SECURITY RESEARCH

SAMSUNG EVALUATION OF THE REPORTES eUICC ISSUES

This document contains the response received from Samsung Mobile Security on Oct 24, 2025. It provides the results of the analysis / review of the reports describing potential security issues affecting eUICC in use by Samsung devices and provided to the company in Aug and Sep 2025.

We apologize for the belated reply, we need additional time for reviewing this with stakeholders.

We completed our analysis with our development team and stakeholders, and please find our response as follows:

- report #1

We confirmed that downloading the test profile issued with a GSMA certificate to the eUICC is a normal operation based on its policy and specification. Additionally, since the authenticated test profile allows the installation of an applet on the security domain using the key set of the profile, we confirmed this as working as intended.

In accordance with AOSP implementation, the eUICC APIs you described can be invoked with system or higher-level privileges. Since this research was conducted using the root privilege, invoking those APIs within your research is an intended behavior that cannot be leveraged for higher practical security impact.

If there are any points we may have overlooked, please kindly share your feedback.

- report #2

Based on our analysis of report #1, the test profile with the updated SPN also needs to be issued with a GSMA certificate.

Additionally, we consider this type of vulnerability as phishing-related issue, which is out of scope for our rewards program.

https://security.samsungmobile.com/rewardsProgram.smsb.

3. Reports related to the following categories are not eligible:

- Scenarios requiring excessive user interaction or tricking users like phishing or clickjacking

We will forward this report to our development team for consideration of future enhancement.

- report #3

Our analysis showed that this needs to be verified from the relevant eUICC vendors.

From the preliminary analysis, although [REDACTED], the attack scenario is not demonstrating as such practical security impact.

If you believe there is any higher security impact to be protected, we recommend reporting this directly to the eUICC vendors such that you get their immediate feedbacks and direct update from them.

On our side, we will keep our own communication flow with our eUICC vendors to follow up on these topics.

- Samsung eSE SDK

We would like to clarify that the Samsung eSE SDK assists service providers to deploy their services using eSE on Samsung devices. And our analysis shows that this is not related to the Samsung eSE SDK.

- Eligibility on our rewards program

In accordance with our policy, "Conditions for rewards qualification", Security vulnerability report ("Report") must be applicable to eligible Samsung Mobile devices (including smartphones, tablets, wearable devices and personal computers), services, applications developed and signed by Samsung Mobile, or eligible 3rd party applications developed for Samsung Mobile.

When we reviewed this ticket, we confirmed that it is a type of common issue that affect not only Samsung devices but also other devices. Therefore, this report falls under the "Reports related to the following categories are not eligible: Vulnerability of a 3rd party code that affects not only Samsung devices but also other Android devices."

Additionally, we couldn't find any practical security impact on this ticket based on our analysis.

As a result, we apologize that this report is not eligible with our rewards program.

If there is any practical security impact or any Samsung-specific issue, please provide additional details to us for further investigation.

Thank you.

Sincerely,

Samsung Mobile Security