ITUEvents

ITU Regional Cybersecurity Forum for Europe and CIS

27–28 February 2020
Sofia, Bulgaria

Follow us on twitter: @ITU_EUR & @ITUMoscow
www.itu.int/go/EURCIS_CSForum20

ITU Regional Initiative for Europe on enhancing trust and confidence in the use of ICTs

ITU Regional Initiative for CIS on the development and regulation of infocommunication infrastructure to make cities and human settlements inclusive, safe, and resilient

POLICIES & STRATEGIES | CERTIFICATION FRAMEWORKS | DATA PROTECTION | SECURITY CHALLENGES | 5G, eSIM IoT, AI

Hosted and co-organized by:

REPUBLIC OF BULGARIA
State e-Government Agency

REPUBLIC OF BULGARIA
Ministry of Transport, Information Technology and Communications

ITU

(e)SIMs using eAes

The way towards **quantum-safe 5G**, *tomorrow*

Stiepan A. Kovac, QRCrypto SA, itk.swiss group

Why quantum-safe technology?

- Quantum computers able to crack 95% of existing cryptography standards used in 99.9% of systems are due within this decade, according to leading experts, ranging from Ibm’s lead researcher in 2018, through EPFL quantum physicist and former advisor to Pres. Obama Prof. Pavuna in 2019, to Google’s CEO in 2020.
- Need to migrate cryptographic techniques now!
- We provide a smooth path to migration to QSC

Quantum-resistant SIM cards?

- “We knew SIM cards are very resilient pieces of hardware – but why would you want to make them secure, and who is gonna pay for that ?” is a question we hear sometimes.
- The answer to this “100 Million EUR question”, to paraphrase a distinguished speaker at the eSIM summit last month, is non-trivial, and goes from **consumer to board-level education.**
- Quantum-safe (e)SIMs provide a tech. solution.

On quantum-resistant SIM cards

- eAES-equipped (e)SIMs increase their side-channel attack resistance, an immediate threat to AES encryption, while dramatically increasing the security margin of the same against quantum computer-enabled (and AI-assisted) attacks.
- They bring back the SIM card business to its “golden age”, with the associated price tag(s).
- choice: autonomous car crash or 5-15€ upmark?

Ask your clients and board members to choose!

Future outlook of quantum-safe SIM

- By 2023, IBM will have fulfilled its promise of delivering large-enough quantum computers to crack existing encryption, but will limit its sales to some governments, giving them a strategic advantage in cyberwar and targeted attacks.
- By 2025, Google will make them available to its peers; by 2030, startups will make it affordable.
- To protect connected cars & the like, QR eSIMs will start being massively adopted still this year.

Zoom on a specific case: fin. serv.

- Nowadays, in most of the developing world, people can pay each other using “Mobile money” or similar, serving as their bank.
- Their common denominator: **no** encryption (like most civilian flying systems up until recently).
- This and laws mandating to secure such services in an increasing number of countries will draw massive quantum-safe SIM adoption, **enabling secure mobile banking at a bargain**.

What about you?

- We have started work on providing a quantum-safe profile for 5G integrating eAES, based on an existing related work item at the ITU-T.
- We decided, during the SG-17 Q6 RGM held in Kuala Lumpur last month, to send a LS to 3GPP, asking them to consider this for the next revision of 5G. Meanwhile, we start pilots.
- You could be among the first to adopt this tech.

Let’s keep the conversation going!

For any questions, please reach out to contact@itk.swiss, respectively, contact@qrcrypto.ch or by phone to +41 22 734 59 96.