CCLAB

THE AGILE SOFTWARE SECURITY LAB

ENISA-CCC

The work of

ENISA ahWG1 Thematic Group N°5

Continuity assurance and handling of vulnerabilities

2020-12-18

Topics of the ahWG1 Thematic Group Nº5

Cybersecurity Act - Regulation (EU) 2019/881 of the European Parliament and of the Council Art. 54 1. :

(j) rules for monitoring compliance

(l) end of compliancy of certified products

(m) handling undetected vulnerabilities

(r) maximum period of validity of certificates

(s) disclosure policy for certificates issued, amended or withdrawn

Topics of the ahWG1 Thematic Group Nº5

Cybersecurity Act - Regulation (EU) 2019/881 of the European Parliament and of the Council Art. 54:

1. A European cybersecurity certification scheme shall include at least the following elements:

(m) rules concerning how previously undetected cybersecurity vulnerabilities in ICT products, ICT services and ICT processes are to be reported and dealt with;

The problem

Certificate is a still picture of a TOE.

If the product changes

– the Assurance continuity process is available, but:

it takes a long time,

re-evaluation of the changes and reissuance of the certificate needs to be done before the changed product is available to the users.

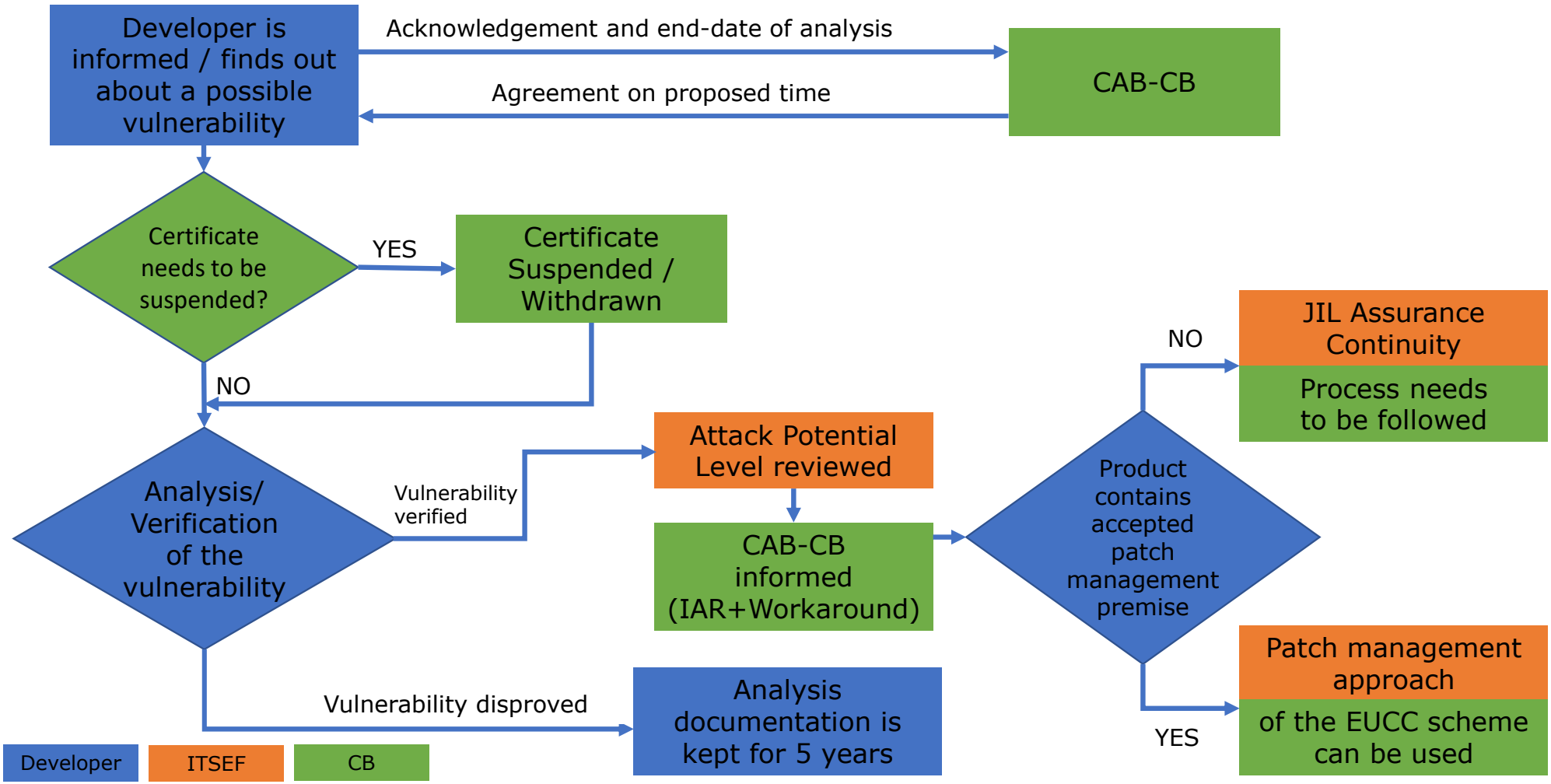
If a security patch needs to be applied to an already certified product, the users need to choose in between:

a changed, but possibly secure product, or

an unchanged, certified, but surely unsecure product.

This is a problem, as the number of discovered vulnerabilities and exposures are growing rapidly.

EUCC scheme rules related to handling vulnerabilities



Proposed requirement on undetected vulnerability handling

Accepted patch management methodologies

ISO SC27 WG3 Technical Report “Extension for Patch Management for 15408 and 18045”

or

the ISCI WG1 Proposal for new SAR components and Packages in CC for Patch Management

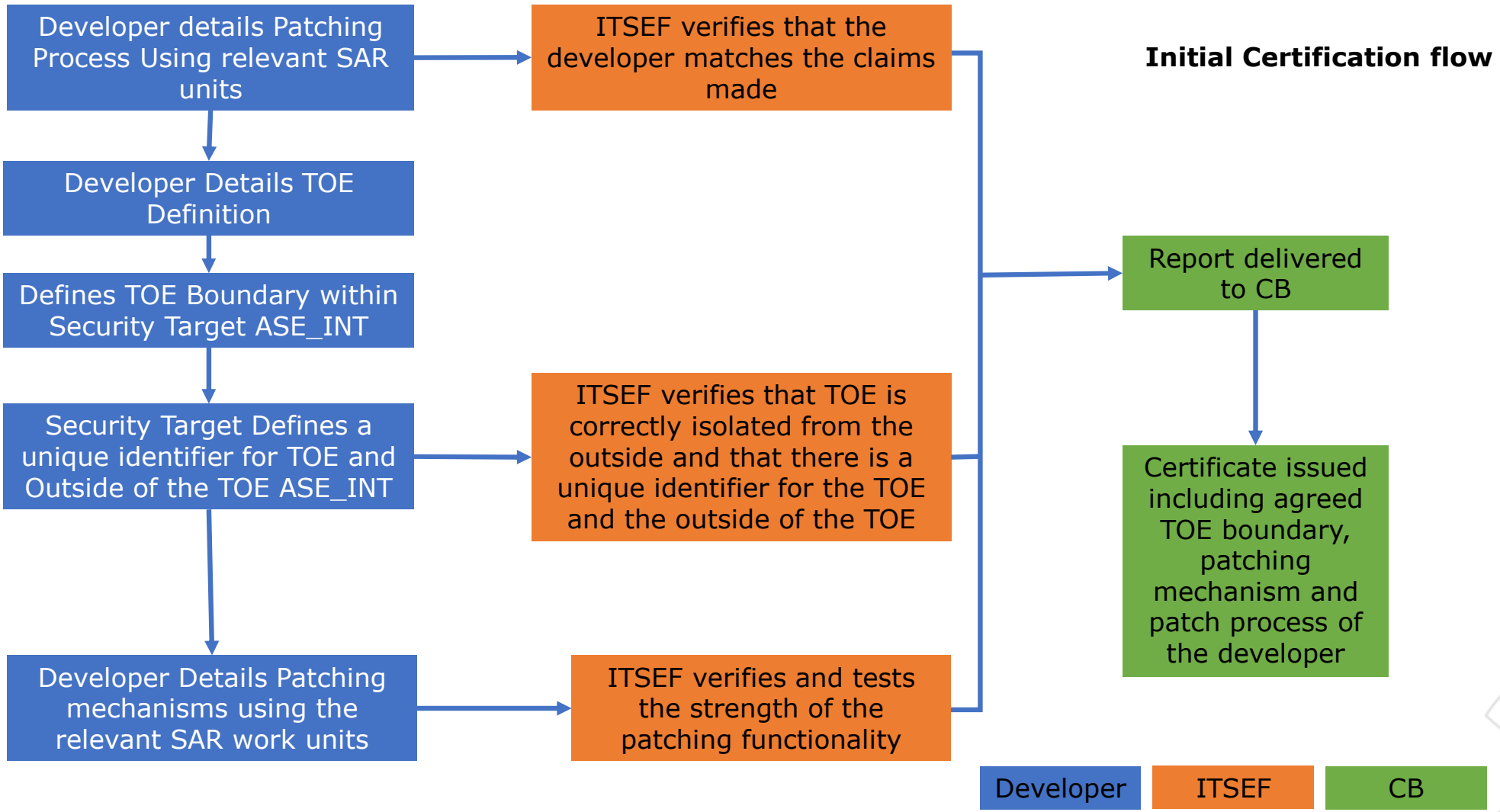
EUCC scheme rules related to handling vulnerabilities 2

Previously undetected vulnerability shall be reported and handled in accordance with the general rules of ISO/IEC 30111 and ISO/IEC 29147, adapted for the EUCC scheme, with the additional possibility of patch management

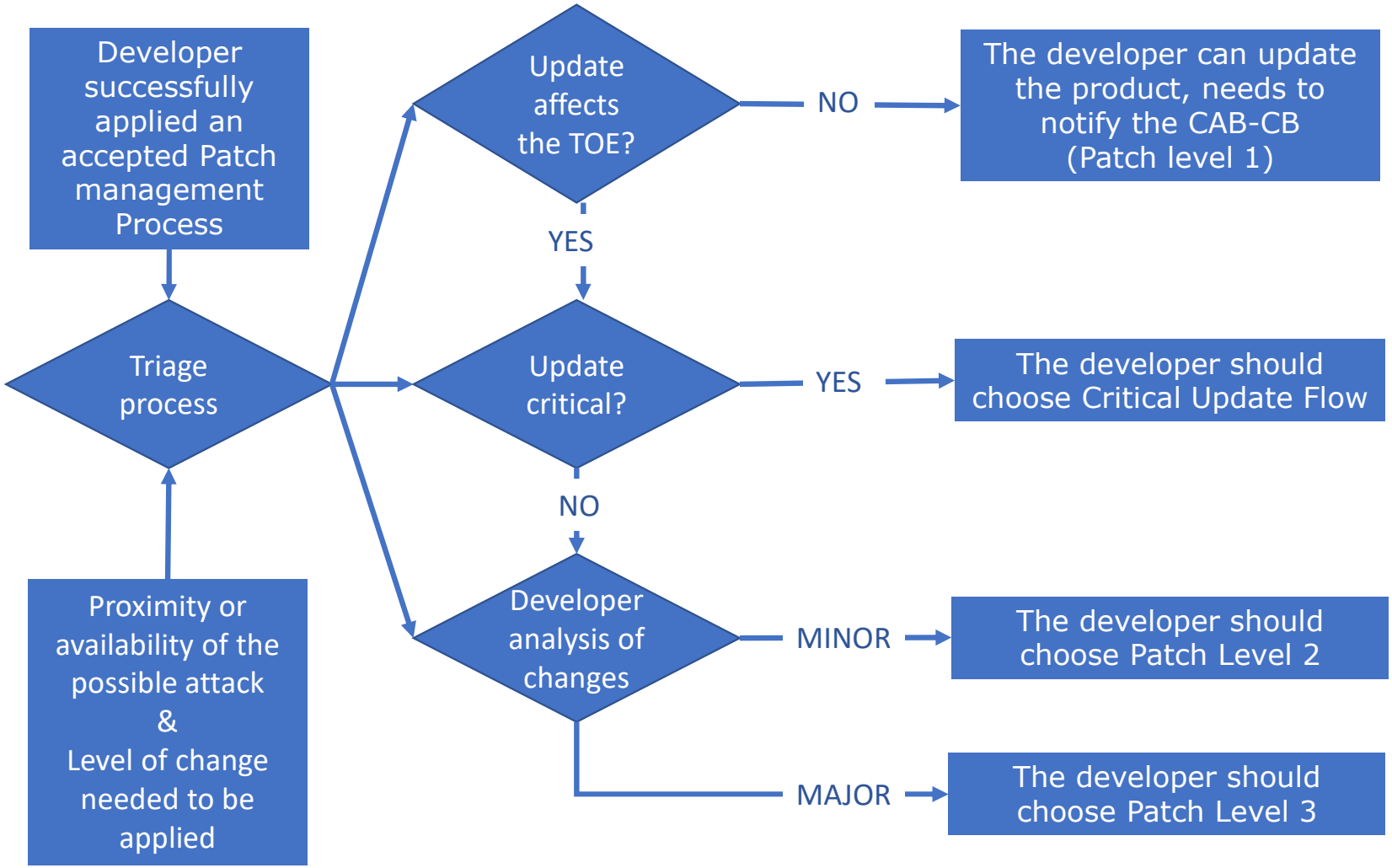
1. Preparation
2. Receipt
3. Verification
4. Remediation development
5. Release and post release

+ Vulnerability disclosure with a possibility of a 1 month embargo period

EUCC scheme rules related to Patch management 1



EU CC scheme rules related to Patch management 2

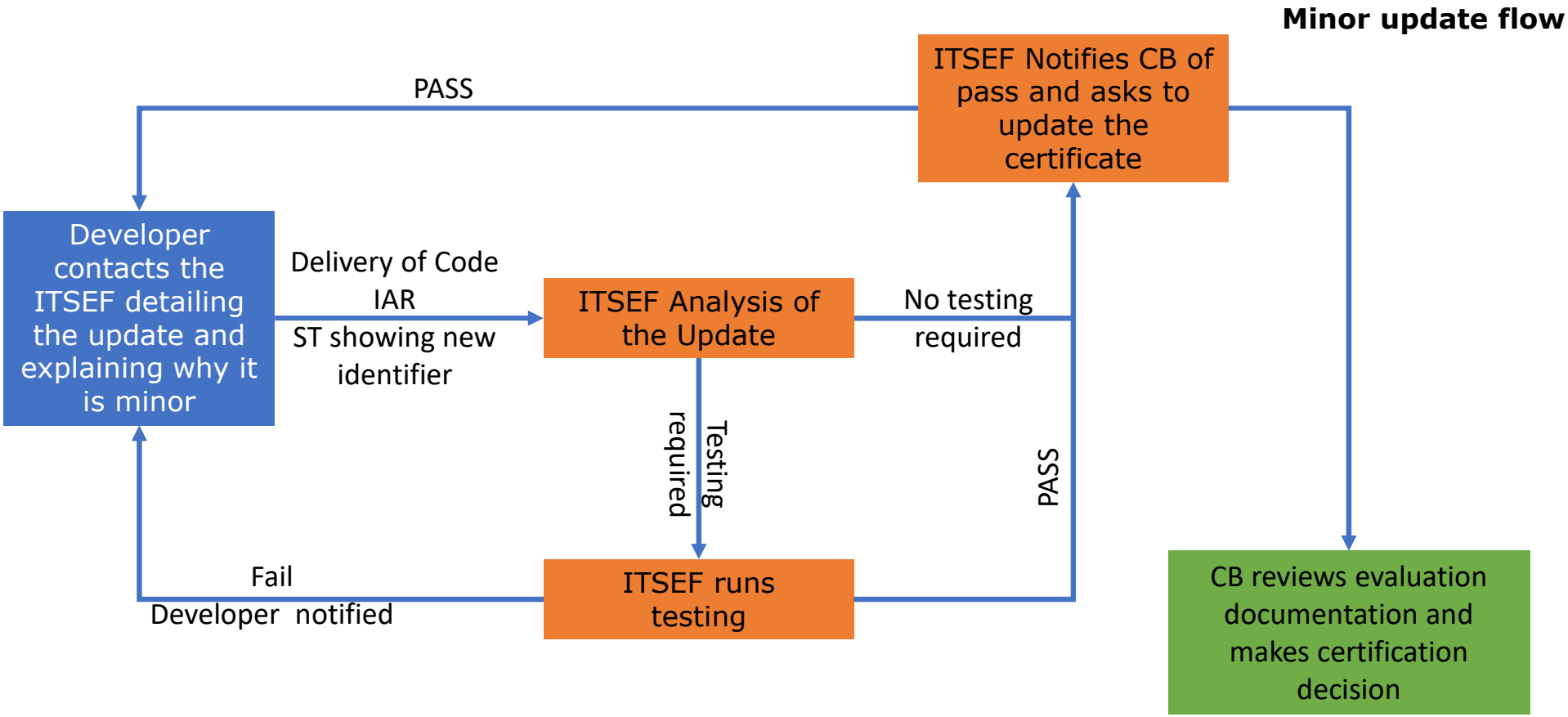


Update process developer view

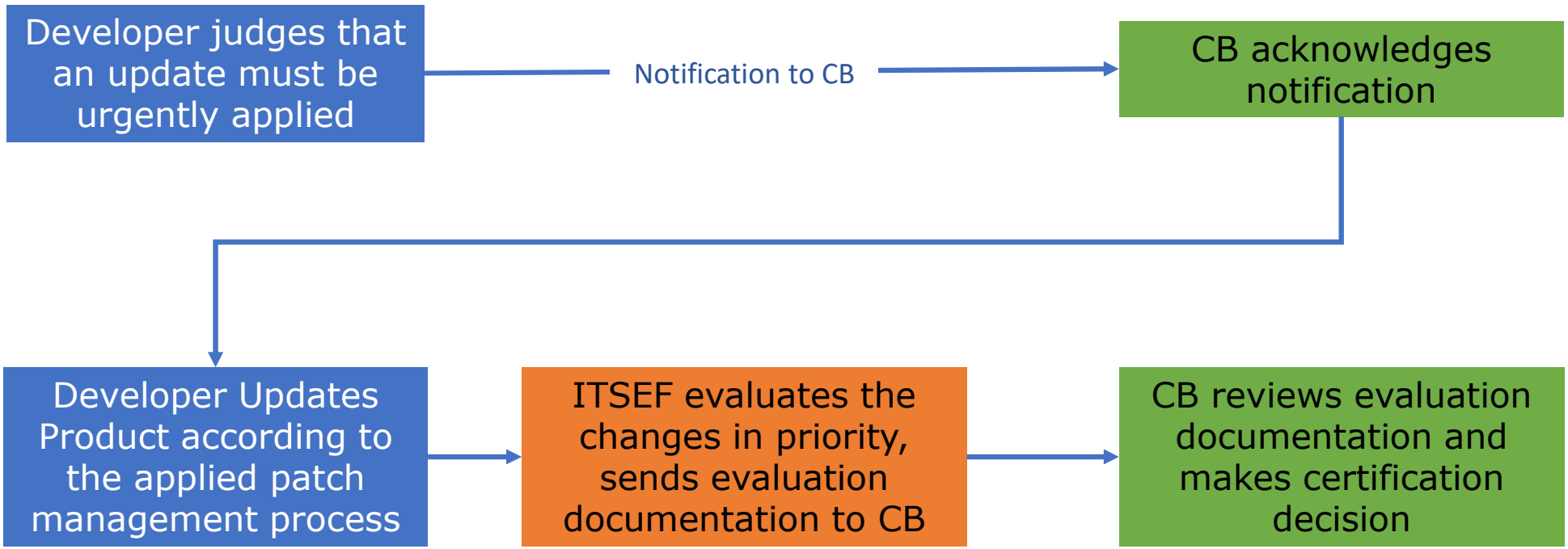
EU CC Scheme rules related to Patch management 3

- the Critical Update Flow Process is asynchronous,
  and for the other levels:
  - in Patch level 1 the CB is notified and able to apply maintenance process if deems necessary;
  - in Patch level 2 the ITSEF evaluates synchronously and CB is again notified and can decide whether to update the version on the certificate.
  - In patch level 3 the process is fully synchronous;
- It is the potential of future review of the scheme to consider applying the fully asynchronous approach as well.

EU CC scheme rules related to Patch management 4



EUCC scheme rules related to Patch management 5



Critical update flow

EUCC scheme rules related to Patch management 6

- Functional patches may be used

only

if the Patch Level 1 approach is used,

or in other cases

bundled with vulnerability patches

and if

do not affect TSFIs neither directly nor indirectly,

and also

do not change the security functionalities satisfying the security functional requirements.

The work of
ENISA ahWG1 Thematic Group Nº5
Continuity assurance and handling of vulnerabilities

CCLAB
THE AGILE SOFTWARE SECURITY LAB

Thank you!

Gábor Hornyák
gabor.hornyak@cclab.com