

**ENCS**

EV-313

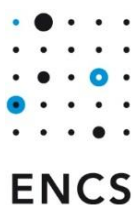
# Coverage of EN 18031 requirements by the IEC 62443 requirements for EV charging stations

Version 2025v1.1

13 June 2025

This document is shared under the Traffic Light Protocol classification:

**TLP White – public**



The European Network for Cyber Security (ENCS) is a non-profit membership organization that brings together critical infrastructure stake owners and security experts to deploy secure European critical energy grids and infrastructure.

## Version history

---

<b>Date</b>	<b>Versions</b>	<b>Description</b>
February 2025	EV-313 2025v1.0	Coverage of EN 18031 requirements by the IEC 62443 requirements for EV charging stations
13 June 2025	2025v1.1	Minor clarifications on the application of the RED delegated act were added.

---

## Coverage of EN 18031 by EV-311

In October 2021, the European Commission approved a delegated act to the Radio Equipment Directive (RED) that puts cybersecurity requirements on all internet-connected radio equipment from 1 August 2025.

The requirements will apply to all EV charging stations that use wireless communications and can be connected to the internet. Even if a CPO would normally use a segregated telecom network not connected to the internet, the requirements would probably still apply, because the charging station can be connected to the internet by changing networks. Hence, most charging stations will have to conform to the requirements.

Manufacturers can comply with the cybersecurity requirements by implementing the harmonized standard under development for the RED delegated act, called EN 18031. They can also comply directly with the delegated act without implementing the standard, but then they must show compliance using a stricter conformity assessment.

To understand what manufacturers will have to do to comply with the harmonized standard, we have compared the EN 18031 standard to the requirements that we have developed for EV charging stations (*EV-311 Security requirements from IEC 62443 for procuring EV charging stations, version 2025v1.0*). The main findings are:

- EN 18031 includes some additional requirements not included in EV-311 that could be challenging to meet for charging station manufacturers. See Table 1 below.
- The EN 18031 requirements cover all relevant topics and are enough to ensure that charging stations are secure enough. But the EN 18031 does not include a well-defined testing method that can assure buyers that the requirements have been properly implemented.

In the analysis below, we will consider all three parts of EN 18031:

- **EN 18031-1** which applies to all internet-connected radio equipment.
- **EN 18031-2** which applies to internet-connected radio equipment processing personal data.
- **EN 18031-3** which applies to internet-connected radio equipment that allows users to transfer money, monetary value, or virtual currency.

Manufacturers should determine which parts apply in their specific situation.

### Additional requirements in EN 18031

The analysis in the Appendix shows that the requirements in EV-311 cover most of the requirements in the EN 18031 harmonized standard. But EN 18031 standard includes

some requirements that are not part of EV-311. These requirements are listed in Table 1. See the Appendix for a more detailed analysis.

*Table 1: Requirements in EN 18031 not covered by EV-311.*

<b>Part</b>	<b>Requirement</b>
EN 18031-3	[AUM-2-2] Requirement two factor authentication
EN 18031-3	[GEC-8] Equipment Integrity

The two additional requirements not included in EV-311 both come from part 3 of the standard. They add new technical security functions to a charging station that may require significant changes to the architecture or hardware:

- [AUM-2-2] requires two-factor authentication for access to financial functions on all interfaces that allow the transfer of money, monetary assets, or virtual currencies. For charging station, these interfaces would be the payment terminal, and possibly the electric vehicle interface if plug & charge is used. For the payment terminal, it could mean that charging with only a charging pass will no longer be allowed. For the electric vehicle interface, authentication with certificates as included in IEC 15118 may no longer be enough to allow plug & charge.  
Note that even if only one-factor authentication would be required, authorizing EV drivers for charging using only the UUID on a smart card would not be compliant with the standard, as not authentication is used at all.
- [GEC-8] requires a secure boot process for charging stations that can transfer money, monetary assets, or virtual currencies. Many charging stations do not currently have secure boot. Implementing secure boot could require moving to a different hardware architecture.

When a charging station does not meet these requirements while EN 18031-3 is applicable, it does not mean that the charging station does not conform with the RED delegated act. It only means that manufacturers cannot show conformity through internal production control (module A). Instead, they must use modules B and C or module H for the conformity assessment. The charging station would then either need to be sent to an independent test lab (a notified body) or the manufacturer must have a certified quality management system.

## Completeness of EN 18031

The EN 18031 requirements cover all requirements in EV-311. So, if a charging station meets all EN 18031 requirements, it should be quite secure.

The problem with EN 18031 is that there is no test process defined for the standard. Assessment criteria have been included in the standard. But currently, there are no test labs that can test against the standard.

The reason to base the EV-311 requirements on IEC 62443, was to allow testing and certification according to the corresponding evaluation method and certification scheme. We think such certification is key to give assurance to buyers. Parties buying charging stations must be sure that it is really meeting the security requirements. Consumers and most local governments do not have the capability to have the charging stations tested on security. So, they must rely on some type of label or certificate.

The CE label that will come out of the RED delegated act and EN 18031 is in our opinion not strong enough for charging stations used by larger CPOs. It requires only self-assessment by the supplier using the internal production control conformity assessment module defined in the RED. CPOs are now considered critical infrastructure under the NIS 2 directive. Given their criticality, we think the stricter evaluation following IEC 62443 is needed to mitigate the risks to the electricity system.

## Appendix: Detailed analysis of EN 18031 coverage

The tables below give a detailed mapping from the EN 18031 standard to the IEC 62443-4-2 requirements that were selected in EV-311 and analyze if the IEC 62443-4-2 requirement covers the EN 18031 requirement.

### Coverage of EN 18031-1

Table 2 provides a mapping from part 1 of EN 18031 to the IEC 62443-4-2 requirements in EV-311.

*Table 2: Coverage of EN 18031-1 requirements by the IEC 62443-4-2 requirements selected in EV-311.*

EN 18031-1 requirement	IEC 62443-4-2 requirements	Coverage
[ACM-1] Applicability of access control mechanisms	CR 2.1 Authorization enforcement  CR 2.1 RE1 Authorization enforcement for all users (humans, software processes and devices)	<i>Fully covered</i> – Access control mechanisms are required for all users. None of the exceptions listed in [ACM-1] is applicable.
[ACM-2] Appropriate access control mechanisms	CR 2.1 Authorization enforcement  CR 2.1 RE1 Authorization enforcement for all users (humans, software processes and devices)	<i>Fully covered</i>
[AUM-1-1] Requirement network interface	CR 1.1 Human user identification and authentication  CR 1.2 Software process and device identification and authentication	<i>Fully covered</i> - Authentication is required on all interfaces. None of the exceptions listed in [AUM-1-1] is applicable.

	CR 1.2 RE1 Unique identification and authentication	
[AUM-1-2] Requirement user interface	CR 1.1 Human user identification and authentication	<i>Fully covered</i> - Authentication is required on all interfaces. None of the exceptions listed in [AUM-1-2] is applicable.
[AUM-2] Appropriate authentication mechanisms	CR 1.1 Human user identification and authentication  CR 1.2 Software process and device identification and authentication  CR 1.2 RE1 Unique identification and authentication	<i>Fully covered</i>
[AUM-3] Authenticator validation	CR 1.9 Strength of public key-based authentication	<i>Fully covered</i> – IEC 62443-4-2 concerns validation of public key-based authentication. For symmetric keys or passwords, the validation is implicit in the general authentication requirements.
[AUM-4] Changing authenticators	CR 1.5 Authenticator management	<i>Fully covered</i>
[AUM-5-1] Requirement for factory default passwords	CR 1.5 Authenticator management	<i>Fully covered</i> – Covered by the contextualization “factor default passwords.”

[AUM-5-2] Requirement for non-factory default passwords		<i>Not covered</i>
[AUM-6] Brute force protection	<p>CR 1.7 Strength of password-based authentication</p> <p>CR 1.9 Strength of public key-based authentication</p>	<i>Fully covered</i> – The IEC 62443 requirements ensure that passwords and cryptographic keys are long enough to protect against brute force attacks.
[SUM-1] Applicability of update mechanisms	EDR 3.10 Support for updates	<i>Fully covered</i>
[SUM-2] Secure updates	EDR 3.10 RE1 Update authenticity and integrity	<i>Fully covered</i>
[SUM-3] Automated updates	EDR 3.10 Support for updates	<i>Fully covered</i> – The remote updates contextualization ensures that updates can be performed automatically by the CSMS.
[SSM-1] Applicability of secure storage mechanisms	<p>EDR 3.11 Physical tamper resistance and detection</p> <p>EDR 3.11 RE1 Notification of a tampering attempt</p>	<i>Fully covered</i> – Stored assets are protected by tamper resistance and detection.
[SSM-2] Appropriate integrity protection for secure storage mechanisms	<p>EDR 3.11 Physical tamper resistance and detection</p> <p>EDR 3.11 RE1 Notification of a tampering attempt</p>	<i>Fully covered</i> – Stored assets are protected by tamper resistance and detection.
[SSM-3] Appropriate confidentiality protection for secure storage mechanisms	<p>EDR 3.11 Physical tamper resistance and detection</p> <p>EDR 3.11 RE1 Notification of a tampering attempt</p>	<i>Fully covered</i> – Stored assets are protected by tamper resistance and detection.

[SCM-1] Applicability of secure communication mechanisms	CR 3.1 Communication integrity  CR 3.1 RE1 Communication authentication  CR 4.1 Information confidentiality	<i>Fully covered</i> – Secure communication is required for the WAN network. Other networks are protected by physical measures.
[SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms	CR 3.1 Communication integrity  CR 3.1 RE1 Communication authentication	<i>Fully covered</i>
[SCM-3] Appropriate confidentiality protection for secure communication mechanisms	CR 4.1 Information confidentiality	<i>Fully covered</i>
[SCM-4] Appropriate replay protection for secure communication mechanisms	CR 3.8 Session integrity	<i>Fully covered</i>
[RLM-1] Applicability and appropriateness of resilience mechanisms	CR 7.1 Denial-of-service protection	<i>Fully covered</i>
[NMM-1] Applicability and appropriateness of network monitoring mechanisms		<i>Not applicable</i> – The charging station is not network equipment.
[TCM-1] Applicability of and appropriate traffic control mechanisms		<i>Not applicable</i> – The charging station is not network equipment.
[CCK-1] Appropriate CCKs	CR 4.3 - Use of cryptography	<i>Fully covered</i>

[CCK-2] CCK generation mechanisms	CR 4.3 - Use of cryptography	<i>Fully covered</i>
[CCK-3] Preventing static default values for preinstalled CCKs		<i>Not covered</i> – There is no requirement that the cryptographic keys used for OCPP authentication to the CSMS are unique.
[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities	CR 3.5 Input validation	<i>Fully covered</i> – The requirement is included in the contextualization “no known vulnerabilities.”
[GEC-2] Limit exposure of services via related network interfaces	CR 7.7 Least functionality	<i>Fully covered</i>
[GEC-3] Configuration of optional services and the related exposed network interfaces		<i>Not applicable</i> – By requirement CR 7.7 optional interfaces should be disable by default.
[GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces		<i>Not covered</i>
[GEC-5] No unnecessary external interfaces	CR 7.7 Least functionality	<i>Fully covered</i>
[GEC-6] Input validation	CR 3.5 Input validation	<i>Fully covered</i>
[CRY-1] Best practice cryptography	CR 4.3 - Use of cryptography	<i>Fully covered</i>

## Coverage of EN 18031-2

Table 3 provides a mapping from part 1 of EN 18031 to the IEC 62443-4-2 requirements in EV-311.

*Table 3: Coverage of EN 18031-1 requirements by the IEC 62443-4-2 requirements selected in EV-311.*

EN 18031-1 requirement	IEC 62443-4-2 requirements	Coverage
[ACM-1] Applicability of access control mechanisms	CR 2.1 Authorization enforcement  CR 2.1 RE1 Authorization enforcement for all users (humans, software processes and devices)	<i>Fully covered</i> – Access control mechanisms are required for all users. None of the exceptions listed in [ACM-1] is applicable.
[ACM-2] Appropriate access control mechanisms	CR 2.1 Authorization enforcement  CR 2.1 RE1 Authorization enforcement for all users (humans, software processes and devices)	<i>Fully covered</i>
[ACM-3] Default access control for children in toys		<i>Not applicable</i> – A charging station is not a toy.
[ACM-4] Default access control to children's privacy assets for toys and childcare equipment		<i>Not applicable</i> – A charging station is not a toy or childcare equipment.
[ACM-5] Parental/Guardian access controls for children in toys		<i>Not applicable</i> – A charging station is not a toy.

[ACM-6] Parental/Guardian access controls for other entities' access to managed children's privacy assets in toys	<i>Not applicable</i> – A charging station is not a toy.
[AUM-1-1] Requirement network interface	<p>CR 1.1 Human user identification and authentication</p> <p>CR 1.2 Software process and device identification and authentication</p> <p>CR 1.2 RE1 Unique identification and authentication</p> <p><i>Fully covered</i> - Authentication is required on all interfaces. None of the exceptions listed in [AUM-1-1] is applicable.</p>
[AUM-1-2] Requirement user interface	<p>CR 1.1 Human user identification and authentication</p> <p><i>Fully covered</i> - Authentication is required on all interfaces. None of the exceptions listed in [AUM-1-2] is applicable.</p>
[AUM-2-1] Requirement one factor authentication	<p>CR 1.1 Human user identification and authentication</p> <p>CR 1.2 Software process and device identification and authentication</p> <p>CR 1.2 RE1 Unique identification and authentication</p> <p><i>Fully covered</i></p>
[AUM-2-2] Requirement two factor authentication	<i>Not applicable</i> – The equipment's primary functionality is not processing of personal information of special categories.

[AUM-3] Authenticator validation	CR 1.9 Strength of public key-based authentication	<i>Fully covered</i> – IEC 62443-4-2 concerns validation of public key-based authentication. For symmetric keys or passwords, the validation is implicit in the general authentication requirements.
[AUM-4] Changing authenticators	CR 1.5 Authenticator management	<i>Fully covered</i>
[AUM-5-1] Requirement for factory default passwords	CR 1.5 Authenticator management	<i>Fully covered</i> – Covered by the contextualization “factor default passwords.”
[AUM-5-2] Requirement for non-factory default passwords		<i>Not covered</i>
[AUM-6] Brute force protection	CR 1.7 Strength of password-based authentication CR 1.9 Strength of public key-based authentication	<i>Fully covered</i> – The IEC 62443 requirements ensure that passwords and cryptographic keys are long enough to protect against brute force attacks.
[SUM-1] Applicability of update mechanisms	EDR 3.10 Support for updates	<i>Fully covered</i>
[SUM-2] Secure updates	EDR 3.10 RE1 Update authenticity and integrity	<i>Fully covered</i>
[SUM-3] Automated updates	EDR 3.10 Support for updates	<i>Fully covered</i> – The remote updates contextualization ensures that updates can be

		performed automatically by the CSMS.
[SSM-1] Applicability of secure storage mechanisms	EDR 3.11 Physical tamper resistance and detection EDR 3.11 RE1 Notification of a tampering attempt	<i>Fully covered</i> – Stored assets are protected by tamper resistance and detection.
[SSM-2] Appropriate integrity protection for secure storage mechanisms	EDR 3.11 Physical tamper resistance and detection EDR 3.11 RE1 Notification of a tampering attempt	<i>Fully covered</i> – Stored assets are protected by tamper resistance and detection.
[SSM-3] Appropriate confidentiality protection for secure storage mechanisms	EDR 3.11 Physical tamper resistance and detection EDR 3.11 RE1 Notification of a tampering attempt	<i>Fully covered</i> – Stored assets are protected by tamper resistance and detection.
[SCM-1] Applicability of secure communication mechanisms	CR 3.1 Communication integrity CR 3.1 RE1 Communication authentication CR 4.1 Information confidentiality	<i>Fully covered</i> – Secure communication is required for the WAN network. Other networks are protected by physical measures.
[SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms	CR 3.1 Communication integrity CR 3.1 RE1 Communication authentication	<i>Fully covered</i>
[SCM-3] Appropriate confidentiality protection for secure communication mechanisms	CR 4.1 Information confidentiality	<i>Fully covered</i>

[SCM-4] Appropriate replay protection for secure communication mechanisms	CR 3.8 Session integrity	<i>Fully covered</i>
[LGM-1] Applicability of logging mechanisms	CR 2.8 Auditable events	<i>Fully covered</i>
[LGM-2] Persistent storage of log data	CR 2.8 Auditable events	<i>Fully covered</i>
[LGM-3] Minimum number of persistently stored events	CR 2.9 Audit storage capacity CR 2.10 Response to audit process failures	<i>Fully covered</i>
[LGM-4] Time-related information of persistently stored dog data	CR 2.8 Auditable events	<i>Fully covered</i>
[DLM-1] Applicability of deletion mechanisms	CR 4.2 Information persistence	<i>Fully covered</i> – Deletion of personal information is included in the contextualization.
[UNM-1] Applicability of user notification mechanisms		<i>Not applicable</i> – User notification is expected to be performed by the CSMS, not each individual charging station.
[UNM-2] Appropriate user notification content		<i>Not applicable</i> – User notification is expected to be performed by the CSMS, not each individual charging station.

[CCK-1] Appropriate CCKs	CR 4.3 - Use of cryptography	<i>Fully covered</i>
[CCK-2] CCK generation mechanisms	CR 4.3 - Use of cryptography	<i>Fully covered</i>
[CCK-3] Preventing static default values for preinstalled CCKs		<i>Not covered</i> – There is no requirement that the cryptographic keys used for OCPP authentication to the CSMS are unique.
[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities	CR 3.5 Input validation	<i>Fully covered</i> – The requirement is included in the contextualization “no known vulnerabilities.”
[GEC-2] Limit exposure of services via related network interfaces	CR 7.7 Least functionality	<i>Fully covered</i>
[GEC-3] Configuration of optional services and the related exposed network interfaces		<i>Not applicable</i> – By requirement CR 7.7 optional interfaces should be disable by default.
[GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces		<i>Not covered</i>
[GEC-5] No unnecessary external interfaces	CR 7.7 Least functionality	<i>Fully covered</i>
[GEC-6] Input validation	CR 3.5 Input validation	<i>Fully covered</i>

[GEC-7] Documentation of external sensing capabilities		<i>Not applicable</i> – Charging stations typically have no external sensing.
[CRY-1] Best practice cryptography	CR 4.3 - Use of cryptography	<i>Fully covered</i>

## Coverage of EN 18031-3

Table 4 provides a mapping from part 1 of EN 18031 to the IEC 62443-4-2 requirements in EV-311.

*Table 4: Coverage of EN 18031-1 requirements by the IEC 62443-4-2 requirements selected in EV-311.*

<b>EN 18031-1 requirement</b>	<b>IEC 62443-4-2 requirements</b>	<b>Coverage</b>
[ACM-1] Applicability of access control mechanisms	CR 2.1 Authorization enforcement  CR 2.1 RE1 Authorization enforcement for all users (humans, software processes and devices)	<i>Fully covered</i> – Access control mechanisms are required for all users. None of the exceptions listed in [ACM-1] is applicable.
[ACM-2] Appropriate access control mechanisms	CR 2.1 Authorization enforcement  CR 2.1 RE1 Authorization enforcement for all users (humans, software processes and devices)	<i>Fully covered</i>
[AUM-1-1] Requirement network interface	CR 1.1 Human user identification and authentication  CR 1.2 Software process and device identification and authentication	<i>Fully covered</i> - Authentication is required on all interfaces. None of the exceptions listed in [AUM-1-1] is applicable.

	CR 1.2 RE1 Unique identification and authentication	
[AUM-1-2] Requirement user interface	CR 1.1 Human user identification and authentication	<i>Fully covered</i> - Authentication is required on all interfaces. None of the exceptions listed in [AUM-1-2] is applicable.
[AUM-2-1] Requirement one factor authentication	CR 1.1 Human user identification and authentication  CR 1.2 Software process and device identification and authentication  CR 1.2 RE1 Unique identification and authentication	<i>Fully covered</i>
[AUM-2-2] Requirement two factor authentication		<i>Not covered</i>
[AUM-3] Authenticator validation	CR 1.9 Strength of public key-based authentication	<i>Fully covered</i> – IEC 62443-4-2 concerns validation of public key-based authentication. For symmetric keys or passwords, the validation is implicit in the general authentication requirements.
[AUM-4] Changing authenticators	CR 1.5 Authenticator management	<i>Fully covered</i>
[AUM-5-1] Requirement for factory default passwords	CR 1.5 Authenticator management	<i>Fully covered</i> – Covered by the contextualization “factor default passwords.”

[AUM-5-2] Requirement for non-factory default passwords		<i>Not covered</i>
[AUM-6] Brute force protection	<p>CR 1.7 Strength of password-based authentication</p> <p>CR 1.9 Strength of public key-based authentication</p>	<i>Fully covered</i> – The IEC 62443 requirements ensure that passwords and cryptographic keys are long enough to protect against brute force attacks.
[SUM-1] Applicability of update mechanisms	EDR 3.10 Support for updates	<i>Fully covered</i>
[SUM-2] Secure updates	EDR 3.10 RE1 Update authenticity and integrity	<i>Fully covered</i>
[SUM-3] Automated updates	EDR 3.10 Support for updates	<i>Fully covered</i> – The remote updates contextualization ensures that updates can be performed automatically by the CSMS.
[SSM-1] Applicability of secure storage mechanisms	<p>EDR 3.11 Physical tamper resistance and detection</p> <p>EDR 3.11 RE1 Notification of a tampering attempt</p>	<i>Fully covered</i> – Stored assets are protected by tamper resistance and detection.
[SSM-2] Appropriate integrity protection for secure storage mechanisms	<p>EDR 3.11 Physical tamper resistance and detection</p> <p>EDR 3.11 RE1 Notification of a tampering attempt</p>	<i>Fully covered</i> – Stored assets are protected by tamper resistance and detection.
[SSM-3] Appropriate confidentiality protection for secure storage mechanisms	<p>EDR 3.11 Physical tamper resistance and detection</p> <p>EDR 3.11 RE1 Notification of a tampering attempt</p>	<i>Fully covered</i> – Stored assets are protected by tamper resistance and detection.

[SCM-1] Applicability of secure communication mechanisms	CR 3.1 Communication integrity  CR 3.1 RE1 Communication authentication  CR 4.1 Information confidentiality	<i>Fully covered</i> – Secure communication is required for the WAN network. Other networks are protected by physical measures.
[SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms	CR 3.1 Communication integrity  CR 3.1 RE1 Communication authentication	<i>Fully covered</i>
[SCM-3] Appropriate confidentiality protection for secure communication mechanisms	CR 4.1 Information confidentiality	<i>Fully covered</i>
[SCM-4] Appropriate replay protection for secure communication mechanisms	CR 3.8 Session integrity	<i>Fully covered</i>
[LGM-1] Applicability of logging mechanisms	CR 2.8 Auditable events	<i>Fully covered</i>
[LGM-2] Persistent storage of log data	CR 2.8 Auditable events	<i>Fully covered</i>
[LGM-3] Minimum number of persistently stored events	CR 2.9 Audit storage capacity  CR 2.10 Response to audit process failures	<i>Fully covered</i>

[LGM-4] Time-related information of persistently stored dog data	CR 2.8 Auditable events	<i>Fully covered</i>
[CCK-1] Appropriate CCKs	CR 4.3 - Use of cryptography	<i>Fully covered</i>
[CCK-2] CCK generation mechanisms	CR 4.3 - Use of cryptography	<i>Fully covered</i>
[CCK-3] Preventing static default values for preinstalled CCKs		<i>Not covered</i> – There is no requirement that the cryptographic keys used for OCPP authentication to the CSMS are unique.
[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities	CR 3.5 Input validation	<i>Fully covered</i> – The requirement is included in the contextualization “no known vulnerabilities.”
[GEC-2] Limit exposure of services via related network interfaces	CR 7.7 Least functionality	<i>Fully covered</i>
[GEC-3] Configuration of optional services and the related exposed network interfaces		<i>Not applicable</i> – By requirement CR 7.7 optional interfaces should be disable by default.
[GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces		<i>Not covered</i>
[GEC-5] No unnecessary external interfaces	CR 7.7 Least functionality	<i>Fully covered</i>

---

[GEC-6] Input validation	CR 3.5 Input validation	<i>Fully covered</i>
[GEC-8] Equipment Integrity		<i>Not covered</i>
[CRY-1] Best practice cryptography	CR 4.3 - Use of cryptography	<i>Fully covered</i>

---