



PANEL DISCUSSION: EIDAS2 - NIS2 INTERPLAY
**COMPLIANCE ASSESSMENTS
AND SUPERVISION**

9TH TRUST SERVICES AND EID FORUM
15TH CA-DAY

CLEMENS WANKO, TÜV TRUST IT
& THE ACCREDITED CONFORMITY ASSESSMENT BODIES COUNCIL

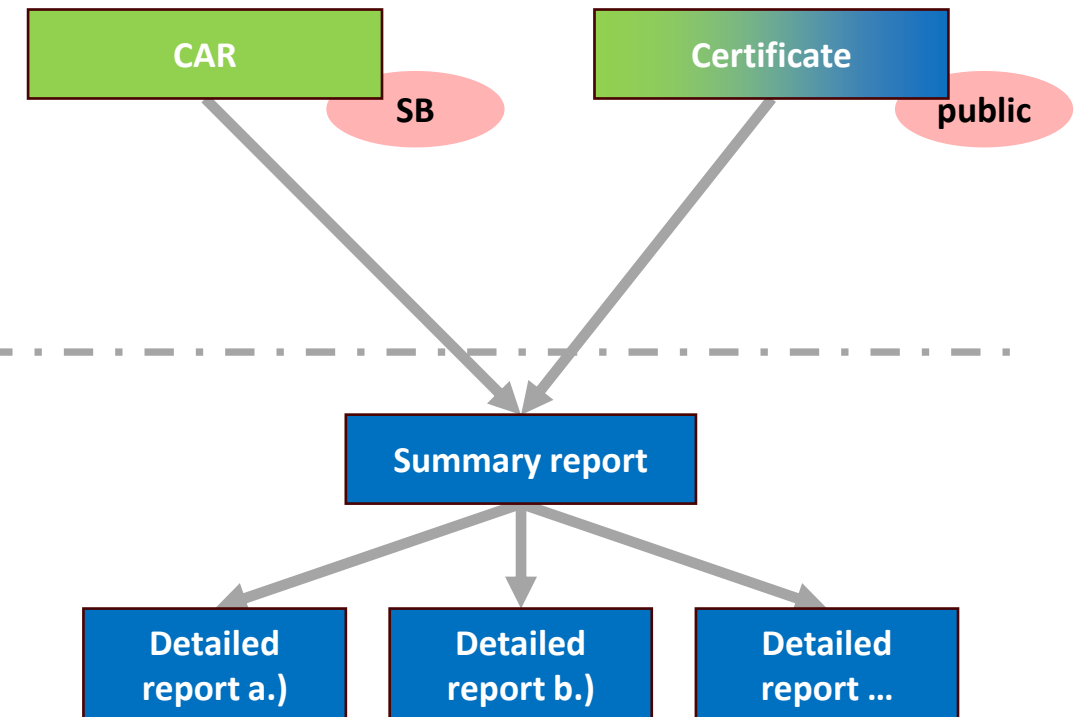
01

REQUIREMENTS, CONFORMITY ASSESSMENT AND REPORTING FOR QTSP EIDAS + X

Current eIDAS set of requirements

- I. eIDAS Regulation**
(EU **legal** requirements)
 - II. EU Memberstates national law on eIDAS**
(nat. **legal** requirements)
-
- III. ETSI/CEN standards**
(**technical/organizational** best practise requirements)

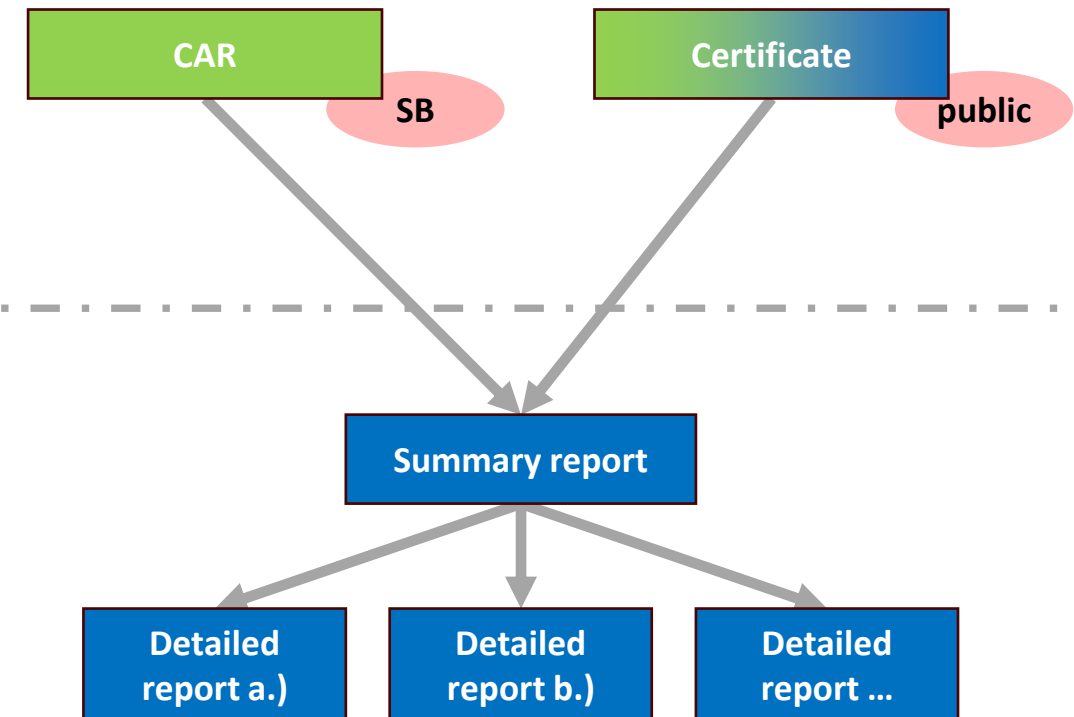
...and its audit reporting hierarchy



Future eIDAS2 + NIS2 set of requirements

- Ia.** eIDAS2 Regulation
(EU **legal** requirements)
- Ib.** NIS2 Directive translated into
EU Memberstates national law
(nat. **legal** requirements)
- II.** EU Memberstates
national law on eIDAS2
(nat. **legal** requirements)
- III.** ETSI/CEN standards + nat. NIS2 add ons
(**technical/organizational** requirements)

...and its audit reporting hierarchy



ALL CLEAR FOR

- ETSI requirements
- processing conformity assessments
(3 stages: document assessment, onsite assessment, reporting)
- reporting hierarchy remains same (NIS2 integrated)
- report processing and eIDAS status granting at eIDAS SB level
- auditor accreditation following ISO/IEC 17065



NOT SO CLEAR FOR

- national NIS2 requirements
 - legal?
 - technical/organizational add ons?
- requirement harmonization between EU MS?



02

QTSP CURRENT COMPLIANCE LEVEL FOR EIDAS + X

eIDAS QTSP evidence already today...

- profound process security measures supporting their full service portfolio
- state of technology general IT- and specific service oriented security measures
- the operation of an asset- and risk-based ISMS
- QTSP management boards responsibility
- third party & supplier integration and security management
- redundancy for service elements with high availability requirements
- comprehensive additional supporting security measures



ALL CLEAR FOR

- generic NIS2 requirements as of EU Directive

UNCLEAR FOR

- new (additional?) national NIS2 requirements
 - legal?
 - technical/organizational??



03

QTSP SUPERVISION EIDAS + X

TO BE CLARIFIED PER EU MS:

- responsibilities: which national bodies are going to be involved?
 - one?
 - > former eIDAS SB or former NIS SB?
 - two or more?
 - > former eIDAS SBs and NIS SB or others?
- interpretation of eIDAS specific requirements
- interpretation of NIS specific requirements





QUESTIONS AND DISCUSSION



CLEMENS WANKO

TÜV TRUST IT / ACAB'C CHAIR

Phone +49 170 80 20 20 7

clemens.wanko@tuv-austria.com



TÜV TRUST IT

Waltherstr. 49-51

51069 Cologne

Germany

WWW.IT-TUV.COM

Network and Information Security Directive 2 - DIRECTIVE (EU) 2022/2555

- The **NIS2 Directive** is a European Union legislative text on **cybersecurity**. It supersedes the first NIS (Network and Information Security) Directive, adopted in July 2016
- Directive (EU) 2016/1148 (the NIS Directive) is **repealed with effect from 18 October 2024 and replaced by NIS2**
- Distinguishes two type of entities, **essential** and **important** entities (**QTSP are essentials, Art 3 1(b)**)
- Entities management bodies have **active role**
- Competent Authorities **can impose fines**
- NIS2 provides list of **framing security measures** that shall be implemented
- Entities to perform **due diligence of their supply chain**
- Entities to submit **incident notification within 24 hours**

**NIS2
DIRECTIVE**