Addressing Smart Energy Solutions in Cyber Resilience Act

ESMIG position paper

Global and European organisations, regardless of whether they are part of the governmental sector, critical infrastructure or private businesses, are subjected to an increased number of cybersecurity risks. As stated in the proposal for a Cyber Resilience Act (CRA)[1], global annual cost of cybercrime is estimated at EUR 5.5 trillion in 2021. With this in mind, we can assume that any product or component manufacturers, software developers, cloud or other service providers agree that both technical implementations and implementation of horizontal regulatory acts are needed to address rising and ever-evolving cybersecurity risks.

Smart energy solution providers and smart metering product manufacturers are aware that their products are used as part of mission critical infrastructure. In the past, the main driver of cybersecurity requirements was related to customer requirements, often emerging from common cyber and information security standards (e.g ISO/IEC 62443, ISO 15408, ISO 27001 standard family, OWASP etc.), general security-related legislation (e.g. GDPR[2], NIS Directive[3]) and the few major cyber-security incidents in electric grid systems, causing black-outs. Based on emerging cybersecurity risks, together with customer requirements, legislation and past experience, smart metering energy solution providers have developed a robust and a highly secure advanced metering infrastructure, assuring a high level of confidentiality, integrity, availability and trust between all critical components.

Avoid overlapping of security requirements and related assessments in obligatory acts

In recent year(s) a significant step forward has been taken by the legislators to adopt high security requirements for several types of products, devices or software. Namely, for smart energy solutions, there are several legislative and regulatory acts, with which smart metering products, solutions and industry must and will have to comply:

- The Measurement Instrument Directive (MID)[4], with articles 8.1 - 8.5 related to protection of functions and data.
- The Cybersecurity Act (CSA)[5], establishing cybersecurity frameworks for products and services. In this regard a separate cybersecurity certification approach for smart meters was prepared, based on Common Criteria.

[1] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

[2] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[3] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[4] DIRECTIVE 2014/32/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of measuring instruments (recast)

[5] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

- The Radio Equipment Directive's (RED) new Delegated Act[6], applicable to smart meters, where several baseline and high-level protection requirements must be respected.
- The Network Code on Cybersecurity (NCCS)[7], as an extension of NIS / NIS 2 directive, applicable specifically for energy sector, proposes and applied new security requirements and risk management approaches for all equipment used in energy systems.
- Cyber Resilience Act (CRA), defining essential cybersecurity requirements for several types of hardware or software products, vulnerability reporting requirements and other relevant economic operators' obligations. The CRA also defines high penalties for non-compliance cases.

We would like to emphasise that it is crucial that any obligatory acts, their security requirements and related obligatory product assessments, do not overlap or compete with one another, causing confusion, misinterpretation and unnecessary high implementation costs for smart energy solution providers and manufacturers.

Smart meters recognised as critical (Class II) products and certified under the CRA

The draft CRA has recognised smart meters as a Class II product with digital elements, based on their *"cybersecurity risk level",* further noting them to be *"class II representing a greater risk"* than other classes. Smart energy solution providers and manufacturers should be included in any risk methodology or assessment, defining classification of products, to share insights on security controls implemented in smart meters. We support transparency and if the European Commission were to provide reference links to the risk methodology used for defining the classification of products, we would highly support such an effort. Only with transparent risk methodology and inputs from relevant stakeholders can the products be classified appropriately. Additionally, several other obligatory acts (e.g. RED, NCCS) define product risk assessment as integral parts, therefore, we strongly support unification of risk assessment methodologies to cover requirements from several (overlapping) security regulatory acts.

Smart energy solution providers and manufacturers would like to express concern regarding the CRA text on highly critical products: *"... the Commission is also empowered to adopt delegated acts to supplement this Regulation by specifying categories of highly critical products with digital elements".* We would emphasise the importance of introducing a transparent cybersecurity risk assessment methodology where relevant stakeholders (economic operators) are included and able to share relevant insight for defining product classification.

Recommendation I:
involve the smart meters industry sector in the introduction of a transparent cybersecurity risk assessment methodology and framework with the aim to classify products according to

[6] COMMISSION DELEGATED REGULATION (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive

[7] Draft network code for cybersecurity aspects of cross-border electricity flows (Network Code) submitted by ENTSO-E and EU DSO entity to ACER in accordance with Article 59(9) of Regulation (EU) 2019/943

Classification of other relevant systems of advanced metering infrastructure

The CRA has not (yet) classified other relevant systems of advanced metering infrastructure (e.g. Head-End Systems, meter data management, field operation applications and similar), meaning they cannot be recognised as part of Class I or Class II products and are automatically recognised as being within the default category. It is important to include relevant stakeholders into risk assessment and support the European Commission in defining which class the specific IT systems will belong to. As with smart meters, all systems of advanced smart energy infrastructure are subjected to similar security requirements and security controls as smart meters, assuring a high level of confidentiality, integrity, availability and trust.

