ID Quantique and CryptoNext Security announce a partnership to deliver the next generation of Quantum-Safe Messaging Solution

- Instant Messaging Applications are largely deployed amongst individual smartphones users.
- This raises the need for a higher level of security today, especially for sensitive communications in enterprises and organizations.
- Quantum Random Number Generation (QRNG) and Post-Quantum Cryptography (PQC) are essential technologies to face the challenge.
- ID Quantique and CryptoNext Security, global technology and market leaders announce their partnership to offer an integrated quantum safe messaging solution

June 30th, 2022 – Geneva based ID Quantique SA (IDQ), a global leader in Quantum Cybersecurity Solutions and Paris-based CryptoNext Security SAS (CryptoNext), a pioneer and leader in Post-Quantum Cryptography (PQC) today announce their partnership to offer an effective and long-term Quantum-Safe Communication Solution for mobile phone users.

While mobile communications are ever more integrated in today's hyper-connected world where flows of data are transmitted continuously, the development of quantum computers has seen a recent acceleration thanks to large investments.

Their development will allow to break existing cryptography in a near future, stressing the need for a new approach to cybersecurity and new solutions in this forthcoming era. It already is an absolute requirement in order to protect long-life high-value data against the "harvest now, decrypt later" attacks. This requirement not to wait is made by almost all national security agencies including the NSA and the National Institute of Standards and Technologies (NIST) in the US, the ANSSI in France and the BSI in Germany, to name a few.

Solutions able to combine and mutually leverage the essential technologies known as Quantum Random Number Generation (QRNG) and Post-Quantum Cryptography (PQC) represent a major step and a clear response to build next generation secured communications in this post-quantum era.

Following a successful test project at NATO, a major global defense organization, IDQ and CryptoNext have joined efforts to design, sell and support customers, integrators and specialized solutions vendors, with next-generation quantum secured communication solutions, through the effective implementation of their respective world-leading QRNG and PQC technologies.

The solution is a quantum-safe messaging application for mobile communications. It combines Cryptonext's Quantum-Safe Messaging Application Plugin (C-QS-MS) and Quantum Safe Library (C-QSL) with automated detection of ID Quantique's QRNG Microchip embedded in some brands of smartphones, which provide the most reliable source of entropy for any cryptographic process. The

result is a full end-to-end text, file exchange, call and video call Quantum-Safe messaging solution. The application is transparent to the user and comes with specific group management features to efficiently manage the security level of specific groups.

The solution aims at enabling governments, enterprises and organizations whether public or private to manage their sensitive communications for specific groups of people such as executive teams and/or specific projects

Mr Grégoire Ribordy (IDQ) has declared: " **We are delighted to team with CryptoNext Security, a recognized leader in Post-Quantum Cryptography to leverage our market leading QRNG chip integrated into smart phones and offer our customers the most secure messaging application."**

Mr Florent Grosmaitre (CEO CryptoNext Security) has declared "**It is great honor for us to be recognized by and team up with IDQ, a clear market leader in QRNG technologies with proven track record in deployment and supporting customers with quantum-safe crypto solutions."**

About ID Quantique

Founded in 2001 as a spin-off of the Group of Applied Physics of the University of Geneva, ID Quantique is the world leader in quantum-safe crypto solutions, designed to protect data for the future. The company provides quantum-safe network encryption, secure quantum key generation and Quantum Key Distribution solutions and services to the financial industry, enterprises and government organizations globally. IDQ's quantum random number generator has been validated according to global standards and independent agencies, and is the reference in highly regulated and mission critical industries – such as security, encryption, critical infrastructure and IoT – where trust is paramount. Additionally, IDQ is a leading provider of optical instrumentation products, most notably photon counters and related electronics. The company's innovative photonic solutions are used in both commercial and research applications.

IDQ's products are used by government, enterprise and academic customers in more than 60 countries and on every continent. IDQ is proud of its independence and neutrality, and believes in establishing long-term and trusted relationships with its customers and partners. For more information, please visit www.idquantique.com.

About CryptoNext Security

CryptoNext Security, founded in 2019 following 20years+ academic research with HQ based in Paris, is a software vendor specialized in quantum resistant cryptography. CryptoNext offers its quantum safe software suite of Tools and Applications, including its world recognized quantum safe library that includes all NIST Quantum algorithms finalists, for enterprise end-users and integrators to help their migration to the post-quantum era security.
CryptoNext Security has been nominated among 5 for post-quantum cryptography leadership by Gartner and awarded Future 40 most promising startup in French competition. For more information, see www.cryptonext-security.com

Contacts
For ID Quantique : Catherine Simondi, VP
Marketing Phone : +41 22 301 83 71
Email:Catherine.simondi@idquantique.com

For CryptoNext Security : Christian d'Orival,
CRO Phone: Email: