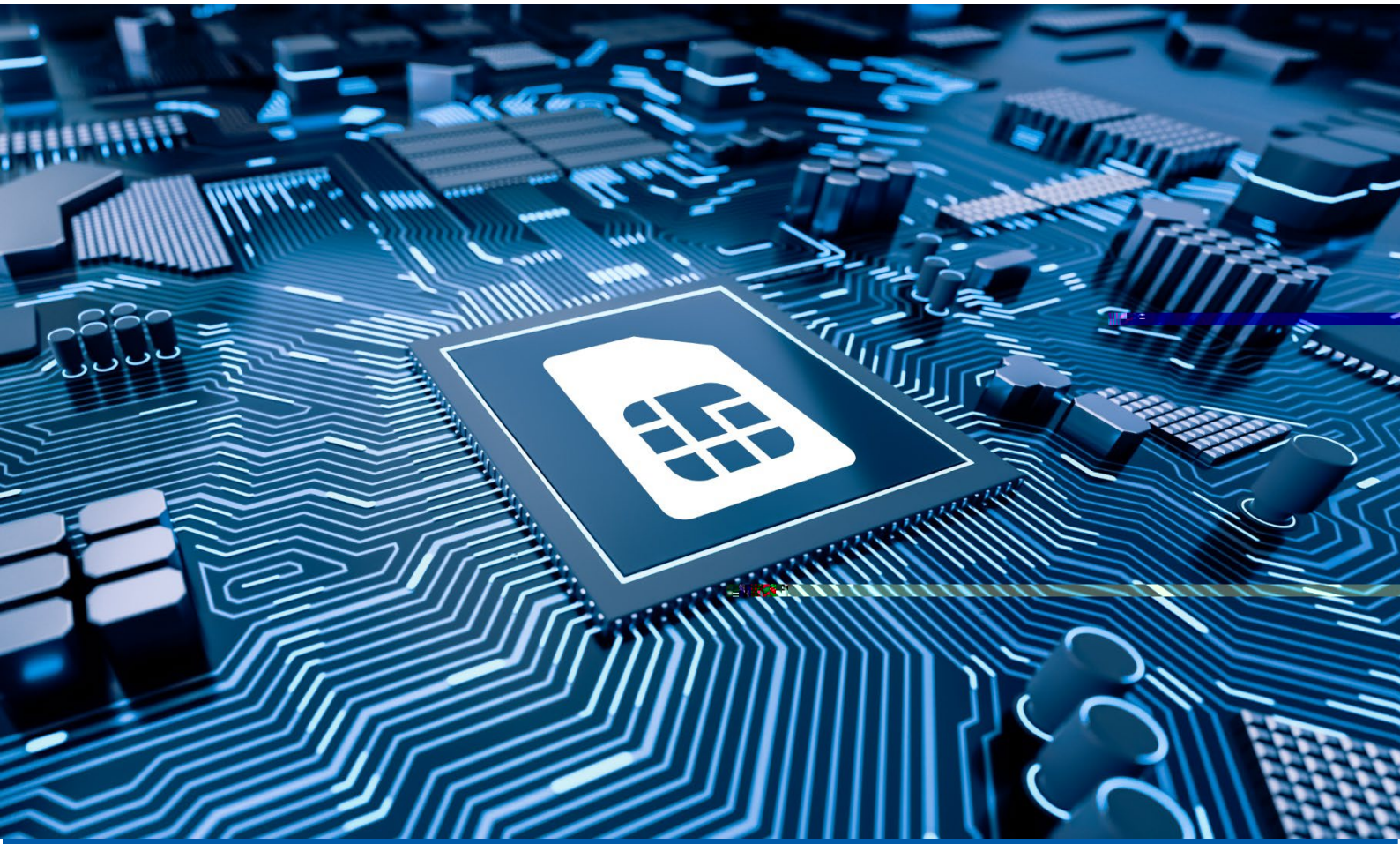
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



