QRC to secure 5G in health: (authenticated) symmetric encryption everywhere

QRCrypto SA, May 2021, Fribourg, Switzerland

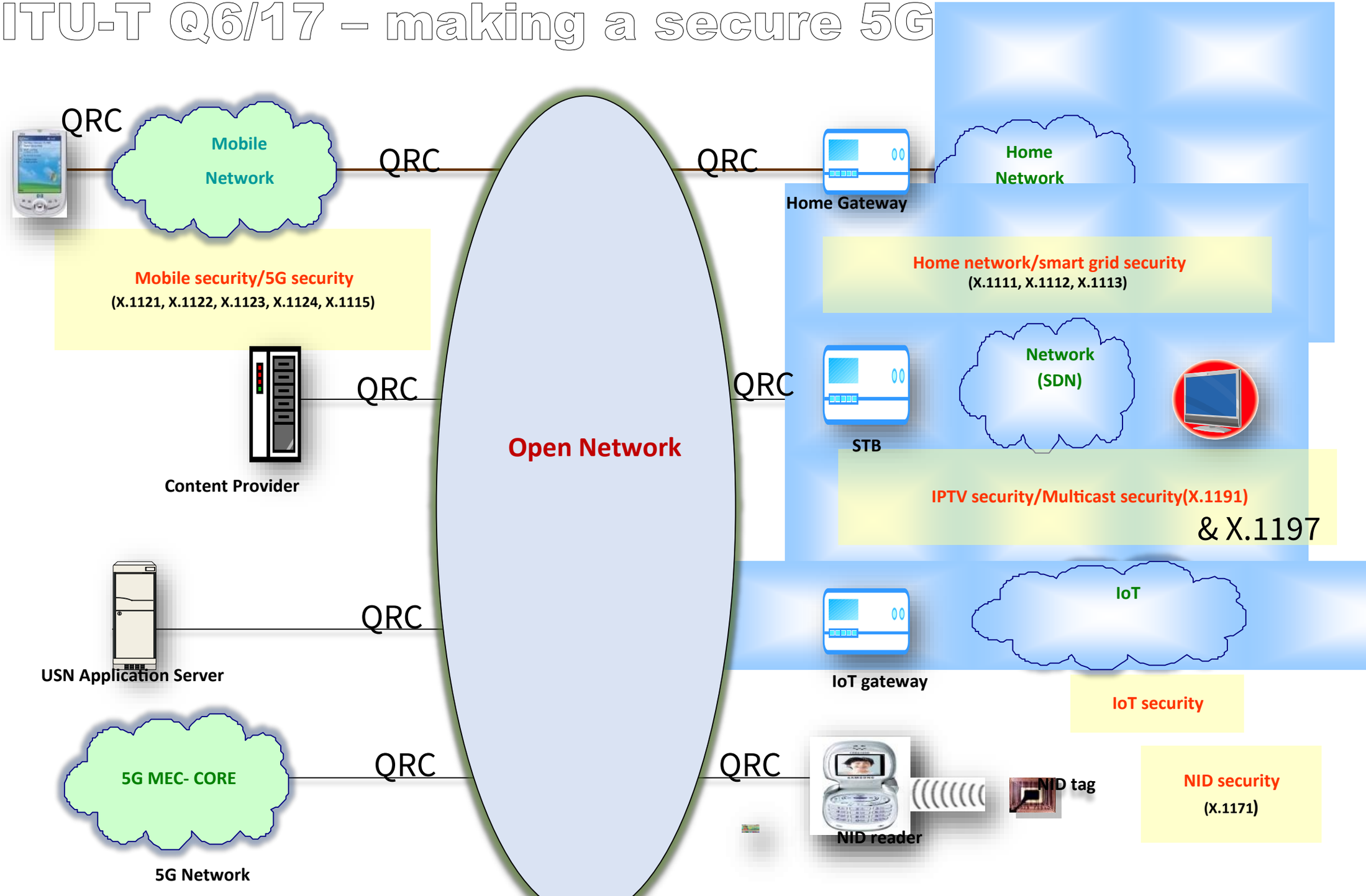
On the need for quantum-resistant e-health systems

- Generalized testing for infectious diseases provides an opportunity for generalized DNA profiling of the full population, as the biological data collection methods are the same. However :
- Given the trans-generational nature of DNA data, it is the civilian data that needs most protection.
- → Technically, it must be safeguarded with the **strongest possible encryption** available.

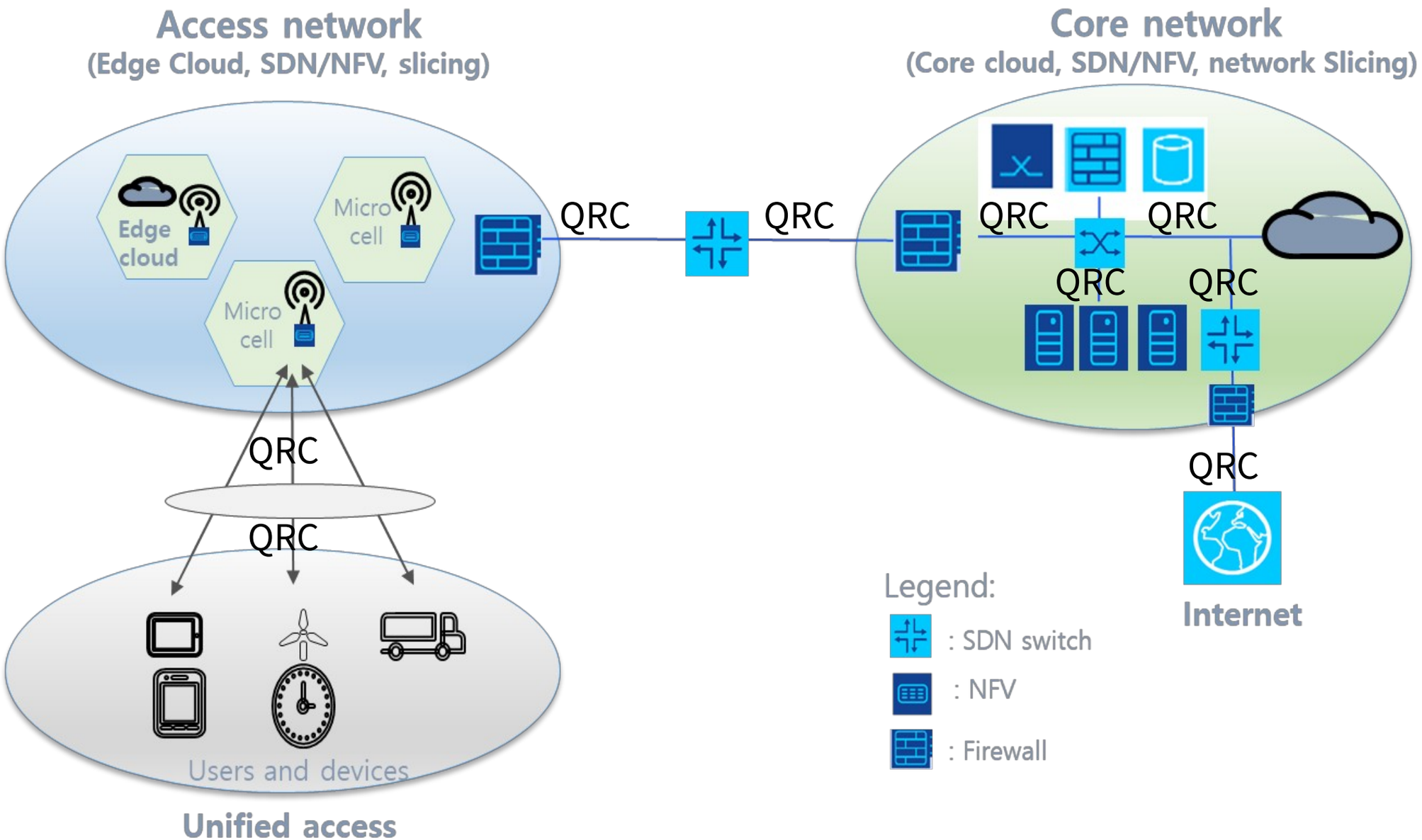
The role of QRC in strong encryption for e-health

- QRC's patented Quantum-resistant SIM, integrating an enhanced AES being standardized at ISO SC27 WG2 enabling key sizes up to 512 bits, and now a good practice in ITU-T X.1811 on quantum-safe 5G, was made to stand the test of time, against both known and unknown attacks, such as those that strong AI in combination with quantum computers may (and actually being to) enable, likewise immediate side-channel SIM attacks.
- EAES® can easily be deployed in 5G systems for closed user groups with the encryption key embedded in SIMs. For FIPS compliance, classical AES-256 can also be used, while still providing some quantum resistance. For best results, our US patent-pending tech enables combining both.
- E-health and especially, DNA data, warrants special protection. For that, 512-bit keys should be used here.

ITU-T Q6/17 – making a secure 5G



5G security Guideline X.1811 – now approved!



Our proposal to European hospitals

- Try our quantum-resistant solution for two months, for free (you provide the infrastructure, we provide the software)
- After the hopefully successful completion of the trial, deploy it to all the e-health infrastructure nationwide.
- By the time of 5G nationwide deployment, provide (e)SIM-based solutions to end users / customers, allowing home e-care, compliant with GDPR / LPD and other national laws. Note: Could be fast-tracked due to COVID-19.

Give me the figures!

- For the server software, we provide licensing per end user / device (in the case of IoT), including full support, on a yearly basis.
- Prices for the medical sector are of 33 CHF per user / device.

Thank you!

- For any questions, please write us to contact[at]qrcrypto [dot]ch, call us or our senior strategic advisor Professor Davor Pavuna, at the following numbers:
- +41 26 466 1084
- +41 79 554 1811
- Our group’s postal address for formal communication: QRCrypto SA, itk.swiss SA group, CH-1700 Fribourg .
- Our free up to 20 persons e-meeting platform: Aaameet.in