













Cybersecurity Certification Framework (EU Regulation)

UNECE Proposal on Cyber Security Regulation

Article 45	Security objectives of cybersecurity certification scheme (Requirement)		<ul style="list-style-type: none"> › Not covered by the proposed regulation › Lacking record of access to data, services and functions
Article 46	Assurance levels of cybersecurity certification schemes (Recommendation)		<ul style="list-style-type: none"> › Cybersecurity Assurance Level (CAL) in ISO/SAE CD 21434 Annex E (informative)
Article 46a	Conformity self-assessment (Recommendation)		<ul style="list-style-type: none"> › Not applicable on the European Market due to Type Approval Regulation
Article 47	Elements of cybersecurity certification schemes (Requirement)		<ul style="list-style-type: none"> › Lacks description of purpose, technical requirements, requirements on skills of TA authorities
Article 47a	Cybersecurity information for certified products, process and services		<ul style="list-style-type: none"> › Not prescribed by UN regulation, but could be considered to be integrated › Relation to Draft UN Regulation for Software Updates
Article 48	Cybersecurity certification		
	2. Certification voluntary unless otherwise specified in Union law (Requirement)		<ul style="list-style-type: none"> › Certification mandatory for type approval
	2a. Check of efficiency and utilization of adopted certifications schemes any whether scheme shall be made mandatory		<ul style="list-style-type: none"> › UN Type Approval is already mandatory › Necessary amendments can be proposed by every contracting party
	3. Issued only by a public body (or accredited) (Requirement)		<ul style="list-style-type: none"> › Only appointed Approval Authority or Technical Service
	4. In duly justified cases a Cybersecurity certificate from a scheme can only be issued by a public body.		<ul style="list-style-type: none"> › Type Approval Authority is a public body
	5. All information necessary to conduct the certification procedure shall be made available to the conformity assessment body.		<ul style="list-style-type: none"> › UN Regulation for Type approval requires provision (Regulation 7.3.3-7.3.6)
	5a. Holder of certificate shall inform certification body about any later detected vulnerabilities or irregularities concerning the security		<ul style="list-style-type: none"> › Not prescribed by UN regulation, but could be considered to be integrated
	6. Certificates shall be issued for the period defined by the particular certification scheme and may be renewed, provided that the relevant requirements continue to be met (Requirement)		<ul style="list-style-type: none"> › CSMS Certificate of Compliance is valid for three years › No expiration of issued type approvals
	7. Certificate issued recognized in all Member States (Requirement)		<ul style="list-style-type: none"> › Recognized by all Contractual Parties of the WP.29 1958 agreement, this includes the EU