Contact

Editors

Acknowledgements

Legal notice

Copyright notice

Abbreviation	Definition

1.1 SECURITY OF ESIMS

-
-
-

1.2 POLICY CONTEXT

2.1 ESIM ECOSYSTEM

Figure 1:

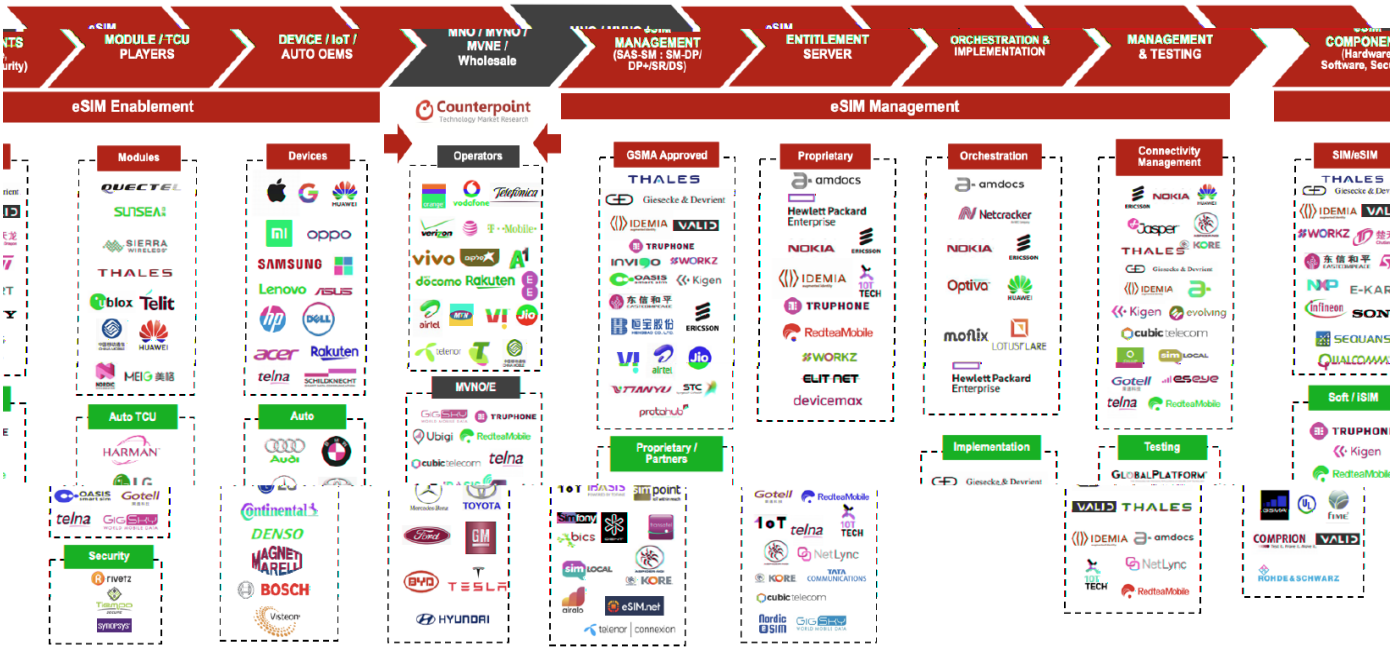


Figure 2:

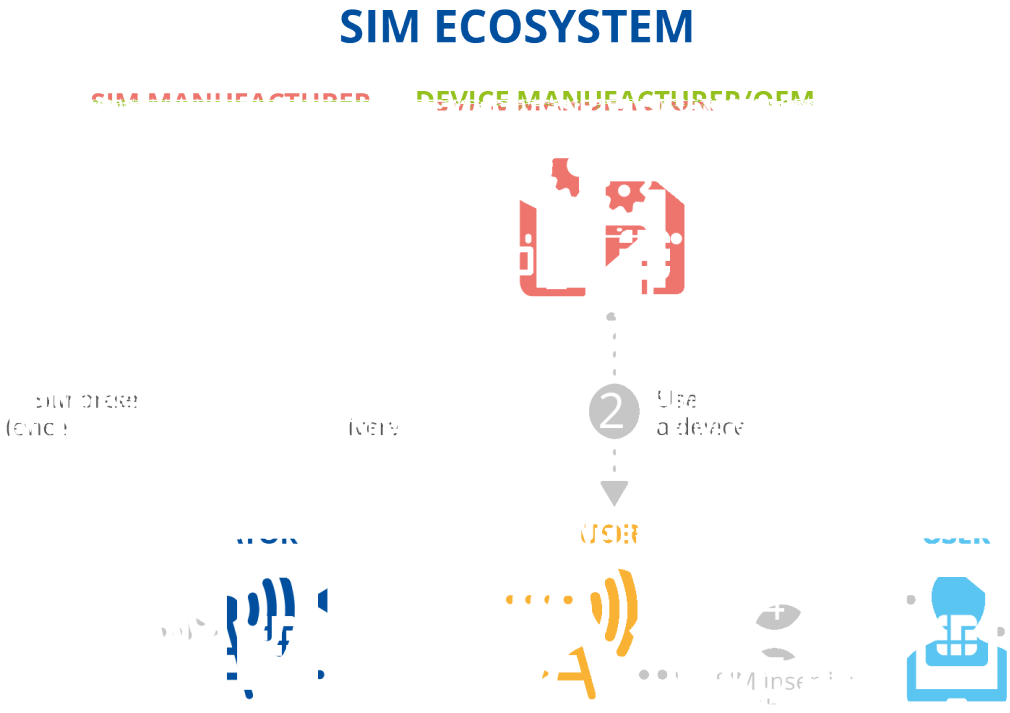


Figure 3:

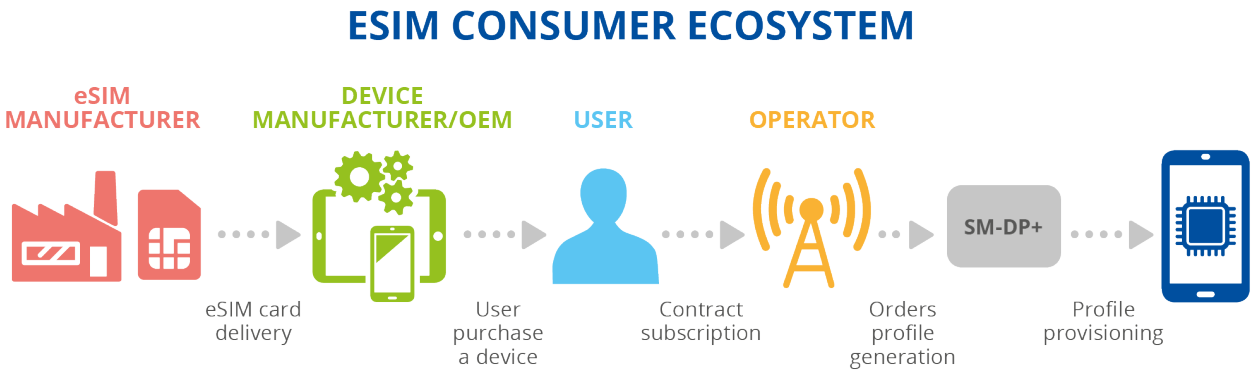
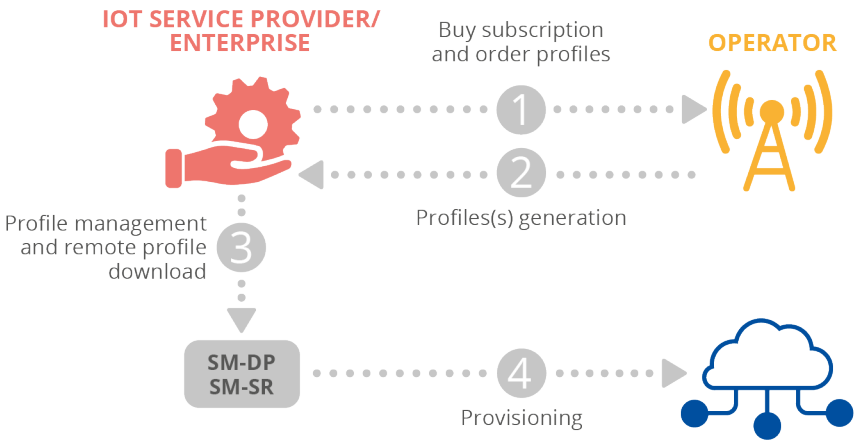


