GSMA eSIM Security

ENISA Article13a - Stockholm

06 March 2019

GSMA

THE GSMA WAS FOUNDED IN 1987

12 OFFICES WORLDWIDE:

The GSMA represents the interests of mobile operators worldwide

UNITING NEARLY **800** MOBILE OPERATORS

WITH **300+** COMPANIES in the broader mobile ecosystem

The world's leading mobile industry events, Mobile World Congress and Mobile World Congress Shanghai, together attract

130,000+

people from across the globe each year

The GSMA works to deliver a regulatory environment that creates value for consumers by engaging regularly with:

- MINISTRIES OF TELECOMS
- TELECOMS REGULATORY AUTHORITIES
- INTERNATIONAL & NON-GOVERNMENTAL ORGANISATIONS

CONNECTING **27,000+** Industry Experts

Exclusively for GSMA Members, InfoCentre[2] is your place to connect with a global community of industry experts

GSMA Working Groups provide frameworks and standards in commercial, operational and technical matters that help maintain and advance mobile industry ecosystems

7.5 BILLION+

MOBILE CONNECTIONS WORLDWIDE

Agenda

- eSIM, how it changes UICC management
- eSIM threats
- eSIM current security controls
- GSMA concerns regarding eSIM security controls
- Next steps

eSIM changes the way the industry purchases and uses SIMs

Physical SIM

1.Operators specify and purchase SIM cards. Security features and assurance are managed by operators

Operator

SIM card

SIM Card

Deliver

Authenticate and Authorise

2. Operators use SIMs to identity and authenticate subscriptions

Device

3. SIM data is used to securely identify and authenticate the subscriber

eSIM

1. A non-removable eUICC is specified and procured by the OEM and soldered directly into the device

Operator

4. The profile data on the eSIM is used to authenticate the subscriber, just as for the SIM card

Authenticate and Authorise

eSIM Profile

Download

eSIM

IMEI

3. An eSIM can store multiple profiles, meaning Devices that can connect to two networks simultaneously will have two IMEIs

EID

2. The profile, once downloaded, is securely stored on an eSIM, which is soldered into the device

Device

ICCID

IMSI

eSIM Threats

- Based on the eSIM architecture the threats of attack include:
  - Poisoned ecosystems and supply chains
  - eSIM profile tampering
  - IP based attacks on infrastructure
  - Phishing based on customer journey

SAS Update for eUICC production and profile download

- Understand emerging production models for eUICC & their risks & controls
- Agree & document principles on the types of activity that need SAS certification
- Ensure that all required activities & entities are SAS certified, based on agreed principles
- Advertise this to GSMA members & other stakeholders

SAS Subgroup

GSMA

Remote SIM Provisioning (RSP)

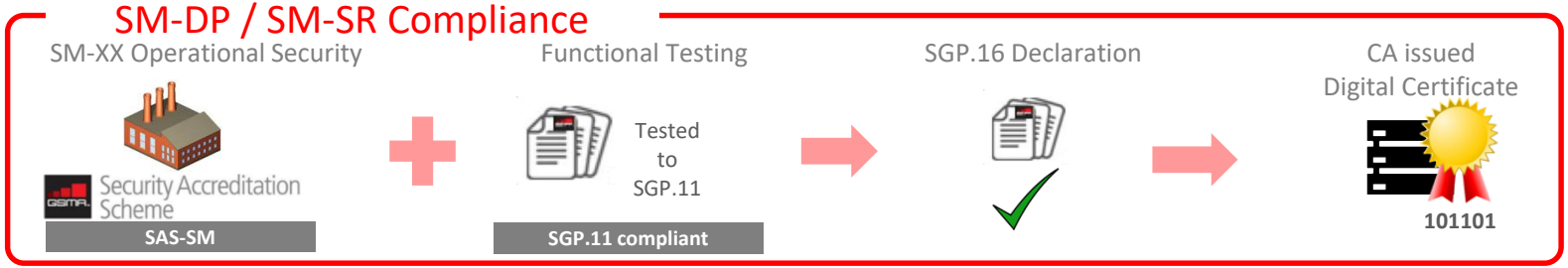
- eSIM provisioning is protected via PKI managed by the GSMA
- At the root of our chain are GSMA PKI certificate issuers
- These entities:
  - Are WebTrust accredited
  - Meet PKI Policies defined by the GSMA
  - Are known to, and in contact with, GSMA

