EUCC-Certified Products

Additional Cybersecurity Information

NXP Semiconductor's Certified Products
Under the European Cybersecurity Certification (EUCC) Scheme:

Production Family	Product Name	Certificate ID	Certification Reference
SN300	NXP JCOP 7.x with eUICC extension on SN300 B1.1 Secure Element	EUCC-2500052-01	Link to EUCC Certificate (TBD)
	NXP JCOP 8.x/9.x with eUICC extension on SN300 B2 Series - Secure Element	EUCC-2500053-01	Link to EUCC Certificate (TBD)

Cybersecurity support:

- The validity period for an EUCC product certificate is established in accordance with the EUCC regulation (Implementing regulation - EU - 2024/482 - EN - EUR-Lex) and is set at five years.
- The product will be maintained during the validity of its certificate. Further arrangements regarding product support should be discussed and agreed upon with the NXP customer account manager.

Guides to maintain the cybersecurity level for eUICC products:

- The eUICC contains multiple MNO Profiles, each associated with a specific International Mobile Subscriber Identity (IMSI). The primary function of each Profile is to authenticate the device's validity when accessing the network. As the property of the MNO, the Profile stores operator-specific information.
- MNOs must ensure that all keys used within the Profile—such as ISD-P, MNO SD, and any other SSD—are securely generated and remain uncompromised prior to transmission to the eUICC via the MNO OTA Platform.

Guides to maintain the cybersecurity level for eSE products:

- The Java Card System is intended to transform a smart card into a platform capable of executing applications written in a subset of the Java programming language. The intended use of a Java Card platform is to provide a framework for implementing IC independent applications conceived to safely coexist and interact with other applications into a single smart card.
- The card manager shall control the access to card management functions such as the installation, update or deletion of applets. It shall also implement the card issuer's policy on the card.

- For further secure usage guidelines, requirements and recommendations, please consult our UGM on NXP docstore : https://www.docstore.nxp.com/
- Contact for reporting vulnerability information, please refer to the NXP PSIRT (NXP Product Security Incident Response Team) website: https://www.nxp.com/psirt
- EU Vulnerability Database: https://euvd.enisa.europa.eu/

nxp.com