Figure 4:



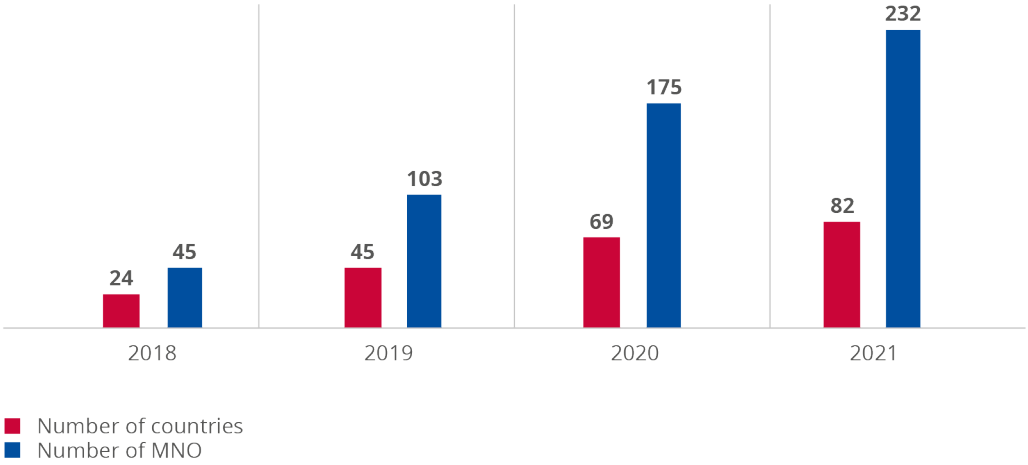
2.2 ESIM BENEFITS AND DRAWBACKS

- **SIM manufacturers**
- **MNOs**
- **Business customers**

- **End users**

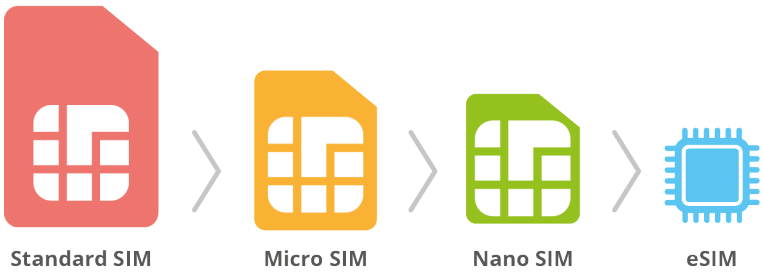
2.3 SIM MARKET AND USAGE IN EUROPE

Figure 5:
Error! Bookmark not defined.



3.1 SIM EVOLUTION

Figure 6:



3.2 ESIM ARCHITECTURE

3.2.1 Consumer solution

- eUICC
- LPA

- eUICC manufacturers

- Consumer device manufacturers

- MNOs/communication service providers

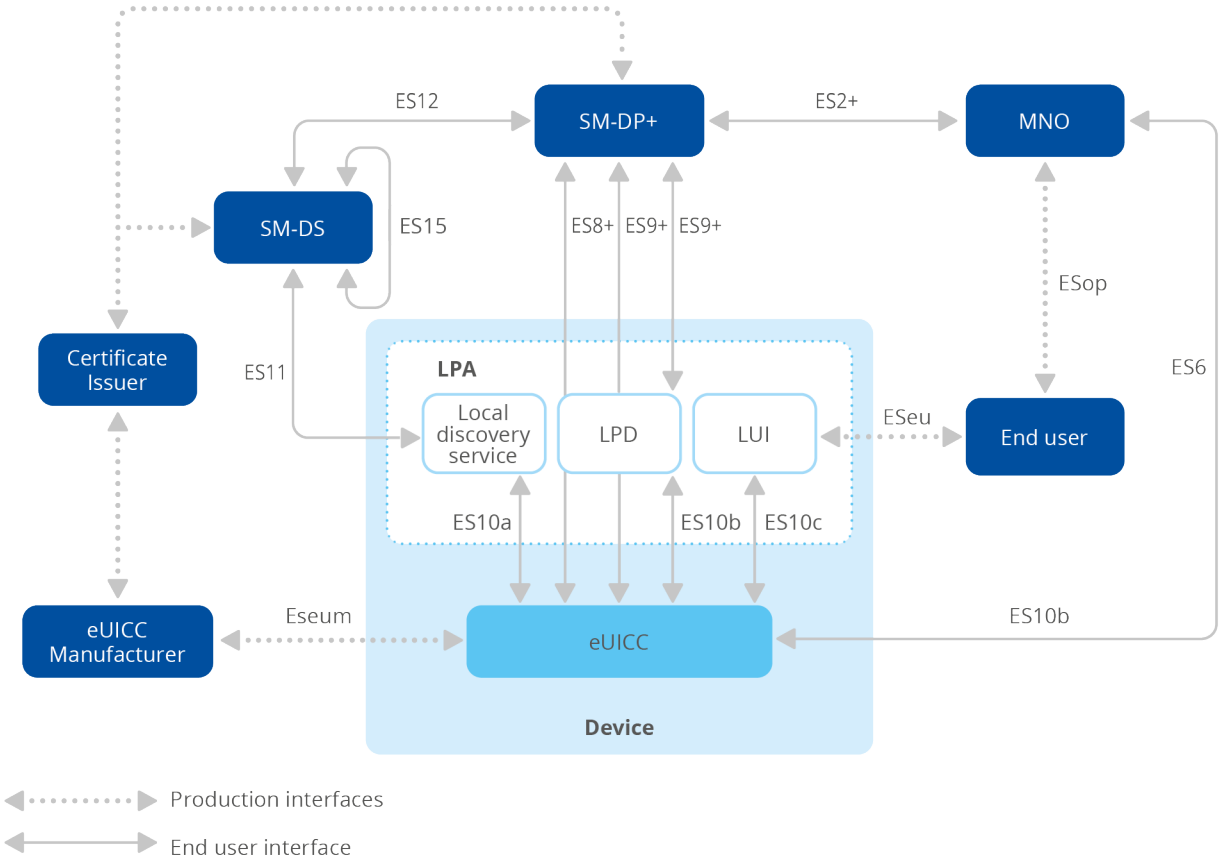
- SM-DP+

- SM-DS

- certificate issuer

- subscriber/end user

Figure 7:



3.2.2 M2M solution

- **eUICC**
- **eUICC manufacturers**

- **M2M device manufacturers**

- **MNOs**

- **SM-DP**
- **SM-SR**
- **Certificate Issuer (CI)**

Figure 8:

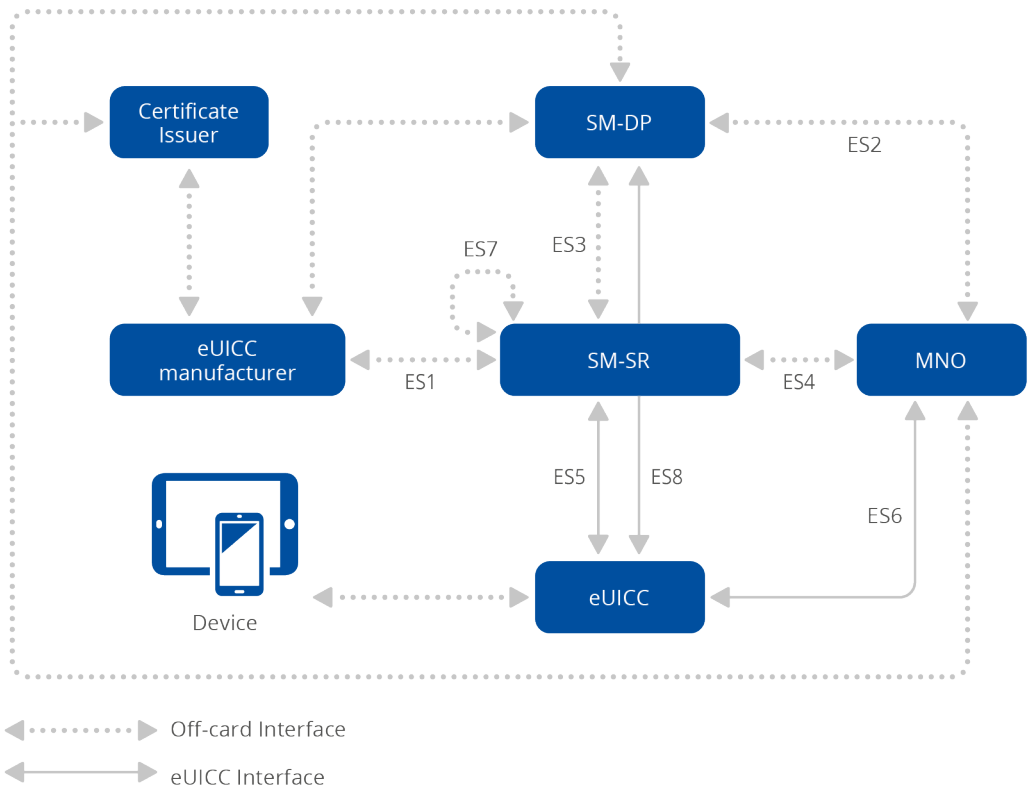


Table 1:

		M2M solution

4.1 Overview of security challenges and risks

Risk 1: eSIM swapping

-
  -
  -
  -
-
  -
  -
-
  -
  -
-
  -
  -
  -

Risk 2: Memory exhaustion

Risk 3: **Undersizing memory**

Risk 4: **Inflated profile**

Risk 5: **Locking profile**

Risk 6: **Protocol attacks**

Risk 7: **Attacks on the MNOs and other entities in the eSIM supply chain**

5.1 GOVERNANCE AND RISK MANAGEMENT

SM1 Risk management and certification

SM2 Security of third-party dependencies

SM3 Security awareness (subscribers)

-
-
-
-

5.2 OPERATIONS MANAGEMENT

SM4 Securing the eSIM provisioning process

-
-
-

5.3 HUMAN RESOURCES SECURITY

SM5 Continuous training and security awareness (personnel)

5.4 SECURITY OF SYSTEMS AND FACILITIES

SM6 ISD-P management

SM7 eUICC's characteristics authentication

SM8 Profile size definition

SM9 Profile locking definition

SM10 Identity and access management

5.5 MAPPING TO THE ENISA GUIDELINE

Table 2:

Risk	Security measure	Security principle	ENISA security objectives

eSIM is a secure evolution of SIM technology.
eSIM is present in international roaming, 5G devices and connected vehicles but is not a consumer mass-market leader.