Recommendation II:
involve relevant stakeholders in any risk assessment and they can support the European Commission in defining which Class the specific IT systems or products will belong to.

Certification as a way forwards to assure conformance with the CRA

Smart metering products and other advanced metering infrastructure components are subject to several standards and national-level requirements and often are subject to certifications, by national based certification laboratories or bodies. In the current version of the CRA, products, certified within the CSA are presumably in conformity with essential requirements of the CRA as defined in following excerpt: *"…products with digital elements that have been certified or for which an EU statement of conformity or certificate has been issued under a European cybersecurity certification scheme pursuant to Regulation (EU) 2019/881, and for which the Commission specified via implementing act that it can provide presumption of conformity for this Regulation, shall be presumed to be in conformity with the essential requirements of this Regulation…"*. Smart energy solution providers and manufacturers would propose that the European Commission clearly defines whether products, certified within the CSA, would "presumably" or "definitely" be conformant with the CRA, so as to avoid any confusion or misinterpretation of regulation in the future.

We fully support the European Commission's efforts to specify a list of European cybersecurity certification schemes and standards, thereby eliminating the obligation for manufacturers, to carry out a third-party conformity assessment and would greatly support manufacturers in avoiding undue administrative burdens.

As smart metering and smart energy products are complex and consist of several components, which would be classified as Default, we have developed a generic cybersecurity certification approach based on the European Common Criteria framework (EUCC) defined by ENISA as part of its responsibility under the CSA. Smart metering manufacturers would propose a clear statement (as part of the CRA text) by the European Commission that, for equipment already certified by the CSA approved framework and conformant with CRA requirements, the test results can be used to prove conformity with other product-oriented legislation such as the MID and RED. With such a proposed statement, manufacturers would avoid unnecessary costs, duplication of formal certification procedures and help provide a level playing field for single EU market.

If such a certification approach is not sufficient or accepted, the European Commission must clarify the certification process of products or systems consisting of several components with different classification levels (e.g., product or system must be certified and conformant with whichever component is the most critical).

Recommendation III:
enable the use of EUCC based cybersecurity certification to be used as proof for conformity with security requirements in product-oriented legislation such as the MID and RED.

Vulnerability reporting is important, but a clear procedure has to be defined at European Union level

Vulnerability discovery, reporting and mitigation presents one of the most important aspects of cybersecurity risk management procedures. To mitigate or eliminate critical vulnerabilities, a procedure with clear roles and responsibilities of relevant stakeholders (e.g. ENISA, manufacturers, 3rd parties etc.), has to be defined at the European Union level. Additionally, the European Commission must define a clear distinction between vulnerability and incident reports, as these terms are disparate and should not be treated in equal manner. An exact definition of *"actively exploited vulnerabilities"* must be prepared as such a statement can support a claim that unexploited critical vulnerabilities fall out of reporting scope.

In general, smart energy solution providers and manufacturers have identified several challenges with the vulnerabilities and incident reporting requirements. Rushed changes in the smart energy products could have several negative impacts on the stability of advanced metering infrastructure. Similarly, as product class is defined on cybersecurity risk-based approach, a cybersecurity risk-based approach must be used when addressing the vulnerability management procedures. Additionally, a clear definition of *"users"* should be defined as related to article 11, point 4 of CRA *("The manufacturer shall inform, without undue delay and after becoming aware, the* ***users*** *of the product…*", as it is unclear whether smart energy meter manufacturer informs customers (e.g. DSO) or end-users.

In relation to vulnerability handling requirements, set out by Annex I, point 2 of CRA, we would like to emphasise the importance of defining a clear framework for risk assessment and criticality thresholds to limit the scope (as proposed in Recommendation I). Without clear framework a vulnerability management could extend product delivery times indefinitely or force manufacturers to put products with known vulnerabilities to the market.

Recommendation IV:
introduce a clear definition of *"users"* in article 11, point 4.

Unclear transition period could bring confusion and negative impacts on general cybersecurity

Transitional provisions, defined in Article 55 of the CRA, could bring additional burdens and confusion for smart energy solution providers and manufacturers as points 2 and 3 are in contradiction. A clear definition of transitional provisions for products that fall out of the CRA scope must be defined or at least a clear statement of what *"substantial modification in their design"* covers. Can obligations on vulnerability reporting and mitigation, defined in Article 11 of the CRA, substantially impact the design of products? We propose the same approach as for other in-scope products: that the Article 11 obligations and requirements must be addressed through the cybersecurity risk-based approach.

Recommendation V: Article 11 obligations and requirements must be addressed through the cybersecurity risk-based approach.

………………………………………………………………

About ESMIG

ESMIG is the European voice of the providers of smart energy solutions. Our members provide products, information technology and services for multi-commodity metering, display and management of energy consumption and production at consumer premises.

Our activities are focused on systems for smart metering, consumer energy management and safe and secure data transfer.

We work closely with EU policy makers and other EU associations to make Europe's energy and water systems cleaner, reliable, more efficient and the European consumer informed, empowered and engaged.