EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CADRE DE CERTIFICATION EUROPÉEN DE LA CYBERSÉCURITÉ: *POURQUOI, COMMENT?*

Eric Vétillard, Ph.D.
Lead Certification Expert, ENISA
Chair, ad hoc Working Group on the cybersecurity certification of cloud services

13 | 10 | 2020

A’

DE LA CONFIANCE À LA CERTIFICATION, ET VICE-VERSA

La certification est quelque part liée à la confiance, commençons donc par regarder de quoi on parle.

Certificate

Standard: Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 4 (ISO/IEC 15408)

Certificate number: **C13-37760**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer: **NXP Semiconductors Germany GmbH, Business Unit Identification**

Stresemannallee 101, D-22529 Hamburg, Germany

Product and assurance level: **NXP J3E145_M64, J3E120_M65, J3E082_M65, J2E145_M64, J2E120_M65, and J2E082_M65 Secure Smart Card Controller Revision 3,**

Assurance Package:
- EAL5 augmented with ALC_DVS.2, AVA_VAN.5, and ASE_TSS.2

Protection Profile Conformance:
- Java Card System - Open Configuration Protection Profile, Version 2.6, Certified by ANSSI, the French Certification Body April, 19th 2010

Project number: **NSCIB-CC-13-37760-CR**

Evaluation facility: **Brightsight BV located in Delft, the Netherlands**

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 4 (ISO/IEC 18045)

Common Criteria Recognition Arrangement for components up to EAL4

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 4 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 4. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity

Date of issue : **12-08-2013**

Certificate expiry : **12-08-2018**

Registration number

PRODUCTS RvA C 078

Accredited by the Dutch Council for Accreditation

Managing Director
TÜV Rheinland Nederland B.V.
P.O. Box 541
7300 AM Apeldoorn
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

Confiance. Sentiment d'assurance, de sécurité qu'inspire au public la stabilité des affaires, de la situation politique.

Assurance. Garantie donnée au sujet de quelque chose ; preuve de quelque chose.

Trust. Assured reliance on the character, ability, strength, or truth of someone or something.

Assurance. A promise to cause someone to feel certain by removing doubt.

Certificate

Standard: Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 4 (ISO/IEC 15408)

Certificate number: C13-37760

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer: NXP Semiconductors Germany GmbH, Business Unit Identification
Stresemannallee 101, D-22529 Hamburg, Germany

Product and assurance level: NXP J3E145_M64, J3E120_M65, J3E082_M65, J2E145_M64, J2E120_M65, and J2E082_M65 Secure Smart Card Controller Revision 3.
Assurance Package:
- EAL5 augmented with ALC_DVS.2, AVA_VAN.5, and ASE_TSS.2

Protection Profile Conformance:
- Java Card System - Open Configuration Protection Profile, Version 2.6, Certified by ANSSI, the French Certification Body April, 19th 2010

Project number: NSCIB-CC-13-37760-CR

Evaluation facility: Brightsight BV located in Delft, the Netherlands
Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 4 (ISO/IEC 18045)

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 4 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 4. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria Recognition Arrangement for components up to EAL4

Validity: Date of issue : 12-08-2013
Certificate expiry : 12-08-2018

Registration number

PRODUCTS
Bvk C.V.8
Accredited by the Dutch Council for Accreditation

Managing Director
TÜV Rheinland Nederland B.V.
P.O. Box 541
7300 AM Apeldoorn
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

Confiance. Sentiment d'assurance, de sécurité qu'inspire au public la stabilité des affaires, de la situation politique.

Assurance. Garantie donnée au sujet de quelque chose ; preuve de quelque chose.

Trust. Assured reliance on the character, ability, strength, or truth of someone or something.

Assurance. A promise to cause someone to feel certain by removing doubt.