A. The role of GSMA in eSIM security

Table 3:

Consumer	M2M

-
-

Figure 9:

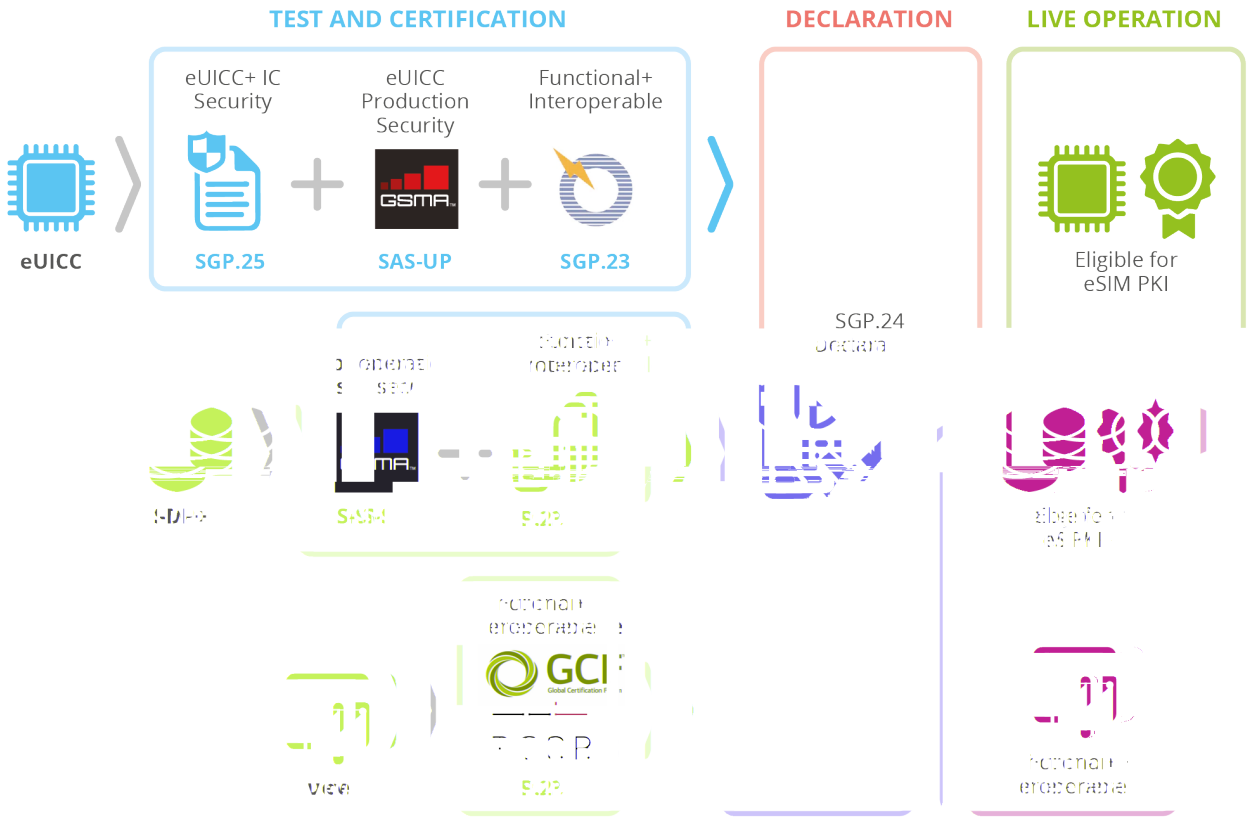

TEST AND CERTIFICATION
DECLARATION
LIVE OPERATION
eUICC+ IC Security
eUICC Production Security
Functional+ Interoperable
eUICC
SGP.25
SAS-UP
SGP.23
Eligible for eSIM PKI
SGP.24

Table 4:

Architecture specifications (includes eSIM Discovery)		
Technical specifications		
Test specifications		
GSMA eID definition and assignment		
Compliance specifications		
Security evaluation of integrated eUICC		
GSMA eUICC SAS		
eUICC for consumer device protection profile		
eUICC PKI certificate policy		
GSMA CI registration criteria		

B. Other initiatives and key organisations

ENISA
European Union Agency for Cybe

Athens Office
Agamemnonos 14, Chalandri 15

enisa.europa.eu