ORACLE RESPONSE TO eUICC COMPROMISE NOTIFICATION WITH THE USE OF JAVA CARD ISSUES

On Apr 10, 2025, we shared a pre-disclosure notification similar to the one shared with GSMA organization with Oracle Java Card team located in Germany.

This document contains the unredacted response received from Oracle company via its Security Alerts Group on Jul 03, 2025. It provides the results of the analysis / review of the notification document conducted by the company.

Hello Adam,

Thank you for your report to Oracle.

Oracle reviewed your report about the possibility of a rogue Java Card Application being installed in an enabled eUICC Test Profile using the associated known keys, without proper bytecode verification and potentially compromising the underlying implementation. This issue doesn't represent a specific vulnerability in the Java Card specifications or in the Oracle Java Card Development Kit Tools, including the bytecode verifier.

As defined in Oracle's Java Card specifications, the bytecode verification process is an integral part of the Java Card security model. The Java Card Virtual Machine specification [0] (section 1.3) mandates the use of bytecode verification prior to the execution of applications on a Java Card product to ensure that each bytecode is valid at execution time. Additionally, the Java Card Protection Profile [1] (section 4.4) used for Common Criteria security certification mandates the use of bytecode verification.

The specification defines two implementation options (on-device verification or off-device verification) to adapt to product constraints and application deployment models. In case the verification is performed off-device, the application deployment process must also ensure that, after verification, a Java Card Application to be executed on a device is not altered in a way that does not satisfy the constraints checked by this verification.

Java Card licensees build their own implementation of Java Card in accordance with the Java Card specifications and implement multi-layered security protections according to the threat model considered, which includes the application deployment security model and the related chain of trust. Oracle provides a Java Card Reference Implementation only as an example of the functional behavior of the Java Card specifications.

As documented, the Reference Implementation is not intended to operate in a production environment and under the threats typically associated with such an environment.

The application deployment security models are market-specific and typically defined by the specifications and standardization bodies relevant to each market. Such deployment models are beyond the scope of the Java Card specifications and your report relates to one of these deployment models. Oracle has shared its recommendations with the relevant standardization group(s).

Please do not hesitate to contact us if you have questions.

Best Regards,

Bill

Oracle Security Alerts

[0] https://docs.oracle.com/en/java/javacard/3.2/jc-vm-spec/F74158_02.pdf

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0099V3b_pdf.pdf?__blob=publicationFile&v=2