Redefining Security

Use Case: Telecom Service Provider

Improving 5G security

User authentication relying on QRNG

Customer: SK Telecom

Industry: Telecom Service Provider

Country: South Korea

Business need	Solution	Results
Strengthen the mobile authentication procedure to restrict unauthorised access to devices	Quantis QRNG Appliance connected to SK Telecom 5G Core Network (Authentication Center)	Reinforcement of mobile authentication and encryption security thanks to QRNG

Business need

5G is set to play a key role in critical applications' such as smart cities and factories, connected vehicles and hospitals. While 2G and 3G have had major security breaches, 5G requires the highest level of security available to resist existing and emerging threats, such as quantum computers' unprecedented computational power.

More specifically, the increasing number of IoT devices connected to mobile networks requires to strengthen the user equipment authentication procedure to restrict unauthorised access to devices.

The authentication procedure specified in the 5G standard uses an authentication vector of 4 parameters: RAND, AUTN, XRES and KASME. The main variable parameter of this vector is obviously the random number RAND which provides the seed for other key generation procedures used for authentication and ciphering.

The subscriber authentication process is the first and essential step in verifying a mobile device user before he/she is granted access to any voice and video data service, SMS, etc. Security in this process is crucial since the leakage of an authentication key value can lead to serious consequences such as eavesdropping and hacking.

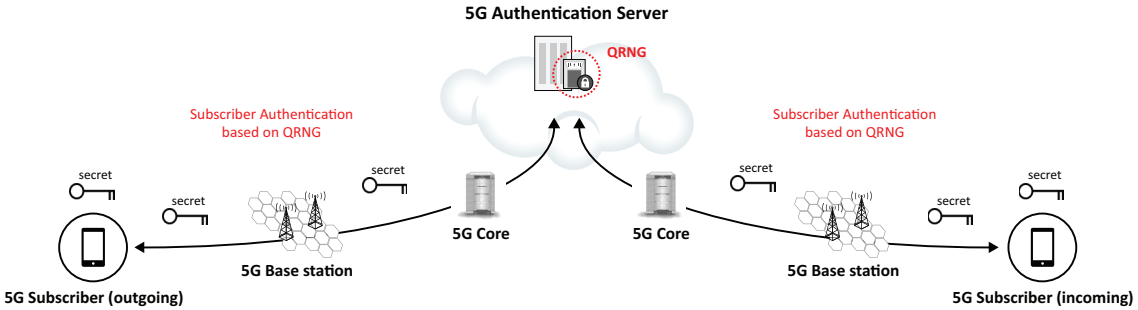
Solution

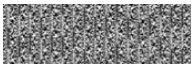
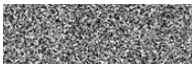
SK Telecom identified that the true randomness of the key used during the mobile authentication procedure was essential to achieve a high security level.

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@idquantique.com
www.idquantique.com

The use of Pseudo Random Number Generator (PRNG) or even True Random Number Generator (TRNG) is not enough to resist to strong computational pattern analysis. A repeating pattern can be observed over time after enough queries and samples.

The chosen solution was to replace the PRNG by a Quantum Random Number Generator (QRNG) which provides instantaneous true randomness and higher entropy. ID Quantique's Quantis Appliance was connected to the Home Subscriber Server providing the Authentication Vector to the Network and User Equipment (5G Mobile). Two Quantis Appliances provide redundancy and a random bit rate sufficient to seed entropy to the authentication servers.



Items	Pseudo Random Number Generator (PRNG)		Quantum Random Number Generator (QRNG)	
Algorithm	Repeating pattern, subject to hacking		No repeating pattern, quantum-safe	
Time of pattern analysis	2019 (classical computer)	Near future (Quantum computer)	2019 (classical computer)	Near future (Quantum computer)
	several years	Several days~months	Impossible to analyse pattern	
Entropy*				

* Entropy: A numerical representation of the degree of certainty of the probability distribution. Physics refers to the degree to which the state is dispersed.

The Quantis Appliance is purpose-built for environments where high availability is essential. Ease of implementation means it can be added or removed from a network without impacting any other devices, allowing service providers to offer QRNG as a service.

The Quantis Appliance is trusted and certified by leading commercial and government entities such as the French ANSSI and Swiss METAS, and is compliant with NIST testing requirements. It is resilient and designed for demanding network environment while supporting multiple operating platforms. IDQ's QRNG is a device that constantly generates quantum random numbers, which are used as the foundation of strong keys that are not biased and cannot be predicted.

Results

By adding Quantum Random Number Generation (QRNG) to its mobile network authentication server, SK Telecom has reinforced its authentication and encryption security. SK Telecom has developed a future-proof solution able to securely connect a high number of 5G devices for IoT applications.

Park Jung-ho, President and CEO of SK Telecom, said he is *"determined to provide the highest level of network security and stability at all times. SK Telecom will continue to work closely with companies across the globe to secure the best technologies."*

SK Telecom plans to expand the application of quantum cryptography technologies such as QRNG and Quantum Key Distribution by stages to further enhance the safety and security of its mobile networks.

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@idquantique.com
www.idquantique.com