Press release

End-to-end encryption technology for governments and companies

SIM card hacking case: how to protect mobile communications

Zurich, 25 February 2015 – For those concerned with the SIM card hacking case reported these days in the media, there are several solutions on the market to protect all kind of communications made with a smartphone in a mobile network. Qnective from Switzerland offers provider independent business and government solutions with a double-layer protection technology that uses end-to-end encryption. The keys are ephemeral for every session and destroyed after their usage – thus, providing forward secrecy in all communications. The solution is available for closed user groups only, being large enterprises or government organizations.

The SIM card encryption keys that have allegedly been stolen from Gemalto serve as identification of the user in the mobile network. Like that, smartphone users with a SIM card are able to use services provided by their local telephone provider. The main purpose of this key is to prevent fraud, so that no one that is not paying for services is using the network illegally. The encryption used in public networks gives some protection for the content of calls, text messages and personal data. If the SIM card keys are openly available, it is possible to impersonate the user in the network and even access session and communication data – except if one is using a secure application that has its own, independent protection and does not rely on the network encryption. This is the reason why end-to-end encryption between smartphones is one of the most reliable and secure communication forms.

Qnective: end-to-end encryption solutions for governments and enterprises

One of the providers for smartphone communication security is the Swiss telecommunications company Qnective. Their product lines are suitable for governmental and military organizations as well as for enterprises. Qtalk Defense is a highly encrypted communication application, used by police forces, ministries and other governmental entities worldwide. Using a standard smartphone, the solution encrypts voice calls, text messages and any file and phone book information end-to-end and with a double encryption layer. For enterprises that want to protect their Intellectual Property from industrial espionage, Qtalk Secure provides a maximum of security combined with a flexible architecture and an easy-to-use interface. The solution can be hosted on customer premises entirely.

About Qnective

Qnective (www.qnective.com) was founded in Switzerland in 2007. The company is headquartered in Zurich. Qnective offers services for secure communications, developing individually designed platforms for governments, military organisations and large-scale enterprises. Qnective delivers tailor-made solutions covering the design, development and deployment of secure communication projects around the world. The company maintains its own, proprietary, encryption communications platform, „made in Switzerland“, for secure telephony and data transmission over wireless networks.

For further information, please contact
Qnective Media Relations
Marlène Frey
Thurgauerstrasse 54, 8050 Zürich
media@qnective.com
+41 (0)79 245 24 10