



The soon-to-be-introduced Cyber Resilience Act will set new EU standards for cybersecurity in digital products. Discover how Wibu-Systems can support your compliance journey in areas like data integrity, access control, data confidentiality, and product recalls.

CRA Source	CRA Terms	CRA Description	Possible Solutions	Wibu-Systems Products	Argumentations
CRA 10 (12)	Measures to Restore Compliance	From the time a product with digital elements is placed on the market and during the expected product lifetime or for a period of five years from the placing on the market, whichever period is shorter, manufacturers who know or have reason to believe that the product with digital elements or the procedures established by the manufacturer do not meet the basic requirements in Annex I shall immediately take the necessary corrective measures to ensure compliance of this product with digital elements or the manufacturer's processes, or, if necessary, to withdraw or recall the product from the market.	Withdrawing licenses / Replacing licenses	<ul style="list-style-type: none"> CodeMeter Runtime CodeMeter License Central Software Activation Wizard 	<ul style="list-style-type: none"> Licenses can be seamlessly withdrawn via CodeMeter License Central, ensuring that affected software is immediately deactivated and ceases to function. Replacing an existing license with a new one effectively disables the affected software, prompting users to update to the latest version for continued access.
CRA 10 (12)	Measures to Restore Compliance	To be able to contact affected customers in the event of an unforeseen problem and effectively withdraw products from the market, it must be known when which software in which version was delivered to which customers.	Version-based licensing, Electronic Software Distribution	<ul style="list-style-type: none"> CodeMeter License Central CodeMeter License Portal (ESD Module) 	<ul style="list-style-type: none"> If licenses are created for specific versions, CodeMeter License Central records which license was delivered for each software version, tracking exactly which versions are compatible with each license. The ESD module in CodeMeter License Portal regularly receives requests with the currently installed version from the user's side. This data can be used to build a database of the deployed versions, enabling visibility into which customer is using each version (planned feature).
CRA Annex 1 (3) b)	Access Protection	... provide protection against unauthorized access through appropriate control mechanisms, including at least authentication, identity, or access management systems,	Using X.509 certificates or private keys to identify devices.	<ul style="list-style-type: none"> CodeMeter Certificate Vault for secure authentication via X.509 certificates. CodeMeter Runtime, CmDongles, CmActLicenses for secure storage of private keys. CodeMeter License Central for key management. 	<ul style="list-style-type: none"> Certificates and/or private keys can be securely stored in a CmDongle or an encrypted, machine-bound CmActLicense file. Keys can be stored as X.509 certificates (CmDongle) or as private keys (CmDongle and CmActLicense). Private keys can be created, delivered, and managed with CodeMeter License Central. CmDongles can be preconfigured with private keys or certificates.
CRA Annex 1 (3) c)	Confidentiality	... protect the confidentiality of stored, transmitted, or otherwise processed personal or other data, e.g., by encrypting relevant data that is stored, used, or transmitted through state-of-the-art mechanisms,	Using private and secret keys to encrypt data.	<ul style="list-style-type: none"> CodeMeter Runtime, CmDongles, CmActLicenses for secure storage of secret and private keys. CodeMeter License Central for key management. 	<ul style="list-style-type: none"> Data encryption and decryption securely performed with CodeMeter Core API. Private and secret keys creation, delivery, and management handled seamlessly with CodeMeter License Central.
CRA Annex 1 (3) d)	Integrity	... protect the integrity of stored, transmitted, or otherwise processed data, whether personal or other data, commands, programs, and configurations from unauthorized manipulation or alteration by the user and report any damage,	Using private keys to sign data, software, and configurations.	<ul style="list-style-type: none"> CodeMeter Runtime, CmDongles, CmActLicenses for secure storage of secret and private keys. CodeMeter License Central for key management. CodeMeter Protection Suite for software and configuration. 	<ul style="list-style-type: none"> Data signing and validation performed securely with CodeMeter Core API. Private keys creation, delivery, and management handled seamlessly with CodeMeter License Central. Software and configurations signing and encryption enabled with CodeMeter Protection Suite, with built-in integrity checks to ensure both software and configuration files remain uncompromised.
CRA Annex 1 (3) e)	Data Minimization	... limit the processing of personal or other data to what is appropriate and relevant and to the extent necessary for the intended use of the product („data minimization“).			All CodeMeter products already adhere strictly to data minimization guidelines, ensuring only essential data is collected and processed.