From: Hemmert, Tobias <tobias.hemmert@bsi.bund.de> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum@list.nist.gov
Subject: [pqc-forum] BSI publication on quantum-safe cryptography
Date: Thursday, May 19, 2022 06:03:06 AM ET

Dear All

I would like to highlight the publication "Quantum-safe cryptography - fundamentals, current developments and recommendations" from the German Federal Office for Information Security (BSI). An English version is now available here:

https://gcc02.safelinks.protection.outlook.com/?
url=https%3A%2F%2Fwww.bsi.bund.de%2FSharedDocs%2FDownloads%2FEN%2FBSI%2FPublications%
2FBrochure%2Fquantum-safe-cryptography.html%3Fnn%3D433196&data=05%7C01%7Cyi-
kai.liu%40nist.gov%7C04d4ace24e8448993f7e08da397ec3c4%7C2ab5d82fd8fa4797a93e054655c61
dec%7C1%7C0%7C637885513864943629%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoi
V2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=gpTFlgC%2FaxubDpfFdC
dZ3iD4uFpP40g7hPSG9%2BIQI0I%3D&reserved=0

The publication provides background information on quantum technologies and their impact on cryptography. It also contains recommendations from BSI on the migration to quantum-safe cryptography, in particular on post-quantum cryptography and QKD.

We hope this document is of interest to many of you.

Kind regards
Tobias (on behalf of the authors)

--