|  |  |
| --- | --- |
| **Country** **国家** | Greater China大中华区 |
| **Procedure Author****程序作者** | Jun QuTÜV Rheinland / CCIC (Qingdao) Co., Ltd.莱茵技术—商检（青岛）有限公司 |
| **Approved** **批准**  | Perry DingTÜV Rheinland / CCIC (Ningbo) Co., Ltd.莱茵技术—商检（宁波）有限公司 |

**Revision date:**

**修订日期：** 2024-09-23

1. **Purpose 目的**

本文件阐述了莱茵检测认证服务(中国)有限公司（TRCHN）认证产品范围内规定的准备、提交、评估和认证程序。

1. **Scope 范围**

本规则适用于无线电产品，具体适用范围如下。

EN 18031-1 适用于可通过互联网进行通信的无线电设备，无论是直接通信还是通过其他联网的无线电设备进行通信。

EN 18031-2 适用于能够处理个人数据或流量数据或位置数据的无线电设备，包括

* 可联网的无线电设备
* 儿童看护类无线电设备
* 儿童玩具类无线电设备（Directive 2009/48/EC指令中的产品）
* 可穿戴类无线电设备

EN 18031-3 适用于允许设备持有者或用户转移资金、金融价值或虚拟货币的可联网无线电设备。

EN 18031-1，EN 18031-2，EN 18031-3不适用于受（EU）2017/745和（EU）2017/746指令监管的医疗设备

EN 18031-2，EN 18031-3不适用于（EU）2018/1139指令监管的民用航空相关设备，(EU) 2019/2144指令监管的机动车辆及相关系统组件，(EU) 2019/520指令监管的道路收费系统。

1. **Type of Approval 认证模式**

无线电设备进行的安全认证模式为：型式测试**+**获证后监督**。**

认证的基本环节包括：



1. **The application of Certification 认证的申请**
	1. **Unit partition of the certified products 认证产品单元划分**

原则上按组成无线电设备的软件、硬件和配置等申请认证。同一名称的无线电设备，不同制造商，不同版本号的软件或配置不同时，一般应分为不同申请单元。无线电设备的主要组成结构相同、制造工艺相同、软件相同，可作为一个申请单元。

* 1. **Application documents 申请材料**
		1. 申请表
		2. 营业执照
		3. TÜV莱茵测试报告或任何其他的TÜV莱茵指定的符合ISO/IEC 17025要求的实验室出具的型式试验报告
		4. 产品的证据信息（E.Info）
		5. 产品有关信息安全的技术配置表
		6. 无线电产品软件及硬件架构图
		7. 中文或英文产品说明书
		8. 中文或英文产品用户手册
		9. 照片文件（如果试验报告中未包括）
1. **Products testing 型式测试**
	1. **Sample 样品**

TRCHN从申请认证单元中抽取代表性样品。申请单元中只有一个型号的，送本型号的样品。以系列产品申请认证时，应从系列产品中选取具有代表性的产品作为主检产品，主检产品应该是该系列产品中对性能影响最不利的产品，其余型号产品为附检产品。

## 5.1.1 Send sample 送样原则

从申请认证单元中抽取代表性样品。申请单元中只有一个型号的，送本型号的样品。以系列产品申请认证时，应从系列产品中选取具有代表性的产品作为主检产品，主检产品应该是该系列产品中对性能影响最不利的产品，其余型号产品为附检产品，附检样品送样要求按和主检产品实际差异评估后在作决定。

## 5.1.2 Sample quantity 样品数量

申请人负责把样品送到TÜV莱茵实验室或任何其他的TÜV莱茵指定的实验室。样品数量见附件1。

## 5.1.3 Disposition of the sample and records 样品及记录处置

试验结束并出具实验报告后，有关试验记录和相关材料由实验室保存，样品按照TÜV莱茵有关规定处置。

* 1. **Product testing 产品测试**

适用于产品测试的认证标准为以下标准的技术测试章节：

EN 18031-1:2024 Common security requirements for radio equipment - Part 1: Internet connected radio equipment

无线电设备的通用安全要求-第一部分：可联网的无线电设备

EN 18031-2:2024 Common security requirements for radio equipment - Part 2: radio equipment processing data, namely Internet connected radio equipment

无线电设备的通用安全要求-第二部分：处理数据，即可联网的无线电设备

EN 18031-3:2024 Common security requirements for radio equipment – Part 3: Internet connected radio equipment processing virtual money or monetary value

无线电设备的通用安全要求-第一部分：处理虚拟货币或金融价值的可联网的无线电设备

## 5.2.1 Acc. Standards 依据标准

对获认可范围内的无线电设备适用技术测试标准如下：

EN 18031-1:2024

EN 18031-2:2024

EN 18031-3:2024

## 5.2.2 Testing items and requirements 试验项目及要求

无线电设备应满足 5.2.1 标准中的技术测试适用的项目及要求。

## 5.2.3 Testing method 试验方法

按照 5.2.1 标准中的建议的技术测试方法并结合实际的技术发展进行试验。

## 5.2.4 Period of Products testing产品测试周期

产品测试周期从收到样品和检测费用算起，通常不超过 5个月（因检测项目不合格，企业进行整改和重新检验的时间不计算在内）。

## 5.2.5 Testing result evaluation 测试结果判定

产品测试应符合 5.2.1 标准的技术要求，产品如有部分试验项目不符合标准的要求，允许申请人整改后重新提交样品进行试验。重新试验的样品数量和试验项目视不合格情况决定，整改期限不超过 6个月。如仍有任何 1 项不符合标准要求时，则判定该认证单元产品不符合认证要求。

## 5.2.6 Testing report 产品测试报告

由 TÜV 莱茵实验室或任何其他的 TÜV 莱茵指定的实验室对样品进行试验，并按规定格式出具测试报告。认证批准后，为申请人提供一份测试报告。

* 1. **Key component requirements关键零部件要求**

为确保获证产品的一致性，关键零部件/材料的技术参数、规格型号、制造商发生变化时，持证人应及时提出变更申请，并送样进行试验（或提供书面材料确认），经批准后方可在获证产品中使用。

1. **Evaluation and approval of the certification 认证结果评价与批准**
	1. **Evaluation and approval of the certification 认证结果评价与批准**

TR CHN莱茵中国根据申请资料、产品测试报告进行综合评价。评价合格后，向申请人颁发认证证书。每一个申请认证单元颁发一份认证证书。

* 1. **Lead-time 交付周期**

完成型式试验后，对符合认证要求的，批准时间、证书制作时间一般不超过25个工作日。

* 1. **Stop the certification 认证终止**

当型式试验不合格，TRCHN做出不合格决定，终止认证。终止认证后，如要继续申请，按新申请进行。

1. **Maintain, Change, suspend, restore, cancel and withdraw the certification 认证证书保持，变更，暂停，恢复，注销和撤销**
	1. **Maintain the certification 保持认证**

## 7.1.1 Certified products changing 认证产品的变更

7.1.1.1 Application for Changing 变更的申请

证书上的内容发生变化时，或产品中涉及安全和/或性能的设计、机构参数、外观、关键零部件/材料发生变更时，证书持有者应向 TRCHN 提出变更申请。

7.1.1.2 Evaluate and approve the changing 变更的评价和批准

TRCHN 根据变更的内容和提供的资料进行评价，确定是否可以变更。如需安排文件评审和/或差异项测试，则评审合格和/或差异项测试通过后方能进行变更。原则上，应以最初进行认证产品为变更评价的基础。评审和工厂检查按照 TRCHN 的规定执行。

对符合要求的，批准变更，并换发新的认证证书。

* 1. **Extending scope of certification 扩大认证范围**

## 7.2.1 Extending process 扩大的流程

认证证书持有者需要增加与已获得认证的产品为同一认证单元的产品认证范围时，应从认证申请开始办理手续，并说明扩大要求。TRCHN 核查扩大范围产品与原认证产品的一致性，确认原认证结果对扩大范围产品的有效性，针对差异和/或扩大的范围做文件审核和/或差异项测试，对符合要求的，依据认证证书持有者的要求换发证书。

原则上，应以最初进行认证产品为扩展评价的基础。

## 7.2.2 Sample 样品要求

持证人应先提供扩大范围产品的有关技术资料，需要送样时，按本方案第 5 章的要求选送样品或进行差异试验。

* 1. **Suspension, Withdrawal and Restoring of certification 认证暂停、撤销和恢复**

无论通过何种方式发现认证产品不符合认证方案和/或检测认证条例规定的基本要求，TRCHN 签证官将暂停或撤销相应证书。

在 TRCHN 签证官允许恢复认证状态前，证书持有者必须报告并完成纠正行动。签证官依照认证流程规定，将证书恢复为有效状态。对于暂停超过 6个月，将撤销相应证书；未完成纠正的，视为自愿放弃，对相应证书予以撤销。如果撤销，需要及时将原证书退回给TRCHN。

当证书暂停或撤销时，相关证书持有者将得到书面通知，说明暂停或撤销的原因，并在记录中标记该证书无效。对可能存在缺陷的认证产品应立即采取纠正行为，包括召回（如果适用）。

1. **Certification mark 认证标志**

本规则覆盖产品的认证证书无认证标志。

1. **Cost 收费**

认证费用按TRCHN有关规定收取。

**附件1**

EN 18031 认证方案样品和文档要求

|  |  |  |
| --- | --- | --- |
| 依据标准  | 送样数量  | 相关文档 |
| 文档名称 | 必须/可选 |
| EN 18031-1EN 18031-2EN 18031-3 | 无线电产品release版本2件  | 1、E.Info (信息表) | 必须 |
| 2、决策树文件  | 必须 |
| 3、型号差异表  | 可选 |
| 4、测试记录  | 必须 |
| 5、测试报告  | 必须 |
| 6、证书 | 可选 |

**附件2**

EN 18031-1标准要求

|  |  |  |
| --- | --- | --- |
| No. | **Reference Table b.1** | Technical / Process |
| **6.1** | **[ACM] Access control mechanism** |
| 6.1.1 | [ACM-1] Applicability of access control mechanisms |
| 6.1.1.1 | The equipment shall use access control mechanisms to manage entities' access to security assets and network assets, except for access to security assets or network assets where: — public accessibility is the equipment’s intended functionality; or — physical or logical measures in the equipment’s targeted operational environment limit their accessibility to authorized entities; or — legal implications do not allow for access control mechanisms. | T |
| 6.1.2 | [ACM-2] Appropriate access control mechanisms |
| 6.1.2.1 | Access control mechanisms that are required per ACM-1 shall ensure that only authorized entities have access to the protected security assets and network assets. | T |
| **6.2** | **[AUM] Authentication mechanism** |
| 6.2.1 | [AUM-1] Applicability of authentication mechanisms |
| 6.2.1.1 | Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities’ access via network interfaces that allow to: — read confidential network function configuration or confidential security parameters; or — modify sensitive network function configuration or sensitive security parameters; or — use network functions or security functions, except for access: — to network functions or network function configuration where the absence of authentication is required for the equipment’s intended functionality; or — via networks where physical or logical measures in the equipment’s targeted operational environment limit accessibility to authorised entities. | T |
| 6.2.1.2 | Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities’ access via user interfaces that allow to: — read confidential network function configuration or confidential security parameters; or — modify sensitive network function configuration or sensitive security parameters; or — use network functions or security functions, except for access: — where physical or logical measures in the equipment’s targeted operational environment limit accessibility to authorized entities; and except for read only access to network functions or network functions configuration where access without authentication is needed: — to enable the intended equipment functionality; or — because legal implications do not allow for authentication mechanisms. | T |
| 6.2.2 | [AUM-2] Appropriate authentication mechanisms |
| 6.2.2.1 | Authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) shall verify an entity’s claim based on examining evidence from at least one element of the categories knowledge, possession and inherence (one factor authentication). | T |
| 6.2.3 | [AUM-3] Authenticator validation |
| 6.2.3.1 | Authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) shall validate all relevant properties of the used authenticators, dependent on the available information in the operational environment of use. | T |
| 6.2.4 | [AUM-4] Changing authenticators |
| 6.2.4.1 | Authentication mechanisms that are required per AUM-1-1 or AUM-1-2 shall allow for changing the authenticator except for authenticators where conflicting security goals do not allow for a change. | T |
| 6.2.5 | [AUM-5] Password strength |
| 6.2.5.1 | If factory default passwords are used by an authentication mechanism that is required per AUM-1-1 or AUM-1-2, they shall: — be unique per equipment; and — follow best practice concerning strength; or — be enforced to be changed by the user before or on first use. NOTE The user may choose to not use any password. | T |
| 6.2.5.2  | If passwords other than factory default passwords are used by an authentication mechanism required per AUM-1-1 or AUM-1-2, they shall:— be enforced to be set by the user before or on first use and before the equipment is logically connected to a network; or — be defined by an authorized entity within a network where access is limited to authorised entities; or — be generated by the equipment using best practice concerning strength and only communicated to an authorized entity within a network where access is limited to authorised entities.NOTE: The user may choose to not use any password. | T |
| 6.2.6 | [AUM-6] Brute force protection |
| 6.2.6.1 | Authentication mechanisms required per AUM-1-1 or AUM-1-2 shall be resilient against brute force attacks. | T |
| **6.3** | **[SUM] SECURE UPDATE MECHANISM** |
| 6.3.1 | [SUM-1] Applicability of update mechanisms |
| 6.3.1.1 | The equipment shall provide at least one update mechanism for updating software, including firmware, affecting security assets and/or network assets, except for software: — where functional safety implications do not allow updatability; or — which is immutable; or — where alternative measures protect the affected security assets and/or network assets during the entire lifecycle of the equipment. | T |
| 6.3.2 | [SUM-2] Secure updates |
| 6.3.2.1 | Each update mechanism as required per SUM-1 shall only install software whose integrity and authenticity are valid at the time of the installation. | T |
| 6.3.3 | [SUM-3] Automated updates |
| 6.3.3.1 | Each update mechanism that is required per SUM-1 shall be capable of updating the software: — without human intervention at the equipment; or — via scheduling the installation of an update under human approval; or — via triggering the installation of an update under human approval or supervision where there is the need to prevent any unexpected damage in the operational environment. | T |
| **6.4** | **[SSM] SECURE STORAGE MECHANISM** |
| 6.4.1 | [SSM-1] Applicability of secure storage mechanisms |
| 6.4.1.1 | The equipment shall always use secure storage mechanisms for protecting the security assets and network assets persistently stored on the equipment, except for persistently stored security assets or network assets where: — the physical or logical measures in the target environment ensures the security asset or network asset stored on the equipment accessibility is limited to authorized entities. | T |
| 6.4.2 | [SSM-2] Appropriate integrity protection for secure storage mechanisms |
| 6.4.2.1 | Each secure storage mechanism that is required per SSM-1 shall protect the integrity of security assets and network assets it stores persistently. | T |
| 6.4.3 | [SSM-3] Appropriate confidentiality protection for secure storage mechanisms |
| 6.4.3.1 | Each secure storage mechanism that is required per SSM-1 shall protect the secrecy of confidential security parameter and confidential network function configuration it stores persistently. | T |
| **6.5** | **[SCM] SECURE COMMUNICATION MECHANISM** |
| 6.5.1 | [SCM-1] Applicability of secure communication mechanisms |
| 6.5.1.1 | The equipment shall always use secure communication mechanisms for communicating security assets and network assets with other entities via network interfaces, except for: — communicating security assets or network assets whose transfer is protected by physical or logical measures in the targeted environment that ensure that network assets or security assets are not exposed to unauthorised entities; or — communicating security assets or network assets whose exposure is part of establishing or managing a connection combined with additional measures to authenticate the connection or trust relation. | T |
| 6.5.2 | [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms |
| 6.5.2.1 | Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the integrity and authenticity of the security assets and network assets communicated, except for communicating security assets or network assets where: — a deviation from best practice for integrity or authenticity protection is required for interoperability reasons. | T |
| 6.5.3 | [SCM-3] Appropriate confidentiality protection for secure communication mechanisms |
| 6.5.3.1 | Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the confidentiality of communicated network assets and security assets where confidentiality protection of those is needed, except for communicating security assets or network assets where: — a deviation from best practice for protecting confidentiality is required for interoperability reasons. | T |
| 6.5.4 | [SCM-4] Appropriate replay protection for secure communication mechanisms |
| 6.5.4.1 | Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the security assets and the network assets communicated against replay attacks, except for communicating security assets or network assets where: — a duplicate transfer does not impose a threat of a replay attack; or — a deviation from best practice for replay protection is required for interoperability reasons. | T |
| **6.6** | **[RLM] RESILIENCE MECHANISM** |
| 6.6.1 | [RLM-1] Applicability and appropriateness of resilience mechanisms |
| 6.6.1.1 | The equipment shall use resilience mechanisms to mitigate the effects of Denial of Service (DoS) Attacks on the network interfaces and return to a defined state after the attack except for: — network interfaces that are only used in a local network that do not interoperate with other networks; or — network interfaces where other devices in the network provide sufficient protection against DoS attacks and loss of essential functions for network operations. | T |
| **6.7** | **[NMM] NETWORK MONITORING MECHANISM** |
| 6.7.1 | [NMM-1] Applicability and appropriateness of network monitoring mechanisms |
| 6.7.1.1 | If the equipment is a network equipment, the equipment shall provide network monitoring mechanism(s) to detect for indicators of DoS attacks in the network traffic between networks which it processes. | T |
| **6.8** | **[TCM] TRAFFIC CONTROL MECHANISM** |
| 6.8.1 | [TCM-1] Applicability of and appropriate traffic control mechanisms |
| 6.8.1.1 | If the equipment is a network equipment, the equipment shall provide network traffic control mechanism(s). | T |
| **6.9** | **[CCK] CONFIDENTIAL CRYPTOGRAPHIC KEYS** |
| 6.9.1 | [CCK-1] Appropriate CCKs |
| 6.9.1.1 | Confidential cryptographic keys that are preinstalled or generated by the equipment during its use, shall support a minimum security strength of 112-bits, except for: — CCKs that are solely used by a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM.NOTE 1: Confidential cryptographic key is a defined term. Other secrets, whose disclosure cannot be used to harm the network or its functioning or for the misuse of network resources, such as secrets solely protecting intellectual property are not covered by the definition of confidential cryptographic key. NOTE 2: The requirement refers to all confidential cryptographic keys chosen by the equipment manufacturer either directly or imposed by a protocol. For instance, the manufacturer directly chooses/configures the cipher suite of TLS protocol to be used by the device, other protocols may impose one single option for cryptographic algorithms and their respective keys. | T |
| 6.9.2 | [CCK-2] CCK generation mechanisms |
| 6.9.2.1 | The generation of confidential cryptographic keys shall adhere to best practice cryptography, except for: — the generation of CCKs for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM.NOTE: Confidential cryptographic key is a defined term. Other secrets, whose disclosure cannot be used to harm the network or its functioning or for the misuse of network resources, such as secrets solely protecting intellectual property are not covered by the definition of confidential cryptographic key. | T |
| 6.9.3 | [CCK-3] Preventing static default values for preinstalled CCKs |
| 6.9.3.1 | Preinstalled confidential cryptographic keys shall be practically unique per equipment, except for: — CCKs that are only used for establishing initial trust relationships under conditions controlled by an authorized entity; or — CCKS key are shared parameters required for the equipment’s intended functionality.NOTE: Confidential cryptographic key is a defined term. Other secrets, whose disclosure cannot be used to harm the network or its functioning or for the misuse of network resources, such as secrets solely protecting intellectual property are not covered by the definition of confidential cryptographic key. | T |
| **6.10** | **[GEC] GENERAL EQUIPMENT CAPABILITIES** |
| 6.10.1 | [GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities |
| 6.10.1.1 | The equipment shall not include publicly known exploitable vulnerabilities that, if exploited, affect security assets and network assets, except for vulnerabilities: — that cannot be exploited in the specific conditions of the equipment; or — that have been mitigated to an acceptable residual risk; or — that have been accepted on a risk basis. | T |
| 6.10.2 | [GEC-2] Limit exposure of services via related network interfaces |  |
| 6.10.2.1 | In factory default state the equipment shall only expose — network interfaces; and — services via network interfaces affecting security assets or network assets which are necessary for equipment setup or for basic operation of the equipment. | T |
| 6.10.3 | [GEC-3] Configuration of optional services and the related exposed network interfaces |
| 6.10.3.1 | Optional network interfaces or optional services exposed via network interfaces affecting security assets or network assets, which are part of the factory default state shall have the option for an authorized user to enable and disable the network interface or service. | T |
| 6.10.4 | [GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces |
| 6.10.4.1 | The equipment’s user documentation shall contain a description of — all exposed network interfaces; and— all services exposed via network interfaces, which are delivered as part of the factory default state. | T+P |
| 6.10.5 | [GEC-5] No unnecessary external interfaces |
| 6.10.5.1 | The equipment shall only expose physical external interfaces if they are necessary for its intended functionality. | T |
| 6.10.6 | [GEC-6] Input validation |
| 6.10.6.1 | The equipment shall validate input received via external interfaces if the input has potential impact on security assets and/or network assets. | T |
| **6.11** | **[CRY] CRYPTOGRAPHY** |
| 6.11.1 | [CRY-1] Best practice Cryptography |
| 6.11.1.1 | The equipment shall use best practice for cryptography that is used for the protection of the security assets or network assets, except for: — cryptography used for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM. | T |

EN 18031-2标准要求

|  |  |  |
| --- | --- | --- |
| No. | **Reference Table b.2** | Technical / Process |
| **6.1** | **[ACM] Access control mechanism** |
| 6.1.1 | [ACM-1] Applicability of access control mechanisms |
| 6.1.1.1 | The equipment shall use access control mechanisms to manage entities' access to security assets and privacy assets, except for access to security assets or privacy assets where: — public accessibility is the equipment’s intended functionality; or— physical or logical measures in the equipment’s targeted operational environment limit their accessibility to authorized entities; or— legal implications do not allow for access control mechanisms | T |
| 6.1.2 | [ACM-2] Appropriate access control mechanisms |
| 6.1.2.1 | Access control mechanisms that are required per ACM-1 shall ensure that only authorized entities have access to the protected security assets and privacy assets. | T |
| 6.1.3 | [ACM-3] Default access control for children in toys |
| 6.1.3.1 | If the equipment is a toy, for each privacy function where children can access external content and children’s access is managed by access control mechanisms required per ACM-1, the access control mechanisms shall by default ensure that children’s access to external content via the privacy function is restricted to content from authorized entities. | T |
| 6.1.4 | [ACM-4] Default access control to children’s privacy assets for toys and childcare equipment |
| 6.1.4.1 | If the equipment is a toy or childcare equipment, any children’s privacy function and personal information access control mechanisms required per ACM-1 shall by default restrict, apart from the child’s or their parental/guardians, any third-party access to the children’s privacy function and personal information processed by the equipment, except for authorised accesses which are required for the equipment’s intended functionality. | T |
| 6.1.5 | [ACM-5] Parental/Guardian access controls for children in toys |
| 6.1.5.1 | If the equipment is a toy, for each security and privacy asset that is accessible by children, any access control mechanism required per ACM-1 managing the children’s access, shall be configurable by an authorized entity to restrict children’s access to the protected security and privacy assets. | T |
| 6.1.6 | [ACM-6] Parental/Guardian access controls for children’s privacy assets in toys |
| 6.1.6.1 | If the equipment is a toy, for each children’s privacy asset that is accessible by entities, other than the children or their parents or guardians, and where those other entities’ access is managed by access control mechanisms required per ACM-1, the access control mechanisms shall be configurable by an authorized entity to restrict the other entities’ access to the managed children’s privacy assets. | T |
| **6.2** | **[AUM] Authentication mechanism** |
| 6.2.1 | [AUM-1] Applicability of authentication mechanisms |
| 6.2.1.1 | Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities’ access via network interfaces that allow to: — read confidential personal information, confidential privacy function configuration or confidential security parameters; or — modify sensitive personal information, sensitive privacy function configuration or sensitive security parameters; or — use privacy functions or security functions, except for access: — to personal information, privacy functions or privacy function configuration where the absence of authentication is required for the intended equipment functionality; or — via networks where physical or logical measures in the equipment’s targeted operational environment limit accessibility to authorised entities. | T |
| 6.2.1.2 | Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities’ access via user interfaces that allow to: — read confidential personal information, confidential privacy function configuration or confidential security parameters; or— modify sensitive personal information, sensitive privacy function configuration or sensitive security parameters; or — use privacy functions or security functions, except for access: — where physical or logical measures in the equipment’s targeted operational environment limit accessibility to authorized entities; and except for read only access to personal information, privacy functions or privacy function configuration where access without authentication is needed: — to enable the intended equipment functionality or — because legal implications do not allow for authentication mechanisms. | T |
| 6.2.2 | [AUM-2] Appropriate authentication mechanisms for external interfaces |
| 6.2.2.1 | Authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) shall verify an entity’s claim based on examining evidence from at least one element of the categories knowledge, possession and inherence (one factor authentication). | T |
| 6.2.2.2 | If the primary equipment’s intended functionality is specifically processing personal information of special categories, for each access to personal information of special categories via user interfaces over network interface the authentication mechanisms shall support the verification of an entity’s claim based on evidence derived from at least two different elements of the categories knowledge, possession and inherence (two factor authentication). | T |
| 6.2.3 | [AUM-3] Authenticator validation |
| 6.2.3.1 | Authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) shall validate all relevant properties of the used authenticators, dependent on the available information in the operational environment of use. | T |
| 6.2.4 | [AUM-4] Changing authenticators |
| 6.2.4.1 | Authentication mechanisms that are required per AUM-1-1 or AUM-1-2 shall allow for changing the authenticator except for authenticators where conflicting security goals do not allow for a change. | T |
| 6.2.5 | [AUM-5] Password strength |
| 6.2.5.1 | If factory default passwords are used by an authentication mechanism that is required per AUM-1-1 or AUM-1-2, they shall: — be unique per equipment; and — follow best practice concerning strength; or — be enforced to be changed by the user before or on first use. NOTE: The user may choose to not use any password. | T |
| 6.2.5.2 | If passwords other than factory default passwords are used by an authentication mechanism required per AUM-1-1 or AUM-1-2, they shall: — be enforced to be set by the user before or on first use and before the equipment is logically connected to a network; or — be defined by an authorized entity within a network where access is limited to authorised entities; or — be generated by the equipment using best practice concerning strength and only communicated to an authorized entity within a network where access is limited to authorised entities. NOTE: The user can choose to not use any password. | T |
| 6.2.6 | [AUM-6] Brute force protection |
| 6.2.6.1 | Authentication mechanisms required per AUM-1-1 or AUM-1-2 shall be resilient against brute force attacks. | T |
| **6.3** | **[SUM] SECURE UPDATE MECHANISM** |
| 6.3.1 | [SUM-1] Applicability of update mechanisms |
| 6.3.1.1 | The equipment shall provide at least one update mechanism for updating software, including firmware, affecting security assets and/or privacy assets, except for software: — where functional safety implications do not allow updatability; or — which is immutable; or — where alternative measures protect the affected security assets and/or privacy assets during the entire lifecycle of the equipment. | T |
| 6.3.2 | [SUM-2] Secure updates |
| 6.3.2.1 | Each update mechanism as required per SUM-1 shall only install software whose integrity and authenticity are valid at the time of the installation. | T |
| 6.3.3 | [SUM-3] Automated updates |
| 6.3.3.1 | When the equipment is internet-connected, each update mechanism that is required per SUM-1 shall be capable of updating the software: — without human intervention at the equipment; or — via scheduling the installation of an update under human approval; or — via triggering the installation of an update under human approval or supervision where there is the need to prevent any unexpected damage in the operational environment. | T |
| **6.4** | **[SSM] SECURE STORAGE MECHANISM** |
| 6.4.1 | [SSM-1] Applicability of secure storage mechanisms |
| 6.4.1.1 | The equipment shall always use secure storage mechanisms for protecting the security assets and privacy assets persistently stored on the equipment, except for persistently stored security assets and privacy assets where: — the physical or logical measures in the target environment ensures the security asset or privacy asset stored on the equipment accessibility is limited to authorized entities. | T |
| 6.4.2 | [SSM-2] Appropriate integrity protection for secure storage mechanisms |
| 6.4.2.1 | Each secure storage mechanism that is required per SSM-1 shall protect the integrity of security assets and privacy assets it stores persistently. | T |
| 6.4.3 | [SSM-3] Appropriate confidentiality protection for secure storage mechanisms |
