歐盟RED指令資安合規：
EN 18031自我評估與測試實務研習

innovating safety & security

RED-DA現況說明

RED Essential Requirements

Directive defines the **Essential Requirements**:

- Provide an overview of the **mandatory technical requirements**
- Give the objective(s) to be met, but **do not specify how**
- **Do not call out technical standards**, refers to private standards-making bodies to draw up product standards (ETSI, IEC, CENELEC,…)
- **Compliance** with the Essential Requirements **is Mandatory**

Essential Requirements			
Article 3.1(a) Health & Safety of the user and animals, but no voltage limit applying **[Equivalent to LVD]**	**Article 3.1(b)** Adequate level of Electromagnetic Compatibility (EMC) **[Equivalent to EMCD]**	**Article 3.2** Efficient use of radio spectrum in order to avoid harmful interference (RF)	**Article 3.3** **Additional Requirements** where decided by European Commission CYBER

3.1(a) – Health and Safety

- RF-Exposure: SAR or MPE
- Safety Hazards: Electrical, Mechanical, Chemical, Thermal, Acoustic,…

3.1(b) – EMC

- Emissions: Radiated and Conducted
- Immunity: Radiated and Conducted

3.2 – RF

- Transmitter and Receiver performance to avoid harmful interference

3.3 – Additional Requirements

- Common Charger for Mobile Phones
- Access to Emergency Services (e.g. Avalanche Beacons, EU-Alert,…)
- Network Protection [*]
- Protection of personal data and privacy [*]
- Protection from Fraud [*]
- Facilitate the device use by users with a disability
- Software Radio (SDR)

Delegated Act of Radio Equipment Directive

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

RED-DA

Cybersecurity (3.3 d/e/f) applicable from August 2025

RED Delegated Regulation (2022/30) activates RED requirements 3.3.d/e/f

3.3.d
Radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service.

3.3.e
Radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected.

3.3.f
Radio equipment supports certain features ensuring protection from fraud.

EXEMPTIONS for RED requirements 3.3.d/e/f

The following radio equipment is fully exempted from RED Articles 3.3(d), 3.3(e) and 3.3(f):

- Medical devices under Regulation (EU) 2017/745 and (EU) 2017/746.

The following radio equipment is exempted from RED Articles 3.3(e) and 3.3(f), but article 3.3(d) still applies:

- Radio equipment under Regulation (EU) 2018/1139 (civil aviation).
- Radio equipment under Regulation (EU) 2019/2144 (motor vehicles).
- Radio equipment under Directive (EU) 2019/520 (road toll systems).

Updated Timeline

Updated application date confirmed on 20 July 2023

Transition period

12 January 2022

Delegated Regulation (EU) 2022/30 published.

1 August 2025

Application

Be Harmonized
30 January 2025

European Commission

5 August 2022

Standardization Request

7 September 2022

Request accepted;
Standards works started

03 February 2023

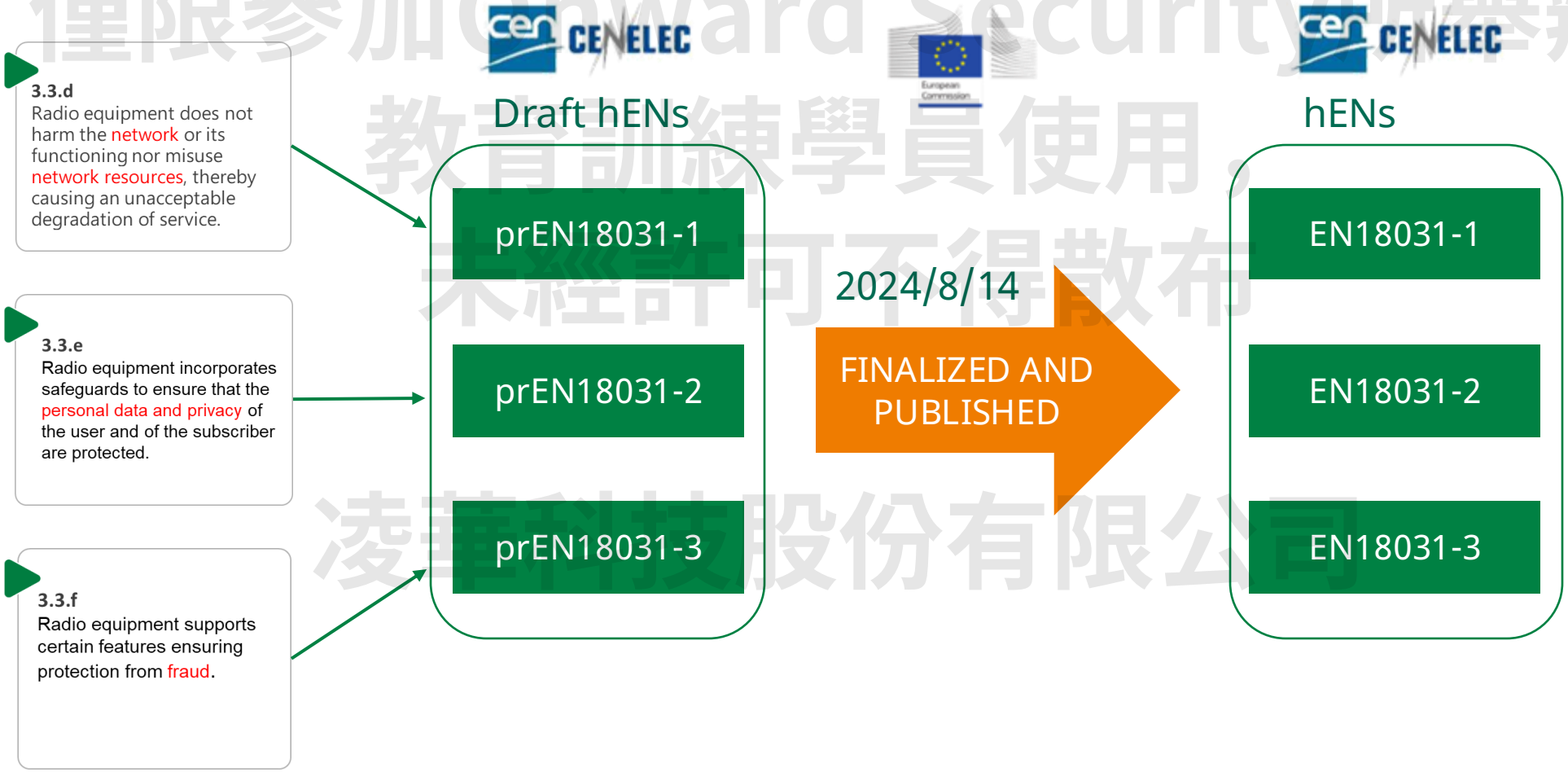
Circulation of 1st WD

14 August 2024

Publication

WE ARE HERE

RED-DA Regulation Current Status



How will the manufacturers comply with this Regulation?

01 Perform a self-assessment, when their product has been designed in accordance with **harmonised standards.**

02 Rely on a third-party assessment performed by an independent inspection body, regardless of **whether or not a harmonised standard was used.**

A Conformance Assessment will be available when the harmonised standards are in place. In the meantime DEKRA can issue a **EU Type Examination Certificate**.

KEY Restrictions in EN 18031 HS

Article 3.3 d

- **Clause 6.2.5.1 and 6.2.5.2 Password authentication requirements**

If the device allows users not to set or use a password, it does not meet the essential requirement under Article 3(3)(d) (network protection)

Notified Body is not required if:

The product fully complies with EN 18031-1 without relying on restricted clauses (password authentication)

Notified Body is required if:

The product allows operation without password authentication

KEY Restrictions in EN 18031 HS

Article 3.3 e

- **Clauses 6.1.3, 6.1.4, 6.1.5, and 6.1.6 Parental/guardian access controls**

If parental control is not properly implemented, it does not meet the essential requirement under Article 3(3)(e) (data and privacy protection)

- **Clause 6.2.5.1 and 6.2.5.2 Password authentication requirements**

If the device allows users not to set or use a password, it does not meet the essential requirement under Article 3(3)(e) (data and privacy protection)

Notified Body is not required if:

The product fully complies with EN 18031-2 without relying on restricted clauses (password authentication and parental control)

Notified Body is required if:

- **The product allows operation without password authentication**
- **No parental control is implemented for childcare devices and toys**

KEY Restrictions in EN 18031 HS

Article 3.3 f

- **Clause 6.2.5.1 and 6.2.5.2 Password authentication requirements**

If the device allows operation without a password, it does not meet the essential requirement under Article 3(3)(f) (fraud protection)

- **Clause 6.3.2.4 Secure update mechanisms for financial transactions**

Different implementation categories are laid down, based on digital signatures, secure communication mechanisms, access control mechanisms or others, but none of the methods alone is sufficient for a product that handle financial assets

If multiple layers of security are not implemented, the product does not meet the essential requirement under Article 3(3)(f)

Notified Body is required in all cases for Article 3(3)(f)

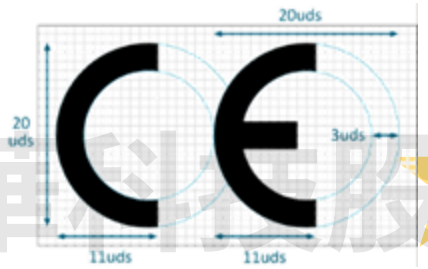
CE Marking Normative Framework

CE Marking refers to the process through which the manufacturer/importer informs users and the competent authorities that the device being sold complies with the essential requirements established by mandatory legislation.

The Manufacturer is responsible for the certification procedures and, where applicable, conformity certification for a product.

Manufacturers must follow these steps to **affix a CE Marking** to their products:

1. Identify the applicable **Directive(s) and Harmonized Standards**
2. Verify **product specific requirements**
3. Identify whether an independent conformity assessment (by a **Notified Body**) is necessary
4. **Test the product** and check its conformity
5. Draw up and keep available the required **Technical Documentation**
6. Affix the **CE marking** and draw up the **EU Declaration of Conformity**



Further Information: http://ec.europa.eu/growth/single-market/ce-marking/

Products and CE Directives

Electric and Electronic Engineering
- Electromagnetic compatibility (EMC)
- Low Voltage (LVD)
- **Radio Equipment (RED)**
- Restriction of the use of certain hazardous substances (RoHS)

Healthcare Engineering
- Active implantable medical devices
- In vitro diagnostic medical devices
- Medical devices (MDD)

Measuring Technology
- Measuring instruments (MID)
- Non-automatic weighing instruments (NAWI)

Consumers and Workers Protection
- Cosmetics products
- General product safety
- Personal protective equipment (PPE)
- Toys safety

Construction
- Construction products (CPD/CPR)

Energy Efficiency
- Ecodesign and energy labelling

Sustainability
- Packaging and packaging waste

Mechanical Engineering and Means of Transport
- Machinery (MD)
- Pressure equipment (PED)
- Equipment for explosive atmospheres (ATEX)
- Gas appliances (GAR)
- Lifts
- Cableway installations designed to carry persons
- Inspection of pesticide application equipment
- Rail system: interoperability
- Recreational craft and personal watercraft
- Simple Pressure Vessels (SPVD)
- Noise emission in the environment

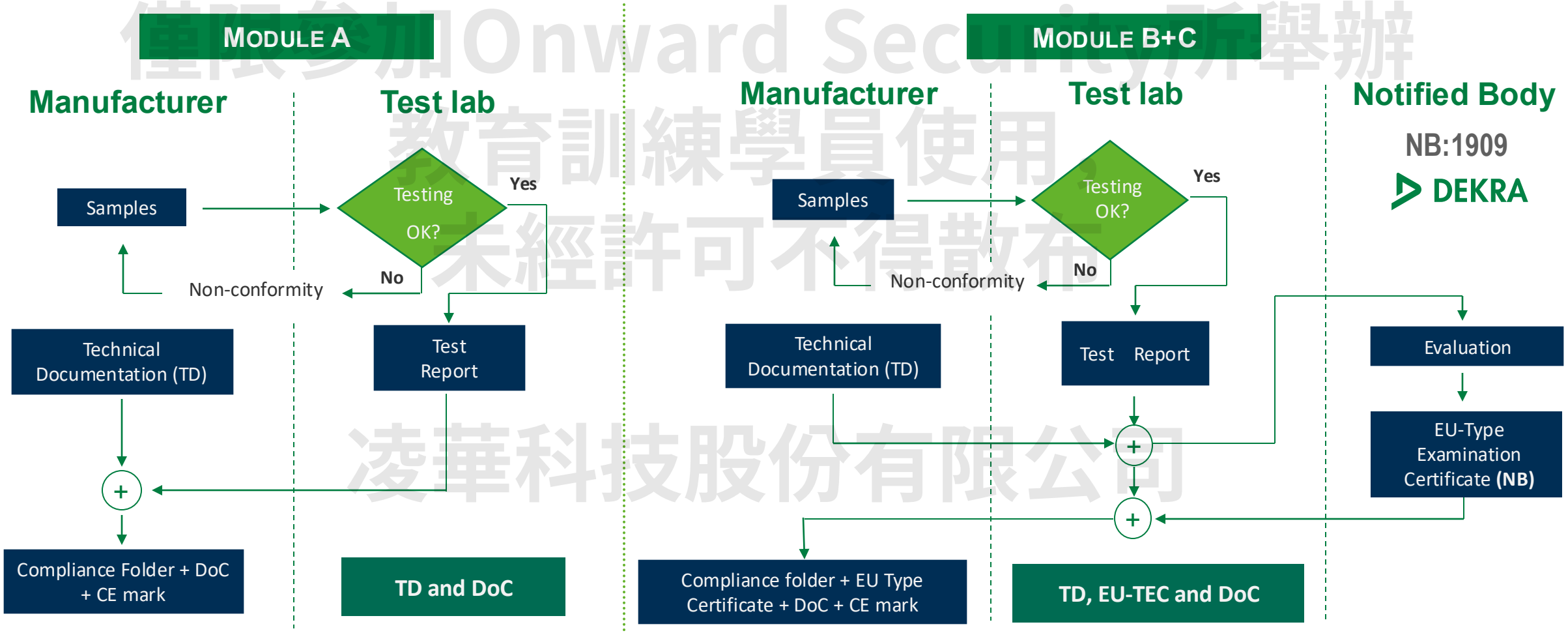
Chemicals
- Chemical Substances (REACH)
- Explosives for civil uses
- Pyrotechnic articles

Accessibility
- Websites and mobile applications of public sector bodies

Conformity Assessment and Management Systems
- New Legislative Framework (NLF) and Eco-Management and Audit Scheme (EMAS)

Services
- Community postal services

Conformity Assessment Modules



Test Reports: EMC, RF, Safety, MPE/SAR, **Cyber**

Technical Documentation: Schematics, BOM, PCB Layout, Operational Description, Internal/External Pictures, User Manual,…

Example of EU-TEC issued by DEKRA NB

DEKRA

DEKRA Testing and Certification, S.A.U.

Product certification body accredited by ENAC with accreditation No. 134/C-PR301
and designated by the competent national authority of Spain
to act as Notified Body (Notified Body No: 1909) in accordance with the Directive 2014/53/EU of 16 April 2014

Directive 2014/53/EU – EU-TYPE EXAMINATION CERTIFICATE

Identification Number: XXXXXRNB.001
Issue date: 2022-11-28

MANUFACTURER DETAILS:

Company name: ACME, Inc.
Address: Rue do Percebe 13, 11300 A Coruña, Spain

EQUIPMENT DETAILS:

Type of equipment: Wireless module
Brand name: ACME
Model names: Sample 1
HW version: -1.0
SW version: A17.15

SCOPE OF OPINION:

Essential requirements	Specifications / Standards	Submitted documents
Article 3.3 (d)	prEN 18031-1:2023, draft V3	Test report
Article 3.3 (e)	prEN 18031-2:2023, draft V3	Test report

Signed on behalf of DEKRA Testing and Certification, S.A.U. in Malaga (Spain)

Name: Ricardo Orejas
Position: Responsible for Certification

FDB027_65 /DEKRA Testing and Certification, S.A.U. Parque Tecnológico de Andalucía C/ Severo Ochoa, 2 & 6 – 29590 Málaga Spain /

DEKRA

Annex I to EU-Type Examination Certificate No. XXXXXRNB.001

TECHNICAL DOCUMENTATION:

Held at: ACME, Inc.
Address: Rue do Percebe 13, 11300 A Coruña, Spain

TECHNICAL FEATURES AND CHARACTERISTICS:

Operating frequency bands: E-GSM 900: Transmitter 880-915MHz, Receiver 925-960MHz
DCS 1800: Transmitter 1710-1785MHz, Receiver 1805-1880MHz
E-UTRA Band 1: 1920.1 ~ 1979.9 MHz / 2110.1 ~ 2169.9 MHz
E-UTRA Band 3: 1710.1 ~ 1784.9 MHz / 1805.1 ~ 1879.9 MHz
E-UTRA Band 20: 832.1 ~ 861.9 MHz / 791.1 ~ 820.9 MHz
E-UTRA Band 28: 703.1 ~ 747.9 MHz / 758.1 ~ 802.9 MHz
GNSS (receiver): 1575.42 MHz, 1561.098 MHz, 1598.0625 ~ 1605.375 MHz
Modulations: GMSK, 8PSK, EPSK, QPSK, 16QAM
Output power: GSM/GPRS900 32 dBm +1.5/-1 dB,
DCS/GPRS1800 29 dBm +1.5 /-1 dB
EGPRS900: 28 dBm +1/-1 dB, EGPRS1800 26 dBm +1/-1 dB
All LTE FDD bands: +23 dBm
GNSS: 1559 - 1610 MHz receiver only
Operating voltage: 3.4 VDC to 4.8 VDC (Nominal: 4.0 VDC)
Operating temperature: -10 ºC to 55 ºC
Antenna: External antenna
Intended use: Module for coyote's traps
Network harm, privacy and fraud supported data:
Internet access ☒
Personal data ☒
Traffic data ☒
Location data ☒
Financial data ☐

CONFORMITY DETAILS:

Essential requirements	Specifications / Standards	Reference documents
Article 3.3 (d)	prEN 18031-1:2023, draft V3	73592RCS.001, Appendix A.1
Article 3.3 (e)	prEN 18031-2:2023, draft V3	73592RCS.001, Appendix A.1

REMARKS AND COMMENTS:

It is mandatory to inform DEKRA Testing and Certification, S.A.U. in writing about any change in the approved equipment identified in this certificate, which could affect the conformity of the apparatus with the essential requirements or the conditions of validity of this certificate.

This device has been evaluated on a test jig. This radio module is for professional installation only. When installing this radio module permanently into a host product to a create new radio equipment device; the manufacturer responsible for placing the final radio product on the market in the EU must assess if the combination of this radio module and the host product complies with the essential requirements of the RE Directive 2014/53/EU.

Host devices integrating this device will need to be evaluated according to the essential requirements of Directive 2014/53/EU following the guidelines provided in the document "REDCA Technical Guidance Note 01 on the RED compliance requirements for a Radio Equipment often referred to as Radio Module and the Final Radio Equipment Product that integrates a Radio Module". This Technical Guidance Note may be accessed in RED Compliance Association website or may be obtained by contacting with DEKRA Testing and Certification, S.A.U. Notified Body at certification.rcb.es@dekra.com.

FDB027_65 /DEKRA Testing and Certification, S.A.U. Parque Tecnológico de Andalucía C/ Severo Ochoa, 2 & 6 – 29590 Málaga Spain /

Essential requirements	Specifications / Standards	Submitted documents
Article 3.3 (d)	prEN 18031-1:2023, draft V3	Test report
Article 3.3 (e)	prEN 18031-2:2023, draft V3	Test report

EU Declaration of Conformity (example)

RE-D Declaration of Conformity (DoC)

Unique identification of this DoC: XXXX

We, <Company Name>
<Address>

declare under our sole responsibility that the product:

Product: XXXX
Type: XXXX
Batch or Serial number: XXXX

Optional: colour image for the identification of the radio equipment

, object of the declaration described above is in conformity with the relevant Union harmonization Legislation: Directive 2014/53/EU (include other Directives as applicable).

The following harmonized standards and/or other normative documents were applied:

SAFETY (art 3.1.a): EN 62311:2008 and EN 60950-1:2006 + A11:2009 + A12:2011 + A1:2010 + AC:2011 + A2:2013
EMC (art 3.1.b): EN 301 489-1 V2.1.1 + Draft EN 301 489-17 V3.2.0
RADIO SPECTRUM (art 3. 2): EN 300 328 V2.1.1
CYBERSECURITY (art 3.3): EN 18031-1/-2/-3

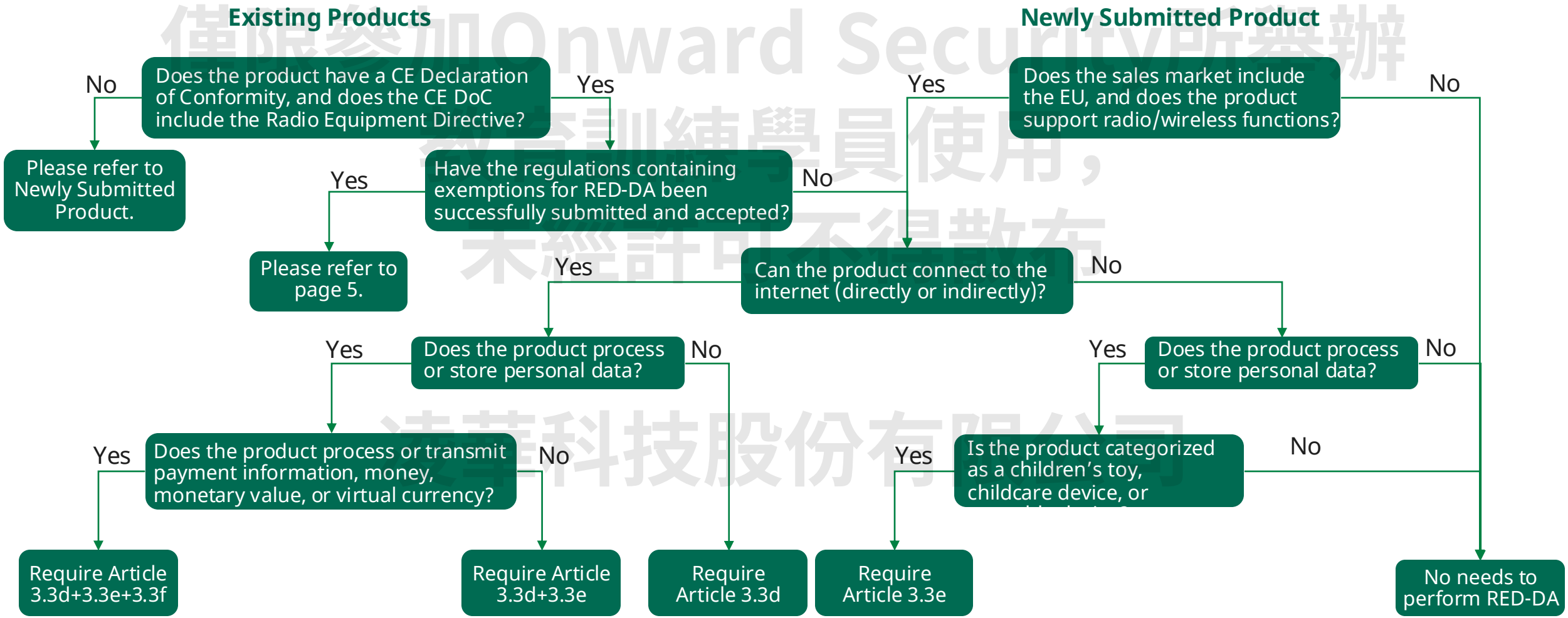
Not yet possible!!!

