ACN/Hexatrust's stance on the proposal for a regulation of the European Commission on the ENISA and on Information and Communication Technology cybersecurity certification (European Cybersecurity Act - COM (2017) 477 final)

October 2, 2017

On the occasion of the State of the Union Address given by the President of the European Commission Jean-Claude Juncker on September 13th, 2017, the European Commission proposed a series of measures relating to cybersecurity, including in particular a communication entitled "*Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*", as well as a proposal for a regulation on the ENISA and on ICT cybersecurity certification.

This proposed regulation aspires to redefine the role and mandate of the ENISA and proposes the creation of a new European cybersecurity certification scheme.

ACN and Hexatrust wholly agree with the European Commission's objectives to harmonise legislation governing cybersecurity mechanisms in Europe, in particular with regard to certification. This is especially timely as the increased digitisation of all economic activity and sectors creates a major strategic need for cybersecurity.

It is ACN and Hexatrust's belief that the response to such a challenge must be a coordinated effort at the European level with the aim of attaining the highest level of security possible in order to counter cyberthreats across all sectors. At the same time, this response must be adapted to security needs and the uses concerned, which will require the definition of multilevel cybersecurity certification criteria that will ensure optimum protection, according to the field concerned, taking into account the economic climate of the sector and allocating reasonable costs and time frames for certification.

In particularly sensitive fields – such as those pertaining to national sovereignty or security – it is essential to preserve a system of certification that would allow guaranteeing a maximum level of protection such as the level achieved from the application of the Common Criteria. Furthermore, products, services and solutions subject to this highest level of certification must undergo tests conducted by experts, the only means of guaranteeing an actual and optimal level of protection. In other less vulnerable or less critical fields, cybersecurity requirements may be less stringent, in particular with the purpose of improving responsiveness and controlling the inherent costs and time involved in any certification process.

ACN and Hexatrust believe that the European Commission's proposal of a regulation will lead to undeniable progress, especially with the introduction of the principle of a single certification valid throughout all the Member States of the European Union. ACN and Hexatrust welcome the idea of reinforcing the ENISA's and European Commission's role as guardians of European schemes that would allow the creation of a single cybersecurity market. The statutory definition of a National Certification Supervision Authority for all member states and their coordination are also a major step forward in view of harmonising the cybersecurity tools available to each State.

Nonetheless, certain points in this proposal require the special attention of businesses in the sector of digital trust that wish, in particular, to:

1) Sustain the major strategic achievements arising from the mutual recognition of the certificate of high levels of security issued by the ANSSI and its European counterparts (SOGIS MRA) under the new model

ACN and Hexatrust laud the implementation of a unified scheme for cybersecurity certifications, as well as the dominant role conferred on the ENISA in initiating, addressing and coordinating these initiatives.

However, ACN and Hexatrust wish for this transition to take place over an extended period to prevent abrupt changes that may be detrimental to the market, and under conditions that are compatible with the preservation of fundamental achievements built up over more than 20 years by all the public and private actors in the sector. Above all, ACN and Hexatrust would like for the requirements set out in particular by the SOG-IS MRA to be fully replicated in the new certification scheme and as such extended to all European countries for the purpose of harmonisation.

The main strengths of European cybersecurity (such as local (secure elements) or centralised (HSM) encryption, secure embedded programs, smartcards and secure components) were developed by capitalising on experience accumulated particularly in France through product evaluation schemes (Common Criteria and SOGIS MRA, CSPN, etc.) that the ANSSI has set up. ACN and Hexatrust are extremely concerned about maintaining the positions of world leaders that European industrial operators have been able to win over in their markets thanks to the effectiveness of the SOG-IS MRA scheme, for example.

Apart from this economic assessment, ACN and Hexatrust also wish to ensure the sanctuarisation of the strategic concepts of sovereignty and preservation of European cyberprotection capabilites. While this proposal demonstrated the ambition to raise the level of cybersecurity in Europe, defining a new organisation of evaluation/certification schemes will, in reality, lead to decreased levels of expertise and therefore of trust, eventually going against the initial objectives.

Proposal

- **Replicate the contents and principles of the SOG-IS – MRA annexed to the regulation to transform it into the baseline certification scheme without prejudice to the development of other certification schemes with lower requirements adapted to the needs of less strategic fields.**

2) Capitalise on national authorities to guarantee greater homogeneity

As cybersecurity topics are consubstantially related to the fields of sovereignty and national security, the industrial actors represented by ACN and Hexatrust wish this national dimension to be integrated in the new proposed schemes.

