Thematic Group #2:
Necessary elements of a harmonised way of specifing, evaluating and certifying products

Elżbieta Andrukiewicz, Rapporteur

(number)Intermediate Report

Virtual Meeting (date)

ENISA Transposition of SOG-IS MRA Ad-hoc Working Group (SOGIS AHWG)

TG#2 scope – art. 54(1)

(c) references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme

(f) where applicable, specific or additional requirements to which conformity assessment bodies are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements;

(k) where applicable, the conditions for issuing, maintaining, continuing and renewing theEuropean cybersecurity certificates, as well as the conditions for extending or reducing the scope of certification;

(g) the specific evaluation criteria and methods to be used, including types of evaluation, in order to demonstrate that the security objectives referred to in Article 51 are achieved

Systematic work on 54(1) k) provisions

(k) where applicable, the conditions for issuing, maintaining, continuing and renewing theEuropean cybersecurity certificates, as well as the conditions for extending or reducing the scope of certification;

In-depth consideration is given to the process of certificate management in its life cycle (i.e. during its validity period) based on

- JIL – Assurance Continuity v.1.0 November 2019 [Annex 11]
- EN-ISO/IEC 17065 „Conformity assessment — Requirements for bodies certifying products, processes and services”

Objective: common view of two approaches

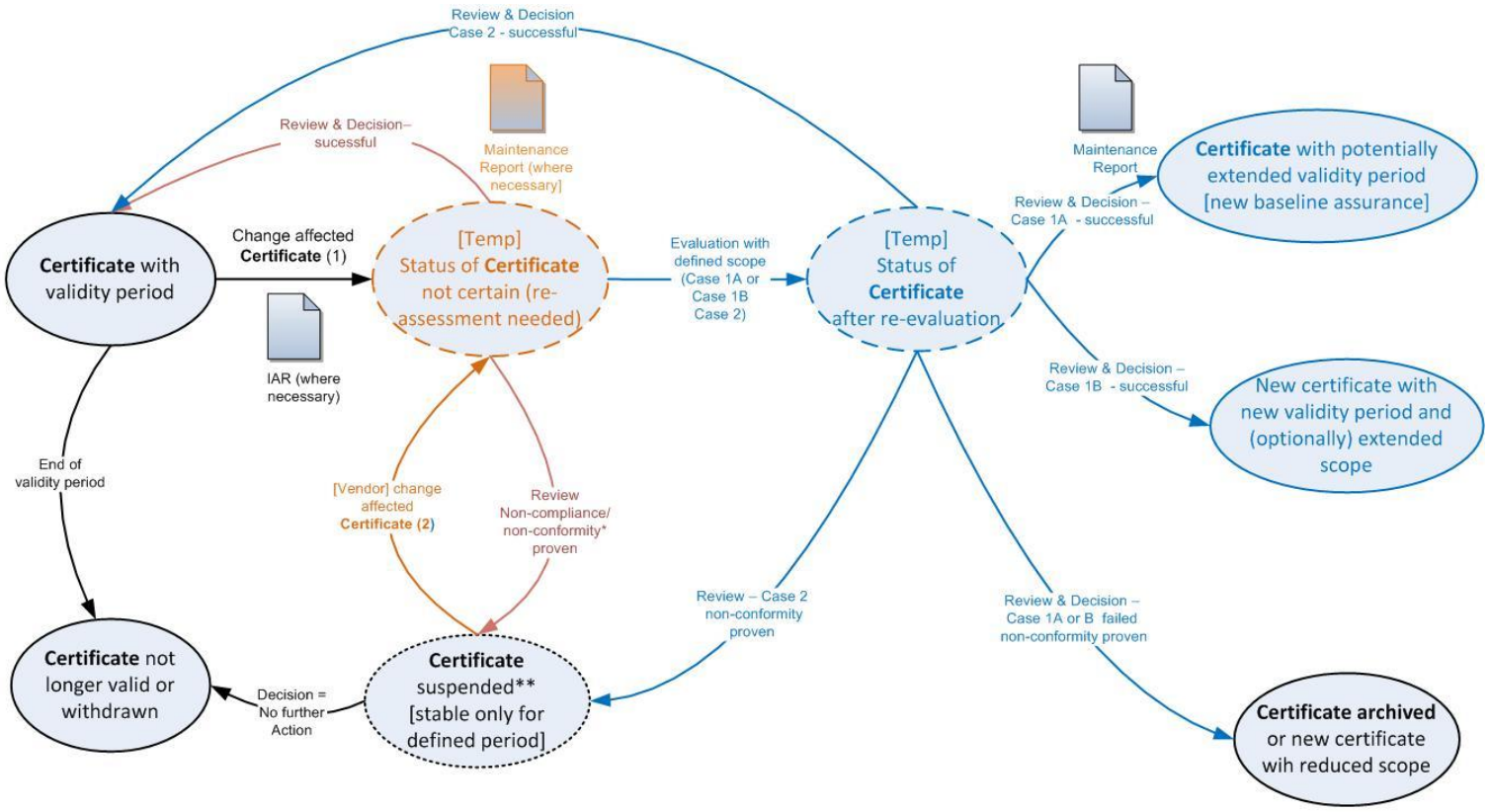
Life cycle of the certificate

- We consider a life cycle of a certificate, starting from its issuance with a defined validity period till its expiration (by validity period or preliminary, due to non-conformities related to the certificate), or renewal (i.e. issuing a new certificate that can happen under specific circumstances).
- One fundamental condition for issuing a certificate for the ICT product is successful evaluation.
- However, certification activities are related to the phase after the certificate is issued:
  - [JIL-AC] described this phase as the ‘maintenance phase’, and related activities are called ‚re-assessment’ and ‚re-evaluation’
  - [17065] uses ‘a change affecting certification’ instead of ‚maintenance’ all relevant activities are the same as for issuing certificate : ‚review/decision’ and ‚evaluation’

Identifying the problem

- Changes affected the certificate can be of various nature: related to its technical content that could result in nonconformities , and related to other factors, including non-compliances (see discussion on nonconformities/non-compliances in Chapter 11).
- [JIL-AC, Annex 11] document covers only part of the maintenance activities related to the certificate: it considers these changes of technical nature which directly relate to the assurance attested by the certificate

Post-certification activities – [JIL-AC - Annex 11] and [17065] common view



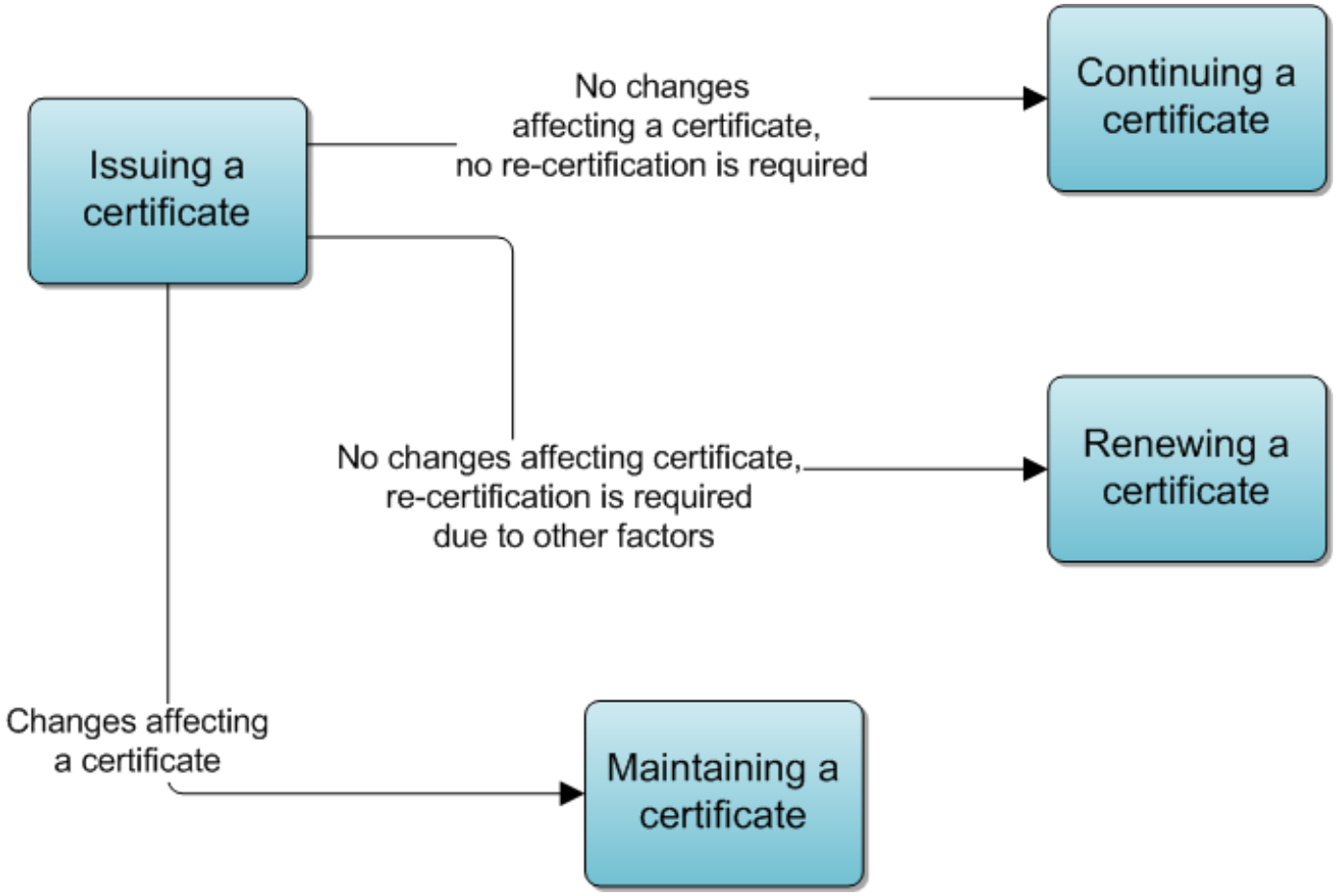
*non-compliance/non-conformity means different nature of a given change subject to the CAB-CB Review

****upon decision of CAB:** If the corrective action Is taken by the Vendor in due time, suspension will not be needed

All nodes/activities depicted in brown font refer to re-assessment in the 'maintenance phase' described in Annex 11

All nodes/activities depicted in blue font refer to re-evaluation in the 'maintenance phase' described in Annex 11

Solving the problem



Nominal decisions associated with the maintenance of certificates (Chapter 13, Table 5) - examples

CASES	NOMINAL DECISIONS
The same ICT product still meets its security requirements for certification.	Maintain the certificate until its expiration date
The expiration date of the certificate has been reached and no request for maintenance has been submitted.	Archive the certificate
New evaluation tasks including vulnerability testing were performed on the same version of the ICT product and are successful (refer to re-assessment described in Annex 11).	Continue the certificate with potentially an extended validity period
The modified/patched version of the ICT product meets its security requirements for certification according to the developer's processes and no new evaluation tasks have been performed (refer to re-evaluation defined in annex 11).	Renew the certificate with a scope corresponding to the new version with the same validity period
Necessary evaluation tasks were performed and identify the same version of ICT product does not meet all applicable requirements, and no action is possible to maintain any certificate (refer to re-assessment defined in Annex 11).	Withdraw the certificate

Questions?