M2M Compliance

SGP.16 Compliance Process

eUICC Compliance

SM-DP / SM-SR Compliance



Consumer Compliance

SGP.24 Compliance Process

eUICC Compliance

eUICC Production Security

Security Accreditation Scheme

SAS-UP

eUICC/IC Security

Bundesamt für Sicherheit in der Informationstechnik

PP-0084-2014
GSMA SGP.25

EAL4+ BSI Certificate

Functional Testing

GlobalPlatform

Certification Programme

SGP.24 Declaration

CA issued Digital Certificate

101101

SM-DP+ / SM-DS Compliance

SM-XX Operational Security

Security Accreditation Scheme

SAS-SM

Functional Testing

Tested to SGP.23

SGP.23 compliant

SGP.24 Declaration

CA issued Digital Certificate

101101

Device/LPA Compliance

Functional Testing

GCF or PTCBB

Certification Programme

SGP.24 Declaration

No PKI certificate is needed for the Device

Providing eUICC security assurance

SGP.25 (PP-0100) + IC based PP-0084

SGP.05 (PP-0087) + IC based PP-0084

Common Criteria

SOG-IS lab and Certification Body

eUICC/IC Security

Bundesamt für Sicherheit in der Informationstechnik

COMMON CRITERIA CERTIFIED EAL4+

Common Criteria EAL4+ compliant

eUICC security assurance

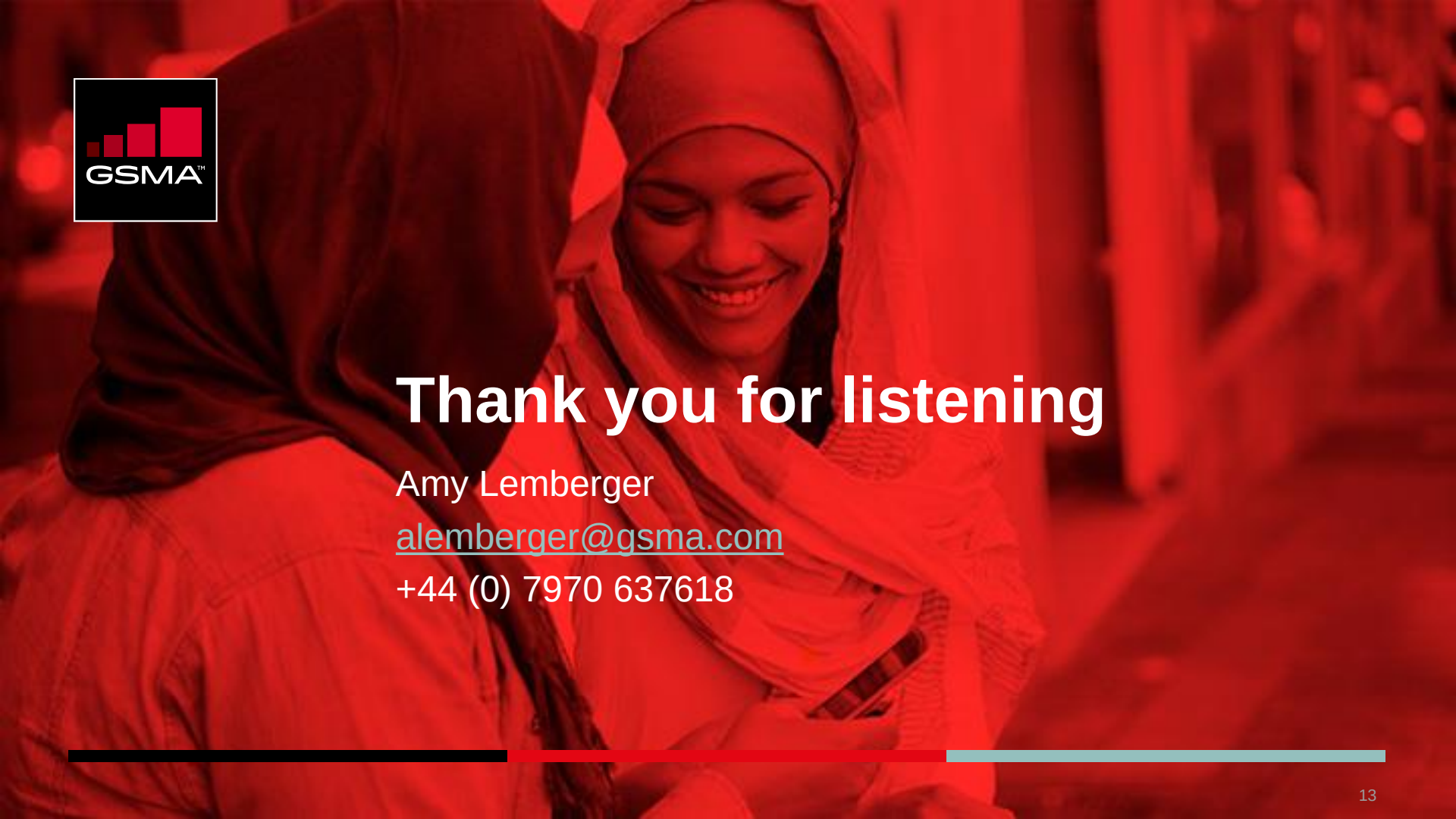
- GSMA created two Common Criteria Protection Profiles (PP-0087 and PP-0100) to provide Security Assurance of the eSIM and M2M functionality
  - In addition to the generic IC based assurance of PP-0084.

- However, GSMA has been unable to get consensus on a timeline to activate a compliance requirement for either of the Common Criteria Protection Profiles.
  - No eSIMs to date have voluntarily certified security assurance referencing the embedded UICC protection profiles

- Common Criteria methodology reported as unfit for commercial eSIM

Next Steps

- Continued absence of Security Assurance for eSIMs is untenable.
- GSMA to extend its SAS scheme to cover eSIM security assurance; possibly as an industry run security assurance scheme under the Cybersecurity Framework
- This scheme should work to achieve a Risk owner based scheme managed by the GSMA, that
  - Addresses current security threats, is
  - Recognised by risk owners globally as a trusted marque for eSIM security assurance, and
  - Provides a fair approach for all stakeholders



Thank you for listening

Amy Lemberger
alemberger@gsma.com
+44 (0) 7970 637618