Supplementary Information:
Where applicable, the **notified body**... (name, number)... performed... (description of intervention)... and issued the EU-type examination certificate:...
*Where applicable, description of **accessories** and components, including **software**, which allow the radio equipment to operate as intended and covered by the EU declaration of conformity:*

Signed for and on behalf of: <COMPANY NAME>
Place and date of issue: <Place and date>
<(name, function) (signature)>

如何知道產品是否適用RED-DA

How to Determine If your Product Requires RED-DA Testing



EU Declaration of Conformity

EU Declaration of Conformity CE

We, the undersigned,

Additional information: ANNEX I

The object of the declaration described above is in conformity with the relevant Union harmonisation legislation:

EMC Directive – 2014/30/EU

EN 55024:2010/A1:2015 , EN 55032:2015/AC:2016 , EN 61000-3-2:2014 , EN 61000-3-3:2013

Low Voltage Directive – 2014/35/EU

EN 62368-1:2014

RoHS Directive – 2011/65/EU

2015/863/EU , EN 50581:2012

Product name: External SSD Enclosure
Model name: ESD-S1C, ESD-S1CL

Additional information: ANNEX I

The object of the declaration described above is in conformity with the relevant Union harmonisation legislation:

EMC Directive – 2014/30/EU

EN 55024:2010/A1:2015 , EN 55032:2015/AC:2016 , EN 61000-3-2:2014 , EN 61000-3-3:2013

Low Voltage Directive – 2014/35/EU

EN 62368-1:2014

RoHS Directive – 2011/65/EU

2015/863/EU , EN 50581:2012

EU Declaration of Conformity

Additional information: ANNEX I

The object of the declaration described above is in conformity with the relevant Union harmonisation legislation:

Radio Equipment Directive – 2014/53/EU

Article 3.1(a)
EN 62311:2008 , EN 62368-1:2014 , EN60950-1:2006/A11:2009/A1:2010/A12:2011/A2:2013
Article 3.1(b)
EN 301 489-1 V2.2.3 , EN 301 489-17 V3.1.1 , EN 301 489-3 V2.1.1 , EN 55024:2010/A1:2015 ,
EN 55032:2015/AC:2016 , EN 61000-3-2:2014 , EN 61000-3-3:2013
Article 3.2
EN 300 328 V2.2.2 , EN 300 440 V2.2.1 , EN 301 893 V2.1.1

EU-Type Examination :
Certificate Number : 1622-RED-203808
Notified Body : Nemko
Notified Body number : 1622

Radio Equipment Class
Class 2

Ecodesign Directive – 2009/125/EC
617/2013/EU

RoHS Directive – 2011/65/EU
2015/863/EU , EN 50581:2012

Additional information: ANNEX I

The object of the declaration described above is in conformity with the relevant Union harmonisation legislation:

Radio Equipment Directive – 2014/53/EU

Article 3.1(a)
EN 62311:2008 , EN 62368-1:2014 , EN60950-1:2006/A11:2009/A1:2010/A12:2011/A2:2013
Article 3.1(b)
EN 301 489-1 V2.2.3 , EN 301 489-17 V3.1.1 , EN 301 489-3 V2.1.1 , EN 55024:2010/A1:2015 ,
EN 55032:2015/AC:2016 , EN 61000-3-2:2014 , EN 61000-3-3:2013
Article 3.2
EN 300 328 V2.2.2 , EN 300 440 V2.2.1 , EN 301 893 V2.1.1

EU-Type Examination :
Certificate Number : 1622-RED-203808
Notified Body : Nemko
Notified Body number : 1622

Radio Equipment Class
Class 2

Overview

- Access Control
- Authentication
- Secure Update / Storage
- SCM / RLM / NMM / TCM
- Logging / Notification / Deletion
- Crypto
- General

RED 3.3(d), (e), (f) 適用產品

Article 3(3), point (d)

- 任何能夠透過網際網路自行通訊的無線電設備，無論是直接連線還是透過其他設備進行通訊，皆屬於「可連網無線電設備」。

Article 3(3), point (e)

適用於下列任何無線電設備，只要該無線電設備能夠處理個人資料、通訊資料或定位資料：

- 可連網的無線電設備（一部設備除外）
- 專為兒童照護設計或預定用途的無線電設備
- 受 2009/48/EC 指令規範的無線電設備
- 設計或預定（無論是否專為此用途）佩戴於、綁在或掛於以下任一位置的無線電設備：人體任何部位，包括頭部、頸部、軀幹、手臂、手、腿和腳人體穿戴的任何衣物，包括頭飾、手部穿戴物和鞋類

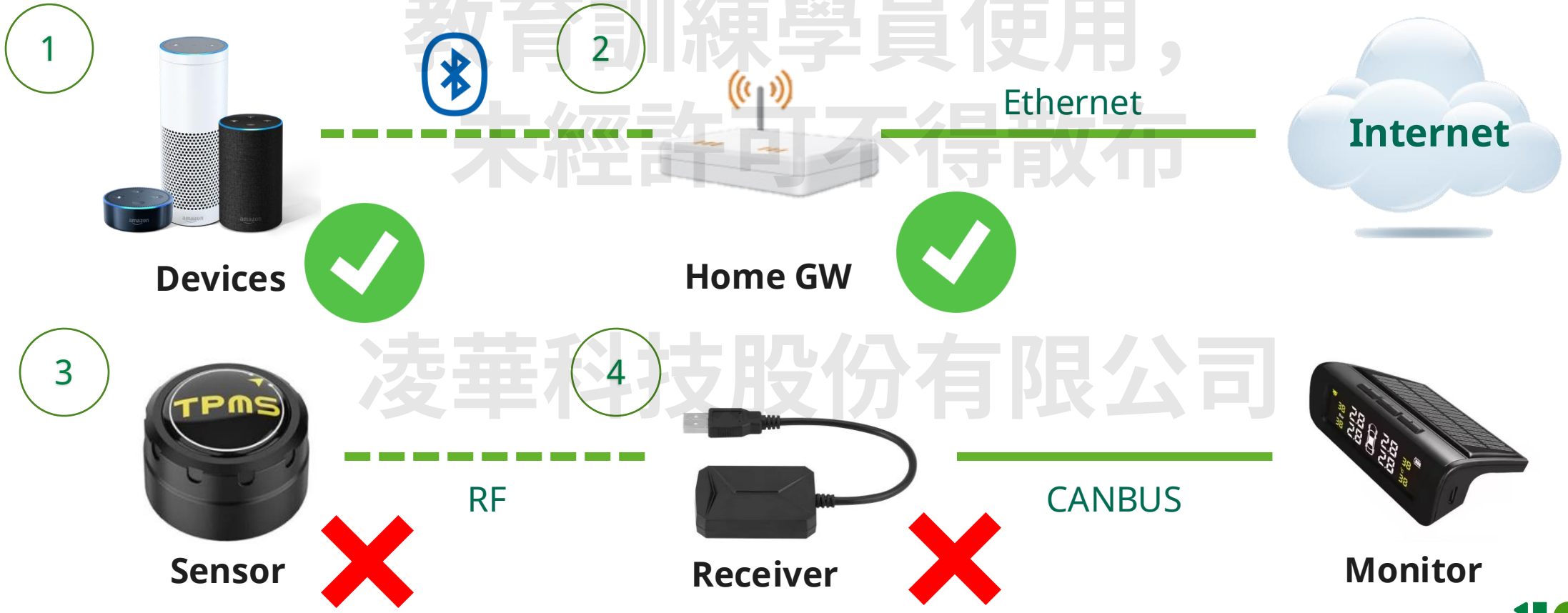
Article 3(3), point (f)

- 任何可連網的無線電設備，只要該設備使持有者或使用者能夠轉移金錢、貨幣價值或虛擬貨幣，就屬於此範疇。

Source: https://eur-lex.europa.eu/eli/reg_del/2022/30/oj

適用 RED-DA 條款與條件

符合／不符合 RED 第 3.3(d) 條的情境範例



適用 RED-DA 條款與條件

符合／不符合 RED 第 3.3(e) 條的情境範例

Stored & Process

Data transmission

1

2

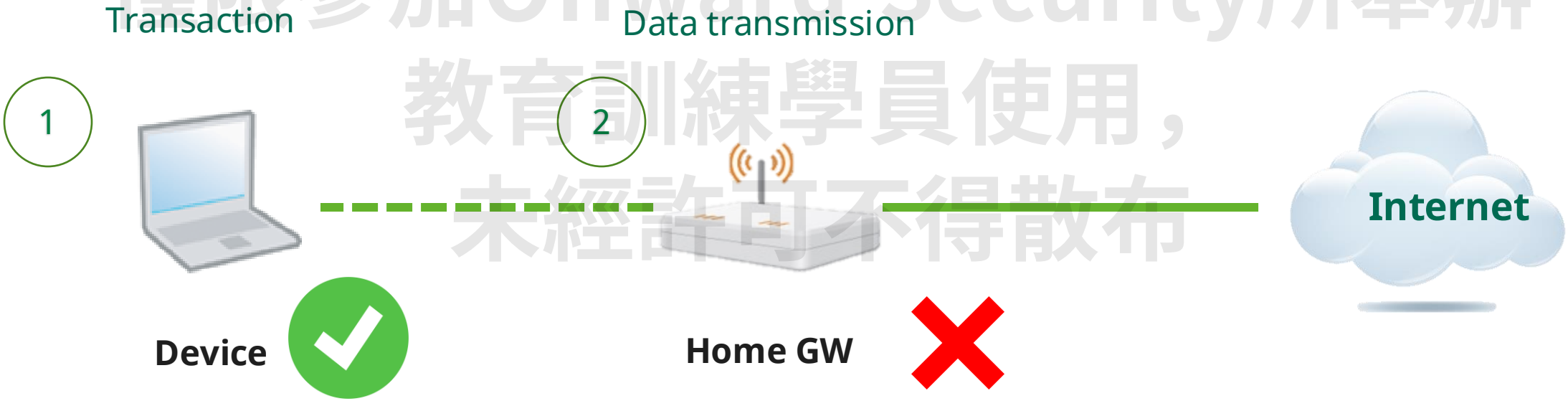
IPCam

Home GW

個人資料：密碼、照片、影片、身份證明、生物識別資訊等

適用 RED-DA 條款與條件

符合／不符合 RED 第 3.3(f) 條的情境範例



RED指令與 EN 18031 安全要求對應 (1/2)

EN 18031-1:2024, EN 18031-2:2024, EN 18031-3:2024 (release on 2024-08-14)

安全要求類型	安全要求	3.3(d)	3.3(e)	3.3(f)
[ACM] Access control mechanism	[ACM-1] Applicability of access control	X	X	X
	[ACM-2] Appropriate access control	X	X	X
	[ACM-3] Default access control for children in toys		X	
	[ACM-4] Default access control to children's privacy assets for toys and childcare equipment		X	
	[ACM-5] Parental/Guardian access controls for children in toys		X	
	[ACM-6] Parental/Guardian access controls for other entities' access to managed children's privacy assets in toys		X	
[AUM] Authentication mechanism	[AUM-1] Applicability of authentication mechanisms	X	X	X
	[AUM-2] Appropriate authentication mechanisms	X	X	X
	[AUM-3] Authenticator validation	X	X	X
	[AUM-4] Changing authenticators	X	X	X
	[AUM-5] Password strength	X	X	X
	[AUM-6] Brute force protection	X	X	X
[SUM] Secure update mechanism	[SUM-1] Applicability of secure update mechanisms	X	X	X
	[SUM-2] Secure updates	X	X	X
	[SUM-3] Automated updates	X	X	X
[SSM] Secure storage mechanism	[SSM-1] Applicability of secure storage mechanisms	X	X	X
	[SSM-2] Appropriate integrity protection for secure storage mechanisms	X	X	X
	[SSM-3] Appropriate confidentiality protection for secure storage mechanisms	X	X	X
[SCM] Secure communication mechanism	[SCM-1] Applicability of secure communication mechanisms	X	X	X
	[SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms	X	X	X
	[SCM-3] Appropriate confidentiality protection for secure communication mechanisms	X	X	X
	[SCM-4] Appropriate replay protection for secure communication mechanisms	X	X	X

RED指令與 EN 18031 安全要求對應 (2/2)

EN 18031-1:2024, EN 18031-2:2024, EN 18031-3:2024 (release on 2024-08-14)

安全要求類型	安全要求	3.3(d)	3.3(e)	3.3(f)
[LGM] Logging mechanism	[LGM-1] Applicability of logging mechanisms		X	X
	[LGM-2] Persistent storage of log data		X	X
	[LGM-3] Minimum number of persistently stored events		X	X
	[LGM-4] Time-related information of persistently stored log data		X	X
[DLM] Deletion mechanism	[DLM-1] Applicability of deletion mechanisms		X	
[RLM] Resilience mechanism	[RLM-1] Applicability and appropriateness of resilience mechanisms	X		
[NMM] Network monitoring mechanism	[NMM-1] Applicability and appropriateness network monitoring mechanisms	X		
[TCM] Traffic control mechanism	[TCM-1] Applicability of and appropriate traffic control mechanisms	X		
[UNM] User notification mechanism	[UNM-1] Applicability of user notification mechanisms		X	
	[UNM-2] Content of user notification		X	
[CCK] Confidential cryptographic keys	[CCK-1] Appropriate CCKS	X	X	X
	[CCK-2] CCK generation mechanisms	X	X	X
	[CCK-3] Preventing static default values for preinstalled CCKs	X	X	X
[GEC] General equipment capabilities	[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities	X	X	X
	[GEC-2] Limit exposure of services via related network interfaces	X	X	X
	[GEC-3] Configuration of optional service and the related exposed network interfaces	X	X	X
	[GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces	X	X	X
	[GEC-5] No unnecessary external interfaces	X	X	X
	[GEC-6] Input validation	X	X	X
	[GEC-7] Documentation of external sensing capabilities		X	
	[GEC-8] Equipment Integrity			X
[CRY] Cryptography	[CRY-1] Best practice cryptography	X	X	X

EN 18031 資安要求架構介紹

XXX Requirement

XXX-1
Applicability of mechanisms

- Requirement
- Rationale
- Guidance

Assessment Criteria

- Assessment objective
- Required information
- *Assessment Type*
  - Conceptual
  - Functional completeness
  - Functional sufficiency

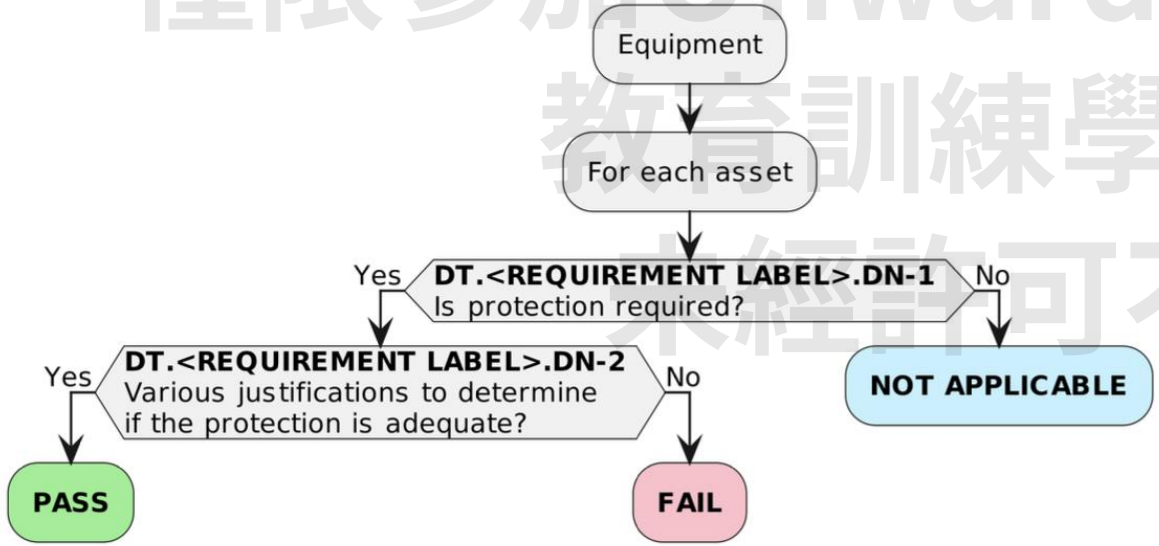
XXX-2
Appropriate mechanisms

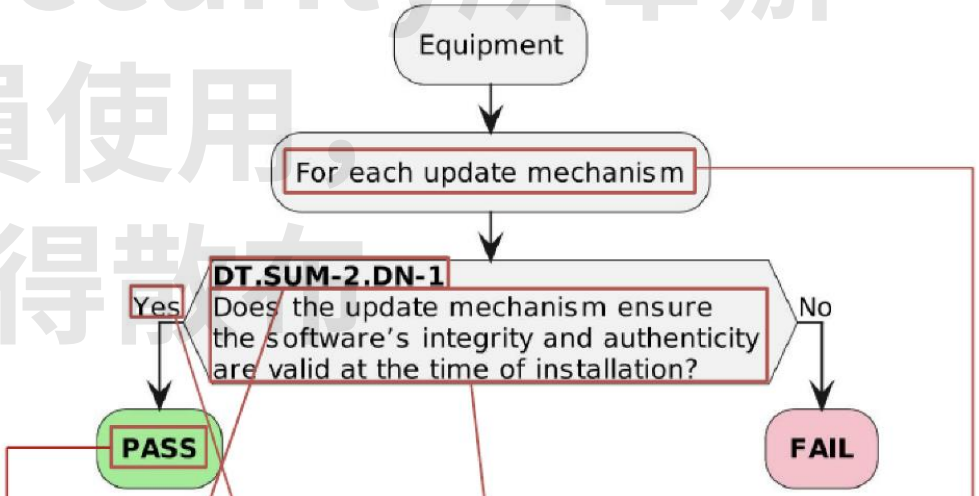
- XXX-# Supporting Requirements
- XXX-# Supporting Requirements
- XXX-# Supporting Requirements
- XXX-# Supporting Requirements

評估方式差異說明

ETSI TS 103 701	Conceptual	Functional	
EN 18031	**Conceptual**	**completeness**	**sufficiency**
目的	檢查所提供的文件和理由是否充分提供所需的證據	檢查並測試提供的文件是否完整	檢查並測試實作是否適當 1) 識別宣告差異 實作方式與書面資料宣告是否一致 2) 識別潛在問題 直接對設備評估其實作是否滿足文件要求
範例 (以ACM-1為例)	所有應管制的資產都有對應的存取控制機制(Access control mechanism)；無需管制的資產，皆有標準本身定義可接受的理由進行排除，且其理由充份且正當	檢查廠商是否已經宣告所有的資產	確認每一個應管制的資產，所使用的存取控制機制與廠商宣告一致

• Decision trees





Identifier	Online Firmware Update Mechanism		
Decision Node	**Decision** [E.Info.DT.SUM-2]		**Justification** [E.Just.DT.SUM-2]
DT.SUM-2.DN-1	Yes (X)	No	The update mechanism validates the integrity and authenticity of an update using a digital signature which is included in the update file (as described in E.Info.SUM-2.SUM.Sign). The update is solely installed if the signature belongs to an authorized entity at the time of installation.
Verdict	Pass		

技術文件 (Technical documentation)

- 預定設備功能資訊
- 設備的技術資訊
- 針對特定使用情境所聲明的最佳實務
- 具體細節，例如外部介面清單
- 資安風險評估

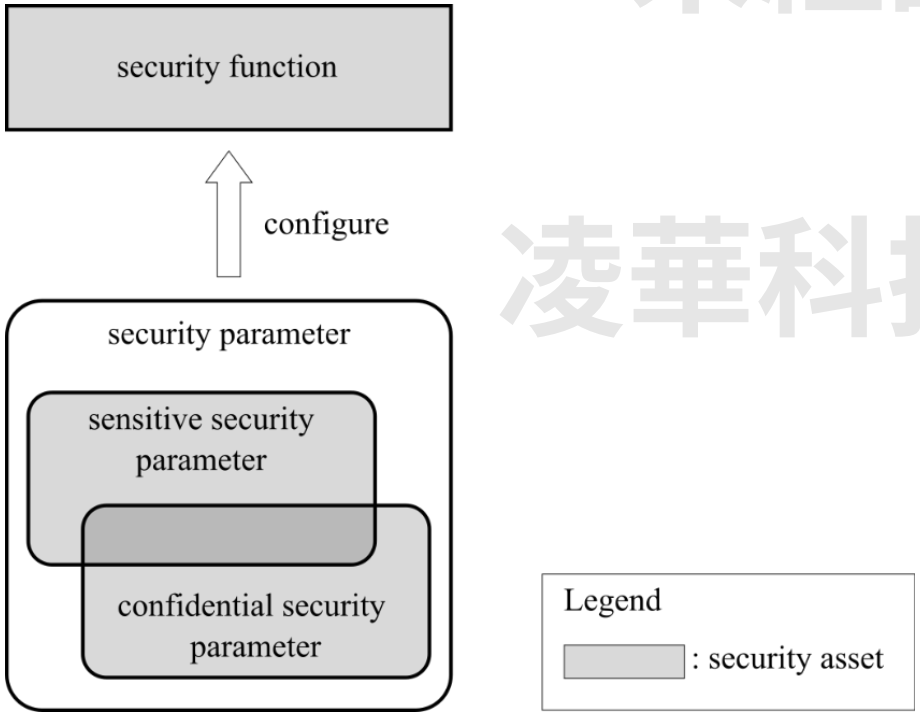
資產 (Assets)

EN 18031-1	X	X		
EN 18031-2	X		X	
EN 18031-3	X			X

適用標準 資產定義	安全資產 Security asset	網路資產 Network asset	隱私資產 Privacy asset	金融資產 Financial asset
資料			X	X
功能	直接影響設備完整性	• 存取網路能力 • 提供網路服務	直接影響隱私資料	直接影響金融資料
設定	X	X	X	X
敏感安全參數	X	X	X	X

安全資產的定義

- 設備的安全功能，若會直接影響設備完整性者，或
- 設備所使用的與資安相關的設定，或
- 影響設備安全功能行為的資料，或
- 設備為確保其完整性所使用的敏感安全參數



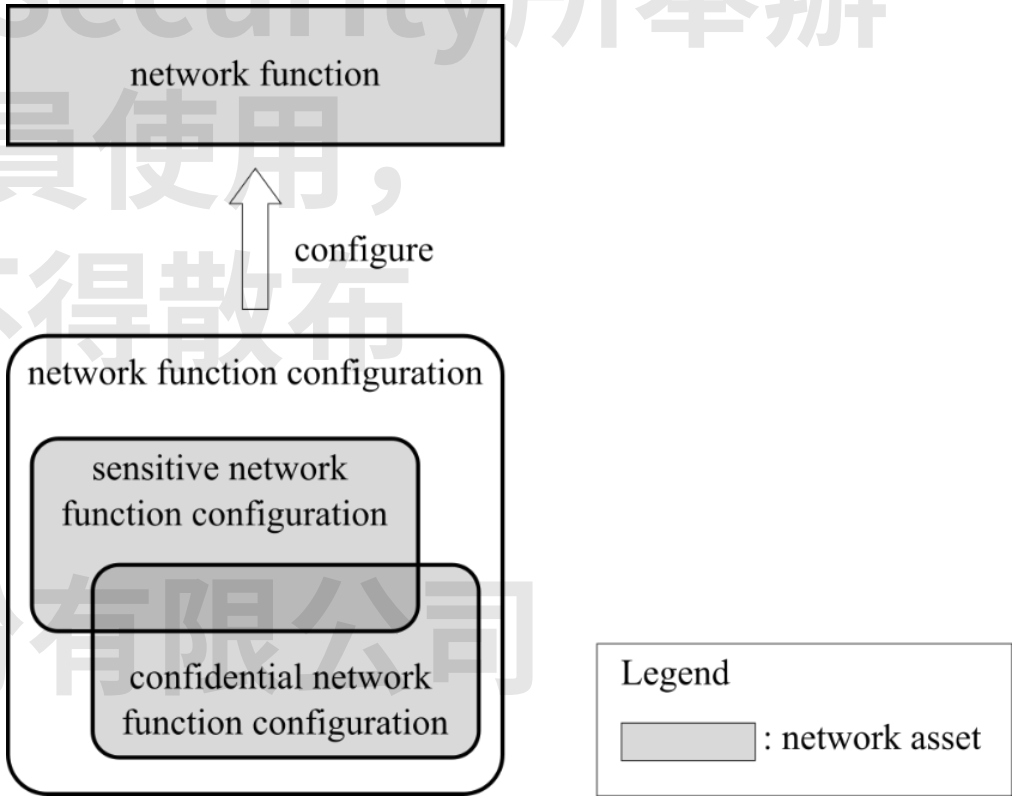
例如：存取控制機制的實作

- 機密安全參數（Confidential Security Parameter, CSP）是指一種與安全相關的機密資訊，其洩漏可能會危及資產安全。典型的例子包括：PIN 碼、密碼、對稱式加密金鑰或非對稱式加密的私鑰。
- 敏感安全參數（Sensitive Security Parameter, SSP）則是指一種與安全相關的資訊，其被竄改可能會危害資產的安全。常見的例子包括：對稱式與非對稱式加密金鑰，或是存取權限設定等。

網路資產的定義

包含：

- 網路功能、或
- 設備用以存取網路功能的功能、或
- 設備所使用的網路功能設定、或
- 決定設備網路功能行為的資料、或
- 儲存在設備中、用於存取網路資源的敏感安全參數



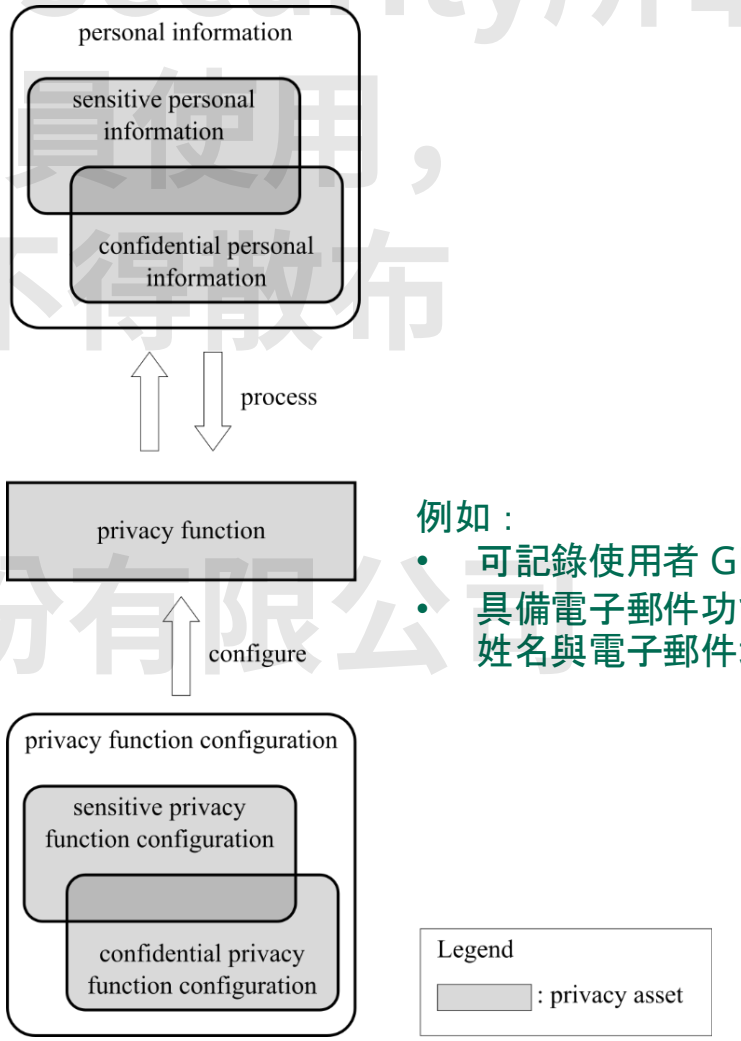
例如：

- TCP/IP 相關功能
- 一個 DNS 服務，提供其他裝置進行網路位址解析的功能

隱私資產的定義

包含：

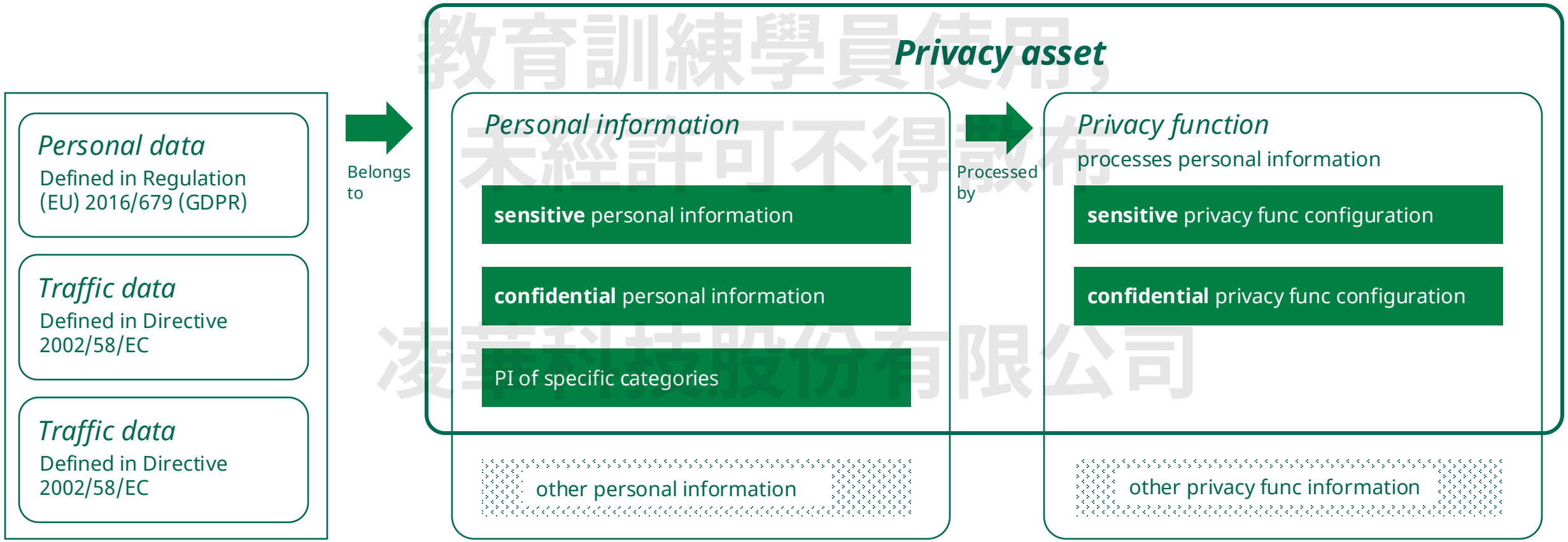
- 隱私功能、或
- 設備可直接影響使用者或用戶隱私的功能、或
- 設備所使用的隱私功能設定、或
- 決定設備隱私功能行為的資料、或
- 由設備儲存、傳輸或以其他方式處理的隱私資料，或
- 儲存在設備中、用於存取個人資訊或隱私功能的敏感安全參數、個人資料、通訊資料或定位資料



例如：

- 可記錄使用者 GPS 軌跡的功能
- 具備電子郵件功能，並儲存使用者姓名與電子郵件地址

隱私資產的定義

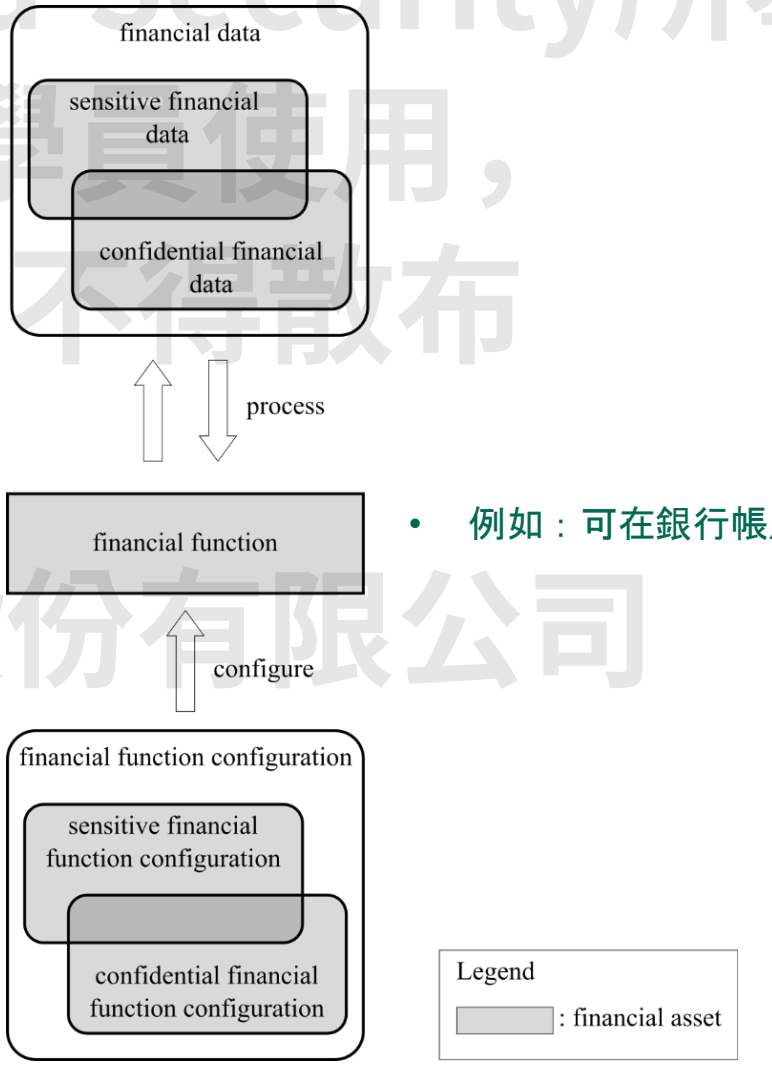


Sensitive: compromise privacy when manipulated
Confidential: compromise privacy when disclosed

金融資產的定義

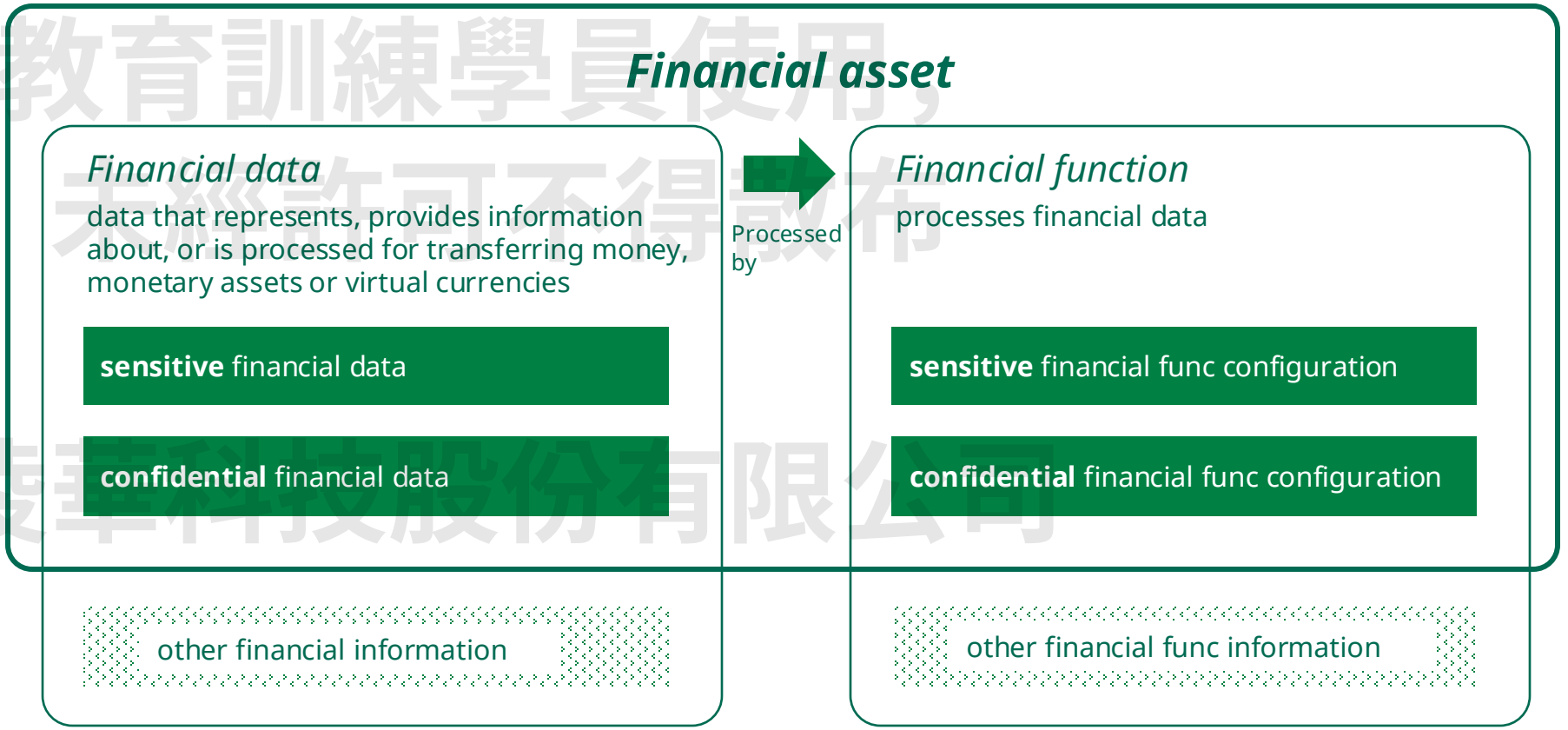
包含：

- 金融功能、或
- 設備可直接影響金融資料的功能、或
- 設備所使用的金融功能設定、或
- 決定設備金融功能行為的資料、或
- 由設備儲存、傳輸或以其他方式處理的金融資料，或
- 代表金錢、提供金錢相關資訊，或用於轉移金錢、貨幣資產或虛擬貨幣的資料、或
- 儲存在設備中、用於存取金融功能、金融功能設定及金融資料的敏感安全參數



- 例如：可在銀行帳戶之間相互轉帳的功能

金融資產的定義



Sensitive: lead to fraud when manipulated
Confidential: lead to fraud when disclosed

100 YEARS SECURING THE FUTURE 1925 – 2025

資產種類介紹

Assets

直接影響裝置完整性者

安全資產 (D,E,F)

- **安全參數:**
  - Root Key
  - Digital signature for firmware update
- **安全功能:**
  - Access Control system
  - Permission system
  - Secure Communication system
  - Secure Transmission

直接存取裝置網路功能者

網路資產 (D)

- **網路功能:**
  - RTSP
  - TCP/IP Services
- **網路連接埠相關 :**
  - TLS Session keys
- **網路安全設定:**
  - IPSec
  - VPN

直接影響裝置用戶隱私資料者

隱私資產 (E)

- **用戶隱私資料:**
  - Name, Gender, ID number, Address,
  - Health information, medical records stored...
- **用戶隱私資料處理功能:** (To collect, transmit, store, analyze, share and delete user info)
  - GPS Function
  - Chat Function
  - Face ID for smart phones
  - Personal records handling

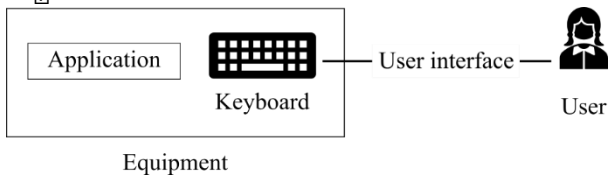
直接影響裝置金融功能者

金融資產 (F)

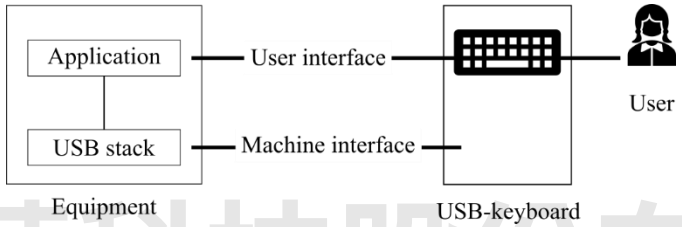
- **金融資訊:**
  - Displaying Bank account info
  - Displaying Cryptocurrency or In-game cash
  - Purchase Records
- **金融功能:**
  - NFC
  - APP money transferring

介面種類

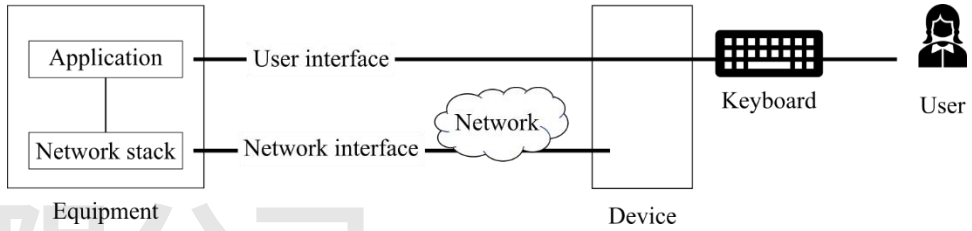
Definition	Note
interface	Abstract base definition
external interface	Definition scoped to the equipment
user interface	Specific interface types scoped to the equipment
machine interface	
network interface	



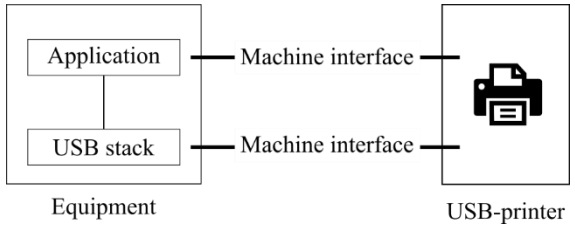
例：筆電內建鍵盤



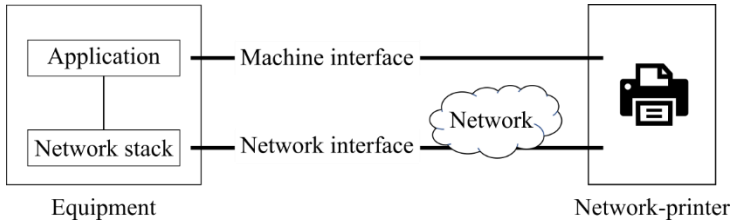
例：USB鍵盤



例：經使用者介面操作設備



例：USB列印機



例：網路列印機

[ACM] Access control mechanism

Access control mechanism (ACM) 安全要求

Identifier	Requirement	3.3(d)	3.3(e)	3.3(f)
ACM-1	Applicability of access control mechanisms	X	X	X
ACM-2	Appropriate access control mechanisms	X	X	X
ACM-3	Default access control for children in toys		X	
ACM-4	Default access control to children's privacy assets for toys and childcare equipment		X	
ACM-5	Parental/Guardian access controls for children in toys		X	
ACM-6	Parental/Guardian access controls for other entities' access to managed children's privacy assets in toys		X	

[ACM-1] Applicability of access control mechanisms

Requirement

設備應提供使用存取控制機制(access control mechanism)，管理可存取資產的個體(Entity)，但以下情況除外：

1) 設備本身預期功能就是開放使用
2) 設備預期的目標使用環境，已透過個體或邏輯措施去限制僅能已被授權的個體存取
3) 法律規定不允許使用存取控制機制

Rationale

資產可能會遭受未經授權個體嘗試存取，而存取控制機制可以用於限制任何未經授權的個體存取資產

[ACM-1] Applicability of access control mechanisms

IXIT	提供資訊	對應欄位
IXIT A-Asset	選擇可存取該資產的個體	Accessed by
	選擇該資產對應的存取控制機制 (IXIT 6.1-ACM)	ACM
	當不需存取控制時，選擇對應的例外排除原因	Exception (Reason)
	例外排除原因的補充說明	Exception (Description)
IXIT 6.1-ACM	說明該存取控制機制如何管理可存取資產的個體	Description of ACM

[ACM-1] Applicability of access control mechanisms

Completeness

- PASS
  - 所有資產皆已記錄於宣告表內
- FAIL
  - 任一個資產未被記錄於宣告表內
- NOT APPLICABLE
  - 其他

評估目的

確認所有可被個體存取的資產皆已記錄於宣告表內

評估方法

評估是否存在可被個體存取的資產未被記錄於宣告表內

[ACM-1] Applicability of access control mechanisms

Sufficiency

- PASS
  - 沒有證據顯示沒有任一個存取控制機制未實作
- FAIL
  - 有證據顯示有任一個存取控制機制未實作
- NOT APPLICABLE
  - 其他

評估目的

確認所有存取控制機制皆被實作

評估方法

針對宣告表內每一個資產，實際存取資產並確認所使用的存取控制機制是否存在

[ACM-2] Appropriate access control mechanisms

Requirement

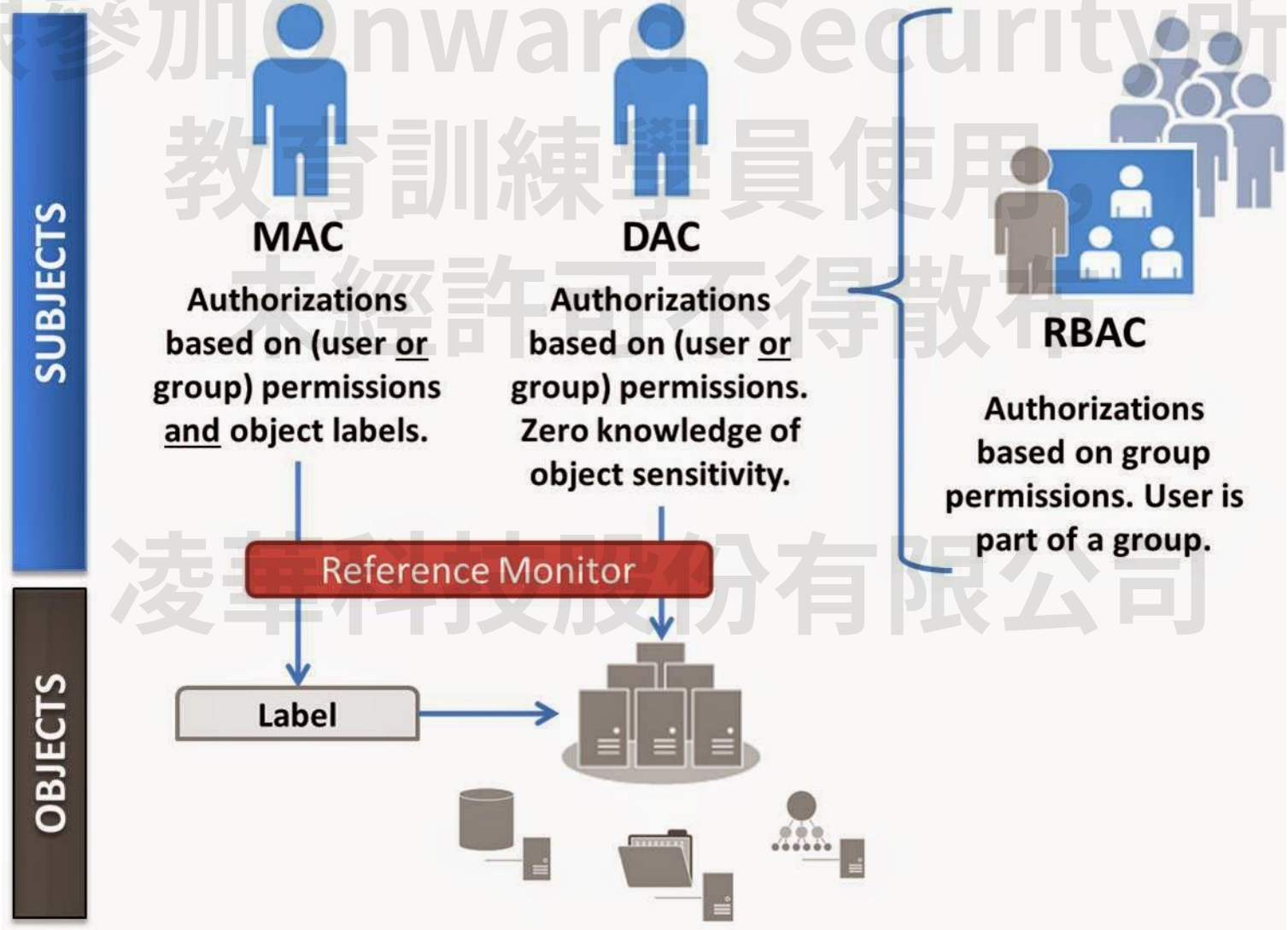
所有存取控制機制，應確保只有被授權個體可以存取受保護的資產

Rationale

資產可能會遭受未經授權個體嘗試存取，而合適的存取控制機制可以用於確保資產可以避免未經授權存取

[ACM-2] Appropriate access control mechanisms

Implementation Category



[ACM-2] Appropriate access control mechanisms

IXIT	提供資訊	對應欄位
IXIT 6.1-ACM	選擇該存取控制機制的實作方式選項 (RBAC, DAC, MAC, Generic)	ACM-2 (Impl Cat.)
	補充說明該實作方式的細節	ACM-2 (Descriprtion)

[ACM-2] Appropriate access control mechanisms

Sufficiency

- PASS
  - 對於宣告表內的每一個資產，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內的任一個資產，其對應的實作測試方法不成功
- NOT APPLICABLE
  - 其他

評估目的

確認所有存取控制機制的實作方式選項已正確實作

評估方法

AU.ACM-2.RBAC:

- **每一個使用者皆被指派為特定角色**
- **每一個角色僅具備必要的權限**
- **每一個資產只允許被特定角色存取**
- **變更角色僅能由被授權人員進行操作**

AU.ACM-2.DAC:

- **每一個使用者皆被指派一個特定的身分**
- **每一個身分僅具備必要權限**
- **每一個資產只允許被特定身分存取**
- **變成身分僅能由被授權人員進行操作**

[ACM-2] Appropriate access control mechanisms

Sufficiency

- PASS
  - 對於宣告表內的每一個資產，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內的任一資產，其對應的實作測試方法不成功
- NOT APPLICABLE
  - 其他

AU.ACM-2.MAC:

- 每一個資產只允許被特定人員存取，而該存取行為需取得作業系統或系統管理者授權
- 該存取行為授權需基於最小權限原則
- 變更負責發放存取行為授權的作業系統或系統管理者僅能由被授權系統管理者進行操作

AU.ACM-2.Generic:

- 每一個資產只能被授權使用者存取
- 需依循最小存取權限原則
- 變更存取控制機制相關設定或變更權限僅能由被授權人員進行操作

[ACM-3] Default access control for children in toys

Requirement

如果設備屬於玩具，每一個可以被兒童用於存取外部內容的隱**私功能，存取控制機制應預設確保，當兒童透過隱私功能存取外部**內容時，僅能存取由被授權**個體所指定的**內容

Rationale

兒童存取的外部來源的內容可用於未經授權的通訊、互動或以**其他方式損害兒童的隱私。預設限制兒童僅能存取被授權個體所指定的**內容，有助於避免相關危險。

[ACM-3] Default access control for children in toys

IXIT	提供資訊	對應欄位
IXIT A-Asset	該資產是否可用於存取外部內容 (Yes, No)	ACM-3 (access external content)
	如果可以，請列出被授權個體允許兒童存取的內容	ACM-3 (TrustedSources)
	選擇該資產對應的存取控制機制 (IXIT 6.1-ACM)	ACM-3 (ACM)
IXIT 6.1-ACM	選擇該存取控制機制的實作方式選項 (RBAC, DAC, MAC, Generic)	ACM-3 (Impl Cat.)
	補充說明該實作方式的細節	ACM-3 (Descriprtion)

[ACM-3] Default access control for children in toys

Completeness

- PASS
  - 所有可用於讓兒童存取外部內容的隱私功能皆記錄於宣告表內
- FAIL
  - 任一個可用於讓兒童存取外部內容的隱私功能未記錄於宣告表內
- NOT APPLICABLE
  - 其他

評估目的

確認所有可讓兒童存取外部內容的隱私功能被已被記錄於宣告表

評估方法

透過以下步驟，確認是否存在允許兒童存取外部內容，沒有被記錄於宣告表內

1) **列出設備所有可以讓兒童存取外部**內容的隱私功能
2) **根據步驟1所發現的隱私功能，與宣告表**內容進行比對是否存在不符合的地方

[ACM-3] Default access control for children in toys

Sufficiency

- PASS
  - 對於宣告表內的每一個ACM-3所使用到的存取控制機制，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內的任一ACM-3所使用到的存取控制機制，其對應的實作測試方法不成功
- NOT APPLICABLE
  - 其他

評估目的

確認存取控制機制是否預設限制兒童只能透過隱私功能，存取可信任來源的外部內容

評估方法

AU.ACM-3.RBAC:

- 被指派為”兒童”個體的角色，僅能存取被允許的外部內容
- 需依循最小存取權限原則
- 角色的變更只能由授權使用者執行

AU.ACM-3.DAC:

- 被指派為”兒童”個體的身分，僅能存取被允許的外部內容
- 需依循最小存取權限原則
- 角色的變更只能由授權使用者執行

[ACM-3] Default access control for children in toys

Sufficiency

- PASS
  - 對於宣告表內的每一個ACM-3所使用到的存取控制機制，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內的任一ACM-3所使用到的存取控制機制，其對應的實作測試方法不成功
- NOT APPLICABLE
  - 其他

AU.ACM-3.MAC:

- **當兒童想要存取外部**內容時，該存取行為需取得作業系統或系統管理者授權
- **該存取行為授權需基於最小權限原則**
- **變更負責發放存取行為授權的作業系統或系統管理者僅能由被授權系統管理者進行操作**

AU.ACM-3.Generic:

- **兒童只能存取被允許的外部**內容
- **需依循最小存取權限原則**
- **變更存取控制機制相關設定或變更權限僅能由被授權人員進行操作**

[ACM-4] Default access control to children’s privacy assets for toys and childcare equipment

Requirement

如果設備屬於玩具或用於兒童照顧，每一個兒童相關的隱私功能與個人資料的存取控制機制應預設限制除了兒童本人/家長/監護者之外，第三方皆無法存取， 但以下情況除外：

- 因設備預期功能需要開放第三方存取

Rationale

即使獲得同意，預設向第三方公開隱私功能或個人資料也可能損害兒童的隱私。將第三方對兒童隱私功能和個人資訊的預設存取權限限制為設備運作所需的權限，以支援隱私保護。

[ACM-4] Default access control to children's privacy assets for toys and childcare equipment

IXIT	提供資訊	對應欄位
IXIT A-Asset	**該資**產是否與兒童相關 (Yes, No)	Children's Asset
	該資產是否可以被兒童與其監護人之外的**個體存取** (Yes, No)	ACM-4 (be accessed by third-parties)
	選擇該資產對應的存取控制機制 (IXIT 6.1-ACM)	ACM-4 (ACM)
IXIT 6.1-ACM	**選擇該存取控制機制的實作方式選項** (RBAC, DAC, MAC, Generic)	ACM-4 (Impl Cat.)
	補充說明該實作方式的細節	ACM-4 (Descriprtion)
	第三方可存取兒童資產是否為設備預期功能?	ACM-4 (AuthorizedAccess|for third-parties?)
	如果是的話，請列出可存取第三方以及對應可存取的資產，以及設備預期功能之關係	ACM-4 (AuthorizedAccess|Description)

[ACM-4] Default access control to children's privacy assets for toys and childcare equipment

Completeness

- PASS
  - 可被兒童本人、家長及監護者存取的所有設備相關的兒童隱私功能與個人資料，皆已記錄於宣告表
- FAIL
  - 可被兒童本人、家長及監護者存取的任一個設備相關的兒童隱私功能與個人資料，未被記錄於宣告表
- NOT APPLICABLE
  - 其他

評估目的

檢查是否除了兒童本人、家長及其監護者之外的第三方可存取的隱私功能與個人資料皆已記錄於宣告表

評估方法

透過以下步驟，確認是否存在第三方可存取的兒童相關的隱私功能與個人資料，沒有被記錄於宣告表內

1) 列出設備所有可以被第三方存取的兒童相關的隱私功能與個人資料
2) 根據步驟1所發現的隱私功能與個人資料，與宣告表內容進行比對是否存在不符合的地方

[ACM-4] Default access control to children's privacy assets for toys and childcare equipment

Sufficiency

- PASS
  - 對於宣告表內每一個ACM-4所使用的存取控制機制，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內任一個ACM-4所使用的存取控制機制，其對應的實作測試方法為不成功
- NOT APPLICABLE
  - 其他

評估目的

檢查預設的存取控制機制是否限制非兒童本人、家長及監護者的第三方，其存取範圍限於設備預期功能的範圍

評估方法

AU.ACM-4.RBAC:

- 被指派為"第三方"個體的角色，僅能存取設備預期功能相關的兒童隱私功能與個人資料
- "第三方"個體需依循最小存取權限原則
- 角色的變更只能由授權使用者執行

AU.ACM-4.DAC:

- 被指派為"第三方"個體的身分，僅能存取設備預期功能相關的兒童隱私功能與個人資料
- "第三方"個體需依循最小存取權限原則
- 角色的變更只能由授權使用者執行

[ACM-4] Default access control to children's privacy assets for toys and childcare equipment

Sufficiency

- PASS
  - 對於宣告表內每一個ACM-4所使用的存取控制機制，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內任一個ACM-4所使用的存取控制機制，其對應的實作測試方法為不成功
- NOT APPLICABLE
  - 其他

AU.ACM-4.MAC:

- 當第三方想要存取設備預期功能範圍的兒童相關的隱私功能與個人資料時，該存取行為需取得作業系統或系統管理者授權
- 該存取行為授權需基於最小權限原則
- 變更負責發放存取行為授權的作業系統或系統管理者僅能由被授權系統管理者進行操作

AU.ACM-4.Generic:

- 第三方所的存取的兒童隱私功能與個人資料，其存取範圍限於設備預期功能的範圍每一個資產只能被授權使用者存取
- 需依循最小存取權限原則
- 變更存取控制機制相關設定或變更權限僅能由被授權人員進行操作

[ACM-5] Parental/Guardian access controls for children in toys

Requirement

當設備是玩具時，每一個可以被兒童存取的安全與隱私資產，其存取控制機制必須可以由被授權的個體進行設定，以限制兒童的存取行為僅限於受保護的安全與隱私資產

Rationale

考慮到兒童的保護需求和不斷發展的能力，特別是考慮到隱私和安全設定的影響，父母或監護人有必要限制其孩子可能訪問的安全和隱私資產，以避免任何相關的危險他們的隱私。

[ACM-5] Parental/Guardian access controls for children in toys

IXIT	提供資訊	對應欄位
IXIT A-Asset	該資產是否可以被兒童存取	Accessed By
IXIT 6.1-ACM	選擇該存取控制機制的實作方式選項 (RBAC, DAC, MAC, Generic)	ACM-5 (Impl Cat.)
	補充說明該實作方式的細節	ACM-5 (Descriprtion)

[ACM-5] Parental/Guardian access controls for children in toys

Completeness

- PASS
  - 所有可以被兒童存取的安全與隱私資產，皆已記錄於宣告表
- FAIL
  - 任一個可以被兒童存取的安全與隱私資產，未被記錄於宣告表
- NOT APPLICABLE
  - 其他

評估目的

檢查是否所有可以被兒童存取的安全與隱私資產皆已記錄於宣告表

評估方法

透過以下步驟，確認是否存在兒童可以存取的安全與隱私資產，沒有被記錄於宣告表內

1) **列出設備所有可以被兒童存取的安全與隱私資**產
2) **根據步驟1所發現的安全與隱私資**產，與宣告表內容進行比對是否存在不符合的地方

[ACM-5] Parental/Guardian access controls for children in toys

Sufficiency

- PASS
  - 對於宣告表內每一個ACM-5所使用的存取控制機制，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內任一個ACM-5所使用的存取控制機制，其對應的實作測試方法為不成功
- NOT APPLICABLE
  - 其他

評估目的

檢查兒童存取安全與隱私資訊所使用的存取控制機制，是否可以由被授權**個體進行設定**

評估方法

AU.ACM-5.RBAC:

- **所有使用者被指派為對應的角色**
- **所有角色需依循最小存取權限原則，以便被授權個體可以透過 RBAC 方式限制兒童所能夠存取的安全與隱私個體**
- **角色的變更只能由授權使用者執行**

AU.ACM-5.DAC:

- **所有使用者被指派為對應的身分**
- **所有身份需依循最小存取權限原則，以便被授權個體可以透過 DAC 方式限制兒童所能夠存取的安全與隱私個體**
- **身份的變更只能由授權使用者執行**

[ACM-5] Parental/Guardian access controls for children in toys

Sufficiency

- PASS
  - 對於宣告表內每一個ACM-5所使用的存取控制機制，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內任一個ACM-5所使用的存取控制機制，其對應的實作測試方法為不成功
- NOT APPLICABLE
  - 其他

AU.ACM-5.MAC:

- 只有當使用者被視為被授權的使用者，且被作業系統或系統管理者授權時，可以管理MAC限制兒童可存取的安全與隱私資產
- 該存取行為授權需基於最小權限原則
- 變更負責發放存取行為授權的作業系統或系統管理者僅能由被授權系統管理者進行操作

AU.ACM-5.Generic:

- 只有當使用者被視為被授權的使用者時，才允許管理存取控制機制限制兒童可存取的安全與隱私資產
- 需依循最小存取權限原則
- 變更存取控制機制相關設定或變更權限僅能由被授權人員進行操作

[ACM-6] Parental/Guardian access controls for other entities' access to managed children's privacy assets in toys

Requirement

如果設備是玩具的話，每一個可以被存取的兒童隱私資產，除了兒童本人、家長及監護人之外，其他第三方的存取需要可以被存取控制機制管理，且存取控制機制必須可以由被授權的個體，以限制其他第三方對於兒童隱私資產的存取

Rationale

考慮到兒童的保護需求和不斷發展的能力，父母或監護人有必要限制個體對兒童隱私資產的訪問，以避免與其隱私相關的任何風險。

[ACM-6] Parental/Guardian access controls for other entities' access to managed children's privacy assets in toys

IXIT	提供資訊	對應欄位
IXIT A-Asset	該資產是否與兒童相關 (Yes, No)	Children's Asset
IXIT 6.1-ACM	選擇該存取控制機制的實作方式選項 (RBAC, DAC, MAC, Generic)	ACM-6 (Impl Cat.)
	補充說明該實作方式的細節	ACM-6 (Descriprtion)

[ACM-6] Parental/Guardian access controls for other entities' access to managed children's privacy assets in toys

Completeness

- PASS
  - 所有可以被除了兒童、家長及監護人之外第三方存取的兒童相關隱私資產，皆已記錄於宣告表
- FAIL
  - 任一個可以被除了兒童、家長及監護人之外第三方存取的兒童相關隱私資產，未被記錄於宣告表
- NOT APPLICABLE
  - 其他

評估目的

檢查是否所有可以被除了家童、家長及監護人之外第三方存取的兒童相關隱私資產，皆已記錄於宣告表

評估方法

透過以下步驟，確認是否存在除了兒童、家長及監護人之外第三方存取的兒童相關隱私資產，沒有被記錄於宣告表內

1) 列出設備所有可以被除了兒童、家長及監護人的兒童相關與隱私資產
2) 根據步驟1所發現的隱私資產，與宣告表內容進行比對是否存在不符合的地方

[ACM-6] Parental/Guardian access controls for other entities' access to managed children's privacy assets in toys

Sufficiency

- PASS
  - 對於宣告表內每一個ACM-6所使用的存取控制機制，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內任一個ACM-6所使用的存取控制機制，其對應的實作測試方法為不成功
- NOT APPLICABLE
  - 其他

評估目的

檢查所有用於管理第三方存取兒童隱私資產的存取控制機制，是否可以透過被授權的個體進行管理

評估方法

AU.ACM-6.RBAC:

- 所有使用者皆被指派對應的角色
- 所有角色需依循最小存取權限原則，以便被授權個體可以透過 RBAC 方式限制第三方存取兒童隱私資產
- 角色的變更只能由授權使用者執行

AU.ACM-6.DAC:

- 所有使用者被指派為對應的身分
- 所有身份需依循最小存取權限原則，以便被授權個體可以透過 DAC 方式限制兒童所能夠存取的安全與隱私個體
- 身份的變更只能由授權使用者執行

[ACM-6] Parental/Guardian access controls for other entities' access to managed children's privacy assets in toys

Sufficiency

- PASS
  - 對於宣告表內每一個ACM-6所使用的存取控制機制，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內任一個ACM-6所使用的存取控制機制，其對應的實作測試方法為不成功
- NOT APPLICABLE
  - 其他

AU.ACM-6.MAC:

- 只有當使用者被視為被授權的使用者，且被作業系統或系統管理者授權時，可以管理MAC限制第三方對兒童隱私資產的存取
- 該存取行為授權需基於最小權限原則
- 變更負責發放存取行為授權的作業系統或系統管理者僅能由被授權系統管理者進行操作

AU.ACM-6.Generic:

- 只有當使用者被視為被授權的使用者時，才允許管理存取控制機制，限制第三方對兒童隱私資產的存取
- 需依循最小存取權限原則
- 變更存取控制機制相關設定或變更權限僅能由被授權人員進行操作

[AUM] Authentication mechanism

Authentication mechanism (AUM) 安全要求

Identifier	Requirement	3.3(d)	3.3(e)	3.3(f)
AUM-1	Applicability of authentication mechanisms	X	X	X
AUM-2	Appropriate authentication mechanisms	X	X	X
AUM-3	Authenticator validation	X	X	X
AUM-4	Changing authenticators	X	X	X
AUM-5	Password strength	X	X	X
AUM-6	Brute force protection	X	X	X

[AUM-1-1] Applicability of authentication mechanisms

Requirement (network interface)

存取控制機制必須使用身分認證機制，當允許個體透過網路:

- 讀取機密個人與金融資訊、機密網路/隱私/金融功能設定或機密安全參數
- 修改敏感個人與金融資訊、敏感網路/隱私/金融功能設定或敏感安全參數
- 使用網路/隱私/金融/安全功能

但以下情況除外 *(例外條件不適用於 3.3(f))*

- 不需要身分認證機制為設備預期功能
- 透過設備的目標操作環境中的個體或邏輯措施，限制被授權個體的存取

Rationale

設備需要提供認證機制，以便相應的存取控制機制防止未經授權的存取

- 來自可能損害網路或濫用網路資源的非其所聲稱的個體
- 與使用者隱私相關的安全和隱私資產，來自非其所聲稱的個體
- 來自非其所聲稱的個體的可用於欺詐的資產

[AUM-1-1] Applicability of authentication mechanisms

IXIT	提供資訊	對應欄位
IXIT 6.1-ACM	選擇使用該 ACM 的網路介面 (IXIT B-Interface)	AUM-1-1 (NetworkInterface)
	選擇 ACM 對應的身分認證機制 (IXIT 6.2-AUM)	AUM-1-1 (AUM)
	若未選擇對應的身分認證機制時，選擇對應的例外排除原因	AUM-1-1 (Exception|Reason)
	例外排除原因的補充說明	AUM-1-1 (Exception|Description)

[AUM-1-1] Applicability of authentication mechanisms

Completeness

- PASS
  - 沒有證據顯示有用於網路介面的存取控制機制未被記錄於宣告表
- FAIL
  - 有證據顯示有任一個用於網路介面的存取控制機制未被記錄於宣告表
- NOT APPLICABLE
  - 其他

評估目的

檢查是否有用於網路介面的存取控制機制未被記錄於宣告表， **該機制可用於**

- **讀取機密個人與金融資訊、機密網路/隱私/金融功能設定或機密安全參數**
- **修改敏感個人與金融資訊、敏感網路/隱私/金融功能設定或敏感安全參數**
- **使用網路/隱私/金融/安全功能**

評估方法

檢查可以透過網路介面的存取控制機制，該機制可用於

- **讀取機密個人與金融資訊、機密網路/隱私/金融功能設定或機密安全參數**
- **修改敏感個人與金融資訊、敏感網路/隱私/金融功能設定或敏感安全參數**
- **使用網路/隱私/金融/安全功能**

未被記錄於宣告表內

[AUM-1-1] Applicability of authentication mechanisms

Sufficiency

- PASS
  - 沒有證據顯示宣告表內用於網路介面的身份認證機制未實作
- FAIL
  - 有證據顯示宣告表內用於網路介面的身份認證機制未實作
- NOT APPLICABLE
  - 其他

評估目的

檢查身分認證機制是否依宣告表內容實作

評估方法

針對宣告表內的每一個可透過網路介面的存取控制機制：

- **針對該存取控制機制可存取的每一個安全/網路/隱私/金融資**產

存取對應的資產，並確認具備對應的身分認證機制

[AUM-1-2] Applicability of authentication mechanisms

Requirement (user interface)

存取控制機制必須使用身分認證機制，若允許個體透過網路:

- 讀取機密個人與金融資訊、機密網路/隱私/金融功能設定或機密安全參數
- 修改敏感個人與金融資訊、敏感網路/隱私/金融功能設定或敏感安全參數
- 使用網路/隱私/金融/安全功能

但以下情況除外 *(例外條件不適用於 3.3(f))*

- 透過設備的目標操作環境中的個體或邏輯措施，限制被授權個體的存取

除了對個人資料、網路/隱私功能或網路/隱私功能設定的唯讀存取(當存取時不需要身分認證)之外:

- 啟用預期的設備功能
- 法律不允許身份驗證機制

Rationale

設備需要提供認證機制，以便相應的存取控制機制防止未經授權的存取

- 來自可能損害網路或濫用網路資源的非其所聲稱的個體
- 與使用者隱私相關的安全和隱私資產，來自非其所聲稱的個體
- 來自非其所聲稱的個體的可用於欺詐的資產

[AUM-1-2] Applicability of authentication mechanisms

IXIT	提供資訊	對應欄位
IXIT 6.1-ACM	選擇使用該 ACM 的使用者介面 (IXIT B-Interface)	AUM-1-2 (UserInterface)
	選擇 ACM 對應的身分認證機制 (IXIT 6.2-AUM)	AUM-1-2 (AUM)
	若未選擇對應的身分認證機制時，選擇對應的例外排除原因	AUM-1-2 (Exception|Reason)
	例外排除原因的補充說明	AUM-1-2 (Exception|Description)

[AUM-1-2] Applicability of authentication mechanisms

Completeness

- PASS
  - 沒有證據顯示有用於使用者介面的存取控制機制未被記錄於宣告表
- FAIL
  - 有證據顯示有任一個用於使用者介面的存取控制機制未被記錄於宣告表
- NOT APPLICABLE
  - 其他

評估目的

檢查是否有用於使用者介面的存取控制機制未被記錄於宣告表， **該機制可用於**

- **讀取機密個人與金融資訊、機密網路/隱私/金融功能設定或機密安全參數**
- **修改敏感個人與金融資訊、敏感網路/隱私/金融功能設定或敏感安全參數**
- **使用網路/隱私/金融/安全功能**

評估方法

檢查可以透過使用者介面的存取控制機制，該機制可用於

- **讀取機密個人與金融資訊、機密網路/隱私/金融功能設定或機密安全參數**
- **修改敏感個人與金融資訊、敏感網路/隱私/金融功能設定或敏感安全參數**
- **使用網路/隱私/金融/安全功能**

未被記錄於宣告表內

[AUM-1-2] Applicability of authentication mechanisms

Sufficiency

- PASS
  - 沒有證據顯示被宣告表內用於使用者介面的身份認證機制未實作
- FAIL
  - 有證據顯示被宣告表內用於使用者介面的身份認證機制未實作
- NOT APPLICABLE
  - 其他

評估目的

檢查身分認證機制是否依宣告表內容實作

評估方法

針對宣告表內的每一個可透過使用者介面的存取控制機制：

- **針對該存取控制機制可存取的每一個安全/網路/隱私/金融資**產

存取對應的資產，並確認具備對應的身分認證機制

[AUM-1-3] Applicability of authentication mechanisms

Requirement (machine interface)

存取控制機制必須使用身分認證機制，當允許個體透過機器介面:

- 讀取機密金融資訊、機密金融功能設定或機密安全參數
- 修改敏感金融資訊、敏感金融功能設定或敏感安全參數
- 使用金融/安全功能

Rationale

設備需要提供身份認證機制，以便相應的存取控制機制防止來自非其所聲稱的個體對可用於詐欺的資產進行未經授權的訪問

[AUM-1-3] Applicability of authentication mechanisms

IXIT	提供資訊	對應欄位
IXIT 6.1-ACM	選擇使用該 ACM 的機器介面 (IXIT B-Interface)	AUM-1-3 (MachineInterface)
	選擇 ACM 對應的身分認證機制 (IXIT 6.2-AUM)	AUM-1-3 (AUM)

[AUM-1-3] Applicability of authentication mechanisms

Completeness

- PASS
  - 沒有證據顯示有用於機器介面的存取控制機制未被記錄於宣告表
- FAIL
  - 有證據顯示有任一個用於機器介面的存取控制機制未被記錄於宣告表
- NOT APPLICABLE
  - 其他

評估目的

檢查是否有用於機器介面的存取控制機制未被記錄於宣告表， **該機制可用於**

- **讀取機密金融資訊、機密金融功能設定或機密安全參數**
- **修改敏感金融資訊、敏感金融功能設定或敏感安全參數**
- **使用金融/安全功能**

評估方法

檢查可以透過網路介面的存取控制機制，該機制可用於

- **讀取機密金融資訊、機密金融功能設定或機密安全參數**
- **修改敏感金融資訊、敏感金融功能設定或敏感安全參數**
- **使用金融/安全功能**

未被記錄於宣告表內

[AUM-1-3] Applicability of authentication mechanisms

Sufficiency

- PASS
  - 沒有證據顯示被宣告表內用於機器介面的身份認證機制未實作
- FAIL
  - 有證據顯示被宣告表內用於機器介面的身份認證未實作
- NOT APPLICABLE
  - 其他

評估目的

檢查身分認證機制是否依宣告表內容實作

評估方法

針對宣告表內的每一個可透過機器介面的存取控制機制：

- 針對該存取控制機制可存取的每一個安全/金融資產

存取對應的資產，並確認具備對應的身分認證機制

[AUM-2(-1)] Appropriate authentication mechanisms

Requirement (one factor)

設備所使用的身分認證機制應基於檢查至少一個身分認證因子來驗證個體的聲明

Rationale

單一因子身份驗證適用於

- 保護設備的網路資源免於濫用，例如：作為 DoS 攻擊的一部分。
- 防止非其所聲稱的個體對與使用者隱私相關的安全資產或隱私資產進行未經授權的存取。
- 防止未經授權的個體存取安全資產或金融資產，這些資產可能被用於詐欺

[AUM-2(-1)] Appropriate authentication mechanisms

IXIT	提供資訊	對應欄位
IXIT 6.2-AUM	說明使用該 AUM 所使用身分驗證因子	1st AuthFactorType

[AUM-2(-1)] Appropriate authentication mechanisms

Sufficiency

- PASS
  - 沒有證據顯示身分認證機制的實作方式與宣告表不一致
- FAIL
  - 有證據顯示身分認證機制的實作方式與宣告表不一致
- NOT APPLICABLE
  - 其他

評估目的

檢查身分認證機制實作內容與宣告表一致

Assessment units

針對宣告表內的每一個身分認證機制

1) **執行身分認證**
2) **確認身分認證實作**內容與宣告表是否一致

[AUM-2-2] Appropriate authentication mechanisms

Requirement (two factor)

如果設備的預期功能是用於處理特殊類別的個人資料，則對於每次通過網路介面的使用者介面存取的個人資訊時，身分認證機制應支援雙因子認證。

根據AUM-1-1(網路介面)或AUM-1-2(使用者介面)所需的身份認證機制，用於透過網路介面上的使用者介面存取金融功能時，傳輸貨幣、貨幣資產或虛擬貨幣，應支援雙因子認證機制。

Rationale

- 如果設備的預期功能是專門處理特殊類別的個人資訊，則此類數據的洩露可能會產生嚴重後果。在這種情況下，需要使用雙因子身份認證透過網路介面的使用者介面進行存取
- 透過網路執行金融交易的能力需要安全的身份驗證機制，以拒絕網路上的詐騙交易。因此，在這種情況下至少需要使用兩種驗證因子進行身份認證。

[AUM-2-2] Appropriate authentication mechanisms

IXIT	提供資訊	對應欄位
IXIT 6.2-AUM	說明使用該 AUM 所使用第二個身分驗證因子	2nd AuthFactorType

[AUM-2-2] Appropriate authentication mechanisms

Sufficiency

- PASS
  - 沒有證據顯示身分認證機制的實作方式與宣告表不一致
- FAIL
  - 有證據顯示身分認證機制的實作方式與宣告表不一致
- NOT APPLICABLE
  - 其他

評估目的

檢查身分認證機制實作內容與宣告表一致

評估方法

針對宣告內內的每一個身分認證機制

1) **執行雙因子身分認證**
2) **確認身分認證實作**內容與宣告表是否一致

[AUM-3] Authenticator validation

Requirement

身分認證機制應根據使用環境的可用資訊，驗證身分驗證因子所有相關屬性

Rationale

即使設備提供了身份認證機制，攻擊者也存在利用典型設計缺陷來繞過該機制的風險。偽造或部分偽造的身分驗證因子的使用通常用於針對這種機制的攻擊。因此，機制的安全設計需要技術來抵抗偽造的身分驗證因子，例如偽造的PKI憑證。

[AUM-3] Authenticator validation

IXIT	提供資訊	對應欄位
IXIT 6.2-AUM	**選擇身分驗證因子的實作方式** (Password, CertificatePrivateKey, Generic)	AUM-3 (AuthVal | Impl Cat.)
	實作方式補充說明	AUM-3 (AuthVal | Description)
	說明身分驗證因子在使用操作環境中的可用資訊	AUM-3 (AuthEnv)

[AUM-3] Authenticator validation

Sufficiency

- PASS
  - 對於宣告表內每一個AUM-3所使用的身分認證機制，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內任一個AUM-3所使用的身分認證機制，其對應的實作測試方法為不成功
- NOT APPLICABLE
  - 其他

評估目的

檢查身分認證機制是否驗證所有必要屬性

評估方法

AU.AUM-3.Password

- 不正確的密碼可以成功通過身分認證
- (如果透過網路介面進行身分認證，其過程當中交換的訊息的機密性未受到保護時)
  重新發送側錄的成功的身分認證行為可以通過身分認證
- 部分的正確密碼可以通過身分認證
- (如果允許多個使用者帳號時)
  其他使用者的密碼可以用於通過身分認證

AU.AUM-3.CertificatePrivateKey

- (如果透過網路介面進行身分認證，其過程當中交換的訊息的機密性未受到保護時)
  重新發送側錄的成功的身分認證行為可以通過身分認證
- 不可信任或無效憑證的有效私鑰可以通過身分認證
- (如果允許多個使用者帳號時)
  其他使用者的私鑰可以用於通過身分認證

[AUM-3] Authenticator validation

Sufficiency

- PASS
  - 對於宣告表內每一個AUM-3所使用的身分認證機制，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內任一個AUM-3所使用的身分認證機制，其對應的實作測試方法為不成功
- NOT APPLICABLE
  - 其他

AU.AUM-3.Generic

- 不正確的身分驗證因子可以通過身分認證
- (如果透過網路介面進行身分認證，其過程當中交換的訊息的機密性未受到保護時)
  重新發送側錄的成功的身分認證行為可以通過身分認證
- (如果允許多個使用者帳號時)
  其他使用者的身份驗證因子可以用於通過身分認證

[AUM-4] Changing authenticators

Requirement

身分認證機制必須允許變更身分驗證因子，除非變更身分驗證因子的行為與安全目的相抵觸

Rationale

固定的身份驗證因子可能會為設備帶來安全風險，例如更容易受到暴力破解和竊聽攻擊。因此，需要支援更改設備上的身份驗證因子。

[AUM-4] Changing authenticators

IXIT	提供資訊	對應欄位
IXIT 6.2-AUM	說明身分驗證因子變更方式	AUM-4 (AuthChange)
	若設備不支援變更身分驗證因子，選擇對應的例外排除原因	AUM-4 (Exception | Reason)
	例外排除原因的補充說明	AUM-4 (Exception | Description)

[AUM-4] Changing authenticators

Sufficiency

- PASS
  - 沒有顯示變更身分驗證因子的實作方式與宣告表不一致
- FAIL
  - 有證據顯示變更身分驗證因子的實作方式與宣告表不一致
- NOT APPLICABLE
  - 其他

評估目的

檢查身分認證機制所支援的身分驗證因子變更方式是否與宣告表一致

評估方法

針對宣告表內的每一個身分認證機制，確認是否可以依據宣告表的內容變更身分驗證因子，**並確認在變更身分驗證因子後**

- **變更後的身分驗證因子可以通過身分認證機制**
- **原本使用的身分驗證因子無法通過身分認證機制**

[AUM-5-1] Password strength

factory default password

Requirement (factory default pass)

如果身分認證機制使用出廠預設密碼時，密碼必須

- 每一台設備都使用唯一的密碼
- 使用密碼安全的最佳實務

或者

- 強制使用者在第一次登入的時候變更

Rationale

預設密碼等弱密碼是最常被利用的密碼攻擊方式之一。已經有許多惡意程式透過預設密碼的方式進行自動化攻擊。因此，必須在出廠設定時強制設定不同的密碼，或在初始化過程為每台設備強制使用者重新設定新的密碼。

[AUM-5-1] Password strength

factory default password

IXIT	提供資訊	對應欄位
IXIT 6.2-AUM	如果使用密碼作為身分驗證因子，請選擇密碼是否為出廠預設密碼	AuthFactor (PasswordType)
	選擇出廠預設密碼安全的實作方式 (UniqueBestPractice, EnforceSettingFirstUse)	AUM-5-1 (PwdProperty|Impl Cat.)
	補充說明實作方式	AUM-5-1 (PwdProperty|Description)

[AUM-5-1] Password strength

factory default password

Sufficiency

- PASS
  - 沒有證據顯示出廠預期密碼的實作方式與宣告表內容不一致
- FAIL
  - 有證據顯示出廠預期密碼的實作方式與宣告表內容不一致
- NOT APPLICABLE
  - 其他

評估目的

若使用出廠預設密碼時，檢查身分認證機制實作方式是否與宣告表一致

前提條件

設備處於出廠預設狀態，並且未開始進行設定

評估方法

針對宣告表內每一個使用密碼的身分認證機制

AU.AUM-5-1.UniqueBestPractice

- 比較實際出廠預設密碼與宣告表所描述的實作方式
- 根據設備使用者手冊讓設備進入正常運作模式，確認實際出廠預設密碼是有效的

AU.AUM-5-1.EnforceSettingFirstUse

- 根據設備使用者手冊讓設備進入正常運作模式
- 使用出廠預設密碼登入，確認是否要求重新設定新密碼

[AUM-5-2] Password strength

non-factory default password

Requirement (other passwords)

如果身分認證機制使用密碼不是出廠預設密碼時，密碼必須

- 強制使用者在第一次登入的時候，並且在連接到網路之前設定密碼
- 由網路內被授權的個體定義，其存取僅限於被授權的個體
- 由設備參考密碼安全的最佳實務自行產生，並且只允許被授權的個體在可信任的網路內進行傳輸

Rationale

預設密碼等弱密碼是最常被利用的密碼攻擊方式之一。已經有許多惡意程式透過預設密碼的方式進行自動化攻擊。因此，必須在出廠設定時強制設定不同的密碼，或在初始化過程為每台設備強制使用者重新設定新的密碼。

[AUM-5-2] Password strength

non-factory default password

IXIT	提供資訊	對應欄位
IXIT 6.2-AUM	如果使用密碼作為身分驗證因子，請選擇密碼是否為出廠預設密碼	AuthFactor (PasswordType)
	選擇出廠預設密碼安全的實作方式 (SettingFirstUse, DefinedAuthEntity, EquipmentGenerated)	AUM-5-2 (PwdProperty|Impl Cat.)
	補充說明實作方式	AUM-5-2 (PwdProperty|Description)

[AUM-5-2] Password strength

non-factory default password

Sufficiency

- PASS
  - 沒有證據顯示出廠預期密碼的實作方式與宣告表內容不一致
- FAIL
  - 有證據顯示出廠預期密碼的實作方式與宣告表內容不一致
- NOT APPLICABLE
  - 其他

評估目的

針對非出廠預設密碼，檢查身分認證機制實作方式是否與宣告表一致

前提條件

設備處於出廠預設狀態，並且未開始進行設定

Assessment units

針對宣告表內每一個使用密碼的身分認證機制

AU.AUM-5-2.SettingFirstUse

- 觀察設備網路是否連線至網路
- 根據設備使用者手冊讓設備進入正常運作模式
- 使用出廠預設密碼登入，確認是否要求設定新密碼

[AUM-5-2] Password strength

non-factory default password

Sufficiency

- PASS
  - 沒有證據顯示出廠預期密碼的實作方式與宣告表內容不一致
- FAIL
  - 有證據顯示出廠預期密碼的實作方式與宣告表內容不一致
- NOT APPLICABLE
  - 其他

AU.AUM-5-2.DefinedAuthEntity

- 根據設備使用者手冊讓設備進入正常運作模式
- (如果設備所連接的網路未限制只能由被授權的個體所存取) 使用已授權個體透過網路介面設定密碼，而該網路未限制僅有能被授權的個體所存取
- 以未授權個體設定密碼
- 以已授權個體透過網路介面設定密碼，而該網路僅能由被授權的個體所存取；或者是透過非網路介面

AU.AUM-5-2.EquipmentGenerated

- 根據設備使用者手冊讓設備進入正常運作模式
- 產生初始化密碼
- 以未授權個體取得密碼
- (如果設備所連接的網路未限制只能由被授權的個體所存取) 使用已授權個體透過網路介面取得密碼，而該網路未限制僅有能被授權的個體所存取
- 由已授權個體透過網路介面設定密碼，，而該網路僅能由被授權的個體所存取；或者是透過非網路介面
- 比較實際產生的密碼與宣告表所描述的實作方式

[AUM-6] Brute force protection

Requirement

身分認證機制必須能夠避免密碼暴力破解攻擊

Rationale

攻擊者可以嘗試使用大量密碼猜測嘗試來繞過身份認證機制或影響設備可用性。因此，需要相關機制來減緩此類攻擊的影響。

[AUM-6] Brute force protection

IXIT	提供資訊	對應欄位
IXIT 6.2-AUM	選擇防止密碼暴力破解的實作方式 (TimeDelay, LimitedAttemps, AuthenticatorComplexity, Generic)	AUM-6 (BFProtection|Impl Cat.)
	補充說明實作方式	AUM-6 (BFProtection|Description)

[AUM-6] Brute force protection

Sufficiency

- PASS
  - 對於宣告表內每一個AUM-6所說明的防止密碼暴力破解機制，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內任一個AUM-6所說明的防止密碼暴力破解機制，其對應的實作測試方法為不成功
- NOT APPLICABLE
  - 其他

評估目的

檢查身分認證機制是否滿足AUM-6的要求

Assessment units

針對宣告表內每一個身分認證機制

AU.AUM-6.TimeDelay

- **使用錯誤身分驗證因子重複執行身分認證**
- **測量連續登入失敗之間，設備所延遲回應的時間**

AU.AUM-6.LimitAttemps

- **使用錯誤身分驗證因子重複執行身分認證**
- **在設備阻止使用者進行身分認證之前，計算連續登入失敗的次數**

AU.AUM-6.AuthenticatorComplexity

- **嘗試設定未滿足宣告表**內的密碼複雜度要求的身分驗證因子
- **針對身分認證機制執行密碼暴力破解**

AU.AUM-6.Generic

- **針對身分認證機制執行密碼暴力破解**

[SUM] Secure update mechanism

Secure update mechanism (SUM) 安全要求

Identifier	Requirement	3.3(d)	3.3(e)	3.3(f)
SUM-1	Applicability of secure update mechanisms	X	X	X
SUM-2	Secure updates	X	X	X
SUM-3	Automated updates	X	X	X

[SUM-1] Applicability of secure update mechanisms

Requirement

若軟韌體影響資產的話，設備應支援至少一種軟體(包括韌體)更新方式，以下情況除外：

- 更新會影響功能安全(functional safety)，因此不允許更新
- 該軟韌體為不可變的(immutable)
- 在設備的生命週期中，有替代措施可以保護受影響的資產

Rationale

具有透過更新機制提供和部署軟體更新的能力是一項基本能力。它有助於維護設備、解決安全漏洞並防止可能危及設備的潛在利用。這類攻擊會為網路帶來風險，破壞其功能，或導致濫用網路資源，導致服務品質下降至不可接受地程度。

然而，某些軟體元件可能是不可變的，或功能安全影響不允許其更新。漏洞也可以透過替代措施來緩解，例如在整個生命週期中更換易受攻擊的設備，或透過確保保護資產的其他設備安全地緩解漏洞。

[SUM-1] Applicability of secure update mechanisms

IXIT	提供資訊	對應欄位
IXIT C-PartOfSoftw	選擇該軟體所影響資產 (IXIT A-Asset)	SUM-1 (Affected Assets)
	選擇對應的安全更新機制 (IXIT 6.3-SUM)	SUM-1 (SUM)
	若設備不支援安全更新，選擇對應的例外排除原因	SUM-1 (Exception | Reason)
	例外排除原因的補充說明	SUM-1 (Exception | Description)

[SUM-1] Applicability of secure update mechanisms

Sufficiency

- PASS
  - 沒有證據顯示宣告表內每一個軟體更新方式，其安裝更新檔案是失敗的
- FAIL
  - 有證據顯示宣告表內有軟體更新方式，其安裝更新檔案是失敗的
- NOT APPLICABLE
  - 其他

評估目的

檢查設備是否支援宣告表的軟體更新方式

前提條件

針對每一種更新方式，製造商應提供更新檔案，且該更新檔案應具備設備本身所提供的完整性(integrity)與真實性(authenticity)保護機制

評估方法

針對宣告表的每一種更新方式，透過該更新方式安裝更新程式

[SUM-2] Secure updates

Requirement

每一種更新方式在安裝更新程式的時候，只能安裝通過完整性與真實性檢查的更新程式

Rationale

安全的軟體更新機制確保設備的軟體不會因更新機制受到攻擊而被竄改。

[SUM-2] Secure updates

IXIT	提供資訊	對應欄位
IXIT 6.3-SUM	選擇更新程式完整性與真實性的實作方式 (Sign, SecChan, AccContMech, Generic)	SUM-2 (Impl Cat.)
	補充說明實作方式	SUM-2 (Description)

[SUM-2] Secure updates

Sufficiency

- PASS
  - 對於宣告表內每一個更新方式，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內任一個更新方式，其對應的實作測試方法為不成功
- NOT APPLICABLE
  - 其他

評估目的

檢查每一個更新方式是否在安裝時會檢查更新程式的完整性與真實性

前提條件

針對每一個更新方式，製造商應提供更新程式

評估方法

針對宣告表內每一個更新方式

AU.SUM-2.Sign:

- 所使用的加密演算法必須滿足 CRY-1 的最佳實務
- 未簽章的更新程式無法被安裝
- 簽章被竄改的更新程式無法被安裝
- 合法簽章，但是竄改過的更新程式無法被安裝
- 簽章來自於未授權的個體的更新程式無法被安裝

[SUM-2] Secure updates

Sufficiency

- PASS
  - 對於宣告表內每一個更新方式，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內任一個更新方式，其對應的實作測試方法為不成功
- NOT APPLICABLE
  - 其他

AU.SUM-2.SecChan:

- **所使用的安全連線機制必須滿足 SCM 安全要求**
- **來自於未經授權來源的更新程式無法被安裝**
- **安全連線通道需要避免中間人攻擊，以防攻擊者偽造授權的軟體更新來源**
- **在傳輸過程被竄改的更新程式無法被安裝**

AU.SUM-2.AccContMech:

- **所使用的存取控管機制必須滿足 ACM 安全要求**
- **合法雜湊值**，但是竄改過的更新程式無法被安裝
- **雜湊值**由不被支援的雜湊演算法所產生的更新程式無法被安裝
- **來自於未授權的個體的更新程式無法被安裝**

AU.SUM-2.Generic:

- **未通過完整性檢查**的軟體更新無法被安裝
- **未通過真實性檢查**的軟體更新無法被安裝

[SUM-3] Automated updates

Requirement

每一個更新機制都必須在透過以下列方式之一提供軟體更新功能

- 無需人為干預
- 在人工核准之下，透過排程方式安裝更新
- 在人工核准或監督下觸發更新安裝，以避免出現任何意外損壞的情況

Rationale

如果裝置中存在已知的可利用漏洞，可能會危及資產，而自動更新機制可確保應用程式解決安全漏洞的安全性更新，可以在無需或只需最少的人為干預下進行安裝。

[SUM-3] Automated updates

IXIT	提供資訊	對應欄位
IXIT 6.3-SUM	說明更新機制所採用的自動更新方式	SUM-3 (Automotation)

[SUM-3] Automated updates

Sufficiency

- PASS
  - 沒有任何證據顯示更新機制所採用的自動更新方式與宣告表不一致
- FAIL
  - 有證據顯示更新機制所採用的自動更新方式與宣告表不一致
- NOT APPLICABLE
  - 其他

評估目的

檢查更新機制其自動更新方式與宣告表是否一致

前提條件

製造商應提供執行自動更新的方式

評估方法

針對宣告表內每一個更新機制，應檢查：

- 檢查目前設備的軟體版本
- **從更新程式的來源取得軟體更新**
- 檢查設備是否可以透過以下方式之一執行軟體更新
  - **無需人為干預**
  - **在人工核准之下，透過排程方式安裝更新**
  - **在人工核准觸發更新安裝**
- 檢查設備軟體版本是否已更新至新的版本

[SSM] Secure storage mechanism

Secure storage mechanism (SSM) 安全要求

Identifier	Requirement	3.3(d)	3.3(e)	3.3(f)
SSM-1	Applicability of secure storage mechanisms	X	X	X
SSM-2	Appropriate integrity protection for secure storage mechanisms	X	X	X
SSM-3	Appropriate confidentiality protection for secure storage mechanisms	X	X	X

[SSM-1] Applicability of secure storage mechanisms

Requirement

設備必須永遠使用安全儲存機制，以保護持續儲存在設備的資產，但資產在**以下情況除外**：

- **目標環境中的個體或邏輯措施，可以確保儲存在設備的資**產僅能被授權個體存取

Rationale

安全儲存機制可保護資產免遭未經授權的存取。如果資產沒有**得到適當的保護，攻擊者可以存取、**篡改或刪除資產，並危害**設備，這可能會導致**

- **濫用網路資源**
- **個人資訊的暴露**
- **詐欺**

[SSM-1] Applicability of secure storage mechanisms

IXIT	提供資訊	對應欄位
IXIT A-Asset	資產是否會持續儲存在設備 (Yes, No)	SSM-1 (Persistently Stored)
	選擇對應的安全儲存機制 (IXIT 6.4-SSM)	SSM-1 (SSM)
IXIT 6.4-SSM	若設備未使用安全儲存機制，選擇對應的例外排除原因	SSM-1 (Exception | Reason)
	例外排除原因的補充說明	SSM-1 (Exception | Description)

[SSM-1] Applicability of secure storage mechanisms

Completeness

- PASS
  - 所有被儲存的資產都已被記錄於宣告表
- FAIL
  - 任一個被儲存的資產未被記錄於宣告表
- NOT APPLICABLE
  - 其他

評估目的

檢查是否所有被儲存的資產已被記錄於宣告表

評估方法

檢查是否所有被儲存在設備的安全資產沒有被列在宣告表內

檢查是否所有被儲存在設備的網路資產沒有被列在宣告表內

檢查是否所有被儲存在設備的隱私資產沒有被列在宣告表內

檢查是否所有被儲存在設備的金融資產沒有被列在宣告表內

[SSM-1] Applicability of secure storage mechanisms

Sufficiency

- PASS
  - 沒有證據顯示有資產使用宣告表之外的方式儲存於設備
- FAIL
  - 有證據顯示有資產使用宣告表之外的方式儲存於設備
- NOT APPLICABLE
  - 其他

評估目的

評估安全儲存機制的實作是否與宣告表一致

評估方法

針對宣告表內的每一個儲存在設備的資產，確認其儲存方式僅透過宣告表所描述的方式**儲存於設備**

[SSM-2] Appropriate integrity protection for secure storage mechanisms

Requirement

當資料儲存在設備時，每一個安全儲存機制必須確保資產的完整性

Rationale

當資產儲存在設備時，資產需要防止篡改。如果儲存的資產的完整性沒有得到適當的保護，攻擊者就可以操縱這些資產，這可能會

- 危害網路資源
- 導致侵犯個人權利，例如濫用個人資訊、虛假歸屬等。
- 導致欺詐，例如濫用財務資料、虛假歸屬、操縱金融交易日誌等

完整性保護適用於儲存於加密與未加密的裝置。

[SSM-2] Appropriate integrity protection for secure storage mechanisms

IXIT	提供資訊	對應欄位
IXIT 6.4-SSM	選擇安全儲存機制完整性保護的實作方式 (DigitalSignature, AccessControl, OTProgrammable, HardwareProtection, Generic)	SSM-2 (Impl Cat.)
	補充說明實作方式	SSM-2 (Description)
	若安全儲存機制通過資安標準或取得資安證書，請提供佐證資料	SSM-2 (ComplianceEvidence)

[SSM-2] Appropriate integrity protection for secure storage mechanisms

Sufficiency

- PASS
  - 對於宣告表內每一個安全儲存機制，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內任一個安全儲存機制，其對應的實作測試方法為不成功
- NOT APPLICABLE
  - 其他

評估目的

檢查安全儲存機制是否提供完整性保護

評估方法

針對宣告表每一個安全儲存機制

AU.SSM-2.DigitalSignature

- **確認是否依據宣告表**內容實作
- **用於簽署資**產的數位簽章金鑰不能被攔截、推算或擷取
- **安全儲存機制可以偵測被修改後資**產無有效的簽章

AU.SSM-2.AccessControl

- **確認是否依據宣告表**內容實作
- **安全儲存機制可阻擋未經授權的嘗試修改資**產的行為

AU.SSM-2.OTProgrammable

- **確認是否依據宣告表**內容實作
- **修改資**產是不可能達成的行為

[SSM-2] Appropriate integrity protection for secure storage mechanisms

Sufficiency

- PASS
  - 對於宣告表內每一個安全儲存機制，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內任一個安全儲存機制，其對應的實作測試方法為不成功
- NOT APPLICABLE
  - 其他

AU.SSM-2.HardwareProtection

- **確認是否依據宣告表**內容實作
- **修改資**產是不可能達成的行為，**或者是可以被安全儲存機制所偵測**

AU.SSM-2.Generic

- **確認是否依據宣告表**內容實作
- **未經授權的修改資**產是不可能達成的行為，**或者是可以被安全儲存機制所偵測**

[SSM-3] Appropriate confidentiality protection for secure storage mechanisms

Requirement

每一個安全儲存機制，必須保護下列內容被儲存在設備的機密性

- 機密安全參數
  (confidential security parameters)
- 機密網路功能設定
  (confidential network function configuration)
- 機密個人資料
  (confidential personal information)
- 機密隱私功能設定
  (confidential privacy function configuration)
- 機密金融資料
  (confidential financial data)
- 機密金融功能設定
  (confidential financial function configuration)

Rationale

當機密安全參數、機密網路功能設定、機密個人資訊、機密隱私功能設定、機密金融資料、機密金融功能設定儲存於設備時需要保護資產不外洩。如果此類資訊沒有適當的保護，攻擊者可以存取和濫用設備和儲存的數據，這可能會導致

- 濫用網路資源
- 個人資訊的暴露
- 詐欺

[SSM-3] Appropriate confidentiality protection for secure storage mechanisms

IXIT	提供資訊	對應欄位
IXIT 6.4-SSM	選擇安全儲存機制完整性保護的實作方式 (Encryption, AccessControl, HardwareProtection, Generic)	SSM-3 (Impl Cat.)
	補充說明實作方式	SSM-3 (Description)
	若安全儲存機制通過資安標準或取得資安證書，請提供佐證資料	SSM-3 (ComplianceEvidence)

[SSM-3] Appropriate confidentiality protection for secure storage mechanisms

Completeness

- PASS
  - 所有儲存在設備的機密資料皆已記錄在宣告表
- FAIL
  - 任一個儲存在設備的機密資料未被記錄在宣告表
- NOT APPLICABLE
  - 其他

評估目的

檢查是否所**有儲存的資**產皆已記錄於宣告表

評估方法

評估是否所有儲存在設備的以下內容未被記錄於宣告表內

- **機密安全參數**
  (confidential security parameters)
- **機密網路功能設定**
  (confidential network function configuration)
- **機密個人資料**
  (confidential personal information)
- **機密隱私功能設定**
  (confidential privacy function configuration)
- **機密金融資料**
  (confidential financial data)
- **機密金融功能設定**
  (confidential financial function configuration)

[SSM-3] Appropriate confidentiality protection for secure storage mechanisms

Sufficiency

- PASS
  - 對於宣告表內每一個安全儲存機制，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內任一個安全儲存機制，其對應的實作測試方法為不成功
- NOT APPLICABLE
  - 其他

評估目的

檢查安全儲存機制是否針對機密資料提供機密性保護功能

評估方法

針對宣告表每一個安全儲存機制

AU.SSM-3.Encryption

- 確認是否依據宣告表內容實作
- 用於加密機密資料的金鑰不能被攔截、推算或擷取
- 在沒有加密資料所使用的金鑰的情況下，讀取機密資料是不可能的

AU.SSM-3.AccessControl

- 確認是否依據宣告表內容實作
- 在未經授權的情況下，讀取機密資料的行為會被安全儲存機制阻擋

[SSM-3] Appropriate confidentiality protection for secure storage mechanisms

Sufficiency

- PASS
  - 對於宣告表內每一個安全儲存機制，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內任一個安全儲存機制，其對應的實作測試方法為不成功
- NOT APPLICABLE
  - 其他

AU.SSM-3.HardwareProtection

- 確認是否依據宣告表內容實作
- 用於提供機密性保護的功能無法被破壞或繞過
- 未經授權讀取機密資料的行為是不可能達成的行為

AU.SSM-3.Generic

- 確認是否依據宣告表內容實作
- 未經授權讀取機密資料的行為是不可能達成的行為

[SCM] Secure communication mechanism

Secure communication mechanism (SCM) 安全要求

Identifier	Requirement	3.3(d)	3.3(e)	3.3(f)
SCM-1	Applicability of secure communication mechanisms	X	X	X
SCM-2	Appropriate integrity and authenticity protection for secure communication mechanisms	X	X	X
SCM-3	Appropriate confidentiality protection for secure communication mechanisms	X	X	X
SCM-4	Appropriate replay protection for secure communication mechanisms	X	X	X

[SCM-1] Applicability of secure communication mechanisms

Requirement

設備透過網頁介面與其他個體在傳輸資產時，應永遠使用安全**連線，但以下情況除外**

(例外條件不適用於 3.3(f))

- **傳輸資**產時透過其他**個體或邏輯機制保護，以確保資**產不**會暴露於未經授權個體**
- **所暴露的資**產是因為建立或管理連線的一部分，並結合其**他措施來驗證連線或信任關係**

Rationale

當使用網路服務時，設備的資產可以傳送給其他個體。持續的**傳輸可能使有權訪問傳輸的攻擊者能**夠竊聽、修改或重送內容，**尤其是在使用無線技術時。設備需要確保使用安全通訊機制來保護傳輸免受這些攻擊。**

[SCM-1] Applicability of secure communication mechanisms

IXIT	提供資訊	對應欄位
IXIT A-Asset	資產會透過網頁介面進行傳輸的情境	SCM-1 (Use case)
	資產是否需要完整性與真實性保護 (Yes, No)	SCM-1 (Protected needed|Integrity and authenticity)
	資產是否需要機密性保護 (Yes, No)	SCM-1 (Protected needed|Confidentaility)
	資產是否需要防止重送攻擊 (Yes, No)	SCM-1 (Protected needed|Replay)
	選擇對應的安全傳輸機制 (IXIT 6.5-SCM)	SCM-1 (SCM)
	若設備未使用安全傳輸機制，選擇對應的例外排除原因	SCM-1 (Exception|Reason)
	例外排除原因的補充說明	SCM-1 (Exception|Description)

[SCM-1] Applicability of secure communication mechanisms

IXIT	提供資訊	對應欄位
IXIT B-Interface	如果該介面為射頻介面，請說明所使用的通訊技術/頻譜/功率等資訊	SCM-1 (Physical characteristics|Radio)
	如果該介面為有線介面，請說明該介面的電子特性	SCM-1 (Physical characteristics|Wired)
	如果該介面為光學介面，請說明該介面所使用的光學技術	SCM-1 (Physical characteristics|Optical)
	如果該介面為聲音介面，請說明該介面所使用的聲學技術	SCM-1 (Physical characteristics|Aoustics)
	設備所使用的設定值，以及可以用來更改介面個體或邏輯行為的選項	SCM-1 (Configuration)
IXIT 6.5-SCM	選擇該安全傳輸方法所使用的通訊協定 (IXIT G-ExposedService)	Protocol
	說明設備是在什麼狀態下會進行資料傳輸	SCM-1 (SCM|States)
	考慮到設備預期功能、威脅分析結果與潛在的功擊場景，所設定的安全目的	SCM-1 (SCM|SecObjectives)
	如果該傳輸用於建立或管理連線，詳細說明建立與管理的流程	SCM-1 (SCM|Manage)

[SCM-1] Applicability of secure communication mechanisms

Completeness

- PASS
  - 所有被傳輸的資產皆已記錄在宣告表
- FAIL
  - 任一個被傳輸的資產未被記錄在宣告表
- NOT APPLICABLE
  - 其他

評估目的

檢查宣告表內容是否完整

評估方法

使用最新的評估方法，檢查是否有被儲存的資產被傳輸至其他個體未被記錄於宣告表

[SCM-1] Applicability of secure communication mechanisms

Sufficiency

- PASS
  - 沒有證據顯示宣告表內的安全傳輸機制沒有被實作
- FAIL
  - 有證據顯示宣告表內的安全傳輸機制沒有被實作
- NOT APPLICABLE
  - 其他

評估目的

檢查安全傳輸機制是否被實作

評估方法

針對宣告表的每一個資產，使用最新評估方法確認，資產是否依據設備的狀態，是否存在安全傳輸機制

[SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms

Requirement

每一個安全傳輸機制必須套用最佳實務，以保護所傳輸的資產完整性與真實性，但以下情況除外：

(例外條件不適用於 3.3(f))

- 為了滿足互通性(interoperability)的要求，無法達成完整性與真實性的最佳實務

Rationale

在傳輸過程中，資產需要防止被操縱。獲得網路存取權限的攻擊者可能會透過中間人攻擊攔截並篡改內容。設備需要透過使用完整性和真實性保護措施來確保傳輸免受這些攻擊。相關保護機制可以透過通訊協定本身所提供的功能，或者是透過額外措施來實現。

無論使用加密或未加密的連線，都必須實施完整性和真實性保護機制

[SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms

IXIT	提供資訊	對應欄位
IXIT 6.5-SCM	說明資產於傳輸過程，用以保護資產完整性與真實性的安全機制與加密模式	SCM-2 (mechanism|Capabilities)
	選擇安全傳輸機制完整性與真實性保護的實作方式 (ManufSecret, SecChanExchange, PKI-based, ThridPartyTrust, Generic)	SCM-2 (mechanism|Impl Cat.)
	補充說明實作方式	SCM-2 (mechanism|Description)
	若有的話，提供實作所參考的標準或規範，以及軟體函式庫	SCM-2 (mechanism|ImplDetail)
	選擇完整性與真實性保護所使用的加密金鑰 (IXIT 6.12-CCK)	SCM-2 (mechanism|CCK)
	說明目前所使用的機制如何避免以下安全威脅 1) 偽造 (spoofing) 2) 篡改 (tampering)	SCM-2 (mechanism|ThreatProtection)

[SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms

Sufficiency

- PASS
  - 對於宣告表內每一個安全傳輸機制，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內任一個安全儲存機制，其對應的實作測試方法為不成功
- NOT APPLICABLE
  - 其他

評估目的

檢查被傳輸的資產是否受保護免於被篡改

評估方法

針對宣告表每一個資產，使用最新評估方法確認資料傳輸機制確保資產的完整性與真實性是根據宣告表內所描述的實作方式：

AU.SCM-2.ManufSecret:

- **當設備透過網路通訊時，生過程中所植入的秘密(secret)無法被截取**
- **被修改的訊息不被認為是完整的**
- **未經授權的訊息不被認為是真實的**
- **如果使用基於通道的資料傳輸，不可能成功執行中間人攻擊**

AU.SCM-2.SecChanExchange:

- **當使用評估的傳輸機制，秘密無法在截取**
- **被修改的訊息不被認為是完整的**
- **未經授權的訊息不被認為是真實的**
- **如果使用基於通道的資料傳輸，不可能成功執行中間人攻擊**

[SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms

Sufficiency

- PASS
  - 對於宣告表內每一個安全傳輸機制，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內任一個安全儲存機制，其對應的實作測試方法為不成功
- NOT APPLICABLE
  - 其他

AU.SCM-2.PKI-based

- 不接受偽造的憑證
- 被修改的訊息不被認為是完整的
- 未經授權的訊息不被認為是真實的
- 如果使用基於通道的資料傳輸，不可能成功執行中間人攻擊

AU.SCM-2.ThirdPartyTrust:

- 第三方的回應無法被操縱
- 被修改的訊息不被認為是完整的
- 未經授權的訊息不被認為是真實的
- 如果使用基於通道的資料傳輸，不可能成功執行中間人攻擊

AU.SCM-2.Generic

- 用來保護真實性和完整性的秘密不能被攔截和濫用
- 被修改的訊息不被認為是完整的
- 未經授權的訊息不被認為是真實的
- 如果使用基於通道的資料傳輸，不可能成功執行中間人攻擊

[SCM-3] Appropriate confidentiality protection for secure communication mechanisms

Requirement

每一個安全傳輸機制必須套用最佳實務，以保護所傳輸的資產機密性，但以下情況除外：

(例外條件不適用於 3.3(f))

- 為了滿足互通性(interoperability)的要求，無法達成機密的最佳實務

Rationale

在資料傳輸中，通常資產需要防止竊聽。攻擊者取得用以傳輸資產的網路存取權後，可以監視資料傳輸以竊取資料。因此設備需要透過提供機密性來確保傳輸免受這些攻擊。

[SCM-3] Appropriate confidentiality protection for secure communication mechanisms

IXIT	提供資訊	對應欄位
IXIT 6.5-SCM	說明資產於傳輸過程，用以保護資產機密性的安全機制與加密模式	SCM-3 (mechanism|Capabilities)
	選擇安全傳輸機制機密性性保護的實作方式 (MessageEnc, ChannelEnc, Generic)	SCM-3 (mechanism|Impl Cat.)
	補充說明實作方式	SCM-3 (mechanism|Description)
	若有的話，提供實作所參考的標準或規範，以及軟體函式庫	SCM-3 (mechanism|ImplDetail)
	選擇機密性保護所使用的加密金鑰 (IXIT 6.12-CCK)	SCM-3 (mechanism|CCK)
	說明目前所使用的機制如何避免以下安全威脅 1) **資訊洩露** (information disclosure) 2) **權限提升** (elevation of privilege)	SCM-3 (mechanism|ThreatProtection)

[SCM-3] Appropriate confidentiality protection for secure communication mechanisms

Sufficiency

- PASS
  - 對於宣告表內每一個安全傳輸機制，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內任一個安全儲存機制，其對應的實作測試方法為不成功
- NOT APPLICABLE
  - 其他

評估目的

檢查被傳輸的資產是否受保護免於被竊聽

評估方法

針對宣告表每一個資產，讓設備和授權個體之間進行資料傳輸，並使用最新評估方法確認資料傳輸機制確保資產的機密性是根據宣告表內所描述的實作方式：

AU.SCM-3.MessageEnc

- 訊息內用於加密資料的金鑰無法洩露
- 被傳輸的資產無法被竊聽

AU.SCM-3.ChannelEnc:

- 加密傳輸通訊通道中用來加密資料的金鑰無法被攔截
- 被傳輸的資產無法被竊聽

AU.SCM-3.Generic

- 用於加密訊息的秘密(secret)不能被攔截或竊聽
- 已加密的訊息內容無法被竊聽或洩漏

[SCM-4] Appropriate replay protection for secure communication mechanisms

Requirement

每一個安全傳輸機制必須套用最佳實務，以保護重送攻擊(replay attack)，但以下情況除外：

- 重複發送不會造成其他資安威脅

(此例外條件不適用於 3.3(f))

- 為了滿足互通性(interoperability)的要求，無法達成機密的最佳實務

Rationale

重送攻擊是一種網路攻擊形式，其中有效的資料傳輸被惡意重新發送。獲得網路存取權限的攻擊者可能會側錄封包內容，並且將內容重新發送，對接收端造成影響。重送攻擊會造成威脅，特別是如果身份認證可能被破壞或可能提交未經授權的控制命令。

例如，如果在使用者登入過程中密碼被加密傳輸，但沒有重送攻擊保護(尤其是會話劫持保護)，則攻擊者可能可以透過重送的加密登入內容，從而獲得授權存取系統。會話劫持攻擊包括利用 Web 會話控制機制，該機制通常是針對會話令牌進行管理的。設備需要保護資料傳輸免受此類攻擊。

基於風險評估，製造商可以識別不需要重送保護的情境，例如，當傳送的資料不會導致接收端的狀態改變時。舉例來說，從伺服器取得 X.509 憑證，便不會造成安全威脅。

[SCM-4] Appropriate replay protection for secure communication mechanisms

IXIT	提供資訊	對應欄位
IXIT 6.5-SCM	說明資產於傳輸過程，用以保護資產機密性的安全機制與加密模式	SCM-4 (mechanism|Capabilities)
	選擇安全傳輸機制機密性性保護的實作方式 (SeqNumb, TimeStamp, OneTimeEncKey, Generic)	SCM-4 (mechanism|Impl Cat.)
	補充說明實作方式	SCM-4 (mechanism|Description)
	若有的話，提供實作所參考的標準或規範，以及軟體函式庫	SCM-4 (mechanism|ImplDetail)
	說明目前所使用的機制如何避免以下安全威脅 1) 否認性 (Repudiation)	SCM-4 (mechanism|Repudiation)

[SCM-4] Appropriate replay protection for secure communication mechanisms

Sufficiency

- PASS
  - 對於宣告表內每一個安全傳輸機制，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內任一個安全儲存機制，其對應的實作測試方法為不成功
- NOT APPLICABLE
  - 其他

Assessment Purpose

檢查被傳輸的資產是否受保護免於**重送攻程**

Assessment units

針對宣告表每一個資產，讓設備和授權**個體之間進行資料傳輸，並使用最新評估方法確認資料傳輸機制避免重送攻擊的方式是根據宣告表**內所描述的實作方式：

AU.SCM-4.SeqNumb

- **不接受帶有重複序號的傳入訊息**

AU.SCM-4.TimeStamp

- **不接受帶有不規則時間戳記的傳入訊息**

AU.SCM-4.OneTimeEncKey:

- **加密金鑰無法被攔截**
- **不接受已接受訊息的複製**內容

AU.SCM-4.Generic

- **不接受已接受訊息的複製**內容

[RLM] Resilience mechanism

Resilience mechanism (RLM) 安全要求

Identifier	Requirement	3.3(d)	3.3(e)	3.3(f)
RLM-1	Applicability and appropriateness of resilience mechanisms	X		

[RLM-1] Applicability and appropriateness of resilience mechanisms

Requirement

設備應具備相關機制，以緩解對網路介面發動的 DoS 攻擊所造成的影響，並且在攻擊之後恢復至指定的狀態，但以下情況除外：

- 網路介面只在本地網路(local network)使用，而本地網路不會與其他網路之間互通；或
- 設備所位於的網路有其他裝置提供足夠的保護，以防止DoS攻擊與喪失與網路相關的基本功能

Rationale

拒絕服務攻擊(DoS)會破壞網路資源的可用性，若受攻擊的裝置無法從 DoS 攻擊中恢復，則可能會導致網路運作永久中斷。在網路裡面的設備（例如，網狀網路節點）需要能夠從 DoS 攻擊中恢復，以便能夠繼續提供網路功能。

一些工控設備要求極高的可用性以維持持續運作。透過限制網路封包速率等機制可能會限制被授權人員對重要功能的授權存取。因此，工業設備的緩解機制可以搭配設備所屬的網路環境實現，而不是在設備本身，以避免對其持續運作產生影響。

[RLM-1] Applicability and appropriateness of resilience mechanisms

IXIT	提供資訊	對應欄位
IXIT B-Interface	選擇對應的DoS攻擊保護機制 (IXIT 6.6-RLM)	RLM-1 (RLM)
	若設備未使用DoS攻擊保護機制，選擇對應的例外排除原因	RLM-1 (Exception|Reason)
	例外排除原因的補充說明	RLM-1 (Exception|Description)
IXIT 6.6-RLM	說明設備緩解DoS攻擊機制，以及攻擊之後會回復至的狀態為何	Description

[RLM-1] Applicability and appropriateness of resilience mechanisms

Completeness

- PASS
  - 所有網路介面皆已經記錄於宣告表內，且
  - 所有保護機制皆已經記錄於宣告表內
- FAIL
  - 任一個網路介面未記錄於宣告表內，或
  - 任一個保護機制未記錄於宣告表內
- NOT APPLICABLE
  - 其他

評估目的

驗證所實施的保護機制是否減輕了DoS攻擊對網路介面的影響，以及設備在被攻擊之後恢復的狀態(網路介面文件的完整性與正確性)

前提條件

設備於處於一般運作狀態，每一個宣告表內的介面需要被啟用或設定，以便執行測試作業

當保護機制被使用時，製造商應提供相關文件說明如何進行保護機制的設定

評估方法

評估是否有網路介面沒有被記錄於宣告表內

評估是否有保護機制沒有被記錄於宣告表內

[RLM-1] Applicability and appropriateness of resilience mechanisms

Sufficiency

- PASS
  - 沒有證據顯示宣告表內的保護機制沒有被實作
- FAIL
  - 有證據顯示有宣告表內的保護機制沒有被實作
- NOT APPLICABLE
  - 其他

評估目的

評估保護機制是否被實作

前提條件

設備於處於一般運作狀態，每一個宣告表內的介面需要被啟用或設定，以便執行測試作業

當保護機制被使用時，製造商應提供相關文件說明如何進行保護機制的設定

評估方法

確認記錄表中所使用的保護機制與其論述

評估保護機制是否在預期的使用環境下，保護機制可以緩解DoS攻擊所造成的影響，並且回復至指定的狀態

[NMM] Network monitoring mechanism

Network monitoring mechanism (NMM) 安全要求

Identifier	Requirement	3.3(d)	3.3(e)	3.3(f)
NMM-1	Applicability and appropriateness network monitoring mechanisms	X		

[NMM-1] Applicability and appropriateness network monitoring mechanisms

Requirement

如果設備屬於網路設備，設備應提供網路監控機制，以偵測網路之間的流量的DoS攻擊指標

Rationale

提高整個系統的網路韌性，防禦與裝置預期用途相關的異常網路流量。作為網路設備都需要能夠偵測此類 DoS 事件的影響，要求設備能夠偵測可能與 DoS 攻擊相關的異常流量和模式。

[NMM-1] Applicability and appropriateness network monitoring mechanisms

IXIT	提供資訊	對應欄位
IXIT 6.7-NMM	請選擇對應的實作方式 (GTPFiltering, IPPackingFiltering, Generic)	Impl Cat.
	補充說明實作方式細節	Description

[NMM-1] Applicability and appropriateness network monitoring mechanisms

Sufficiency

- PASS
  - 對於宣告表內每一個網路監控機制，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內任一個網路監控機制，其對應的實作測試方法為不成功
- NOT APPLICABLE
  - 其他

評估目的

驗證宣告表內的網路監控機制是否適合，驗證經由網路設備的流量是否被監控與分析，**以降到對於資產**的安全威脅

前提條件

設備需處於正常運作模式，並且與網路流量相關功能已經生效

建立個體網路連線

評估方法

AU.NMM-1.GTPFiltering

- **GTP訊息必須被網路設備監控**
- **GTP訊息的發送來源授權必須由網路設備驗證**
- **網路設備能**夠定義與套用規則在不同的**GTP訊息**

AU.NMM-1.IPPacketFiltering

設備網路可以監聽ICMP與ARP等封包，並且

- **偵測基於ICMP的DoS攻擊**
- **偵測基於ARP的DoS攻擊**
- **已採取措施限制DoS造成的影響**

[NMM-1] Applicability and appropriateness network monitoring mechanisms

Sufficiency

- PASS
  - 對於宣告表內每一個網路監控機制，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內任一個網路監控機制，其對應的實作測試方法為不成功
- NOT APPLICABLE
  - 其他

AUM.NMM-1.Generic

評估經由網路設備的流量可以被處理與控制

- **使用封包分析工具評估網路設備可以處理的網路封包類型**
- **評估所發現的網路流量是否與宣告表的一致**

根據宣告表的內容模擬產生可觸發網路監控機制的網路封包流量，評估宣告表內的行為**或輸出是否依宣告**內容產生

[TCM] Traffic control mechanism

Traffic control mechanism (TCM) 安全要求

Identifier	Requirement	3.3(d)	3.3(e)	3.3(f)
TCM-1	Applicability and appropriate traffic control mechanisms	X		

[TCM-1] Applicability of and appropriate traffic control mechanisms

Requirement

如果設備屬於網路設備，設備必須支援網路流量控制機制

Rationale

惡意資料流量可能是由被入侵的設備所產生的。雖然運營商網路可以根據資料封包的表頭資訊實施相關防護機制，以減輕惡意流量的影響，但他們對網路的了解可能會阻礙有效地處理。旨在用於設備到公共網路的網路設備可以有足夠的資訊來檢測惡意流量，並且流量控制機制可以防止公共網路受到相應的損害，透過實施這些安全流量控制機制，網路設備可以建立強大的防禦防止異常流量，保護敏感數據，並透過其應用程式和網路維護預期設備功能的完整性和可用性。

[TCM-1] Applicability of and appropriate traffic control mechanisms

IXIT	提供資訊	對應欄位
IXIT 6.8-TCM	請選擇對應的實作方式 (DatagramRules, TrafficSeparation, Generic)	Impl Cat.
	補充說明實作方式細節	Description

[TCM-1] Applicability of and appropriate traffic control mechanisms

Sufficiency

- PASS
  - 對於宣告表內每一個流量控制機制，其對應的實作測試方法皆為成功
- FAIL
  - 對於宣告表內任一個流量控制機制，其對應的實作測試方法為不成功
- NOT APPLICABLE
  - 其他

評估目的

確認宣告表內的流量控制機制是否合適，確認網路設備是否可以以透過封包轉送，避免已經被入侵的其他設備對於資產造成影響

Preconditions

設備需處於正常運作模式，並且與網路流量相關功能已經生效

Assessment units

AU.TCM-1.DatagramRules

- 網路必須可以監控資料封包(Datagrams)
- 可丟棄或封鎖帶有異常行為模式的惡意封包
- 可丟棄或封鎖未經授權的來源或位址目的地的資料封包

AU.TCM-1.TrafficSeparation

- 針對每一個網段，網路設備不允許資料於網段之間轉送

AU.TCM-1.Generic

- 網路設備所轉送的流量已建立對應的控制機制，其控制機制與宣告表一致

[LGM] Logging mechanism

Logging mechanism (LGM) 安全要求

Identifier	Requirement	3.3(d)	3.3(e)	3.3(f)
LGM-1	Applicability of logging mechanisms		X	X
LGM-2	Persistent storage of log data		X	X
LGM-3	Minimum number of persistently stored events		X	X
LGM-4	Time-related information of persistently stored log data		X	X

[LGM-1] Applicability of logging mechanisms

Requirement

設備應使用日誌記錄關於隱私/財務資產與其保護機制的內部事件，但以下情況除外：

- 法律禁止記錄內部事件

Rationale

為了提供有關此類事件的信息，設備將產生相關日誌。此類日誌資訊可以幫助識別例如潛在的異常設備行為、安全/資料外洩。

[LGM-1] Applicability of logging mechanisms

IXIT	提供資訊	對應欄位
IXIT 6.9(1)-LOGEVENT	選擇該事件對應的資產 (IXIT A-Asset)	Assets
	說明觸發該事件的的行為	Activity
	選擇該事件所使用的日誌記錄機制 (IXIT 6.9-LGM)	LGM
	若設備未使用日誌記錄機制，選擇對應的例外排除原因	LGM-1 (Exception|Reason)
	例外排除原因的補充說明	LGM-1 (Exception|Description)
IXIT 6.9-LGM	選擇使用該機制的日誌事件	LGM-1 (LogEvent)

[LGM-1] Applicability of logging mechanisms

Sufficiency

- PASS
  - 沒有證據顯示宣告表內的日誌記錄機制沒有被實作
- FAIL
  - 有證據顯示宣告表內的日誌記錄機制沒有被實作
- NOT APPLICABLE
  - 其他

評估目的

評估日誌紀錄機制是否被實作

評估方法

針對宣告表內的每一個日誌紀錄，透過以下方法確認相關事件是否被日誌記錄機制所記錄

- **觸發相關事件**
- **存取所**產生的日誌紀錄

[LGM-2] Persistent storage of log data

Requirement

日誌記錄機制必須保存日誌紀錄於設備的儲存裝置，除非
- 相關日誌紀錄儲存在設備之外

Rationale

設備重新啟動後，事件日誌必須保持不變，以防止意外或故意刪除。

[LGM-2] Persistent storage of log data

IXIT	提供資訊	對應欄位
IXIT 6.9-LGM	選擇該日誌記錄機制將日誌紀錄儲存於何處 (Internal, External)	LGM-2 (Location)
	若日誌儲存於內部，請詳細說明日誌儲存的路徑，以及如何確保資料不會消失；若日誌儲存於外部，請說明將日誌儲存至外部的機制為何	LGM-2 (Description)

[LGM-2] Persistent storage of log data

Sufficiency

- PASS
  - 沒有證據顯示日誌紀錄處理方式與宣告表的內容有差異
- FAIL
  - 有證據顯示日誌紀錄處理方式與宣告表的內容有差異
- NOT APPLICABLE
  - 其他

評估目的

評估日誌記錄機制實作方式是否如宣告表內容一致

評估方法

針對宣告表內的每一個日誌記錄機制，當該機制使用內部儲存空間時，透過以下方式確認日誌紀錄是否持續保存於儲存裝置：

- 觸發相關事件
- 存取日誌紀錄所儲存的路徑，確認日誌紀錄是否存在

[LGM-3] Appropriate Logging mechanisms – Minimum number of events

Requirement

所有儲存於設備內部的日誌紀錄，應確保可保存

- 最新事件的最小數量
- 最新事件

Rationale

需要保留最少數量的事件，以確保有足夠的稽核軌跡，以便有效地進行事件調查。

[LGM-3] Appropriate Logging mechanisms – Minimum number of events

IXIT	提供資訊	對應欄位
IXIT 6.9-LGM	說明可保存最新事件的最小數量	LGM-3 (Quantity)

[LGM-3] Minimum number of persistently stored events

Sufficiency

- PASS
  - 沒有證據顯示日誌紀錄所保存的數量可能小於宣告表所宣告的最小數量
- FAIL
  - 有證據顯示日誌紀錄所保存的數量可能小於宣告表所宣告的最小數量
- NOT APPLICABLE
  - 其他

評估目的

評估設備是否可以永久儲存同時記錄宣告表內所定義的日誌紀錄數量

評估方法

透過以下方式，評估日誌紀錄最少可以保存的數量

- 觸發相關事件，以達到宣告表內最小可記錄之筆數
- 存取日誌紀錄所儲存的路徑，計算日誌紀錄所保存的筆數

[LGM-4] Time-related information of persistently stored log data

Requirement

所有儲存於設備內部的日誌紀錄，應確保其時間相關資訊

- 如果設備可取得實際時間，使用時間戳記(timstamp)
- 如果設備無法取得實際時間，使用相對時間資訊

Rationale

需要包含每個事件發生時間的時間戳記或時間資訊，以協助調查事件的時間順序，並與其他裝置上的日誌進行比較。

[LGM-4] Time-related information of persistently stored log data

IXIT	提供資訊	對應欄位
IXIT 6.9-LGM	說明時間戳記所使用的真實時間來源	LGM-4 (Real time available)
	說明時間相關資訊為何	LGM-4 (Real time unavailable)

[LGM-4] Time-related information of persistently stored log data

real time information available

Sufficiency

- PASS
  - 沒有證據顯示所保存的日誌紀錄不包括時間戳記
- FAIL
  - 有證據顯示所保存的日誌紀錄不包括時間戳記
- NOT APPLICABLE
  - 其他

評估目的

評估日誌記錄機制是否如宣告表內容實作，記錄其時間資訊

評估方法

針對宣告表內每一個日誌記錄機制，透過以下方式確認在可取得真實時間的情況下，儲存於設備的日誌記錄皆包括時間戳記

- 確保設備可取得真實時間資訊
- 觸發相關事件
- 存取日誌紀錄應儲存的路徑，確認是否皆帶有時間戳記

[LGM-4] Time-related information of persistently stored log data

real time information unavailable

Sufficiency

- PASS
  - 沒有證據顯示所保存的日誌紀錄不包括時間相關資訊
- FAIL
  - 有證據顯示所保存的日誌紀錄不包括時間相關資訊
- NOT APPLICABLE
  - 其他

評估目的

評估日誌記錄機制是否如宣告表內容實作，記錄其時間資訊

評估方法

針對宣告表內每一個日誌記錄機制，透過以下方式確認在無法取得真實時間的情況下，儲存於設備的日誌記錄皆包括時間相關資訊

- 確保設備無法取得真實時間資訊
- 觸發相關事件
- 存取日誌紀錄應儲存的路徑，確認是否皆帶有時間相關資訊

[DLM] Deletion mechanism

Deletion mechanism (DLM) 安全要求

Identifier	Requirement	3.3(d)	3.3(e)	3.3(f)
DLM-1	Applicability of deletion mechanisms		X	

[DLM-1] Applicability of deletion mechanisms

Requirement

設備應提供資料刪除機制，允許使用者刪除儲存於設備的個人資料與敏感安全參數

Rationale

這項要求是為了防止當更換或報廢設備時，造成個人資料暴露。

[DLM-1] Applicability of deletion mechanisms

IXIT	提供資訊	對應欄位
IXIT A-Asset	選擇對應的資料刪除機制 (IXIT 6.10-DLM)	DLM-1 (DLM)
IXIT 6.10-DLM	說明資料刪除機制，是否可以確保刪除裝置上所儲存的資料 1) 透過使用者 2) 當授權個體有其監督責任時，可以代替使用者執行	DLM-1 (Description)

[DLM-1] Applicability of deletion mechanisms

Completeness

- PASS
  - 所有個人資料與敏感安全參數皆已記錄於宣告表
- FAIL
  - 任一個個人資料與敏感安全參數未被記錄於宣告表
- NOT APPLICABLE
  - 其他

評估目的

評估是否有個人資料與敏感安全參數未被記錄於宣告表

評估方法

評估是否有儲存於設備的個人資料未被記錄於宣告表

評估是否有儲存於設備的敏感安全參數未被記錄於宣告表

[DLM-1] Applicability of deletion mechanisms

Sufficiency

- PASS
  - 沒有證據顯示資料刪除機制未被使用
- FAIL
  - 有證據顯示資料刪除機制未被使用
- NOT APPLICABLE
  - 其他

評估目的

評估資料刪除機制是否被實作

評估方法

針對宣告表內的每一個資料刪除機制，確認其刪除機制是否被設備所使用

[UNM] User notification mechanism

User notification mechanism (UNM) 安全要求

Identifier	Requirement	3.3(d)	3.3(e)	3.3(f)
UNM-1	Applicability of user notification mechanisms		X	
UNM-2	Appropriate user notification content		X	

[UNM-1] Applicability of user notification mechanisms

Requirement

設備應提供使用者通知機制，以通知使用者關於影響個人資料或隱私的變更，除非該變更：

- 存在其他通知機制，而該機制不涉及設備本身

Rationale

目的是在發生可能影響設備收集、儲存或處理的個人資訊的保護和隱私的變化時，確保對設備使用者的透明度。透明度允許設備的使用者決定是否進行某些操作或更新。即時通知用戶可以讓他們做出如何處理這些變更的明智決定。

[UNM-1] Applicability of user notification mechanisms

IXIT	提供資訊	對應欄位
IXIT A-Asset	描述變更會影響個人資料的保護或隱私的所有案例(Use case)	UNM-1 (UseCase|Description
	選擇使用的使用者通知機制 (IXIT 6.11-UNM)	UNM-1 (UseCase|UNM)
	若未選擇使用者通知機制時，選擇例外排除的原因	UNM-1 (Exception|Reason)
	詳細說明例外排除的原因	UNM-1 (Exception|Description)
IXIT 6.11-UNM	說明變更會影響個人資料的保護或隱私的案例	UNM-1 (UseCase)
	詳細說明關於通知使用者相關變更的機制	UNM-1 (Notification|Description)

[UNM-1] Applicability of user notification mechanisms

Completeness

- PASS
  - 所有個人資料與案例皆已記錄於宣告表
- FAIL
  - 任一個個人資料或案例未被記錄於宣告表
- NOT APPLICABLE
  - 其他

評估目的

評估個人資料與其相關案例是否完整被記錄於宣告表

評估方法

評估是否有個人資料未被記錄於宣告表

評估是有關於變成個人資料的案例未被記錄於宣告表

[UNM-1] Applicability of user notification mechanisms

Sufficiency

- PASS
  - 沒有證據顯示宣告表內有案例未被涵蓋在使用者通知機制
- FAIL
  - 有證據顯示宣告表內有案例未被涵蓋在使用者通知機制
- NOT APPLICABLE
  - 其他

評估目的

評估是否有所有的變更所對應的通知皆有實作

評估方法

確認宣告表內的每一種案例，皆存在/使用至少一種使用者通知機制

[UNM-2] Appropriate user notification content

Requirement

使用者通知機制所提供的通知內容，至少需要包括以下內容

- 該此變更內容的相關描述
- 變更將如何影響個人資料的保護與隱私的相關描述

Rationale

透明且易於理解的資訊讓設備的使用者能夠了解影響資料保護和個人資訊隱私的變化。

[UNM-2] Appropriate user notification content

IXIT	提供資訊	對應欄位
IXIT 6.11-UNM	說明通知使用者的內容	UNM-2 (Notification|Content)

[UNM-2] Appropriate user notification content

Sufficiency

- PASS
  - 沒有證據顯示使用者通知機制偏離宣告表的內容
- FAIL
  - 有證據顯示使用者通知機制偏離宣告表的內容
- NOT APPLICABLE
  - 其他

評估目的

評估通知是否包括本條文所要求的資訊

Assessment units

確認宣告表的每一個使用者通知機制的通知內容，是否包括UNM-2所要求的資訊

[CRY] Cryptography

Cryptography (CRY) 安全要求

Identifier	Requirement	3.3(d)	3.3(e)	3.3(f)
CRY-1	Best practice Cryptography	X	X	X

[CRY-1] Best practice cryptography

Requirement

用來保護資產的密碼學技術(cryptography)，設備必須使用最佳實務，以下情況除外

- 該密碼學技術僅使用於特定安全機制，而其與最佳實務的偏離已於 ACM, AUM, SCM, SUM, SSM 等安全類型內完成識別與評估

Rationale

使用最佳實務或更先進、明顯合適的加密技術可以支援對這些資產的加密保護的信任。

如果加密演算法被破解或密碼學原語遭到破壞，則可能需要相應地更新裝置（請參閱要求 SUM），以保護加密所保護的資產。雖然不能絕對保證這種情況不會發生在任何被視為最佳實務的加密技術上，但當已經有證據表明此類加密技術可能在預期生命週期內被棄用時，加密技術更有可能變得不適合特定用例的設備。

然而，如果設備包含基於硬體的加密加速器，本身可以透過網路進行通信，則它可能無法被更新密碼學技術。在這些情況下，重要的是沒有證據表明密碼學技術在預期的使用期限命內不會變成不是最佳實務。

[CRY-1] Best practice cryptography

IXIT	提供資訊	對應欄位
IXIT 6.14-CRY	說明用於加密保護的密碼學技術	CRY-1 (Description)
	選擇使用該密碼學技術的資產與安全機制	CRY-1 (Cryptography used to protect assets)
	說明加密保護的目的	CRY-1 (ProtectionGoal)
	為了滿足加密保護的目的，所選用的密碼學技術是最佳實務的證據	CRY-1 (Best Practice|Evidence)
	所使用的密碼學技術的最佳實務建議是依循哪一份國際標準	CRY-1 (Best Practice|Standard)
	若使用的密碼學技術非最佳實務建議時，說明理由與所依據的資訊	CRY-1 (Best Practice|Deviation)

Reference of Best Practice

- SOGIS agreed Cryptographic Mechanisms
- ETSI TS 119 312 Electronic Signatures and Infrastructures; Cryptographic Suites
- NIST SP800 series
- BSI TR-02102-1

[CRY-1] Best practice cryptography

Completeness

- PASS
  - 沒有證據顯示有設備使用的密碼學技術未被記錄於宣告表
- FAIL
  - 有證據顯示有設備使用的密碼學技術未被記錄於宣告表
- Not Applicable
  - 其他

評估目的

評估宣告表的密碼學技術是否完整記錄

評估方法

檢查是否有證據說明設備使用密碼學技術保護資產，而該密碼學技術未被記錄於宣告表

[CRY-1] Best practice cryptography

Sufficiency

- PASS
  - 沒有證據顯示設備使用的密碼學技術與宣告表不一致
- FAIL
  - 有證據顯示設備使用的密碼學技術與宣告表不一致
- Not Applicable
  - 其他

評估目的

評估密碼學技術是否依宣告表的內容實作

評估方法

針對宣告表每一個密碼學技術，檢查是否有證據顯示其實作方式與宣告內容不一致

[CCK] Confidential cryptographic keys

Confidential cryptographic keys (CCK) 安全要求

Identifier	Requirement	3.3(d)	3.3(e)	3.3(f)
CCK-1	Appropriate CCKs	X	X	X
CCK-2	CCK generation mechanisms	X	X	X
CCK-3	Preventing static default values for preinstalled CCKs	X	X	X

[CCK-1] Appropriate CCKs

Requirement

機密加密金鑰(Confidential cryptographic keys)若是預先安裝在設備或由設備在使用時自行產生，其CCK長度至少需有112個位元，但以下情況除外：

- CCK僅被特定安全機制所使用，且相關偏離已經在對應的安全機制中識別與完成評估。

Rationale

設備可以使用加密技術，因此CCK可以用於許多不同的目的，例如用於身份驗證以強制執行對資產的存取控制、用於保護資產的機密性或完整性，或在與另一個個體通訊時或用於保護資產的機密性或完整性。如果 CCK的機密性受到損害，則 CCK保護的資產也會受到損害。

