European Parliament

Brussels, 12 March 2024

Dear Commissioner Breton,
Dear Mr. Roberto Viola,
Dear Mr. Juhan Lepassaar,
Dear Ms. Anu Talus,
Dear Mr. Leonardo Cervera Navas,

In the coming ten years, there is a chance that a quantum computer will be built that will break public key encryption. In a recent report, experts tried to estimate the chances of a quantum computer being developed that is able to break commonly used RSA-2048 keys within 24 hours. Pessimistic estimates consider there is a 33% chance that such a computer will be built in the coming fifteen years, and the optimistic estimates even consider an 11% chance that such a computer will be developed in the coming five years.

A full transition to another cryptographic algorithm in the past took more than a decade. For example, NIST standardised the hashing algorithm SHA2 in 2002. The RAND Corporation reports that by 2016, 35% of all websites were still using an older standard. And whereas NIST adopted the symmetrical algorithm AES as a standard in 2001, the average adoption year for surveyed organisations was 2014. Meanwhile, these transitions were relatively simple, confined to a relatively small domain, whereas replacing current public key algorithms would affect a wide range of technological domains, from servers, to banking cards, to internet-of-things devices, etc.

Fortunately, NIST has already in 2022 determined which PQC-algorithms will be used for inclusion in a standard: for public key encryption it chose CRYSTALS-Kyber and for digital signatures it chose CRYSTALS-Dilithium, FALCON and SPHINCS+.

The Commission, ENISA, EDPS and EDPB should play an important role in spurring this transition now, by explaining in joint guidance what taking “appropriate” security measures under the different regulatory regimes (GDPR, NIS2, etc.) means, in the view of the development of quantum computers.

To be precise they could clarify that this means that organisations must start preparing for a full transition of their encryption suites as soon as possible, inter alia by:

- making an inventory of algorithms existent in their organisational infrastructure;
- reviewing the extent to which new cryptographic libraries can be used as a drop-in for current libraries in their infrastructure;
- ensuring that hybrid encryption, e.g. using classical as well as PQC-algorithms, is deployed where possible; and
- start with a phased deployment as soon as NIST has adopted relevant standards.

This is especially urgent for essential and important entities in sectors of high criticality that fall under the scope of the NIS2, which will enter into force in October 2024.

Sincerely,
Bart Groothuis
Miriam Lexmann
Dragos Tudorache
Morten Løkkegaard
Patrick Breyer
Christophe Grudler
Evžen Tošenovský
Malik Azmani
Erik Poulson
Kim van Sparrentak
Alin Mituta
Miapetra Kumpula-Natri
Fabio Massimo Castaldo
Ivars Ijabs
Caroline Nagtegaal
Riho Terras
Asger Christensen
Markéta Gregorová
Karen Melchior
Jan-Christoph Oetjen