European Semiconductor Industry Association

ESIA's comments on China's *Opinions on the Implementation of Commercial Cryptography Testing and Certification (Draft for Comments)*

Brussels, 6 March 2020

I. Introduction

The European Semiconductor Industry Association (ESIA) is pleased to provide the below set of comments and recommendations on China's *Opinions on the Implementation of Commercial Cryptography Testing and Certification - Draft for Comments* (hereinafter "the Opinions").

II. General comments

ESIA is grateful for the opportunity to provide inputs to the ongoing public consultation on the above Opinions. The provisions in their current form contain several elements of vagueness, which should be clarified. In particular, the roles and responsibilities of the various bodies mentioned in the Opinions should be further defined, and the nature of the cryptographic products subject to certification should be further clarified. In addition, the Opinions should be made consistent with other public notices and regulations, as well as existing commitments made by China under international agreements. Similarly, the World Semiconductor Council (WSC) principles for commercial cryptographic technologies in mass marketed ICT products limit the regulation of such commercial encryption and prohibit encryption technology mandates.

Finally, ESIA believes that the scope of the certification needs to be assessed. The requirements for a testing and certification framework are potentially very broad. If authentication related functionality is included, even for mass market products excluded from licensing, it will result in massive volumes of products undergoing testing, since all ICT products today contain elements of encryption used for integrity or authentication, as a secondary function (non-core). More alignment with

World Trade Organisation (WTO) and WSC/GAMS commitments is needed.[1] **ESIA recommends to:**

- **Further assess the scope and the organizational structure supporting the testing and certification framework,**
- **Explicitly exclude mass market products from certification and testing requirements,**
- **Explicitly eliminate products where according to SEMC (State Encryption Management Commission) March 2000 clarification encryption is not a core function from any mandatory testing and certification; Reflect this in the Opinions and any other implementing regulation[2] and**
- **Set up an additional consultation with the private sector to obtain detailed comments**

Appropriate encryption regulations that are in line with international best practices are crucial to ensure a free flow of innovative products and technologies into PRC. The Core Function Test and the mass market exclusion, point to the arrangement where products and solutions can be imported without restrictions or licenses. ESIA's hope is that this intent will be reinforced in the more detailed implementation directives that do not include mandatory testing and certification for these categories of products.

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.

III. Article-by-article comments:

Article I

- Based on this article the State Administration for Market Regulation (SAMR) and the State Cryptography Administration (SCA) *"shall, in line with their respective duties, strengthen the organisation, implementation, supervision, administration and results acceptance relating to testing and certification, and*

[1] WTO (TBT Agreement Article 4.1 and Annex 3, Paragraph F) and the World Semiconductor Council (WSC) Encryption Principles, adopted by China, that "strongly encourage the use of global or international standards, including normative algorithms, as essential to avoid fracturing the global digital infrastructure and creating unnecessary obstacles to trade." The WSC Encryption Principles further support the adoption of international testing frameworks and self-testing requirements.

[2] The March 2000 clarification issued by China's State Encryption Management Commission clarified that: "the scope of the management of 'encryption products and equipment containing encryption technology' incorporated in the [commercial encryption] regulations, only limits specialized hardware and software for which encryption and decoding operations are core functions; other things, including wireless telephones, Windows software, browser software, etc., are not included in the scope." Announcement issued March 2000 by the People's Republic of China State Encryption Management Commission General Office (SEMC).

build a favourable market environment that is conducive to the development of commercial cryptography".

ESIA observes that the overarching legislation - the Cryptography Law – does not clarify the responsibilities of the SAMR and the SCA on testing and certification of commercial cryptography.

ESIA recommends amending the Opinions by specifying the roles and responsibilities of the SAMR and the SCA in relation to the testing and certification of commercial cryptography, in addition to when it comes to releasing the certification catalogue(s) and rules.

We further recommend commercial products where encryption is not a core function as well as well as mass-market products be specifically excluded from testing.

- This article further establishes that "*the certification catalogue(s) of commercial cryptography shall be released jointly by SAMR and SCA, whereas SAMR shall release the certification rules for commercial cryptography".*

  ESIA observes that differently from above article II, the SCA & SAMR Public notice No. 39 of 30 December 2019 state that "*in consultation with the SCA, the SAMR shall formulate and release a separate product catalogue, a separate set of certification rules and the corresponding implementation requirements for the State-promoted commercial cryptography certification*".