In addition, it is essential that in the process leading to the formulation of new schemes, the EU Cybersecurity certification Group and Member States, along with ENISA, hold codecision powers both for the initiation and for the validation of new certification schemes.

Furthermore, in implementing schemes at a national level, particularly with the aim of improving the communication of best practices, ACN and Hexatrust propose the possibility of national certification supervisory authorities to be validated by all European national authorities as part of a peer review system.

Proposals

- Subject the initiation and formal validation of new certification schemes to formal validation by national security entities (via the European Cybersecurity Certification group) for the highest levels of security (currently corresponding to levels higher than EAL4+) before the ENISA's finalisation of schemes and the publication of certificates of implementation.
- Set up a trialogue between the European Commission, the ENISA and the European Cybersecurity Certification group, allowing the possibility of reaching a compromise in the creation of schemes.
- Establish a peer review system between national certification supervisory authorities, which should be reviewed by their peers before being able to accredit laboratories in such manner as to guarantee the perfect homogeneity of security levels.

3) Reinforce the level of dialogue between the representatives of digital trust companies and the ENISA

Cross-functionality and upgradability are inherent to the concept of cybersecurity, and adequate cybersecurity measures are defined through the combination of the strongest expertise in cybersecurity and particular expertise in the field to be secured. This synergy can only be achieved via a representation of businesses in the field of digital trust, which may work together with representatives from the sector to be secured.

Nonetheless, in order to ensure the consistency and legitimacy of this dialogue between companies and the ENISA, it is essential to ensure the legitimacy of the stakeholders involved in the process, and in such a way as to ensure that the message communicated indeed reflects that of a legitimate profession instead of the individual interests of a company or any other entity seeking to wield influence over an extremely strategic field, i.e., the definition of cybersecurity requirements.

ACN and Hexatrust therefore take pride in the fact that the proposed regulation places great importance on the consultation of actors in the private sector, but immediately request that interlocutors invited to participate in such committees be subject to thorough vetting.

Proposal

- Subject stakeholders that are company representatives to accreditation by each national authority or by the EU Cybersecurity certification Group.

ACN/Hexatrust's stance
European Cybersecurity Act
October 2, 2017

About ACN:

The Alliance pour la Confiance Numérique (ACN - Alliance for Digital Trust) represents organisations (world leaders, SMEs and mid-sized enterprises) in the digital trust sector, particularly those specialising in cybersecurity, digital identity, secure communications, traceability / anti-counterfeiting and safe city technologies. In this field, France boasts highly efficient industrial cooperation and internationally recognised excellence thanks to world leaders, SMEs, mid-sized enterprises, and the various dynamic actors in the sector. Currently about 850 organisations in France generate turnover of almost 9 billion Euros in this rapidly growing sector (growth of more than 12% every year since 2014). ACN is a member of the Fédération des Industries Electriques, Electroniques et de Communication (FIEEC - Federation of Electric, Electronic and Communications Industries) and therefore actively participates in the work of the CoFIS committee (Comité de filière des Industries de Sécurité). ACN is also a founding member of the ECSO (European CyberSecurity Organisation).

About Hexatrust:

HEXATRUST was established by a group of French SMEs, mid-sized enterprises, and complementary players specialising in information system security, cybersecurity and digital trust sharing a common desire to pool their expertise.
Publishers and integrators of innovative solutions representative of French excellence, they joined forces to provide a range of high-performance, consistent and comprehensive products and services that secure critical infrastructures. This alliance addresses the needs of corporations, administrations and organisations of all sizes, in both the public and private sectors, in search of innovative, French-made product offerings that cater to all their information security requirements. Encouraged by their foothold in the European market, the members of HEXATRUST also wish to speed up their international expansion by sharing their experience, networks and resources for accessing markets worldwide.

Alliance pour la Confiance Numérique - 17 rue de l'amiral Hamelin, 75783 Paris cedex 16 - http://www.confiance-numerique.fr
Contact: Yoann KASSIANIDES, Delegate-General - Tel: 06 26 78 57 55, ykassianides@confiance-numerique.fr- SIRET: 797 543 550 00017