即便是對設備的成功攻擊時，CCK用合適的演算法所產生時，不會影響該設備或其他設備使用或生成的其他CCK，且該演算法具有足夠的安全強度，可用來抵抗攻擊。

[CCK-1] Appropriate CCKs

IXIT	提供資訊	對應欄位
IXIT 6.12-CCK	CCK使用目的	Description
	CCK是否為預先安裝或使用時自行產生	Type
	CCK長度	CCK-1 (KeyLength)
	若CCK長度不足112位元時，說明理由與相關資訊	CCK-1 (Deviation)
	加密金鑰長度所能提供的安全強度所參考的國際標準	CCK-1 (SecurityStrength)

[CCK-1] Appropriate CCKs

Completeness

- PASS
  - 所有CCK皆被記錄於宣告表
- FAIL
  - 任一個CCK未被記錄於宣告表
- NOT APPLICABLE
  - 其他

評估目的

評估宣告表內的CCK是否完整記錄

評估方法

評估是否有預先安裝或者是由設備所產生的CCK未被記錄於宣告表

[CCK-1] Appropriate CCKs

Sufficiency

- PASS
  - 沒有證據顯示有任何CCK的長度與宣告表不一致
- FAIL
  - 有證據顯示有CCK的長度與宣告表不一致
- Not Applicable
  - 其他

評估目的

評估CCK是否如宣告表內容實作

評估方法

針對宣告表的每一個CCK，評估其金鑰長度是否與宣告表內所參考的國際標準一致

[CCK-2] CCK generation mechanisms

Requirement

CCK的產生方式必須遵循最佳實務(best practice)，但以下情況除外：

- CCK的產生方式僅用於特定安全機制，且安全機制的偏離已在對應的安全機制內識別與完成評估

Rationale

由設備產生的且用於保護資產的CCK必須以適當地方式產生，以防止基於安全強度不足的CCK進行攻擊。適當的 CCK 產生機制可確保 CCK 具有基於相關風險和設備運作條件的必要屬性。

[CCK-2] CCK generation mechanisms

IXIT	提供資訊	對應欄位
IXIT 6.12-CCK	**選擇所使用的**CCK產生機制 (IXIT 6.12(1)-CCKGEN)	CCK-2 (Generate)
IXIT 6.12(1)-CCKGEN	說明CCK產生機制	Description
	選擇CCK產生機制是基於哪種方式 (RNSource, RNG, Derived mechanism)	CCK-2 (Method)
	詳細說明實作方式	CCK-2 (Description)
	選擇CCK產生機制所遵循的國際標準	CCK-2 (Best Practice|Standard)
	若非最佳實務時，說明理由與相關資訊	CCK-2 (Best Practice|Deviation)

Possible Best Practice

- Recognised best practices for Random Number Generators
  - NIST SP800-90A Rev.1
  - NIST SP800-90B
  - NIST SP800-90C
  - BSI AIS20
  - BSI AIS31
  - ISO/IEC 18031

- Recognised best practices for key derivation
  - SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms
  - NIST SP 800-108r1
  - NIST SP 800-132

[CCK-2] CCK generation mechanisms

Conceptual completeness assessment of documentation

- PASS
  - 沒有證據顯示有CCK產生機制未被記錄於宣告表
- FAIL
  - 有證據顯示有任一個CCK產生機制未被記錄於宣告表
- NOT APPLICABLE
  - 其他

評估目的

評估是否所有設備使用的CCK產生方式皆記錄於宣告表

評估方法

透過與CCK-1的CCK清單一致性檢查，檢查是否沒有證據顯示設備所使用的CCK產生機密沒有被記錄於宣告表

[CCK-3] Preventing static default values for preinstalled CCKs

Requirement

每個設備預先安裝的CCK必須是唯一的，但以下情況除外：

- CCK僅用於在授權個體控制的條件下建立初始信任關係；或者
- CCK 是設備預期功能所需的共享參數。

Rationale

設備可以使用加密技術以及 CCK 來保護設備上的資產。 CCK 有時是預先定義的，例如在製造過程中。用於上述目的的CCK需要適當，以防止基於強度不足的CCK的成功攻擊，特別是在預先安裝時。

[CCK-3] Preventing static default values for preinstalled CCKs

IXIT	提供資訊	對應欄位
IXIT 6.12-CCK	說明讓每台設備具有唯一的CCK的實作方式	CCK-3 (Unique)
	選擇CCK不需要每台唯一的排除原因 (Controlled, Shared)	CCK-3 (Excpetion|Reason)
	補充說明例外排除原因	CCK-3 (Excpetion|Description)

[CCK-3] Preventing static default values for preinstalled CCKs

Completeness

- PASS
  - 所有CCK皆已記錄於宣告表
- FAIL
  - 任一個CCK未被記錄於宣告表
- NOT APPLICABLE
  - 其他

評估目的

評估是否所有預先安裝的CCK皆已記錄

前提條件

設備處於出廠預設狀態

評估方法

評估設備是否有預先安裝的CCK未被記錄於宣告表

[CCK-3] Preventing static default values for preinstalled CCKs

Sufficiency

- PASS
  - 沒有證據顯示有CCK應為每台唯一，但實際上不是每台唯一
- FAIL
  - 有證據顯示有CCK應為每台唯一，但實際上不是每台唯一
- NOT APPLICABLE
  - 其他

評估目的

評估預先安裝的CCK宣告應為每台唯一是否足夠獨立

前提條件

2台設備皆屬於出廠預設狀態

評估方法

針對宣告表每一個應為每台唯一的預先安裝CCK，透過以下方面評估2台設備對應的CCK是否實際為唯一

- (如果可以存取CCK)
  比較CCK，並確認不是相同的，且沒有明顯方法可以識別出其衍生關係
- (如果無法存取CCK，但是可以存取對應的公開金鑰)
  比較對應的公開金鑰，並確認不是相同的

[GEC] General equipment capabilities

General equipment capabilities (GEC) 安全要求

Identifier	Requirement	3.3(d)	3.3(e)	3.3(f)
GEC-1	Up-to-date software and hardware with no publicly known exploitable vulnerabilities	X	X	X
GEC-2	Limit exposure of services via related network interfaces	X	X	X
GEC-3	Configuration of optional service and the related exposed network interfaces	X	X	X
GEC-4	Documentation of exposed network interfaces and exposed services via network interfaces	X	X	X
GEC-5	No unnecessary external interfaces	X	X	X
GEC-6	Input validation	X	X	X
GEC-7	Documentation of external sensing capabilities		X	
GEC-8	Equipment Integrity			X

[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities

Requirement

設備不得包括公開已知可利用的漏洞，這些漏洞一旦被利用會影響資產，但以下漏洞除外

- 在設備在特定條件下無法被利用；或
- 已被緩解至可接受的殘餘風險；或
- 經風險評估後可以接受

Rationale

設備可能由許多第三者提供的硬體和軟體組成，製造商可能無法了解第三方元件是否存在安全漏洞，這給製造商帶來了風險。

製造商必須能夠識別設備中使用的硬體和軟體（包括商業軟體和開源軟體）中已知的可利用漏洞，並能夠處理這些漏洞。

[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities

IXIT	提供資訊	對應欄位
IXIT E-SBOM IXIT F-HBOM	第三方元件名稱	GEC-1 (Name)
	元件版本	GEC-1 (Version)
	存在的已知安全漏洞編號	GEC-1 (CVE-ID)
	公開後所對應的安全等級	GEC-1 (Severity)
	是否可被利用 (存在公開的攻擊程式)	GEC-1 (Exploitable)
	選擇漏洞不需要修補的原因 (Remediated, SpecificCondition, Mitgated, Accepted)	GEC-1 (Excpetion|Reason)
	補充說明例外排除原因	GEC-1 (Excpetion|Description)

[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities

Completeness

- PASS
  - 所有發現的公開已知軟體與硬體漏洞皆已記錄於宣告表
- FAIL
  - 任一個發現的公開已知軟體與硬體漏洞未被記錄於宣告表
- NOT APPLICABLE
  - 其他

評估目的

評估文件的完整性，設備上面所存在的弱點皆記錄於宣告表

前提條件

設備必須為正常運作狀態

公開漏洞來源所參考的日期必須是最新的

評估方法

使用當下最新的評估方法，評估硬體元件是否有公開的已知安全漏洞未被記錄於宣告表

使用當下最新的評估方法，評估軟體元件是否有公開的已知安全漏洞未被記錄於宣告表

[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities

Sufficiency

- PASS
  - 沒有證據顯示用來確保漏洞被利用時不會影響資產的措施未依宣告表內容進行實作
- FAIL
  - 有證據顯示用來確保漏洞被利用時不會影響資產的措施未依宣告表內容進行實作
- NOT APPLICABLE
  - 其他

評估目的

評估設備於宣告表列出的漏洞，如果被利用時，不會影響資產

前提條件

設備必須為正常運作狀態

公開漏洞來源所參考的日期必須是最新的

評估方法

針對宣告表上的每一個安全漏洞，評估所採取的措施是否與宣告一致，並且確保漏洞被利用不會影響資產

[GEC-2] Limit exposure of services via related network interfaces

Requirement

在出廠預設狀態下，設備只能對外開放設備設定或基本運作相關，且會影響設備資產的

- 網路介面
- 透過網路介面提供的服務

Rationale

降低設備的網路資源受到損害的一個重要因素是暴露的服務。因此，這些公開的服務需要僅限於設備設定和在預期使用操作環境中操作設備所需的服務。

[GEC-2] Limit exposure of services via related network interfaces

IXIT	提供資訊	對應欄位
IXIT B-Interface	此介面在預設狀態下的狀態 (Enabled, Disabled)	GEC-2 (factory default|State)
	該介面在預設狀態下是否為必要 (Essential, Optional)	GEC-2 (factory default|Necessity)
	若該介面在預設狀態下為必要，說明該介面為必要之原因	GEC-2 (factory default|Desc)
IXIT D-Documents	設備設定安裝手冊	Documentation of Secure Setup
IXIT G-ExposedService	此服務在預設狀態下的狀態 (Enabled, Disabled)	GEC-2 (factory default|State)
	該服候在預設狀態下是否為必要 (Essential, Optional)	GEC-2 (factory default|Necessity)
	若該服務在預設狀態下為必要，說明該服務為必要之原因	GEC-2 (factory default|Desc)

[GEC-2] Limit exposure of services via related network interfaces

Completeness

- PASS
  - 在出廠預設狀態下，所有的網路介面或網路服務皆已記錄於宣告表，並且其用途為設備設定或基本操作相關
- FAIL
  - 在出廠預設狀態下，任一個網路介面或網路服務未被記錄於宣告表，或其用途非設備設定或基本操作相關
- NOT APPLICABLE
  - 其他

評估目的

評估設備在出廠預設狀態下僅對外開放設備設定或基本操作相關的網路介面與相關服務

前提條件

設備必須處於可操作的出廠預設狀態，並且還沒有開始進行相關設定

建立個體網路連線以檢查所開放的網路服務

評估方法

評估設備在出廠預設狀態下，是否有對外開放的網路介面或服務沒有被記錄在宣告表，或者是網路介面或服務非不屬於設備設定或基本操作相關

[GEC-3] Configuration of optional services and the related exposed network interfaces

Requirement

在設備出廠預設狀態所開放的非必須使用(optional)的網路介面與網路服務，被授權的使用者必須可以選擇啟用和停用該介面或服務

Rationale

這將減少與網路介面與網路服務相關的攻擊面

[GEC-3] Configuration of optional services and the related exposed network interfaces

IXIT	提供資訊	對應欄位
IXIT B-Interface	**是否有選項可以讓被授權的使用者**啟用或停用 (Yes, No)	GEC-3 (factory default, but optional|Manual disable)
	若有，說明被授權的使用者如何啟用或停用服務	GEC-3 (factory default, but optional|Description)
IXIT G-ExposedService	**是否有選項可以讓被授權的使用者**啟用或停用 (Yes, No)	GEC-3 (factory default, but optional|Manual disable)
	若有，說明被授權的使用者如何啟用或停用服務	GEC-3 (factory default, but optional|Description)

[GEC-3] Configuration of optional services and the related exposed network interfaces

Completeness

- PASS
  - 沒有任何非必須使用的網路介面或服務沒有被記錄在宣告表
- FAIL
  - 任一個非必須使用的網路介面或服務沒有被記錄在宣告表
- NOT APPLICABLE
  - 其他

評估目的

評估是否所有出廠預設的非強制使用的網路介面或服務皆已記錄於宣告表

前提條件

設備需處於一般運作狀態，並且已完成相關安裝設定

使用具有設定網路介面與服務的角色權限

評估方法

評估是否有非必須使用的網路介面或服務沒有被記錄在宣告表

[GEC-3] Configuration of optional services and the related exposed network interfaces

Sufficiency

- PASS
  - 有證據顯示出廠預設的所有非必要使用的網路介面或服務皆至少提供啟用或停用的選項，而且只能由被授權的使用者執行
- FAIL
  - 沒有證據顯示出廠預設的所有非必要使用的網路介面或服務皆至少提供啟用或停用的選項，而且只能由被授權的使用者執行
- NOT APPLICABLE
  - 其他

評估目的

評估是否出廠預設的所有非必要使用的網路介面或服務，至少提供啟用或停用的選項

前提條件

設備需處於一般運作狀態，並且已完成相關安裝設定

使用具有設定網路介面與服務的角色權限

評估方法

針對宣告表每一個出廠預設的網路介面與服務，執行以下評估作業:

- 是否可進行設定
- 是否至少可以啟用或停用
- 相關設定只能由被授權的使用者執行

[GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces

Requirement

設備的使用者手冊必須包括以下內容描述

- 出廠預設的所有網路介面
- 出廠預設的所有網路服務

Rationale

設備本身與所處的網路需要正確配置，以確保設備的功能並支援網路的安全。因此，提供有關對外開放的網路介面與網路服務與預期使用操作環境的資訊非常重要

[GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces

IXIT	提供資訊	對應欄位
IXIT D-Documents	出廠預設所提供的網路介面與網路服務資訊	Documentation of exposed services via network interfaces

[GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces

Completeness

- PASS
  - 在出廠預設狀態下，所有網路介面與服務皆已記錄於宣告表
- FAIL
  - 在出廠預設狀態下，任一個網路介面與服務未被記錄於宣告表
- NOT APPLICABLE
  - 其他

評估目的

評估是否每一個出廠預設狀態的網路介面與服務皆已被記錄於使用者手冊

前提條件

設備必須處於出廠預設狀態

建立網路連線以檢查所開放的網路介面與服務

評估方法

評估網路介面與網路服務的文件資訊是否完整：

- 評估是否存在出廠預設狀態下對外開放的網路介面沒有被記錄於宣告表
- 評估是否存在出廠預設狀態下對外開放的網路服務沒有被記錄於宣告表

[GEC-5] No unnecessary external interfaces

Requirement

設備只能開放因設備預設功能所需要的實體外部介面

Rationale

透過保持最少的個體外部介面，以最大限度地減少潛在的攻擊面

[GEC-5] No unnecessary external interfaces

IXIT	提供資訊	對應欄位
IXIT B-Interface	實體介面描述	GEC-5 (PhsyicalInt|Type)
	說明該實體介面所對應之預期使用功能	GEC-5 (PhsyicalInt|IntFunc)

[GEC-5] No unnecessary external interfaces

Completeness

- PASS
  - 所有實體外部介面皆已記錄於宣告表
- FAIL
  - 任一個實體外部介面未被記錄於宣告表
- NOT APPLICABLE
  - 其他

評估目的

評估是否只開放設備本身預期功能所必須的實體外部介面

評估方法

透過以下方式嘗試尋找所有實體外部介面

- 檢查設備相關的文件，包括但不限於設計文件、使用案例及使用者手冊
- 檢查設備本身具備的**實體外部介面，包括但不限於麥克風、螢幕、按鈕或記憶卡插槽**

[GEC-6] Input validation

Requirement

如果輸入資料對資產有潛在影響，設備應驗證透過外部介面所**接收的輸入資料**

Rationale

設備需要驗證對資產有潛在影響的任何輸入資料，減少潛在的**誤用、損壞或未經授權取得資**產的資料。

輸入驗證對於驗證作為預期輸入提供的任何輸入資料的語法、長度和內容以及具有正確處理資料所需的屬性是必要的。

不正確的輸入驗證被認為是最常見和最危險的軟體弱點之一，它還會導致其他一些軟體弱點，SQL Injection, OS Command Injection, Path traversal

特別是來自潛在不受信任來源的資料（例如透過網路介面接收的任何輸入）需要透過檢查輸入的語法和格式正確性來進行輸**入驗證。在處理任何輸入時應儘早進行這些檢**查，以避免傳播**無效甚至惡意輸入。**

[GEC-6] Input validation

IXIT	提供資訊	對應欄位
IXIT B-Interface	說明此介面所使用的通訊協定, API, 輸入資料格式	GEC-6 (Capabilities)
	選擇所使用的輸入驗證方式 (IXIT 6.13(1)-GEC6)	GEC-6 (Validation)
IXIT 6.13(1)-GEC6	說明該機制如何針對資料內容、長度及格式進行驗證	Description

[GEC-6] Input validation

Completeness

- PASS
  - 所有外部介面皆已記錄於宣告表
- FAIL
  - 任一個外部介面未被記錄於宣告表
- NOT APPLICABLE
  - 其他

評估目的

針對設備外部介面與相關輸入驗證機制的文件完整性進行評估

前提條件

設備處於正常運作狀態，並且作為預期功能的所有外部介面都必須啟用且完成設定，以便針對每個外部介面進行測試

在需要身份認證才能存取外部介面的情況下，必須提供可以測試該介面的方法

評估方法

透過以下方式評估是否有輸入方法未被記錄於宣告表：

- 透過分析網路介面的流量找出輸入方法
- 透過目視檢測、使用者手冊及設計文件找出非網路介面的外部介面輸入方法
- 根據宣告表的內容觸發相關輸入方法

[GEC-6] Input validation

Sufficiency

- PASS
  - 沒有證據顯示任何輸入驗證測試可以成功破壞, 竊取, 濫用對應的資產
- FAIL
  - 有證據顯示有輸入驗證測試可以成功破壞, 竊取, 濫用對應的資產
- NOT APPLICABLE
  - 其他

評估目的

評估宣告表所描述的實作技術

前提條件

設備處於正常運作狀態，並且作為預期功能的所有外部介面都必須啟用且完成設定，以便針對每個外部介面進行測試

在需要身份認證才能存取外部介面的情況下，必須提供可以測試該介面的方法

評估方法

透過以下方式評估每一個外部介面是否可以抵抗異常資料輸入攻擊：

- 根據宣告表的內容產生格式錯誤或者是無效的訊息，執行 SQL Injection, Ajax Injection, OS command Injection, Path Traversall等攻擊，嘗試破壞, 竊取, 濫用相對應的資產
- 評估設備行為或輸出結果是否與宣告表一致

[GEC-7] Documentation of external sensing capabilities

Requirement

所有跟使用者或訂閱者隱私相關的設備外部感測能力皆應文件化，並提供給使用者

Rationale

外部感測功能可能被濫用來刺探設備的使用者。如果使用者不知道設備的感測功能，則可能會無意中在與隱私相關的位置使用該設備。記錄外部感測功能可以讓使用者意識到設備在技術上可能會暴露他們的隱私。有了這種認識，使用者就可以調整設備的使用，以盡量減少隱私受到損害的風險。

[GEC-7] Documentation of external sensing capabilities

IXIT	提供資訊	對應欄位
IXIT B-Interface	此介面是否具備外部感測能力 (Yes, No)	GEC-7 (Sensing Capability)
	若有，該能力是否會影響使用者隱私 (Yes, No)	GEC-7 (Affect Privacy)
IXIT D-Documents	記錄設備外部感測功能的文件	Documentation of Sensors

[GEC-7] Documentation of external sensing capabilities

Completeness

- PASS
  - 所有會影響使用者隱私的非網路外部介面皆已記錄於宣告表
- FAIL
  - 任一個會影響使用者隱私的非網路外部介面未被記錄於宣告表
- NOT APPLICABLE
  - 其他

評估目的

評估是否所有會影響使用者隱私的非網路外部介面皆已於使用者手冊中說明

評估方法

評估是否有會影響使用者隱私的非網路外部介面未被記錄於使用者手冊

[GEC-8] Equipment Integrity

Requirement

若設備處理金融資產時，應使用不可變的信任根或者是基於密**碼學技術的身分認證與驗證的可信的信任根(root of trust)，驗證開機流程軟體的完整性與真實性**

Rationale

開機完整性驗證是許多產品中的實用功能，可確保軟體可以在**已驗證狀態下**啟動。它還可以在裝置軟體的啟動、重新啟動或**待機（或休眠）後恢復期間偵測攻擊者損壞或修改的軟體。**

與重新啟動裝置的管理功能和開機完整性功能相結合，這提供**觸發合法軟體復原的可靠方法。或者，至少可以通知個體該軟體未經驗證，設備可視為該軟體為已損壞，且不能被信任。**

[GEC-8] Equipment Integrity

IXIT	提供資訊	對應欄位
IXIT C-PartOfSoftw	**選擇對應的安全**啟動機制 (IXIT 6.13(2)-GEC8	GEC-8 (IntegrityProtect)
IXIT 6.13(2)-GEC8	說明啟動流程如何透過密碼學技術驗證軟體的完整性	Description
	說明啟動流程所使用的信任根(root of trust)**與信任錄**(chain of trust)	GEC-8 (TrustAnchor)
	說明啟動流程所使用的安全機制細節	GEC-8 (SecMech)
	說明軟體完整性檢查所使用的演算法或通訊協定模式	GEC-8 (Modes)

[GEC-8] Equipment Integrity

Completeness

- PASS
  - 沒有證據顯示每個軟體部件的開機完整性流程沒有被記錄於宣告表軟體完整性
- FAIL
  - 有證據顯示有任一軟體部件的開機完整性流程沒有被記錄於宣告表軟體完整性
- NOT APPLICABLE
  - 其他

評估目的

評估開機完整性流程是否完整被記錄於宣告表

評估方法

針對宣告表內每個軟體組件，評估是否有開機完整性流程未被記錄於宣告表

[GEC-8] Equipment Integrity

Sufficiency

- PASS
  - 沒有證據顯示開機完整性流程與宣告表不一致，且
  - 沒有證據顯示有任何一個評估方法未滿足
- FAIL
  - 有證據顯示開機完整性流程與宣告表不一致，或者
  - 有證據顯示有至少一個評估方法未滿足
- NOT APPLICABLE
  - 其他

評估目的

評估開機完整性流程是否可保護被啟動的軟體部件的完整性

評估方法

針對宣告表裡面的每個開機完整性流程，執行以下評估作業

- **宣告表**內所有的用於開機完整性檢查的資訊與設備本身一致
- **開機完整性流程已**啟用
- **開機完整性流程正確地使用密碼學技術驗證軟體的完整性**
- **開機流程使用不可變的信任根或使用基於密碼學的身分認證與授權下使用可變的信任根**

滿意度調查

100 YEARS SECURING THE FUTURE 1925 - 2025

Thank you.

contact.onward@dekra.com
www.onwardsecurity.com

Onward Security

Realize Ultimate Security | every step starts with the labs