  ESIA recommends that any future catalogues and rules should follow international standards and best practices, and we strongly recommend that there be a public consultation also including stakeholders from industry before their release will be conducted.

  ESIA further recommends clarifying whether the Opinions cover both the mandatory and voluntary testing and certifications mentioned in Articles 26 and 25 of the Cryptography Law respectively, and clarifying the processes for drafting testing and certification catalogues and rules, as well as the roles and responsibilities of relevant government agencies.

  ESIA also recommends a consultation on the scope and nature of testing and certification.

  Finally, ESIA believes that, in the spirit of the Cryptography Law, mass market products and products where cryptography is not a core function should be excluded from mandatory testing and certification.

- The article also states that "*The SAMR and the SCA shall jointly establish a commercial cryptography certification technical committee, to coordinate and handle any technical issues that may arise in the course of certification, provide regulatory authorities with technical support, come up with work proposals, etc*".

  ESIA recommends publishing detailed information about the establishment procedures and composition of the commercial cryptography certification technical committee, including whether it will take in companies including Foreign Invested Companies.

  ESIA further recommends a consultation and comment period to allow a response to such information when it is published.

  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 from certification.

Article II

According to Article II (1) provision "*Commercial cryptography certification bodies shall meet the basic requirements prescribed by relevant administrative regulations and departmental rules, and possess the professional capability to carry out commercial cryptography certification activities. Qualifications shall be granted by the SAMR in consultation with the SCA*".

ESIA observes that based on the *Certification and Accreditation Regulation*, in commercial cryptography like in any given field of certification, there needs to be at least two certification bodies. It is also not clear whether commercial cryptography certification bodies are private business entities or government entities. More information is needed and how these "bodies" would be elected and announced, including the applicable qualifications and processes.

Further, 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 baseline for a broadly applicable certification framework. In the area of accreditation and evaluation rules, international standards such as ISO/IEC 17025 (General requirements for the competence, impartiality and consistent operation of laboratories) and ISO 17065 (Conformity assessment — Requirements for bodies certifying products, processes and services) are widely used. International standards and experience would enable non-discriminatory transparent testing

and certification frameworks, as well as the development of certification-related processes, with global industry involvement, to overcome fragmented approaches.

ESIA recommends that international standards and practices related to cryptography[3] are adopted are used for testing and certification.

ESIA further recommends the acceptance of testing and certification performed by accredited foreign labs in accordance with international standards to avoid unnecessary duplication.

Article II (4)

This paragraph states that "*Commercial cryptography certification bodies shall publicly disclose certification fees as well as information relating to the validity, suspension, cancellation, withdrawal or other status of relevant certificates, accept public supervision and handle inquiries from the public*".

In order to bring the Opinions in line with the *Certification and Accreditation Regulation*, ESIA recommends amending the Opinions by clarifying that commercial cryptography certification bodies shall publicly disclose also "*basic certification specifications and rules*" and "*information relating to certified products and their manufacturers*".

Article III (2)

This paragraph states that "*If a certification applicant has an objection to the testing/certification work of a testing or certification body and the testing/certification decision made thereby, it may appeal to the testing/certification body making the decision. If it still has an objection to the appeal handling result, it may complain to the market regulation department or cryptography administration department*".

ESIA observes that this is too general and needs refinement by adding appropriate referencing according to the good practices of international testing organisations.

IV. Conclusions

ESIA expresses its readiness to continue to support by providing information and expertise as the framework develops. We look forward to further cooperating with the authorities on the further developments in this area.

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

ABOUT ESIA

The European Semiconductor Industry Association (ESIA) is the voice of the Semiconductor Industry in Europe. Its mission is to represent and promote the common interests of the Europe-based semiconductor industry towards the European Institutions and stakeholders in order to ensure a sustainable business environment and foster its global competitiveness. As a provider of key enabling technologies the industry creates innovative solutions for industrial development, contributing to economic growth and responding to major societal challenges. Being ranked as the most R&D intensive sector by the European Commission, the European Semiconductor ecosystem supports approx. 200.000 jobs directly and up to 1.000.000 induced jobs in systems, applications and services in Europe.

Overall, micro- and nano-electronics enable the generation of at least 10% of GDP in Europe and the world. Website: http://www.eusemiconductors.eu/esia/home