CYBERSECURITY ACT, ARTICLE 46

Cadre européen de certification de cybersécurité

1. Le cadre européen de certification de cybersécurité est établi afin d'améliorer les conditions de fonctionnement du marché intérieur en renforçant le niveau de cybersécurité au sein de l'Union et en permettant de disposer, au niveau de l'Union, d'une approche harmonisée en ce qui concerne les schémas européens de certification de cybersécurité, en vue de créer un marché unique numérique pour les produits TIC, services TIC et processus TIC.
2. Le cadre européen de certification de cybersécurité prévoit un mécanisme visant à établir des schémas européens de certification de cybersécurité et à attester que les produits TIC, services TIC et processus TIC qui ont été évalués conformément à ces schémas satisfont à des exigences de sécurité définies, dans le but de protéger la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou traitées ou des fonctions ou services qui sont offerts par ces produits, services et processus ou accessibles par leur intermédiaire tout au long de leur cycle de vie.

CYBERSECURITY ACT, ARTICLE 46

Cadre européen de certification de cybersécurité

1. Le cadre européen de certification de cybersécurité est établi afin d'améliorer les conditions de fonctionnement du marché intérieur en renforçant le niveau de cybersécurité au sein de l'Union et en permettant de disposer, au niveau de l'Union, d'une approche harmonisée en ce qui concerne les schémas européens de certification de cybersécurité, en vue de créer un marché unique numérique pour les produits TIC, services TIC et processus TIC.
2. Le cadre européen de certification de cybersécurité prévoit un mécanisme visant à établir des schémas européens de certification de cybersécurité et à **attester** que les produits TIC, services TIC et processus TIC qui ont été **évalués** conformément à ces **schémas** satisfont à des exigences de sécurité définies, dans le but de protéger la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou traitées ou des fonctions ou services qui sont offerts par ces produits, services et processus ou accessibles par leur intermédiaire tout au long de leur cycle de vie.

CYBERSECURITY ACT, ARTICLE 46

Cadre européen de certification de cybersécurité

1. Le cadre européen de certification de cybersécurité est établi afin d'améliorer les conditions de fonctionnement du marché intérieur en renforçant le niveau de cybersécurité au sein de l'Union et en permettant de disposer, au niveau de l'Union, d'une approche harmonisée en ce qui concerne les schémas européens de certification de cybersécurité, en vue de créer un marché unique numérique pour les produits TIC, services TIC et processus TIC.
2. Le cadre européen de certification de cybersécurité prévoit un mécanisme visant à établir des schémas européens de certification de cybersécurité et à attester que **les produits TIC, services TIC et processus TIC qui ont été évalués conformément à ces schémas** satisfont à des exigences de sécurité définies, dans le but de protéger la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou traitées ou des fonctions ou services qui sont offerts par ces produits, services et processus ou accessibles par leur intermédiaire tout au long de leur cycle de vie.

Attester. Certifier, garantir l'exactitude ou la réalité de quelque chose.

Évaluation. Action d'évaluer, d'apprécier la valeur (d'une chose); technique, méthode d'estimation.

Attest. To show something or to say or prove that something is true.

Evaluation. The process of judging or calculating the quality, importance, amount, or value of something.

Attestation. Délivrance d'une affirmation basée sur une *décision* (7.2) indiquant que le respect des *exigences spécifiées* (5.1) a été démontré.

Évaluation de la conformité. Démonstration que les *exigences spécifiées* (5.1) sont respectées.

Attestation. Issue of a statement, based on a *decision* (7.2), that fulfilment of *specified requirements* (5.1) has been demonstrated.

Conformity assessment. Demonstration that *specified requirements* (5.1) are fulfilled.

Attestation. Délivrance d'une affirmation basée sur une *décision* (7.2) indiquant que le respect des *exigences spécifiées* (5.1) a été démontré.

Certification. Attestation (7.3) par tierce partie portant sur un objet de l'évaluation de la conformité (4.2).

Attestation. Issue of a statement, based on a decision (7.2), that fulfilment of specified requirements (5.1) has been demonstrated.

Certification. Third-party attestation (7.3) related to an obj of *conformity assessment* (4.2).

B’

LE CYBERSECURITY ACT

Quelques mots sur le cadre Européen de certification de la cybersécurité défini par le Cybersecurity Act, et où nous en sommes aujourd’hui.

THE CYBERSECURITY ACT

Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the EU Cybersecurity Agency) and on information and communications technology cybersecurity certification.

Making ENISA permanent and adding new missions

- From cybersecurity awareness to capacity building to CSIRTs network secretariat and the organization of EU-level exercises
- Also adding a mission related to certification, supporting policy making

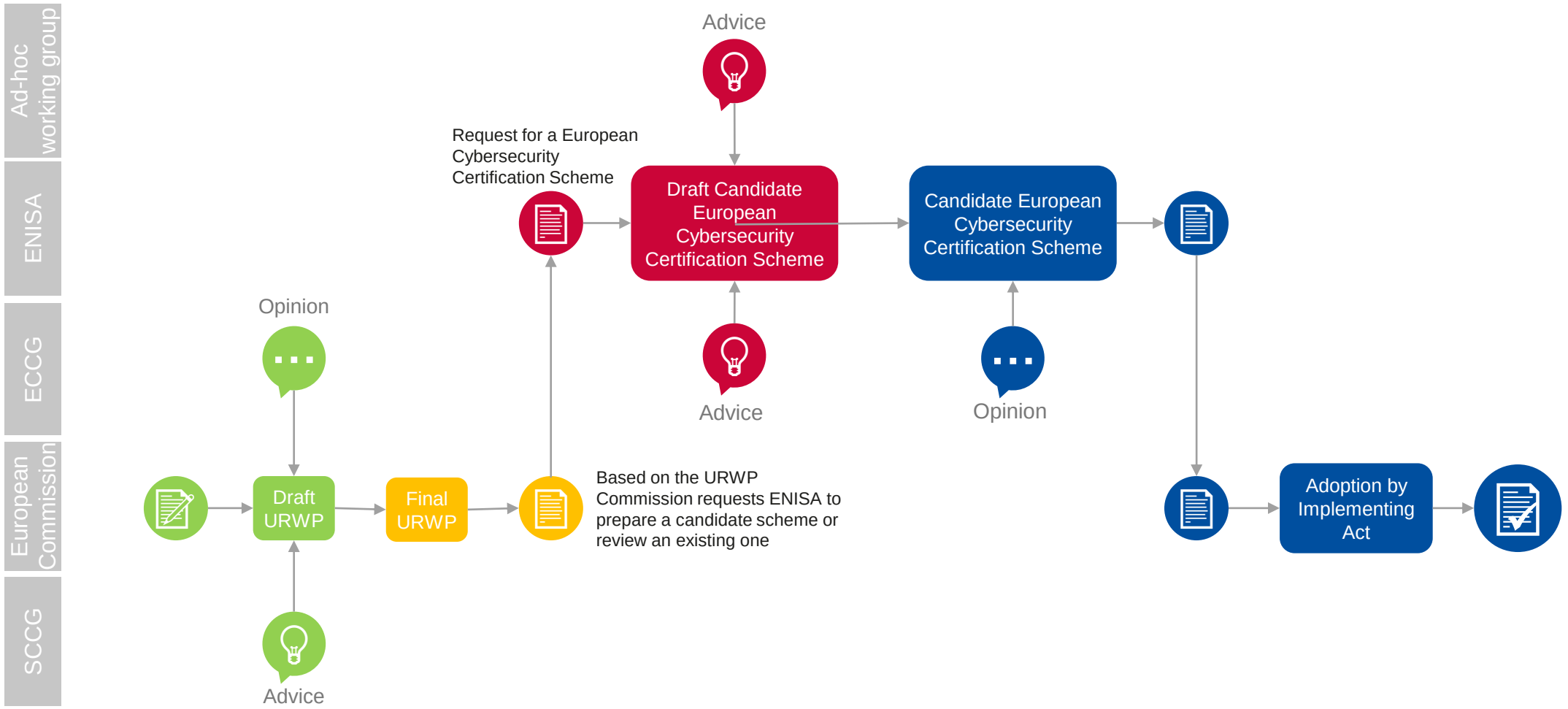
Also defining a Cybersecurity certification framework

- To increase the use of cybersecurity certification in Europe
- To go beyond national schemes and offer mutual recognition at European level
- Enabling customers to take informed decisions about cybersecurity
- Based on regulation 765/2008 and ISO/IEC 17065, and the existing accreditation network

WHAT IS IN A CYBERSECURITY SCHEME?

a) Subject matter and scope
b) Clear description of the purpose of the scheme and of how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme
c) References to the international, European or national standards applied in the evaluation, and if not available to technical specifications
d) One or more assurance levels
e) An indication whether conformity self-assessment is authorized
f) Specific requirements for the CABs
g) Specific evaluation criteria and methods to be used
h) The information necessary for the evaluation or otherwise to be made available by the applicant
i) If applicable, conditions of use of marks and labels
j) Rules for monitoring compliance of certified and self-assessed products
k) Conditions for issuing, maintaining, continuing certificates, and for extending/reducing scope
l) Rules concerning the consequences for products that have been certified or self-assessed and do not comply
m) Rules concerning how previously undetected vulnerabilities should be reported and handled
n) Rules concerning the retention of records by CABs
o) Identification of national and international schemes with the same scope
p) Content and format of the certificates and EU statements of conformity
q) The period of the availability of EU statements of conformity and related documentation
r) Maximum period of validity of certificates
s) Disclosure policy for certificate issuance, withdrawal, amendment
t) Conditions for mutual recognition with third countries
u) Where applicable, rules for peer assessment
v) Formats and procedures to be followed by suppliers to provide supplementary cybersecurity information

SCHEME PREPARATION PROCESS



TWO SCHEME REQUESTS

EUCC: Successor to SOGIS

First request, received in July 2019

- Scheme submitted, currently in final stages of review by the ECCG
- Work on implementing act to start soon

Mostly procedural work

- Using existing Common Criteria and guidance
- Adapting to the Cybersecurity Act
- Ensuring a smooth transition

EUCS: Cloud services

Second request, received November 2019

- Currently in the Working Group
- First delivery in December, with public and ECCG review in early 2021

Mostly technical work

- Benefitting from EUCC experience
- But no unified scheme in Europe for cloud
- A lot of work on controls and assessment methods

GETTING A SCHEME

The challenges for any scheme, and in particular for an IoT scheme.

- Multiple assurance levels
- Products vs. services
- Supply chain

UNDERSTANDING THE LEVELS

‘basic’

Demonstrates an **intention** from the CSP to implement security controls

Intended to resist **simple** known attacks

Document review is required

Entry level with limited guarantees, as a first step or for low-risk applications

‘substantial’

Demonstrates that the CSP has **correctly** implemented security controls

Intended to resist **known** attacks by actors with limited means

Functional testing is required

Core level with real guarantees, for mainstream applications in all fields

‘high’

Demonstrates the **effectiveness** of the controls implemented by the CSP against attacks

Intended to resist **complex** attacks using state-of-the-art techniques

Pen testing is required

Level with strong guarantees, for critical uses in sensitive fields

Gradual increase of assurance in scope, depth, and rigour

DIFFERENT EFFECT OF TIME

Product: Mostly static, with history

Cloud: Mostly dynamic, no past

DIFFERENT EFFECT OF TIME

Product: Mostly static, with history

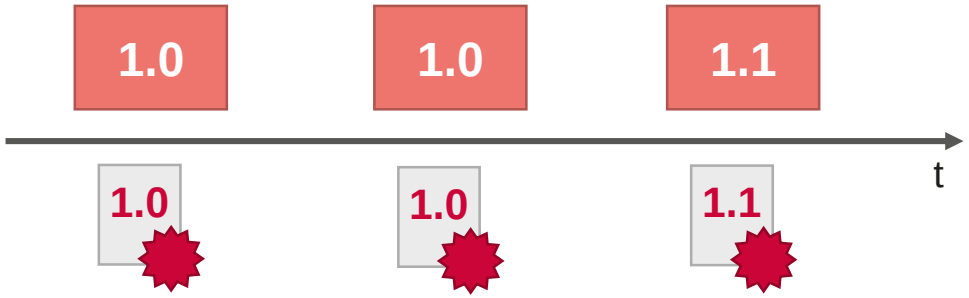
After some time, the same product

Cloud: Mostly dynamic, no past

After some time, a different service

DIFFERENT EFFECT OF TIME

Product: Mostly static, with history



After some time, the same product

After more time, a patch/update

- The old product still exists
- Two certificates may cohabit at a given time

Cloud: Mostly dynamic, no past

After some time, a different service

After more time, another different service

- Only one service exists at any time
- Only one certificate is valid at any time

The lifecycle of certification is deeply affected

RISKS AND ASSURANCE LEVELS: *ASSURANCE CONTINUITY*

A product after one year

The product will still be the same

- The threat environment may be different
- No or limited adaptation

What is important?

- Some level of resistance against future threats

What makes a higher level?

- Better assurance that no attack is economically viable in the near future
- A patching mechanism is also useful

A cloud service after one year

The service will be different

- The threat environment may be different
- Adaptation to new threats is possible

What is important?

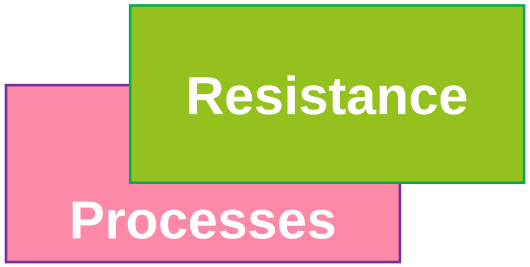
- No loss of security in operation and evolution

What makes a higher level?

- Better operation monitoring ➔ automation
- Better compliance ➔ continuous assessment

PRIORITIES IN ASSURANCE

Products focus on resistance



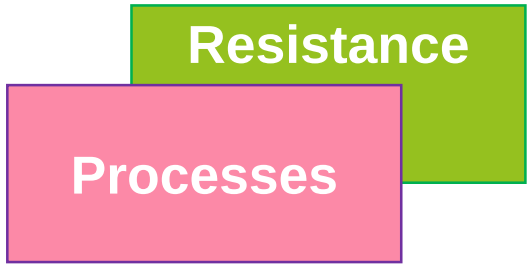
Resistance against attacks is essential

- Vulnerability analysis is central

Processes are in the background

- Providing some assurance on

Cloud services focus on processes



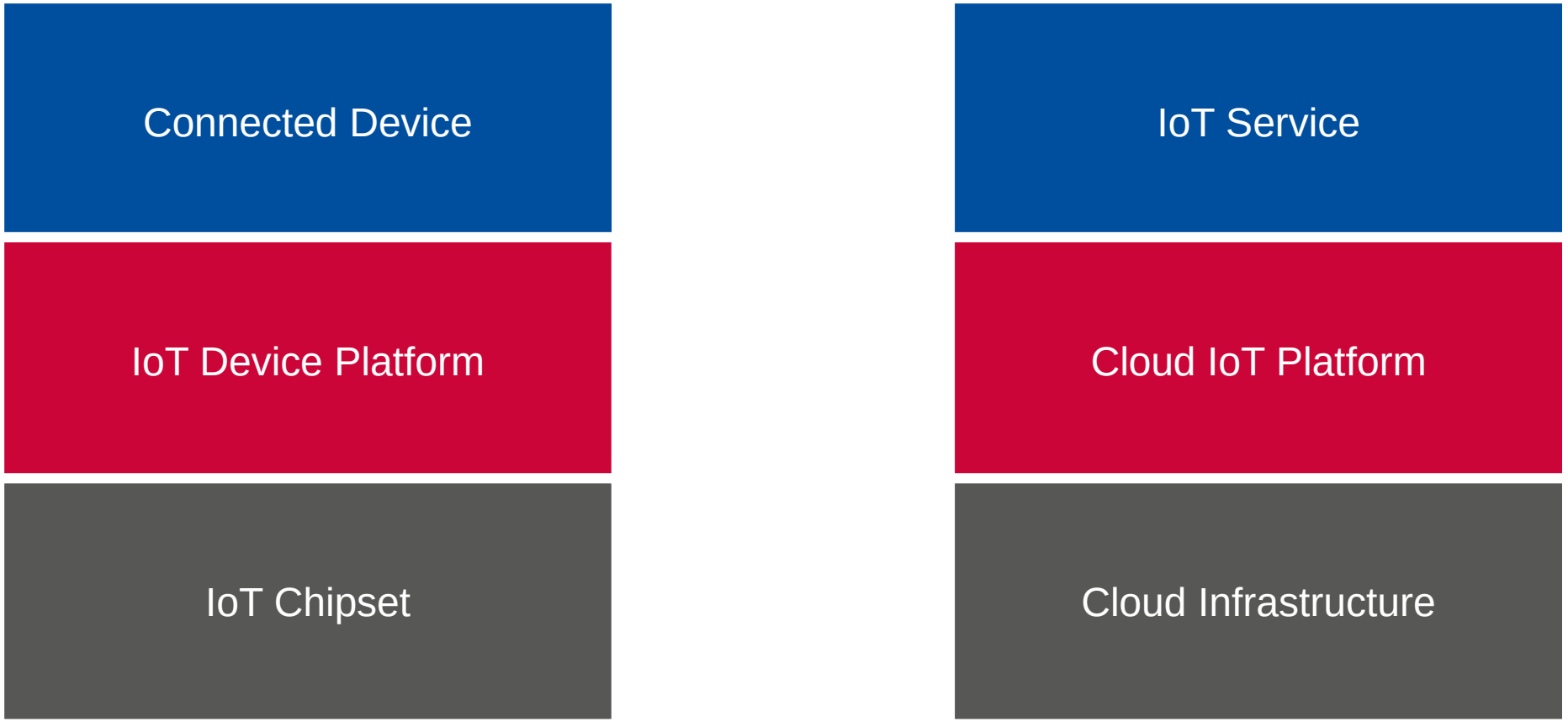
Well-running processes are essential

- Daily process operation is central

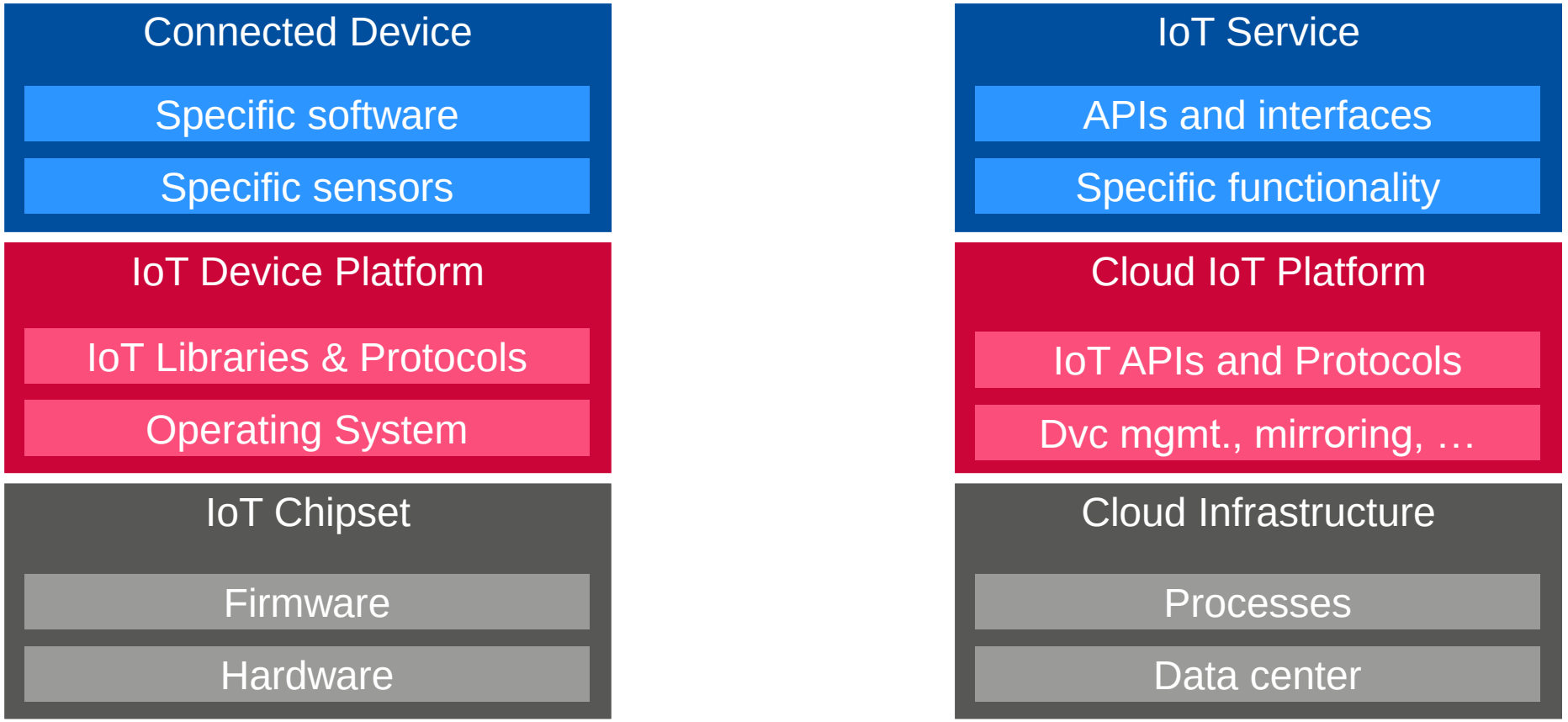
Products/resistance are in the background

- Part of a few processes (procurement, testing)

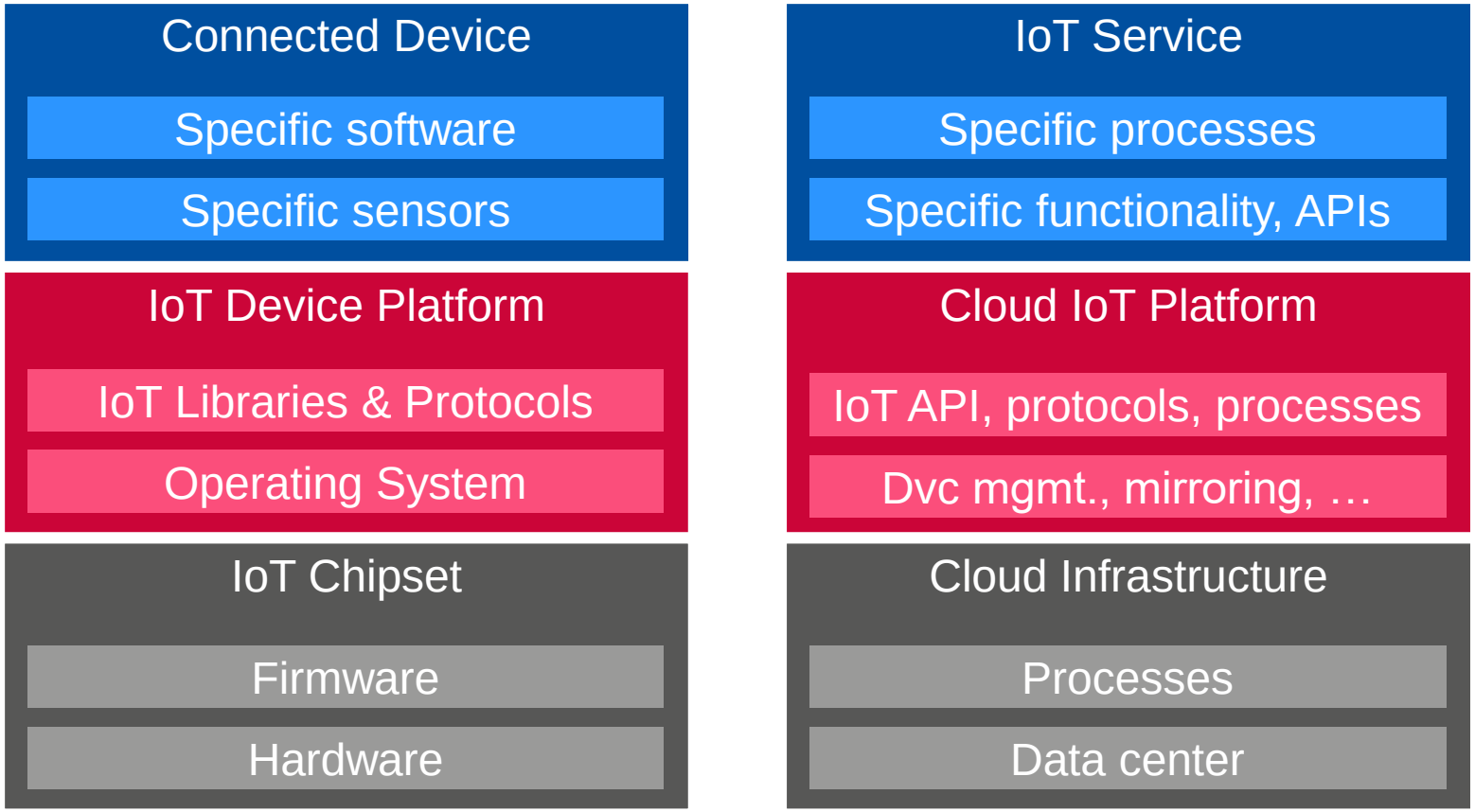
SUPPLY CHAIN



SUPPLY CHAIN



SUPPLY CHAIN



And much more…

Device provisioning

- Some other cloud service
  - From another provider?

Human interfaces

- Mobile applications
- Web applications

…

A SCHEME FOR IOT

		Connected device	IoT service
Basic	Requirements	ETSI 303 645	
	Method	ETSI on-going work	
Substantial	Requirement		
	Method		
High	Requirement		
	Method		

A SCHEME FOR IOT

		Connected device	IoT service
Basic	Requirements	ETSI 303 645	
	Method	ETSI on-going work	
Substantial	Requirement		
	Method	EUCC	
High	Requirement		
	Method	EUCC	

A SCHEME FOR IOT

		Connected device		IoT service
Basic	Requirements	ETSI 303 645		
	Method	ETSI on-going work		
Substantial	Requirement			
	Method	EUCC	SESIP, …	
High	Requirement			
	Method	EUCC		

A SCHEME FOR IOT

		Connected device		IoT service
Basic	Requirements	ETSI 303 645		
	Method	ETSI on-going work		
Substantial	Requirement	SESIP, PSA Certified, …		
	Method	EUCC	SESIP, …	
High	Requirement			
	Method	EUCC		

A SCHEME FOR IOT

		Connected device		IoT service
Basic	Requirements	ETSI 303 645		ETSI 303 645
	Method	ETSI on-going work		
Substantial	Requirement	SESIP, PSA Certified, …		
	Method	EUCC	SESIP, …	
High	Requirement			
	Method	EUCC		

A SCHEME FOR IOT

		Connected device		IoT service
Basic	Requirements	ETSI 303 645		ETSI 303 645
	Method	ETSI on-going work		
Substantial	Requirement	SESIP, PSA Certified, …		
	Method	EUCC	SESIP, …	EUCS
High	Requirement			
	Method	EUCC		EUCS

ET ALORS?

Il existe maintenant un Cadre Européen de Certification de la Cybersécurité

Pour faire advancer la cybersécurité au niveau Européen

Pour connecter des schémas au sein d'un cadre cohérent

Cependant, ce que nous certifions doit être clairement défini

Dans l'IoT, Objets Connectés ou Services IoT?

Aussi grand public ou usage privé ou industriel/sensible

Attention, pas de lien simple avec les niveaux de certification

MERCI POUR VOTRE ATTENTION!

European Union Agency for Cybersecurity
Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europa.eu