enisa 20 years!

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CYBERSECURITY, SOVEREIGNTY AND CERTIFICATION
HOW DO THEY MIX?

Eric Vetillard, Ph.D.
Lead Certification Expert, MCS, ENISA
Char, EUCS AHWG

12 | 06 | 2024

certification
third party attestation, based on a decision following a review, that fulfilment of specified requirements has been demonstrated

cybersecurity
safeguarding of people, society, organizations and nations from cyber risks
Note 1 to entry: Safeguarding means to keep cyber risks at a tolerable level.

Derived from ISO standards

sovereignty
the defining authority within an individual consciousness, social construct or territory

sovereignty
of a nation or other polity: the state of being able to control resources, make laws independently, and otherwise govern itself without the coercion or concurrence of other polities.

From Wikipedia and Wiktionary

EU CYBERSECURITY CERTIFICATION SCHEME FOR CLOUD SERVICES (EUCS)

All capabilities

Also based on ISO/IEC 22123-1

All cloud capabilities are supported: Infrastructure, Platform, Application

Covers the full stack

No mention of deployment model

Horizontal

Defines a baseline of requirements that are applicable to all services.

Enables the same methodology for all services

Does not assess the security of product-specific security features (Security as a Service)

3 evaluation levels

Mapped to assurance levels as defined in the European Cybersecurity Act

‘basic’

‘substantial’

‘high’

All levels based on an assessment by an accredited third-party

EUCS TECHNICAL CHALLENGES

Which requirements?

There is no clear standard, so we need to define a list of requirements on security controls, drawing from existing schemes, adding the notion of assurance levels

Which assessment?

Several assessment methods, mostly based on ISO270xx and on ISAE standards, and an ability to combine with both assessments

Which evaluation levels?

Evaluation levels must bring added value and be simple enough to understand in order to bring a clear message

How to make results matter for customers?

A key objective of the scheme is to allow customers to make informed choices, and this is about available documentation and information

SOVEREIGNTY IS EASY

In the EU

Data storage and processing

- Only in the EU/specific locations

Cloud service operations

- Employees based in the EU
- Working from the EU

Technical measures

Encryption, key management

- BYOK and friends
- Runtime access control

Decision making on data

- In the EU (with keys)
- From people liable in the EU

Company control

Headquarters

- Local HQ in the EU
- Global HQ in the EU

Control from the EU

- Limit on ownership, board representation, voting rights

SOVEREIGNTY IS EASY 🤥

In the EU

Data storage and processing

- Only in the EU/specific locations

Cloud service operations

- Employees based in the EU
- Working from the EU

What about the UK subsidiary?

What about global customers?

Technical measures

Encryption, key management

- BYOK and friends
- Runtime access control

Decision making on data

- In the EU (with keys)
- From people liable in the EU

Company control

Headquarters

- Local HQ in the EU
- Global HQ in the EU

Control from the EU

- Limit on ownership, board representation, voting rights

Which rules to adopt?

What about global companies?

EUCS AND SOVEREIGNTY

Is sovereignty cybersecurity?

“protecting nations from cyber risks”: Looks good

Is a risk from the application of a law a cyber risk? Now, this is a more difficult question, but the EDPB seems to think that it is a risk to personal data.

Is sovereignty certifiable?

Some elements are rather easy, like the location of data storage and processing, and the technical measures.

Requirements on personnel are more difficult.

Control requirements are difficult and out of the competences of (most) IT auditors

Sovereignty for doing what?

This ended up being a key question, because of unrealistic scenarios used in arguments.

Sovereignty is important for the most sensitive data and processing, and the needs vary greatly.

What about shared responsibility?

The responsibility for the security of cloud services is shared between the cloud service provider and customer.

The customer (hopefully) knows their problems better than their provider.

THREE GUIDING PRINCIPLES

Use case-based

Only the user knows

- Especially for IaaS/PaaS

Very specific needs

- Not entire domains or industries
- Not even entire IT systems

Transparent

Making information available

- Detailed information
- Summary for basic decisions

Mandatory and optional

- Mandatory if required in EUCS
- Optional if going beyond

Evaluated

In the evaluation scope

- From the requirements
- From the controls fulfilling the requirements

Covered by surveillance

THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Ethnikis Antistaseos 72 & Agamemnonos 14, Chalandri 15231
Attiki, Greece

☎ +30 28 14 40 9711

✉ certification@enisa.europa.eu

🌐 www.enisa.europa.eu