properly controlled. While an eUICC should be secure, it shouldn't be possible for an application to be installed within a Profile without proper authorisation. We have recently made changes to the TS.48 Generic Test Profile (v7.0) to make the keys used for application installation confidential and profile specific. In the case of devices destined for sale it is not expected that any installed TS.48 GTP will allow Java Card Applet installation within a profile. It's worth adding that not all of the devices in the field have a TS.48 GTP installed.

[Question 2]

According to GSMA web pages and documents such as this one:

https://www.gsma.com/solutions-and-impact/industry-services/wp-content/uploads/2025/02/eSIM-Compliance-and-Certification-Webinar-17-PDF.pdf

eSIM Compliance and Certification are key to eSIM security. The above doc showcases the risks without eUICC SW Certification of which some

include those demonstrated by my research.

Theoretically, the certification process (such as eSA) should catch the issues in JavaCard due to the scope of the certification (the application / platform / SOC and runtime environment layers).

How come target eUICC (approved by GSMA by the means of consumer cert) has successfully passed the certification and found its way into the field ?

What's GSMA stance on that ?

The vulnerabilities in question were not within the scope of the initial programme. The GSMA is currently reconsidering the scope of the scheme in order to address these vulnerabilities.

There may be implementation specific mechanisms to avoid this kind of attack. However, GSMA is not able to answer questions about any specific product.

[Question 3]

Is the certification process obligatory for eUICC manufacturers in order to have GSMA consumer cert be issued for the eUICC ?

Yes, all eUICC manufacturers are required to have carried out the compliance requirements described in the GSMA certification process SGP.24. This Certification process in all its past and future versions, has been unanimously agreed by GSMA members.

This process allows the eUICC manufacturers to request, from the GSMA CI, a GSMA PKI Consumer EUM CA Certificate upon verification that all the requirements have been implemented successfully. This EUM certificate is used to issue the eUICC Certificates for credential installation in their eUICCs.

[Question 4]

The doc depicted in the beginning of this message says that certications are valid for 5 years (for both eSA and Common Criteria schemes). How come, the GSMA approved (by the means of a cert chain) leaf eUICC cert issued for arbitrary eUICC could outlive that (could be valid for much more than 5 years) ?

Once the GSMA PKI EUM CA Certificate is issued, the GSMA PKI EUM CA Certificates are used to issue the eUICC certificate that authenticate the eUICC against the SM-DP+. The EUM PKI CA certificate validity period was estimated with the life cycle of the device. That is why the security certification of the eUICC is shorter than the EUM PKI CA certificate validity period. However, a revocation technical mechanism and its revocation process were defined to be able to revoke an EUM PKI CA certificate if necessary.

[Question 5]

Can you provide the list of parties (such as eUICC manufacturers)

OR

their number (the number of parties)

OR

their geo-location (such as country)

that have been issued the sub-CA GSMA consumer cert that can be used to generate arbitrary leaf eUICC cert ?

There is public information on UICC/eUICC manufacturers that are SAS-UP certified, this is an essential part of being able to produce/develop/manufacture these products. SAS-UP is a mandatory requirement for eUICC manufacturers to be able to obtain a GSMA PKI certificate for their products. The link below contains company names, locations and the scope of their SAS-UP Certification.

https://www.gsma.com/solutions-and-impact/industry-services/assurance-services/security-accreditation-scheme-sas/sas-accredited-sites/

The eUICC that has declared functional compliance with the GSMA technical and technical specifications are publicly available on GlobalPlatform.com.

Information on certified eUICC products is only available to GSMA members.

[Question 6]

Can you provide the list of parties (such as SMDPP / RSP server owners)

OR

their number (the number of parties)

OR

their geo-location (such as country)

that have been issued the SMDPP / RSP server cert that can be used to sign arbitrary profile bundles and deliver these to GSMA consumer eUICCs ?

There is public information on SAS-SM accredited sites (SM Providers which include SM-DP) that are SAS-SM certified (an essential part of being able to produce these products). SAS-SM is a mandatory requirement for Subscription Managers to be able to obtain a GSMA PKI certificate for their products. The link below contains company names, locations and the scope of their SAS-SM Certification.

https://www.gsma.com/solutions-and-impact/industry-services/assurance-services/security-accreditation-scheme-sas/sas-accredited-sites/

Information on certified RSP servers is only available to GSMA members.

[Question 7]

The following lists eUICC products that have undertaken the GSMA eSA Scheme and obtained a GSMA eSA certificate to the level of EAL4, augmented with AVA_VAN.5 and ALC_DVS.2:

https://www.gsma.com/solutions-and-impact/industry-services/assurance-services/euicc-security-assurance-esa/esa-certified-products/

Does GSMA eSA certification scheme implicates the products listed on the above web page are immune (not vulnerable) to JavaCard issued from 2019 ?

The vulnerabilities in question were not within the scope of the initial programme. The GSMA is currently reconsidering the scope of the scheme in order to address these vulnerabilities.

[Question 8]

Assuming GSMA received the administration fee, who covers the costs of the evaluation work by the security lab. Is it GSMA (from its budget / member fees / etc.) or maybe that's an extra cost for the eUICC vendor (beyond administration fee) ? If that's an extra cost, what budget or its range does an arbitrary eUICC vendor needs to be prepared for in order to complete (achieve) GSMA certification (eUICC certification)?

The GSMA eSA Administration fee Price list is publicly available and can be found on gsma.com HERE.

The evaluation and certification costs are covered by the eUICC Manufacturers (EUMs) directly with the eSA Licensed Laboratories and eSA Certification Body (list of providers available HERE) and the price list for each is available on each provider's web page or upon request.

[Question 9]

Should an eUICC vendor be refunded all (or any) of certification costs in case its product which successfully passed GSMA certification scheme was later found vulnerable to some security issues (such as in Java Card)? What's GSMA stance on that?

As stated in Response 8 above, matters of a commercial nature are between the respective recipients and the suppliers of the service. GSMA is currently discussing how to address technically later found vulnerabilities within the scheme.

[Question 10]

GSMA certification scheme is described as providing assurance and trust for eUICC Software Products. Yet, buggy eUICC(s) were allowed into the market. On what basis should MNOs and eUICC vendors in particular continue trust in GSMA certification scheme knowing that known to be insecure Java Card component hasn't been flagged / detected by the process?

The same as above.

The vulnerabilities in question were not within the scope of the initial programme. The GSMA is currently reconsidering the scope of the scheme in order to address these vulnerabilities.

[Question 11]

Should eUICC products already certified by GSMA be reevaluated in the context of Java Card security (type / memory safety) ?

GSMA is currently considering how to address the vulnerabilities.