EUROSMART
The Voice of the Digital Security Industry

A Cartography of Security Certification Schemes/Standards for IOT

Authors: Internet of Trust S.A.S. (IOTR) – TÜV Informationstechnik GmbH (TÜViT)

Release: 1.2 –Final report for Eurosmart members distribution

Date: 30/12/2019

Forward – Disclaimer

The present report is based on data collected during the following period: June 19-Sept 19.

The content of this document does not reflect the official opinion of Eurosmart. This is intended for informative purposes only, Eurosmart is not liable for the accuracy of the information contained in this cartography.

Answers collected during this work are quoted as appropriate. Eurosmart is not responsible for the content of the received questionnaires including external websites referenced in this report.

Eurosmart does not accept any liability for the consequences of any action taken as a result of the work or any recommendations made or inferred.

Acknowledgement

IOTR and TÜViT would like address a warm thank you to all the people who accepted to spend time to fill the questionnaires. These contributions were essential to collect the information gathered in this report.

Thank you also to Eurosmart members that spent time to check the report before its release.

Table of Contents

Table of Contents 2
List of Tables 3
1 Introduction 4
1.1 Objective 4
1.2 Information collected method 5
1.3 List of schemes 6
2 Result Synthesis 7
2.1 Schemes Overview 7
2.2 Targeted Market and Users 9
2.3 Operational Description and Governance of the Scheme 12
2.4 Products Evaluated by the Scheme 17
2.5 Evaluation Methodologies 19
2.5.1 Evaluation Labs 19
2.5.2 Evaluation Process 21
2.5.3 Testing Process 27
2.6 Compliance Level with Art. 54 of the Cyber Security Act 30
3 Links to the scheme documentation when available 32
4 Revision History 34

List of Tables

Note that the numbers relate to the questionnaire and are not meaningful in this report.

Table 1: Scheme overview (Q3, Q5) 7
Table 2: Targeted markets (Q1) 9
Table 3: Users of schemes (Q2) 10
Table 4: Scheme details (Q4, Q6, Q7, Q8, Q9) 12
Table 5: Scheme maintenance (Q10, Q11) 14
Table 6: Risk Analysis and Management (Q31, Q32, Q33, Q34) 16
Table 7: Mapping between schemes and products (Q22, Q23, Q24) 17
Table 8: Evaluation Labs (Q18, Q19, Q20, Q21) 19
Table 9: Evaluation Process (Q12, Q13) 21
Table 10: Evaluation requirements (Q14, Q16) 22
Table 11: Supporting documents of the schemes (Q17) 25
Table 12: Compliance overview (Q25, Q26, Q27, Q28, Q29, Q30) 27
Table 13: Compliance overview (Q35) 30

1 Introduction

1.1 Objective

The work consists in a cartography of certification schemes selected by Eurosmart that are applicable to IoT (Internet of Things) in Europe. The selection includes national, proprietary certification scheme, security standards, guidelines or framework and they are collectively called 'scheme' in the rest of the document.

This report provides an overview of the selected schemes on several criteria that are important to the industry: the main targeted product or group of products, the associated markets and users, the technical characteristics and the compliance with the European Cybersecurity Certification framework. This report is built on a compilation of data collected through interview and questionnaires.

It is intentional to keep the rough information as it has been collected and to leave the analysis and any inferred information to the reader.

It is important to note that the report is based on answers have been collected from June to September 2019. Therefore, the information might be outdated.

We have done our best to have up to date information at that time but note that the responsibility of TÜViT and IOTR is limited to the collection and the aggregation of the answers.

Because of these two characteristics that are inherent of this kind of work, this report is only a tool to understand the certification landscape. In case you need reliable and up-to-date information about the schemes, please contact them directly (list of websites available in the last section).

For any comment, question, suggestion about this report and its possible updates please contact.

Pierrejean.verrando@eurosmart.com

1.2 Information collected method

The following steps have been conducted to prepare this report:

1. Selection/validation by Eurosmart of the schemes list (see next section);
2. Design of a questionnaire by IOTR, TÜViT and validation by Eurosmart;
3. Selection/validation by Eurosmart of the Interviewees to fill the questionnaire among end-users, labs, editors or scheme owners;
4. Distribution of the questionnaire to the Interviewees by IOTR and TÜViT;
5. Collection and the aggregation of the answers by IOTR and TÜViT;
6. First version of the report distributed to Eurosmart members;
7. This version of the report incorporating Eurosmart members comments.

1.3 List of schemes

The following IoT certification schemes have been chosen (links to scheme description are given in §3):

1. BSPA: Baseline Security Product Assessment
2. BSZ: Accelerated Security Certification
3. CPA: Commercial Product Assurance from CESG
4. CSPN: First Level Security Certification (Certification de sécurité de premier niveau)
5. e-IoT-SCS: Eurosmart IoT Security Certification Scheme
6. ETSI TS 103 645: Cybersecurity for consumer IoT standard
7. GP TEE: GlobalPlatform Trusted Execution Environment
8. GP SE: GlobalPlatform Secure Element
9. GSMA IoT SA: GSMA IoT Security Assessment
10. IEC 62443 standard
11. IoTSCF: IoT Security Compliance Framework
12. LINCE: National Essential Safety Certification evaluation (Certificación Nacional Esencial de Seguridad)
13. PSA Certified: Platform Security Architecture Certified.
14. SESIP: Security Evaluation Standard for IoT Platforms
15. SOG-IS (CC): Senior Official Group Information Security Systems (Common Criteria)
16. TÜViT-SQ: Security Qualification
17. UL IoT Security Rating
18. UL 2900

The web links for all these schemes are available in the last section of this document when they are available.

Note that for the grey ones we could not receive the filled questionnaire on time. Therefore, they are not represented in the rest of the report.

2 Result Synthesis

2.1 Schemes Overview

Table 1: Scheme overview (Q3, Q5)

Identifier	Description	Public or private[1]	Owner	Launched
BSPA	The Dutch Scheme for Baseline Security Product Assessment	Public	AIVD/NLNCSA	2015
CSPN	French First Level Certification	Public	ANSSI	2008
e-IoT-SCS	Eurosmart IoT Security Certification Scheme for IoT devices with a focus on the Substantial security assurance level	Private	Eurosmart organisation	June 2019
IoTSCF	IoT Security Compliance Framework is a structured list of security requirements and an evidence gathering process (Compliance Checklist) to guide an organization through assurance and evidence gathering. It can be used to declare conformance with Best Practice Guidelines provided by IoTSF.	Private	IoT Security Foundation (IoTSF)	2016
LINCE	This methodology is designed for ICT products requiring certification with medium or low security criticality.	Public	CCN	June 2018
PSA certified Level 1	Security model based critical security questions with lab interview • For Chip vendors • For OS suppliers • For OEMs	Private	ARM	February 2019
PSA certified Level 2	Lab based evaluation of the PSA-RoT Mid assurance & mid robustness • For Chip Vendors	Private	ARM	February 2019
UL IoT Security Rating	UL's IoT Security Rating is a highly efficient and comprehensive evaluation process that assesses critical security aspects of smart products against common attack methodologies and known IoT vulnerabilities, to create a 'security baseline' among the consumer IoT industry.	Private	UL	May 2019

[1] Public or private relates to the governmental state ownership (not the fact that they are available publicly).

Identifier	Description	Public or private[1]	Owner	Launched
UL 2900	UL 2900 is a series of standards published by UL (formerly Underwriters Laboratories), a global safety consulting and certification company. The standards present general software cyber security requirements for network-connectable products (UL 2900-1), as well as requirements specifically for medical and healthcare systems (UL 2900-2-1) and security and life safety signaling systems (UL 2900-2-3).	Public	UL	2016: UL test outline 2017: ANSI standard
IEC 62443	The IEC 62443 family of standards has cybersecurity requirements for industrial automation control systems that a manufacturer or system integrator needs to instill cybersecurity rigor into their processes. It also applies to (factory) owners, who operate the systems in place.	Private Private Private	ISA (International Society of Automation) IECEE (IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components) UL (all schemes differ in scope and content)	2011 2017 2019
BSZ	Security scheme like CSPN and BSPA	Public	BSI	Q4 2019
SOG-IS	Common Criteria certification scheme	Public	SOG-IS	March 1992
SESIP	The Security Evaluation Standard for IoT Platforms (SESIP) defines a standard for trustworthy assessment of the security of the IoT platforms, such that this can be re-used in fulfilling the requirements of various commercial product domains.	Private	GlobalPlatform (GP)	December 2018
TÜViT-SQ	Security Qualification for trusted products and trusted sites	Private	TÜV Informationstechnik GmbH (TÜViT)	Current version is 10.0 The scheme was launched more than 10 years ago
ETSI TS 103 645	A standard for cybersecurity in the Internet of Things, to establish a security baseline for internet-connected consumer products and provide a basis for future IoT certification schemes.	Private	ETSI	No answer provided
GP TEE	GlobalPlatform Trusted Execution Environment	Private	GlobalPlatform	2015
GP SE	GlobalPlatform Secure Element	Private	GlobalPlatform	
GSMA IoT SA	Global System for Mobile Communications	Private	GSMA	

Identifier	Description	Public or private[1]	Owner	Launched
CPA	Commercial Product Assurance	Public	NCSC	

2.2 Targeted Market and Users

The following table provides an overview of the targeted markets of each scheme.

Table 2: Targeted markets (Q1)

List of targeted markets	BSPA (NLNCSA)	CSPN (ANSSI)	e-IoT-SCS	LINCE	PSA certified Level 1	PSA certified Level 2	UL IoT Security Rating	UL 2900	IEC 62443	IOTSCF	BSZ	SOG-IS	SESIP	TÜViT-SQ	ETSI TS 103 645	GP TEE
Automotive	x	x	x	x	x	x				x		x	x	x		x
Energy metering	x	x	x	x	x	x	x	x	x			x	x			x
Industry 4.0	x	x	x	x	x	x		x	x	x	x	x	x	x		x
IoT Device (components of PCB)	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Medical devices	x	x	x	x	x	x		x		x	x	x	x	x		x
Payment applications / online banking	x	x	x	x												
Connectivity (eUICC, network products)	x	x	x	x	x	x	x	x				x	x		x	
Government (Qscd, passport, …)	x	x		x								x				
Access control	x	x		x	x	x	x	x	x			x	x	x		x
Time stamping	x	x		x	x	x							x	x		
Other answers provided	(1) (8)	(8)	(4)	(8)			(5)	(5)	(5)	(6)	(2)			(7)		

Other answers:

(1) Network Security, Network filtering, detection and response, secure messaging, Media and file security

(2) Network Devices

(3) Smart Home, Smart Cities, Smart health, Tracking system (vehicle), etc.

(4) Consumer (smart home, consumer electronics, etc.), Enterprise (Businesses, Connected Schools, Smart Building, Financial Institutions, etc.)

(5) Smart home, smart building and Industry 4.0/industrial IoT security standards or frameworks applicable at product-, system- and/or process-level.

(6) Cross-sector: IoT-class component, device, product and service providers

(7) The SQ based on TOE specific security requirements and is suitable for evaluation of a wide variety of IT systems/products.

(8) General purpose methodology (could be applicable for any markets).

The following table summarizes users of the scheme:

Table 3: Users of schemes (Q2)

List of targeted markets	BSPA (NLNCSA)	CSPN (ANSSI)	e-IoT-SCS	LINCE	PSA certified Level 1	PSA certified Level 2	UL IoT Security Rating	UL 2900	IEC 62443	IOTSCF	BSZ	SOG-IS	SESIP	TÜViT-SQ	ETSI TS 103 645	GP TEE
Chip manufacturers (Silicon and Firmware)	x	x	x	x	x	x			x		(13)		x	x	(14)	x
OS Developers	x	x	x	x	x								x	x		x
Application Developers	x	x	x	x	x		x	x	x				x	x		x
Device Makers	x	x	x	x	x		x	x	x				x	x		x
Governments								x	x			x	x			
Other answers provided	(1)	(2)								(3)			(4)			
Service Providers			x				x	x	x				x	x	(14)	
Product vendors		x	x				x	x	x		x		x	x		x

List of targeted markets	BSPA (NLNCSA)	CSPN (ANSSI)	e-IoT-SCS	LINCE	PSA certified Level 1	PSA certified Level 2	UL IoT Security Rating	UL 2900	IEC 62443	IOTSCF	BSZ	SOG-IS	SESIP	TÜViT-SQ	ETSI TS 103 645	GP TEE
Integrators			x				x	x	x					x		
Operators		x	x				x	x	x					x		
Evaluation Laboratory																
Certification Body				x				x	x							
Government organisations		x						x	x		x	x				
Other answers provided		(5)					(6)	(6)	(6)	(7)			(8)			
End-Customers	x	x	x	x	x	x	x	x	x		x		x		x	
Service Providers	x	x	x	x	x	x	x	x	x		x		x	x		x
Integrators		x	x	x	x	x	x	x	x				x	x		x
Government organisations	x	x		x				x	x			x	x			
Telco operators, banking, energy, etc.		x	x		x	x	x	x	x				x			
Other answers provided	(1)	(9)					(10)	(10)	(10)	(11)			(12)			

Other answers:

(1) Governmental organizations. Can vary from top government (SSC-IT) to local governmental bodies. Also, organizations involved in NL vital sectors or industry. Also, vendors / developers are welcome. This scheme is open to whoever pays for the assessment.

(2) French Administration (due to French general security framework, aka RGS), Undisclosed private risk owners: energy, banking, etc.

(3) The scheme is comprehensive and voluntary and can be applied broadly. It is especially attractive to start-ups and traditional manufacturers that rely on embedded systems which are now introducing connectivity to enhance those products or create new services.

(4) Could be anybody.

(5) Public risk owners such as ANSSI/SGDN, ANTS. Private risk owners such as Orange, GIE SESAME VITALE.

(6) Banks, Insurers, Real estate developers, Any asset owner, Any network connectivity provider, Any service provider, Any buyer, Any manufacturer

(7) IOT solution vendors and their customers throughout a supply chain. The power of the scheme is that it is risk based, and can be used at component, service and product level.

(8) Any form of platform developer.

(9) The direct users are the developers and sponsors. Sponsors can be either:

a. French Administration or Private risk owners (who need certification for procurement reasons),

b. Product vendors themselves (who need certification for marketing reasons)

(10)Retailers / distributors, Tech giants, Telco operators, Consumers, Building owners / operators, Factory owners / operators, Installers / architects / designers, Utilities"

(11)Those that have a need to demonstrate IoT cybersecurity assurance for their business. This covers most IOT product or solution vendor. It also includes those providing security services for vendors such as IoT security consultants and evaluation laboratories.

(12)Could be anybody

(13)The scheme BSZ is currently still in market entry. Therefore, there is no group available that actually insists on used certificates issued by the scheme.

(14)No assurance scheme.

2.3 Operational Description and Governance of the Scheme

Table 4: Scheme details (Q4, Q6, Q7, Q8, Q9)

	Scheme documentation owner	Certificate issuer	Number of issued certificates	Location of published certificates	Certification fees
BSPA (NLNCSA)	AIVD/NLNCSA	(3)	N/A, (3)	Not yet available	(6)
CSPN (ANSSI)	ANSSI	ANSSI	>100	https://www.ssi.gouv.fr/administration/produits-certifies/cspn/produits-certifies-cspn/	Free
e-IoT-SCS	Eurosmart	Accredited CAB-R	0, pilot phase	Eurosmart and CAB websites	(6, 7), 2k-5k EUR
LINCE	CCN and SSB	CCN	12	Not answered	Free

	Scheme documentation owner	Certificate issuer	Number of issued certificates	Location of published certificates	Certification fees
PSA certified Level 1	PSA	ARM	33	https://www.psacertified.org/certified-products/	PSA Certified Level 1 and Level 2 certification costs are fixed: €500 and €7.500. See https://trustcb.com/iot/psa-certified/ Pricelist
PSA certified Level 2	PSA	ARM	0, pilot is planned		
UL IoT Security Rating	UL	UL (no certificate but UL verified listing)	0	https://verify.ul.com	(6, 7)
UL 2900	(1)	(1)	>10	https://iq.ulprospector.com/info/	(6, 7)
IEC 62443	(1)	(1)	>50		(6, 7)
IOTSCF	IoTSF	N/A, (4)	N/A, (4)	N/A, (4)	Free
BSZ	BSI	BSI	0, pilot phase		4k EUR
SOG-IS	SOG-IS	CC scheme bodies	> 10		Nation specific
SESIP	GP	(2)	3	https://trustcb.com/iot/sesip/sesip-certificates/	(6), 3k – 20k EUR
TÜViT-SQ	TÜViT	TÜViT	10 products, 23 systems	https://www.tuvit.de/de/leistungen/zertifizierung/sicherheitstechnische-qualifizierung-sq-von-it-installationen/ https://www.tuvit.de/de/leistungen/zertifizierung/sicherheitstechnische-qualifizierung-sq-von-it-produkten/	(7,8) 5k-10k EUR
ETSI TS 103 645	ETSI is not a certification scheme but rather a standard for consumer IoT security				
GP TEE	GP and GP TEE technical committee	GP secretariat	3 certificates are published on the web page, more certificates not published have been indicated.	https://globalplatform.org/certified-products/?filter-certification-type=security	For GP members: 5,5k EUR / 12k EUR For others: 11k EUR / 17k EUR (9)

Note: Certification fees include only certification and not evaluation.

Other answers:

(1) ANSI or IECEE accredited organizations including UL.

(2) Currently TrustCB is the CB responsible. SESIP's ownership is now transferred to GlobalPlatform (GP).

(3) There is no delivery of certificates. A deployment advisory with a Statement of Conformity (SoC) is issued. A Statement of Conformity (SoC) is part of the Deployment Advisory (DA) and is only valid if the recommendations and obligations in the DA are being followed.

(4) Currently in self-certification state.

(5) Until June 2019, the scheme issued more than 100 certificates (295 evaluations led to 141 certifications).

(6) Was not answered.

(7) Depends on the product complexity and/or addressed evaluation level.

(8) Price list is private.

(9) The price list is public: http://globalplatform.org/wp-content/uploads/2019/02/Security-Certification-Fees_02082019.pdf

Table 5: Scheme maintenance (Q10, Q11)

Scheme	Scheme documentation is maintained by a group of experts	Certificate lifetime	Vulnerability management after certificate has been issued?
BSPA (NLNCSA)	Yes (NLNCSA)	Unlimited	Yes
CSPN (ANSSI)	Yes (ANSSI)	3 years	No
e-IoT-SCS	Yes	Not yet defined	Yes
LINCE	Yes (CCN and SSB)	5 years	Yes

PSA certified Level 1	Yes	Unlimited	No
PSA certified Level 2	Yes	Unlimited	No
UL IoT Security Rating	Yes	1 year	Yes, customers are required to adhere to a vulnerability management process, which may or may not be facilitated by UL. It depends on issues found, their risk-level and how they are mitigated.
UL 2900	Yes	1 year	
IEC 62443	Yes	Product: snapshot, no lifetime per IE Process: no limitation. Operations: as ISMS	
IOTSCF	Yes (IoTSF)	Unlimited	Yes. The scheme has supporting documentation (a best practice guide, a compliance checklist) and the recommended process follows ISO/IEC 29147
BSZ	Under definition		
SOG-IS	Yes	Domain specific	Nation-specific
SESIP	Yes	2 years	Yes. Certificates can be withdrawn
TÜViT-SQ	Yes	2 years	Yes, for highest evaluation level SEAL5)
ETSI TS 103 645	ETSI is not a certification scheme but rather a standard for consumer IoT security		
GP TEE	Yes	3 years	Regular expert meeting to update attack methodology and certified products should review new attacks. Based on that, certificates can be withdrawn and a reevaluation has to be conducted.

Table 6: Risk Analysis and Management (Q31, Q32, Q33, Q34)

	BSPA (NLNCSA)	CSPN (ANSSI)	e-IoT-SCS	LINCE	PSA certified Level 1	PSA certified Level 2	UL IoT Security Rating	UL 2900	IEC 62443	IOTSCF	BSZ	SOG-IS	SESIP	TÜViT-SQ	ETSI TS 103 645	GP TEE
Yes, during the life cycle of the evaluation		x	x				x	x	x	x	x	x	x	x		
Yes, after the certificate issuance			x				x	x	x							x
No	x			x	x	x									x	
Yes, to be performed by the developer or vendor							x	x	x	x						
Yes, to be performed in collaboration between developer and evaluator			x													
No, it is not based on a risk analysis	(1)	x		x	x	x	x				x	x	x	x	x	x
Yes	x	(5)	x					x				(5)	(2)	(3)		(4)
No				x	x	x	x	x	x		x					

Other answers:

(1) Developer choice, customer choice

(2) SOG-IS for SESIP5; PSA Certified (ARM), FIPS140, ICA, and others such as GlobalPlatform

(3) CC and FIPS 140-2

(4) SOG-IS and EMVCo

(5) Common Criteria (CC)

2.4 Products Evaluated by the Scheme

Table 7: Mapping between schemes and products (Q22, Q23, Q24)

	BSPA (NLNCSA)	CSPN (ANSSI)	e-IoT-SCS	LINCE	PSA certified Level 1	PSA certified Level 2	UL IoT Security Rating	UL 2900	IEC 62443	IOTSCF	BSZ	SOG-IS	SESIP	TÜViT-SQ	ETSI TS 103 645	GP TEE
Secure elements (SE)	x	x										x	x		(7)	
Multi-application processors	x	x	x	x	x	x					x	x	x	x		x
System on Chip (SoC)	x	x	x	x	x	x					x	x	x	x		x
xG baseband hardware/software for mobile communication	x	x	x	x							x	x	x	x		
Sigfox baseband hardware/software for IoT services	x	x	x	x							x	x	x	x		
Sensors	x	x	x	x			x	x	x		x	x	x	x		x
Hardware Security Modules (HSM)	x	x	x	x							x	x	x	x		
Network devices like routers, switches, etc.	x	x	x	x			x	x	x		x	x	x	x		x
Trusted Platform Module (TPM)	x	x	x	x							x	x	x	x		
Security ICs (hardware only)	x	x	x	x							x	x	x	x		x
Security ICs including embedded software like operating systems and applications	x	x	x	x	x	x	x	x	x		x	x	x	x		x
Software applications running on SOC or SE or any mobile environment	x	x	x	x			x	x	x		x	x	x	x		x
Software applications running Cloud servers	x	x	x	x				x	x		x	x	x	x		
Database servers	x	x	x	x				x	x		x	x	x	x		
Qualified Electronic Signature Creation Device (QSCD)	x	x	x	x							x	x	x	x		
Other answers added by the scheme	(1) (8)	(8)	(8)	(2) (8)			(3)	(3)	(3)	(4)	(8)	(8)	(8)	(8)		

	BSPA (NLNCSA)	CSPN (ANSSI)	e-IoT-SCS	LINCE	PSA certified Level 1	PSA certified Level 2	UL IoT Security Rating	UL 2900	IEC 62443	IOTSCF	BSZ	SOG-IS	SESIP	TÜViT-SQ	ETSI TS 103 645	GP TEE
System level	x	x					x	x	x	x		x		(6)	(7)	
Component level	x	x	x	x	x	x	x	x	x	x	x		x	x		x
Process/enterprise level									x					x		
Yes	x	x	x		x					x		x (5)	x	x	(7)	x
No				x		X										

Other answers:

(1) Government, Access Control, Network Security, Network filtering, detection and response, secure messaging, Media and file security

(2) IoT device

(3) Consumer products, commercial products, industrial/OT products and systems, and medical devices

(4) The scheme is best applied at the product level however it is also applicable at the component (hardware and software) level too.

(5) CC defines the class ACO – Composition. In addition, there is a composite process defined for smartcards only.

(6) The scheme TÜViT-SQ allows a certification of an IoT device including a corresponding backend (cloud server).

(7) ETSI TS 103 645 is not a certification scheme but rather a standard for consumer IoT security.

(8) General purpose (can be applied for any type of products).

2.5 Evaluation Methodologies

2.5.1 Evaluation Labs

Table 8: Evaluation Labs (Q18, Q19, Q20, Q21)

	BSPA (NLNCSA)	CSPN (ANSSI)	e-IoT-SCS	LINCE	PSA certified Level 1	PSA certified Level 2	UL IoT Security Rating	UL 2900	IEC 62443	IOTSCF	BSZ	SOG-IS	SESIP	TÜViT-SQ	ETSI TS 103 645	GP TEE
No security evaluation										(1)					x	
Self-assessment					x											
Independent security evaluation by an approved lab	x	x	x	x		x	x	x	x		x	x	x	x		x
The scheme already has approved security labs	x	x		x	x	x	x	x	x	(7)	(2)	(3)	x	x	(7)	x
Number of approved laboratories	3	10		2	4	4						(5)	4	1		7
Accreditation in progress			x	5									7			
No specific approval process					x	x				x				x	x	
Laboratories already approved by other schemes are accepted			x	x												(6)
Specific approval process	(4)	x	X	x			x	x	x		x	x	(8)			
Software only																
Hardware and/or software	x	x	x	x	x	x				x	x	x	x	x		x
Technology used by the evaluated products	x	x	x	x						x	x	x	x			

Other answers:

(1) Not explicitly however sub-elements of a product may rely on independent lab certificates – this is for the user to determine and is guided by the application use case.

(2) Pilot phase.

(3) Accreditation by national certification bodies.

(4) The scheme implements a licensing process. A lab has to apply to become licensed. A lab makes a request to be licensed on certain categories, they provide evidences that prove experience, this is assessed and audit is performed by NLNCSA. With doing a good first / trial assessment the lab is licensed for products of a certain category. The next assessment is performed with NLNCSA doing less oversight.

(5) Nation Specific

(6) Delta based on SOG-IS or EMVCo.

(7) No labs available. Self-assessment at the present time.

(8) Specific approval requirements including ISO 17025 with Common Criteria.

2.5.2 Evaluation Process

Table 9: Evaluation Process (Q12, Q13)

Scheme	Support of Maintenance / continuous assurance procedures	Supported Evaluation Levels	Evaluation Level (short description)
BSPA (NLNCSA)	Yes, delta assessments	Only one level	Baseline: Basic evaluation level.
CSPN (ANSSI)	Yes	Only one level	High evaluation level: Equivalent to CC AVA_VAN.3.
e-IoT-SCS	Yes	Only one level	Substantial evaluation level.
LINCE	Yes	Basic, Basic + MEC, Basic + MCF, Basic + MC + MCF	Basic corresponds to the LINCE evaluation which can be augmented with a cryptographic evaluation (+ MEC), a source code review (+ MCF), or both (+MEC + MCF).
PSA Certified	No	PSA Certified Level 1, Level 2	L1: Critical security questions for chip vendors, OS providers and OEMs. L2: Evidence of protection against scalable, remote software attacks through lab-based evaluation of chips with a PSA Root of Trust security component.
UL IoT Security Rating	(1)	Bronze, Silver, Gold, Platinum, Diamond	The levels range from a baseline evaluation (Bronze) to a more comprehensive security capability.
UL 2900	(1)	3 levels in UL 2900-2-3	For UL, levels are defined in sub-standards.
IEC 62443	(1)	Multiple security and maturity levels as matrices, 4 maturity levels	The scheme defines security and maturity levels
IOTSCF	(2)	(3)	(3)
BSZ	Yes	Only one level	Substantial evaluation level.
SOG-IS	Yes	EAL1 to EAL7 with augmentations EAL: Evaluation Assurance Level	EAL1 is a basic evaluation level with only a few formal requirements. EAL7 is the highest assurance level which requires the usage of formal proofs and representation (for instance).
SESIP	Yes	SESIP1 to SESIP 5	SESIP1 corresponds to a developer statement; SESIP5 relates to an EAL4+ augmented with AVA-VAN.5, this is to allow re-use of SOG-IS certificates.
TÜViT-SQ	No	SEAL1 to SEAL5 SEAL: Security Assurance Level	SEAL1 is the lowest evaluation level for which the security requirements need to be specified. No penetration testing is done. SEAL2 can be considered as a consulting process, as in addition to SEAL1, penetration testing is performed. A certificate is issued for SEAL3+. SEAL5 includes change management.

Scheme	Support of Maintenance / continuous assurance procedures	Supported Evaluation Levels	Evaluation Level (short description)
ETSI TS 103 645	ETSI TS 103 645 is not a certification scheme but rather a standard for consumer IoT security		
GP TEE	Not yet. Continuous assurance will be introduced in the SE scheme in 2020 and then ported to TEE.	Only one evaluation level.	The GP TEE certification scheme aims for a moderate evaluation level.

Other answers:

(1) Depends on certification validity and any re-testing/re-certification needs based on surveillance and vulnerability management processes.

(2) The scheme is a blend of assurance and certification assessments – some are one time, others require maintenance.

(3) The scheme has general applicability as it is risk-based. The user is guided to identify a compliance class and the security requirements follow the level of the chosen compliance class. The basic mechanism is in place and more materials are being produced to help users select a compliance class to self-certify against.

Table 10: Evaluation requirements (Q14, Q16)

	BSPA (NLNCSA)	CSPN (ANSSI)	e-IoT-SCS	LINCE	PSA certified Level 1	PSA certified Level L2	UL IoT Security Rating	UL 2900	IEC 62443	IOTSCF	BSZ	SOG-IS	SESIP	TÜViT-SQ	ETSI TS 103 645	GP TEE
No documentation requirements													(11)		x	
High-level information		x	x	(4)	x		(12)				x			(17)		
Complete information including low-level design information		(2)	x			x		x	x		(2)	(8)				x
Source code		(13)	(13)			x		x	x		(2)	(8)				
Scheme-specific information	(1)	x				x				(11)	(2)	(9)		(18)		

	BSPA (NLNCSA)	CSPN (ANSSI)	e-IoT-SCS	LINCE	PSA certified Level 1	PSA certified Level L2	UL IoT Security Rating	UL 2900	IEC 62443	IOTSCF	BSZ	SOG-IS	SESIP	TÜViT-SQ	ETSI TS 103 645	GP TEE
No functional testing required							x	x	x		x	x		x	x	
Required for the developer			x	x	x	x				x			x			(18)
Required for the evaluator		x		x									(5)			
No penetration testing required					x					(14)			(6)		x	
Required for the evaluator	x	x	x	x		x	x	x	x		x	x				x
No site security requirements (The Scheme recognizes third party audits when applicable)	x	x	(3)	x	x	x	x	x	(16)	x	x	(15)	(7)		x	
Site audits for all development sites																x
Site audits for all production sites																

Other answers:

(1) The lab has to use templates provided by the certifier (ETR and DA (Deployment Advisory)).

(2) For crypto only.

(3) Self-assessment of site audits. Required information are filled within the questionnaire by the developer and there is no audit by the Lab.

(4) High-level documentation for the evaluation level Basic; MEC required low-level documentation; MCF requires low-level documentation and source code.

(5) For SESIP2 and higher.

(6) Only in case of SESIP1, no penetration testing is performed.

(7) For SESIP1 to SESIP3: no site security requirements; for SESIP4: Secure development practices have to be shown but not necessarily in a site audit; for SESIP5: a lab has to audit all production and development sites (Site certificates and STARs are accepted for SESIP5).

(8) For EAL3 and higher.

(9) For EAL2 and higher: Security Architecture and test documentation; for EAL6 and higher: formal security policy model.

(10)SESIP1: only a self-declaration is required; SESIP2: high-level documentation and optionally a dedicated source code analysis; SESIP3/4: source code analysis; SESIP5: It relates to an EAL4+ augmented with AVA-VAN.5, this is to allow re-use of SOG-IS certificates.

(11)Evaluation file is constructed by the user – A questionnaire is provided to support the scheme and provides all necessary links to supporting documentation within the user's organization.

(12)Bronze / Silver: high-level documentation; Gold / Platinum / Diamond: low-level documentation; Diamond: source code.

(13)For critical parts only.

(14)The scheme may include penetration testing however this is self-directed by the user and the evidence of the tests can be included in the evaluation file.

(15)EAL1/2: No site security requirements; EAL3 and higher: all development and production sites have to be audited; Audit recognition within SOG-IS.

(16)Depends on which sub-standard is applied.

(17)SEAL1/2: Security Requirements need to be defined; SEAL3: Architectural design required; SEAL4: Source code review; SEAL5: Change management.

(18)The lab has to perform functional tests. However, if a functional compliance is available, the developer can use a specific test suite. This reduces the efforts for the evaluation lab.

This is how the different schemes support patching of certified products **(Q15)**:

- BSPA (NLNCSA) supports delta evaluations.
- CSPN (ANSSI): The scheme allows the evaluation of secure patching mechanisms, but it does not extend the certificate validity to patched products.
- BSZ: Not supported. For changed/updated products a re-evaluation is required.
- The schemes e-IoT-SCS, LINCE, PSA L1, PSA L2, UL IoT Security Rating, UL 2900, IEC 62443, and IoTSCF support patching without further restrictions.
- The scheme SOG-IS supports 'Assurance Continuity'. It allows the evaluation of secure patching mechanisms, but it does not extend the certificate validity to patched products.
- The scheme TÜViT-SQ certifies a fixed version of the product. However, in case of SEAL5, the evaluators check the change management processes of the developer to provide further assurance that updates are done in a reasonable and secure way.
- The scheme GP TEE supports patching. No further description has been provided.

- The scheme SESIP supports delta evaluation. When the certified product is modified, a new certificate is required. In addition, flaw remediation procedures are mandatory for all SESIP levels. It asks for proof on patching mechanism + developer update procedures.

Table 11: Supporting documents of the schemes (Q17)

Scheme	Questionnaire	Security Profile / Protection Profile	Templates for Developer Documents	Guidance for Developers	Guidance for Evaluators	Mandatory Technical Specifications / Standards that need to be applied
BSPA (NLNCSA)	Not available.	Not available.	Not available.	Not available.	ETR template and DA (1)	None
CSPN (ANSSI)	Not available.	Available.	Template for Security Target.	Not available.	Available.	RGS guidance; CEM / ISO 18045 (2)
e-IoT-SCS	Available.	Available.	Not available.	Not available.	Not available.	None.
LINCE	Not available.	Available.	Not available.	Available.	Available.	(3)
PSA certified Level 1	Available.	Not available.	Not available.	Available.	Not available.	(3)
PSA certified Level 2	Available.	Available.	Not available.	Available.	Available.	(3)
UL IoT Security Rating	Available.					
UL 2900	Available.					
IEC 62443	Available.					
IOTSCF	Available.	Not available.	Not available.	Not available.	Not available.	None.

Scheme	Questionnaire	Security Profile / Protection Profile	Templates for Developer Documents	Guidance for Developers	Guidance for Evaluators	Mandatory Technical Specifications / Standards that need to be applied
BSZ	Not available.	Not available.	Not available.	AIS B1 to B5	AIS B1 to B5	None.
SOG-IS	Not available.	Available.	Available	Available.	Available.	Product-specific, ISO/ IEC 15408 and ISO/IEC 18045
SESIP	Not available.	Available.	Template for Security Target.	Not available.	Product-specific.	modified ISO / IEC 15408, ISO17025
TÜViT-SQ	Not available.	Not available.	Not available.	Not available.	Not available.	Not available.
ETSI TS 103 645	Not available.	Available.	Not available.	Not available.	Not available.	Not available.
GP TEE	Not available.	Available.	Available.	Not available.	Available.	TEE protection profile, TEE specific APIs

Other answers:

(1) The developer should deliver a product that is able to resist the Baseline level (no state actors etc.). The scheme uses a black box approach. A baseline assessment is a job for a lab to black box pentest / break the claimed security functions in any way they can in 25-man days. The lab has to convince our experts in the technical report they have been using their time wisely making the right and expected choices given the nature of the product and the current knowledge about the used technologies etc. The lab should do what a hacker would do. Anything that's available or can be found should be used to break the product. For example, if code for an attack is only, it should be used.

(2) In addition, application notes are available that are public or restricted to specific sponsors and evaluators.

(3) Mandatory documentation has to be used. However, no details have been provided.

2.5.3 Testing Process

Table 12: Compliance overview (Q25, Q26, Q27, Q28, Q29, Q30)

	BSPA (NLNCSA)	CSPN (ANSSI)	e-IoT-SCS	LINCE	PSA certified Level 1	PSA certified Level 2	UL IoT Security Rating	UL 2900	IEC 62443	IOTSCF	BSZ	SOG-IS	SESIP	TÜVIT-SQ	ETSI TS 103 645	GP TEE
No attack catalog	(1)			x						x	x				x	
Maintained by a group of experts		x			x	x	x	x	x			x	x (2)	x		x
Maintained by the scheme		x														
Definition and maintenance processes are not yet defined			x													
Other																
Black box analysis, no inputs required	x										x		(7)	(27)	(35)	
via workshops with the developer				x									(6)			
Set of documents (examples: Questionnaire including required evidences, Security Target, etc.)			x	x	x	x	x	x	x	x	(4)	x	(5)	(28)		x
Other		(3)														
No security evaluation					(9)					(9)			(7)		x	
Functional tests [%]		40	15	24		0					0	0	0			30
Penetration tests [%]		40	30	64		90					92	30	75	80		50
Document review [%]		20	30	12		10					8	70	25	20		20
Other	(8)		(29)													
Full Evaluation	(10)	(11)	(13)	(14)	(15)	(16)					(17)	(18)	(19)	(30)	(35)	(33)
Re-Evaluation or Delta																
No security evaluation					(9)					(9)			(7)	(31)	x	
Black-box testing	x	x	x	(21)							x		(7)			

	BSPA (NLNCSA)	CSPN (ANSSI)	e-IoT-SCS	LINCE	PSA certified Level 1	PSA certified Level 2	UL IoT Security Rating	UL 2900	IEC 62443	IOTSCF	BSZ	SOG-IS	SESIP	TÜViT-SQ	ETSI TS 103 645	GP TEE
Grey-box testing	(20)	(20)	x													
White-box testing		(4)	x	(22)		x					(4)	x	(23)			x
No requirements regarding implemented crypto algorithms	x											(24)				
Implementation of state-of-the-art cryptographic algorithms and key sizes from national security agencies (such NIST for U.S., BSI for Germany, CESG for U.K., ANSSI for France), SOG-IS or from academia.		x	x		x	x				x	x		x	x	x	(34)
Proprietary cryptographic algorithms or customization of standard cryptographic algorithms				x										x		
No verification										(25)					x	
Only documentary verification					x											
Verification by functional tests only				x												
Verification by documentation, functional tests and source code review		x	x			x					x					x
Verification by penetration tests only																
Other	(24)											(26)	(26)	(32)		

Other answers:

(1) We do a review by experts that will assess the lab technical report. When our experts feel the lab did not consider what they would expect (like a specific attack) we will question the lab.)

(2) For SESIP there is a GP task force. It reuses JIL Smart card rating.

(3) Mostly black-box but: Cryptography requires dedicated and detailed documentation from the dev and specific contexts may mandate documentation (will typically be mandated in application notes)

(4) For Crypto only

(5) For SESIP5. A security target is required for all SESIP levels.

(6) For SESIP3/4

(7) SESIP1: no evaluation; SESIP2: black box or dedicated code review

(8) The lab may convince us in the technical report why they made the right choice in approach on the specific product.

(9) Self-assessment

(10)25-man days

(11)25 work days + 10 days for the crypto

(13)2 weeks

(14)8 weeks

(15)One week

(16)2 to 3 months

(17)40-50-man days

(18)9-12 months

(19)SESIP1: 3-5 days, SESIP5: 3-5 months

(20)if code is available

(21)Basic

(22)MCF

(23)SESIP 3, 4 and 5

(24)Correct implementation should be assessed in a smart way given the limited amount of time the lab has, with the goal to find mistakes to break the product.

(25)User determined

(26)code review, security testing / pentest

(27)For SEAL2 only

(28)For SEAL3+

(29)15% source code review

(30)6 months

(31)SEAL2: Black-box testing; SEAL3+: White-box testing

(32)SEAL4+ requires a source code review. In this case, the correct implementation of standards can be verified in case a corresponding security requirement is defined.

(33)100 days

(34)GP TEE defines which algorithms are accepted. This list is not public.

(35)No security evaluation

2.6 Compliance Level with Art. 54 of the Cyber Security Act

Table 13: Compliance overview (Q35)

Scheme	Recognition by the EU Cyber Security Act	Is the scheme already compliant?
BSPA (NLNCSA)	To be determined.	No answer provided.
CSPN (ANSSI)	Recognition is intended.	Partially.
e-IoT-SCS	Recognition is intended.	Partially
LINCE	Recognition is intended.	Partially
PSA certified Level 1	Recognition is not intended.	Partially
PSA certified Level 2	Recognition is not intended.	Partially
UL IoT Security Rating	Recognition is intended.	No answer provided.
UL 2900	Recognition is intended.	No answer provided.
IEC 62443	Recognition is intended.	No answer provided.
IOTSCF	Recognition is intended.	Partially
BSZ	Recognition is intended.	No answer provided.

Scheme	Recognition by the EU Cyber Security Act	Is the scheme already compliant?
SOG-IS	Recognition is intended.	No answer provided.
SESIP	Recognition is intended.	Partially
TÜViT-SQ	To be determined.	No answer provided.
ETSI TS 103 645	Recognition is intended.	Partially.
GP TEE	Recognition is intended.	No answer provided.

3 Links to the scheme documentation when available

Scheme name	Web links
ETSI TS 103 645	Cyber Security for Consumer Internet of Things, ETSI TS 103 645, Version 1.1.1, 2019-02. https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf
BSZ	https://www.bsi.bund.de/EN/Topics/Certification/product_certification/Accelerated_Security_Certification/Accelerated-Security-Certification_node.html
SESIP	Security Evaluation Standard for IoT Platforms, Version 1.3, NXP Semiconductors N.V. (https://www.trustcb.com/iot/sesip/) http://globalplatform.org/wp-content/uploads/2019/11/SESIP_GP-0_0_0_5a.pdf
SOG-IS	see https://www.sogis.eu/ Common Criteria for Information Technology Security Evaluation available on https://www.commoncriteriaportal.org/cc/ • Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001 • Part 2: Security functional components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002, • Part 3: Security assurance components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003. • Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004.
TÜViT-SQ	Not published
BSPA	Not published
CSPN	https://www.ssi.gouv.fr/administration/produits-certifies/cspn/
e-IoT-SCS	https://www.eurosmart.com/eurosmart-iot-certification-scheme/
GSMA IoT SA	https://www.gsma.com/iot/iot-security-assessment/
GP TEE	TEE System Architecture, TEE Internal API Specification, TEE Client API Specification, TEE Protection profile on GlobalPlatform certification website https://globalplatform.org/certifications/security-certification/
GP SE	https://globalplatform.org/certifications/security-certification/)
IoTSCF	https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/IoTSF-IoT-Security-Compliance-Framework-Release-2.0-December-2018.pdf
LINCE	Not published.
PSA	https://www.psacertified.org

Scheme name	Web links
UL IoT Security Rating	https://ims.ul.com/iot-security-rating https://www.shopulstandards.com/ProductDetail.aspx?UniqueKey=35953 https://verify.ul.com)
UL 2900	https://www.ul.com/offerings/cybersecurity-assurance-and-compliance https://www.shopulstandards.com/Catalog.aspx https://iq.ulprospector.com/info/
IEC 62443	www.iecee.org for IECEE CB schemes, https://iq.ulprospector.com/info/ for UL schemes, https://isasecure.org/en-US/ for ISA Secure schemes
CPA	https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa

4 Revision History

Version		Changes / Application Note	Author
1.0		Version for Eurosmart board review	IOTR & TÜViT
1.1		Version shared with Eurosmart Board members	IOTR & TÜViT
1.2		Version Updated according to notes from Eurosmart members for public distribution	IOTR