| 6.4.3.1 | Each secure storage mechanism that is required per SSM-1 shall protect the secrecy of confidential personal information, confidential privacy function configuration, and confidential security parameter persistently stored on the equipment. | T |
| **6.5** | **[SCM] SECURE COMMUNICATION MECHANISM** |
| 6.5.1 | [SCM-1] Applicability of secure communication mechanisms |
| 6.5.1.1 | The equipment shall always use secure communication mechanisms for communicating security assets and privacy assets with other entities via network interfaces, except for: — communicating security assets or privacy assets whose transfer is protected by physical or logical measures in the targeted environment that ensure that security assets or privacy assets are not exposed to unauthorised entities; or — communicating security assets whose exposure is part of establishing or managing a connection combined with additional measures to authenticate the connection or trust relation. | T |
| 6.5.2 | [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms |
| 6.5.2.1 | Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the integrity and authenticity of the security assets and privacy assets communicated, except for communicating security assets or privacy assets where: — a deviation from best practice for integrity or authenticity protection is required for interoperability reasons. | T |
| 6.5.3 | [SCM-3] Appropriate confidentiality protection for secure communication mechanisms |
| 6.5.3.1 | Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the confidentiality of communicated privacy assets and security assets where confidentiality protection of those is needed, except for communicating security assets or privacy assets where: — a deviation from best practice for protecting confidentiality is required for interoperability reasons. | T |
| 6.5.4 | [SCM-4] Appropriate replay protection for secure communication mechanisms |
| 6.5.4.1 | Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the security assets and the privacy assets communicated against replay attacks, except for communicating security assets or privacy assets where: — a duplicate transfer does not impose a threat of a replay attack; or — a deviation from best practice for replay protection is required for interoperability reasons. | T |
| **6.6** | **[LGM] LOGGING MECHANISM** |
| 6.6.1 | [LGM-1] Applicability of logging mechanisms |
| 6.6.1.1 | The equipment shall use logging mechanisms for internal activities that are relevant to privacy assets and their protection (referred to as events), except for: — internal activities where a legal obligation prohibits logging. | T |
| 6.6.2 | [LGM-2] Persistent storage of log data |
| 6.6.2.1 | Logging mechanisms that are required per LGM-1 shall store log data for related events in the equipment’s persistent storage, except for events where: — related log data is stored outside the equipment. | T |
| 6.6.3 | [LGM-3] Minimum number of persistently stored events |
| 6.6.3.1 | All log data stored in equipment’s persistent storage by logging mechanisms that are required per LGM-1 shall always include: — a minimum number of the latest events; and — the latest event. | T |
| 6.6.4 | [LGM-4] Time-related information of persistently stored dog data |
| 6.6.4.1 | All log data stored in equipment’s persistent storage by logging mechanisms that are required per LGM-1 shall include: — a timestamp if real time is available on the equipment; and — time-related information if real time is not available on the equipment. | T |
| **6.7** | **[DLM] DELETION MECHANISM** |
| 6.7.1 | [DLM-1] Applicability of deletion mechanisms |
| 6.7.1.1 | The equipment shall provide a deletion mechanism that allows a user to delete their personal data and sensitive security parameters stored on the equipment. | T |
| **6.8** | **[UNM] USER NOTIFICATION MECHANISM** |
| 6.8.1 | [UNM-1] Applicability of user notification mechanisms |
| 6.8.1.1 | The equipment shall provide user notification mechanism(s) for informing the user of the equipment about changes affecting the protection or privacy of personal information, except for changes where: — other methods of informing the user exist, which do not involve the equipment. | T |
| 6.8.2 | [UNM-2] Appropriate user notification content |
| 6.8.2.1 | The content of a notification provided by a user notification mechanism that is required per UNM-1 shall include at least: — a description of a change; and — a description of how a change will affect the protection and privacy of personal information. | T |
| **6.9** | **[CCK] CONFIDENTIAL CRYPTOGRAPHIC KEYS** |
| 6.9.1 | [CCK-1] Appropriate CCKs |
| 6.9.1.1 | Confidential cryptographic keys that are preinstalled or generated by the equipment during its use shall support a minimum security strength of 112-bits, except for: — CCKs that are solely used by a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM.NOTE 1: Confidential cryptographic key is a defined term. Other secrets, whose disclosure cannot be used to compromise the user’s or subscriber’s privacy, such as secrets solely protecting intellectual property are not covered by the definition of confidential cryptographic key.NOTE 2: The requirement refers to all confidential cryptographic keys chosen by the equipment manufacturer either directly or imposed by a protocol. For instance, the manufacturer directly chooses/configures the cipher suite of TLS protocol to be used by the device, other protocols may impose one single option for cryptographic algorithms and their respective keys. | T |
| 6.9.2 | [CCK-2] CCK generation mechanisms |
| 6.9.2.1 | The generation of confidential cryptographic keys shall adhere to best practice cryptography, except for: — the generation of CCKs for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM. | T |
| 6.9.3 | [CCK-3] Preventing static default values for preinstalled CCKs |
| 6.9.3.1 | Preinstalled confidential cryptographic keys shall be practically unique per equipment, except for: — CCKs that are only used for establishing initial trust relationships under conditions controlled by an authorized entity; or — CCKs that are shared parameters required for the equipment’s intended functionality.NOTE: Confidential cryptographic key is a defined term. Other secrets, whose disclosure cannot be used to compromise the user’s or subscriber’s privacy, such as secrets solely protecting intellectual property are not covered by the definition of confidential cryptographic key. | T |
| **6.10** | **[GEC] GENERAL EQUIPMENT CAPABILITIES** |
| 6.10.1 | [GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities |
| 6.10.1.1 | The equipment shall not include publicly known exploitable vulnerabilities that, if exploited, affect security assets and privacy assets, except for vulnerabilities: — that cannot be exploited in the specific conditions of the equipment; or — that have been mitigated to an acceptable residual risk; or — that have been accepted on a risk basis. | T |
| 6.10.2 | [GEC-2] Limit exposure of services via related network interfaces |
| 6.10.2.1 | In factory default state the equipment shall only expose — network interfaces; and — services via network interfaces affecting security assets and privacy assets which are necessary for equipment setup or for basic operation of the equipment. | T |
| 6.10.3 | [GEC-3] Configuration of optional services and the related exposed network interfaces |
| 6.10.3.1 | Optional network interfaces or optional services exposed via network interfaces affecting security assets or privacy assets, which are part of the factory default state shall have the option for an authorized user to enable and disable the network interface or service. | T |
| 6.10.4 | [GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces |
| 6.10.4.1 | The equipment’s user documentation shall contain a description of — all exposed network interfaces; and — all services exposed via network interfaces, which are delivered as part of the factory default state. | T+P |
| 6.10.5 | [GEC-5] No unnecessary external interfaces |
| 6.10.5.1 | The equipment shall only expose physical external interfaces if they are necessary for its intended functionality. | T |
| 6.10.6 | [GEC-6] Input validation |
| 6.10.6.1 | The equipment shall validate input received via external interfaces if the input has potential impact on security assets and/or privacy assets. | T |
| 6.10.7 | [GEC-7] Documentation of external sensing capabilities |
| 6.10.7.1 | All external sensing capabilities of the equipment that are related to the user’s or subscriber’s privacy shall be documented for the user. | T+P |
| **6.11** | **[CRY] CRYPTOGRAPHY** |
| 6.11.1 | [CRY-1] Best practice Cryptography |
| 6.11.1.1 | The equipment shall use best practice for cryptography that is used for the protection of the security assets or privacy assets, except for:— cryptography used for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM. | T |

EN 18031-3标准要求

|  |  |  |
| --- | --- | --- |
| No. | **Reference Table b.1** | Technical / Process |
| **6.1** | **[ACM] Access control mechanism** |
| 6.1.1 | [ACM-1] Applicability of access control mechanisms |
| 6.1.1.1 | The equipment shall use access control mechanisms to manage entities' access to security assets and financial assets, except for access to security assets or financial assets where: — public accessibility is the equipment’s intended functionality; or — physical or logical measures in the equipment’s targeted operational environment limit their accessibility to authorized entities; or — legal implications do not allow for access control mechanisms. | T |
| 6.1.2 | [ACM-2] Appropriate access control mechanisms |
| 6.1.2.1 | Access control mechanisms that are required per ACM-1 shall ensure that only authorized entities have access to the protected security assets and financial assets. | T |
| **6.2** | **[AUM] Authentication mechanism** |
| 6.2.1 | [AUM-1] Applicability of authentication mechanisms |
| 6.2.1.1 | Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities’ access via network interfaces that allow to: — read confidential financial data, confidential financial function configuration or confidential security parameters; or — modify sensitive financial data, sensitive financial function configuration or sensitive security parameters; or — use financial functions or security functions. | T |
| 6.2.1.2 | Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities’ access via user interfaces that allow to: — read confidential financial data, confidential financial function configuration or confidential security parameters; or — modify sensitive financial data, sensitive financial function configuration or sensitive security parameters; or — use financial functions or security functions. | T |
| 6.2.1.3 | Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities’ access via machine interfaces that allow to: — read confidential financial data, confidential financial function configuration or confidential security parameters; or — modify sensitive financial data, sensitive financial function configuration or sensitive security parameters; or — use financial functions or security functions. | T |
| 6.2.2 | [AUM-2] Appropriate authentication mechanisms |
| 6.2.2.1 | Authentication mechanisms that are required per AUM-1-1 (network interface), AUM-1-2 (user interface) or AUM-1-3 (machine interface) shall verify an entity’s claim based on evidence derived from at least one element of the categories knowledge, possession and inherence (one factor authentication). | T |
| 6.2.2.2 | Authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) for access to financial functions via user interfaces over network interface that transfer money, monetary assets or virtual currencies shall verify an entity’s claim based on evidence derived from at least two different elements of the categories knowledge, possession and inherence (two factor authentication). | T |
| 6.2.3 | [AUM-3] Authenticator validation |
| 6.2.3.1 | Authentication mechanisms that are required per AUM-1-1 (network interface), AUM-1-2 (user interface) or AUM-1-3 (machine interface) shall validate all relevant properties of the used authenticators, dependent on the available information in the operational environment of use. | T |
| 6.2.4 | [AUM-4] Changing authenticators |
| 6.2.4.1 | Authentication mechanisms that are required per AUM-1-1, AUM-1-2 or AUM-1-3 shall allow for changing the authenticator except for authenticators where conflicting security goals do not allow for a change. | T |
| 6.2.5 | [AUM-5] Password strength |
| 6.2.5.1 | If factory default passwords are used by an authentication mechanism that is required per AUM-1-1, AUM-1-2 or AUM-1-3, they shall: — be unique per equipment; and — follow best practice concerning strength; or— be enforced to be changed by the user before or on first use. NOTE: The user can choose to not use any password. | T |
| 6.2.5.2 | If passwords other than factory default passwords are used by an authentication mechanism required per AUM-1-1, AUM-1-2 or AUM-1-3, they shall: — be enforced to be set by the user before or on first use and before the equipment is logically connected to a network; or — be defined by an authorized entity within a network where access is limited to authorised entities; or — be generated by the equipment using best practice concerning strength and only communicated to an authorized entity within a network where access is limited to authorised entities. NOTE: The user can choose to not use any password. | T |
| 6.2.6 | [AUM-6] Brute force protection |
| 6.2.6.1 | Authentication mechanisms required per AUM-1-1, AUM-1-2 or AUM-1-3 shall be resilient against brute force attacks. | T |
| **6.3** | **[SUM] SECURE UPDATE MECHANISM** |
| 6.3.1 | [SUM-1] Applicability of update mechanisms |
| 6.3.1.1 | The equipment shall provide at least one update mechanism for updating software, including firmware, affecting security assets and/or financial assets, except for software: — where functional safety implications do not allow updatability; or — which is immutable; or — where alternative measures protect the affected security assets and/or financial assets during the entire lifecycle of the equipment. | T |
| 6.3.2 | [SUM-2] Secure updates |
| 6.3.2.1 | Each update mechanism as required per SUM-1 shall only install software whose integrity and authenticity are valid at the time of the installation. | T |
| 6.3.3 | [SUM-3] Automated updates |
| 6.3.3.1 | Each update mechanism that is required per SUM-1 shall be capable of updating the software: — without human intervention at the equipment; or — via scheduling the installation of an update under human approval; or — via triggering the installation of an update under human approval or supervision where there is the need to prevent any unexpected damage in the operational environment. | T |
| **6.4** | **[SSM] SECURE STORAGE MECHANISM** |
| 6.4.1 | [SSM-1] Applicability of secure storage mechanisms |
| 6.4.1.1 | The equipment shall always use secure storage mechanisms for protecting the security assets and financial assets persistently stored on the equipment, except for persistently stored security assets and financial assets where: — the physical or logical measures in the target environment ensures the security asset or financial asset stored on the equipment accessibility is limited to authorized entities. | T |
| 6.4.2 | [SSM-2] Appropriate integrity protection for secure storage mechanisms |
| 6.4.2.1 | Each secure storage mechanism that is required per SSM-1 shall protect the integrity of security assets and financial assets it stores persistently. | T |
| 6.4.3 | [SSM-3] Appropriate confidentiality protection for secure storage mechanisms |
| 6.4.3.1 | Each secure storage mechanism that is required per SSM-1 shall protect the secrecy of confidential financial data, confidential financial function configuration, and of confidential security parameter persistently stored on the equipment. | T |
| **6.5** | **[SCM] SECURE COMMUNICATION MECHANISM** |
| 6.5.1 | [SCM-1] Applicability of secure communication mechanisms |
| 6.5.1.1 | The equipment shall always use secure communication mechanisms for communicating security assets and financial assets with other entities via network interfaces. | T |
| 6.5.2 | [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms |
| 6.5.2.1 | Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the integrity and authenticity of the security assets and financial assets communicated. | T |
| 6.5.3 | [SCM-3] Appropriate confidentiality protection for secure communication mechanisms |
| 6.5.3.1 | Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the confidentiality of communicated financial assets and security assets where confidentiality protection of those is needed. | T |
| 6.5.4 | [SCM-4] Appropriate replay protection for secure communication mechanisms |
| 6.5.4.1 | Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the security assets and the financial assets communicated against replay attacks, except for communicating security assets or financial assets where: — a duplicate transfer does not impose a threat of a replay attack. | T |
| **6.6** | **[LGM] LOGGING MECHANISM** |
| 6.6.1 | [LGM-1] Applicability of logging mechanisms |
| 6.6.1.1 | The equipment shall use logging mechanisms for internal activities that are relevant to financial assets and their protection (referred to as events), except for: — internal activities where a legal obligation prohibits logging. | T |
| 6.6.2 | [LGM-2] Persistent storage of log data |
| 6.6.2.1 | Logging mechanisms that are required per LGM-1 shall store log data for related events in the equipment’s persistent storage, except for events where: — related log data is stored outside the equipment. | T |
| 6.6.3 | [LGM-3] Minimum number of persistently stored events |
| 6.6.3.1 | All log data stored in equipment’s persistent storage by logging mechanisms that are required per LGM-1 and shall always include: — a minimum number of the latest events; and — the latest event. | T |
| 6.6.4 | [LGM-4] Time-related information of persistently stored dog data |
| 6.6.4.1 | All log data stored in equipment’s persistent storage by logging mechanisms that are required per LGM-1 shall include: — a timestamp if a real time is available on the equipment; and — time-related information if real time is not available on the equipment. | T |
| **6.7** | **[CCK] CONFIDENTIAL CRYPTOGRAPHIC KEYS** |
| 6.7.1 | [CCK-1] Appropriate CCKs |
| 6.7.1.1 | Confidential cryptographic keys that are preinstalled or generated by the equipment during its use shall support a minimum security strength of 112-bits, except for: — CCKs that are solely used by a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM. NOTE 1: Confidential cryptographic key is a defined term. Other secrets, whose disclosure cannot be used for fraud, such as secrets solely protecting intellectual property are not covered by the definition of confidential cryptographic key. NOTE 2: The requirement refers to all confidential cryptographic keys chosen by the equipment manufacturer either directly or imposed by a protocol. For instance, the manufacturer directly chooses/configures the cipher suite of TLS protocol to be used by the device, other protocols may impose one single option for cryptographic algorithms and their respective keys. | T |
| 6.7.2 | [CCK-2] CCK generation mechanisms |
| 6.7.2.1 | The generation of confidential cryptographic keys shall adhere to best practice cryptography, except for: — the generation of CCKs for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM. NOTE: Confidential cryptographic key is a defined term. Other secrets, whose disclosure cannot be used to harm the network or its functioning or for the misuse of network resources, such as secrets solely protecting intellectual property are not covered by the definition of confidential cryptographic key. | T |
| 6.7.3 | [CCK-3] Preventing static default values for preinstalled CCKs |
| 6.7.3.1 | Preinstalled confidential cryptographic keys shall be practically unique per equipment, except for: — CCKs that are only used for establishing initial trust relationships under conditions controlled by an authorized entity; or — CCKs that are shared parameters required for the equipment’s intended functionality. NOTE: Confidential cryptographic key is a defined term. Other secrets, whose disclosure cannot be used for fraud, such as secrets solely protecting intellectual property are not covered by the definition of confidential cryptographic key. | T |
| **6.8** | **[GEC] GENERAL EQUIPMENT CAPABILITIES** |
| 6.8.1 | [GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities |
| 6.8.1.1 | The equipment shall not include publicly known exploitable vulnerabilities that, if exploited, affect security assets and financial assets, except for vulnerabilities: — that cannot be exploited in the specific conditions of the equipment; or — that have been mitigated to an acceptable residual risk; or — that have been accepted on a risk basis. | T |
| 6.8.2 | [GEC-2] Limit exposure of services via related network interfaces |
| 6.8.2.1 | In factory default state the equipment shall only expose — network interfaces; and — services via network interfaces affecting security assets and financial assets which are necessary for equipment setup or for basic operation of the equipment. | T |
| 6.8.3 | [GEC-3] Configuration of optional services and the related exposed network interfaces |
| 6.8.3.1 | Optional network interfaces or optional services exposed via network interfaces affecting security assets or financial assets, which are part of the factory default state shall have the option for an authorized user to enable and disable the network interface or service. | T |
| 6.8.4 | [GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces |
| 6.8.4.1 | The equipment's user documentation shall contain a description of — all exposed network interfaces; and — all services exposed via network interfaces, which are delivered as part of the factory default state. | T+P |
| 6.8.5 | [GEC-5] No unnecessary external interfaces |
| 6.8.5.1 | The equipment shall only expose physical external interfaces if they are necessary for its intended functionality. | T |
| 6.8.6 | [GEC-6] Input validation |
| 6.8.6.1 | The equipment shall validate input received via external interfaces if the input has potential impact on security assets and/or financial assets. | T |
| 6.8.8 | [GEC-8] Equipment Integrity |
| 6.8.8.1 | Equipment, which processes financial data, shall cryptographically verify the boot process integrity and authenticity of its software (provided by the manufacturer or its sub-contractor), using a root of trust which is immutable or, mutable under cryptographically authenticated authorization, for each part of its software which processes financial assets and security assets. | T |
| **6.9** | **[CRY] CRYPTOGRAPHY** |
| 6.9.1 | [CRY-1] Best practice Cryptography |
| 6.9.1.1 | The equipment shall use best practice for cryptography that is used for the protection of the security assets or financial assets, except for: — cryptography used for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM. | T |