DIGITALEUROPE

6 MARCH 2020

DIGITALEUROPE comments to "Opinions on the Implementing of Testing and Certification of Commercial Cryptography"

Executive Summary.

DIGITALEUROPE greatly appreciates the opportunity to comment on "**Opinions on the Implementing of the Testing and Certification of Commercial Cryptography**" (herewith the "**Opinions"**) released by the State Administration for Market Regulation (SAMR), for public comment on 20 February 2020.

Last year we submitted a response to the consultation on the second draft **Cryptography Law** put forward by to the Office of State Commercial Cryptography Administration (OSSCA). The issues and concerns raised on that occasion still hold true today, and we would like to reiterate them.

- Modern Information and Communication Technology (ICT) products include elements of encryption (not as core function) for cybersecurity purposes. Most governments around the world do not regulate the importation or domestic use of cryptographic features in mass-market products. Regulating market access because of the use of commercial encryption functionalities translates to restricting the Chinese market and impinging on competition, trade flows and innovation.
- According to the World Semiconductor Council (WSC) principles for commercial cryptographic technologies in mass marketed ICT products, the regulation of commercial encryption should be limited, and encryption technology mandates prohibited, acknowledging the widespread use of encryption and limited value in regulating the commercial market. The approach outlined in the SAMR Opinions may not be consistent to the obligations and commitments taken the Government of China, along with the other members of the Government and Authorities Meeting on Semiconductors (GAMS), under the WSC's Encryption principles. [1]

[1] Joint Statement of the 17th Meeting of the World Semiconductor Council (WSC), 23 May, 2013 (Lisbon, Portugal), as endorsed by member country governments in Government/Authorities Meeting on Semiconductors, September 26, 2013 (Jeju, Korea).

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Recommendations:

Further assess the scope.

The scope of the current proposal for a testing and certification framework is potentially very broad. If authentication related functionality is included, this would generate massive volumes of products undergoing testing, since almost all ICT products nowadays contain minimal elements of encryption used for integrity or authentication. More alignment with World Trade Organisation (WTO) and WSC/GAMS commitments is needed. We recommend to:

- Further assess the scope and the organizational structure supporting the testing and certification framework.
- Set up an additional consultation with the private sector to obtain detailed comments.

Preserve and apply the core function concept to all cryptography products and services.

For the past two decades industry has relied upon the concept of Core Function Concept for market access in China since the Commercial Encryption Management Regulation was issued and then clarified (1999-2000). The scope of management has limited to “specialized hardware and software for which encrypting and decoding operations are core functions”.[2] Today products with non-core encryption features are commonplace, therefore **preserving and apply the core function concept to all commercial cryptography is essential to avoid market access barriers for many products and services.**

This approach should be applied to all commercial cryptography products and services, including “Commercial cryptography-based products”, “Commercial cryptography-based services”, commercial cryptography used in “mass consumer products,” and commercial cryptography more generally as addressed under the Cryptography Law (2020), in order to avoid certification restrictions or regulations for commercial products with encryption as a secondary feature.

Adequate encryption regulations are crucial to ensure a free flow of innovative products and technologies into PRC. The Core Function Concept and the mass market exclusion point to the arrangement where products and solutions can be imported without restrictions or licenses. We hope this intent will be reinforced in the more detailed implementation directives.

[2] Announcement issued March 2000 by the People’s Republic of China State Encryption Management Commission General Office (SEMC)

Free flow of the most innovative technologies into China would be negatively impacted by the institution of very broad certification requirements, even if these requirements are voluntary.

Rely on international standards and avoid duplication in implementation requirements.

International standards in the area of assessment and certification, such as ISO/IEC 19790 or ISO/IEC 15408, created with the participation of PRC experts, represent a solid baseline for a broadly applicable certification framework, with the understanding that it is not required for general purpose consumer environments. International standards and experience would enable non-discriminatory transparent testing and certification frameworks, as well as the development of certification-related processes, with industry involvement, to overcome fragmented approaches.

- We recommend that international standards and practices related to cryptography[3] are adopted and that existing relevant guides or recommendations issued by international standards bodies are used for testing and certification.
- We encourage also the acceptance of testing and certification performed by accredited foreign labs in accordance with globally recognized standards as equivalent to that of licensed local labs to avoid unnecessary duplication.
- We suggest also additional consultation with the private sector and industry on the structure and governance of testing and certification bodies.

Further clarify the definition and scope of certification regulatory requirements applicable to “commercial encryption.”

The 2020 Draft Cryptography Law has the merit of separating “commercial cryptography,” from “core” and “common” cryptography. Article 28 clarifies that “Commercial cryptography used in mass consumer products is not subject to the import licensing system or export control.

[3] Among relevant standards we can list ISO/IEC 18033 (Encryption Algorithms) and ISO/IEC 29192 (Lightweight Cryptography)

This approach – that we welcomed in our letter to OSSCA in September 2019 – should be reflected also in the SAMR Opinions, distinguishing between encryption as a core or secondary function.

- Certification should be strictly limited to cases where encryption is the core function, rather than a subsidiary feature of the product or one of its components.
- Commercial-off-the-shelf products used by business enterprises for commercial purposes, commercial products used internally and not for commercial sale, and all other commercial products and technologies with elements of cryptography that are not core function should be completely exempt.

Ensure that IP, confidential information and privacy rights are protected during supervision and enforcement.

Non-discriminatory transparent testing and certification frameworks, as well as the development of certification-related processes, should include proper mechanisms to safeguard confidentiality and intellectual property rights.

Conclusion.

We welcome the opportunity to comment the SAMR Opinions and we stand ready to provide further input on the implementation of the Cryptography Law.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Senior Policy Manager for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25

Martin Bell

Privacy and Cybersecurity Policy Officer

martin.bell@digitaleurope.org / +32 492 58 12 80

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Airbus, Amazon, AMD, Apple, Arçelik, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Epson, Ericsson, Facebook, Fujitsu, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, MasterCard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Qualcomm, Red Hat, Ricoh Europe PLC, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Xerox.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK