ENISA TRUST SERVICES FORUM - CA DAY 2021

EIDAS 2.0 - SERVICE MODULES RELOADED
CROSS BORDER PROVISIONING OF SERVICE MODULES FOR TSP

Clemens Wanko - TÜV TRUST IT / TÜV AUSTRIA CERT

I. What are „Modules" and why are they a good idea?

II. eIDAS Regulation (EU) 910/2014 – what's the state of play?
- Requirements for Module Operators

III. eIDAS Regulation 2.0* – what's the future?
- New level of complexity
- Variety of responsible bodies to serve

*draft as of June 3rd, 2021

I. **What are „Modules" and why are they a good idea?**

II. eIDAS Regulation (EU) 910/2014 – what's the state of play?
- Requirements for Module Operators

III. eIDAS Regulation 2.0* – what's the future?
- New level of complexity
- Variety of responsible bodies to serve

*draft as of June 3rd, 2021

I. What are „Modules" and why are they a good idea?

Functional segregation of process elements for Qualified Trust Services (QTS)

Example:
QTS issuing qualified certificates

| user identification
natural/legal person
eIDAS Art. 24 (1) and (2) | user data
registration
eIDAS Art. 24 (2) | certificate
generation and
disemination
eIDAS Art. 24 (2) | certificate
status service
eIDAS Art. 24 (2), (3)
and (4) | certificate
revocation
eIDAS Art. 24 (2), (3)
and (4) |

Note: the term "module" is synonymous with "component" as used within ETSI standards

I. What are „Modules" and why are they a good idea?

Functional segregation of process elements for Qualified Trust Services (QTS)

Example:
QTS issuing qualified certificates

user identification
natural/legal person
eIDAS Art. 24 (1) and (2)

...er data ...ation ...Art. 24 (2)

certificate generation and disemination
eIDAS Art. 24 (2)

certificate status service
eIDAS Art. 24 (2), (3) and (4)

certificate revocation
eIDAS Art. 24 (2), (3) and (4)

I. What are „Modules" and why are they a good idea?

Functional segregation of process elements for Qualified Trust Services (QTS)

Example:
QTS issuing qualified certificates

user identification
natural/legal person
eIDAS Art. 24 (1) and (2)
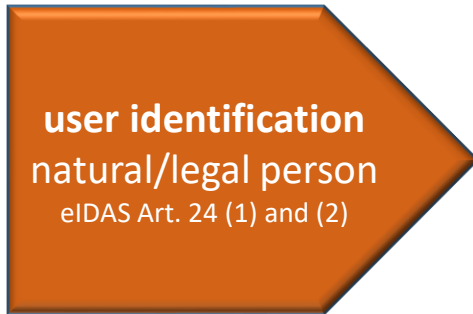
- dedicated specialized service provider (third party) may offer eIDAS compliant process elements of a QTS

- QTSP may rely on a third party, e.g. for verification of users identity and attributes – eIDAS Art. 24(1), 24(2 b)

User identification at appropriate assurance level for natural/legal persons, provided by external party!

I. What are „Modules" and why are they a good idea?

Example:
Module for user identification for QTSP issuing qualified certificates

- operated by external specialized ident service provider (IDSP)

- IDSP must be eIDAS compliant

Integration

user identification natural/legal person eIDAS Art. 24 (1) and (2)	user data registration eIDAS Art. 24 (2)	certificate generation and disemination eIDAS Art. 24 (2)

Option A: integrate IDSP
Compliance can be evidenced through integration in QTSPs policy model

Disadvantages for IDSP and QTSP:

- IDSP conformity assessment must be repeated for every QTSP serviced / IDSP is assessed multiple times

- QTSP must integrate IDSP in own policy and sync conformity assessments

- IDSP does NOT receive own compliance status document (e.g. a certificate)

establish independent
Module

I. What are „Modules" and why are they a good idea?

Example:
Module for user identification for QTSP issuing qualified certificates

- operated by external specialized ident service provider (IDSP)

- IDSP must be eIDAS compliant

| user identification natural/legal person eIDAS Art. 24 (1) and (2) | user data registration eIDAS Art. 24 (2) | certificate generation and disemination eIDAS Art. 24 (2) |

Option B: modularize IDSP
IDSP receives own eIDAS Conformity Assessment Report (CAR) for the „Module"

Advantages for IDSP and QTSP:

+ IDSP can re-use Module CAR for different QTSP serviced

+ IDSP ensures eIDAS compliance independently from QTSP = QTSP can interface to IDSP without
  re-assessment of identification processes (only interfacing will be subject to assessment)

+ IDSP has own compliance status document CAR which can be accompanied by a corresponding certificate

I. What are „Modules" and why are they a good idea?

Example:
Module for user identification for QTSP issuing qualified certificates

- operated by external specialized ident service provider (IDSP)

- IDSP must be eIDAS compliant

user identification natural/legal person
eIDAS Art. 24 (1) and (2)

user data registration
eIDAS Art. 24 (2)

certificate generation and dissemination
eIDAS Art. 24 (3)

user data registration
eIDAS Art. 24 (2)

certificate generation and dissemination
eIDAS Art. 24 (3)

user data registration
eIDAS Art. 24 (2)

certificate generation and dissemination
eIDAS Art. 24 (3)

Option B: modularize IDSP
IDSP receives own eIDAS Conformity Assessment Report (CAR) for the „Module"

Advantages for IDSP and QTSP:

+ IDSP can re-use Module CAR for different QTSP serviced

+ IDSP ensures eIDAS compliance independently from QTSP = QTSP can interface to IDSP without re-assessment of identification processes (only interfacing will be subject to assessment)

+ IDSP has own compliance status document CAR which can be accompanied by a corresponding certificate

I. What are „Modules" and why are they a good idea?

II. eIDAS Regulation (EU) 910/2014 – what's the state of play?
- **Requirements for Module Operators**

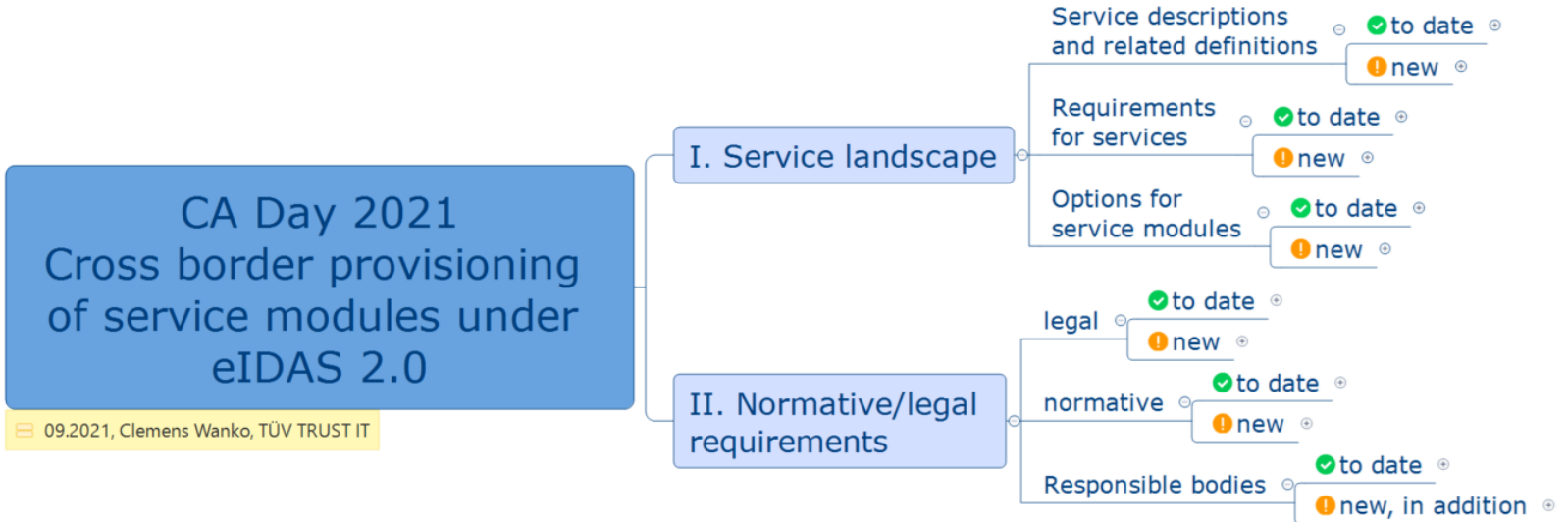III. eIDAS Regulation 2.0* – what's the future?
- New level of complexity
- Variety of responsible bodies to serve

*draft as of June 3rd, 2021

II. eIDAS Regulation (EU) 910/2014 – what's the state of play?

- Requirements for Module Operators <u>as of today</u>

(1) eIDAS Regulation (EU) 910/2014

(2) Technical/process related
typ. ETSI EN 319 401, ETSI EN 319 411-1 and -2, etc.

Per EU memberstate:

(3) National law and regulations on Trust Services = memberstate specifics
<u>Example:</u> IDSP servicing QTSP in Germany and using video based identification must comply with supplementing criteria established by SB, BNetzA

Upon successful assessment:

- **Issuance of Conformity Assessment Report for the TSP or Module SP**
- **National SB takes final compliance decision based upon CAR**

I. What are „Modules" and why are they a good idea?

II. eIDAS Regulation (EU) 910/2014 – what's the state of play?
 ▪ Requirements for Module Operators

III. eIDAS Regulation 2.0* – what's the future?
 ▪ New level of complexity
 ▪ Variety of responsible bodies to serve
 *draft as of June 3rd, 2021

III. eIDAS Regulation 2.0 – what's the future?

- New level of complexity

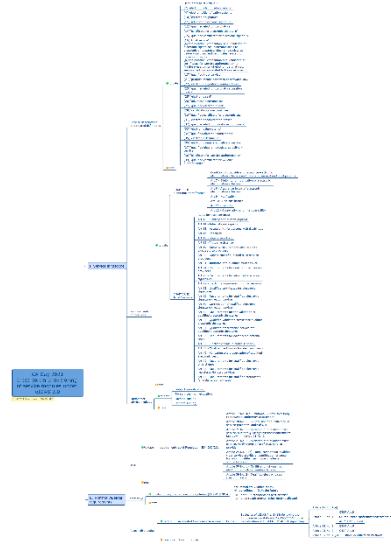## III. eIDAS Regulation 2.0 – what's the future?

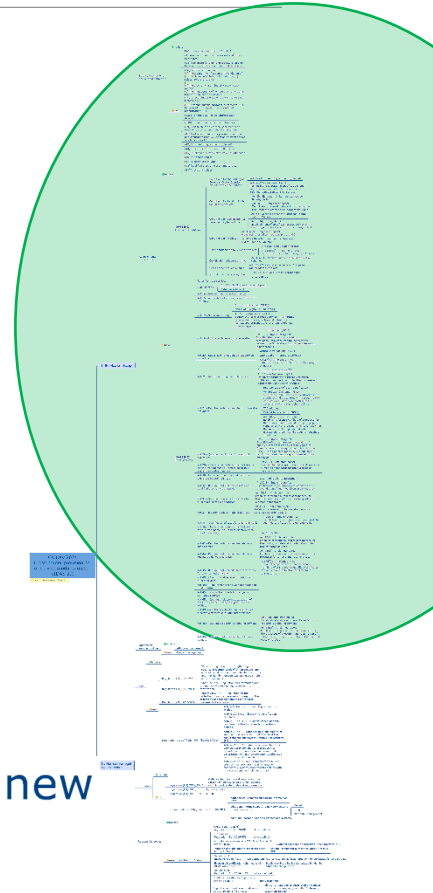- New level of complexity

Complexity footprint

III. **eIDAS Regulation 2.0 – what's the future?**

- New level of complexity

Complexity footprint
Current Regulation (EU) 910/2014

✅ to date

III. eIDAS Regulation 2.0 – what's the future?

- New level of complexity

Complexity footprint
revised eIDAS Regulation 2.0*
*draft as of June 3rd, 2021
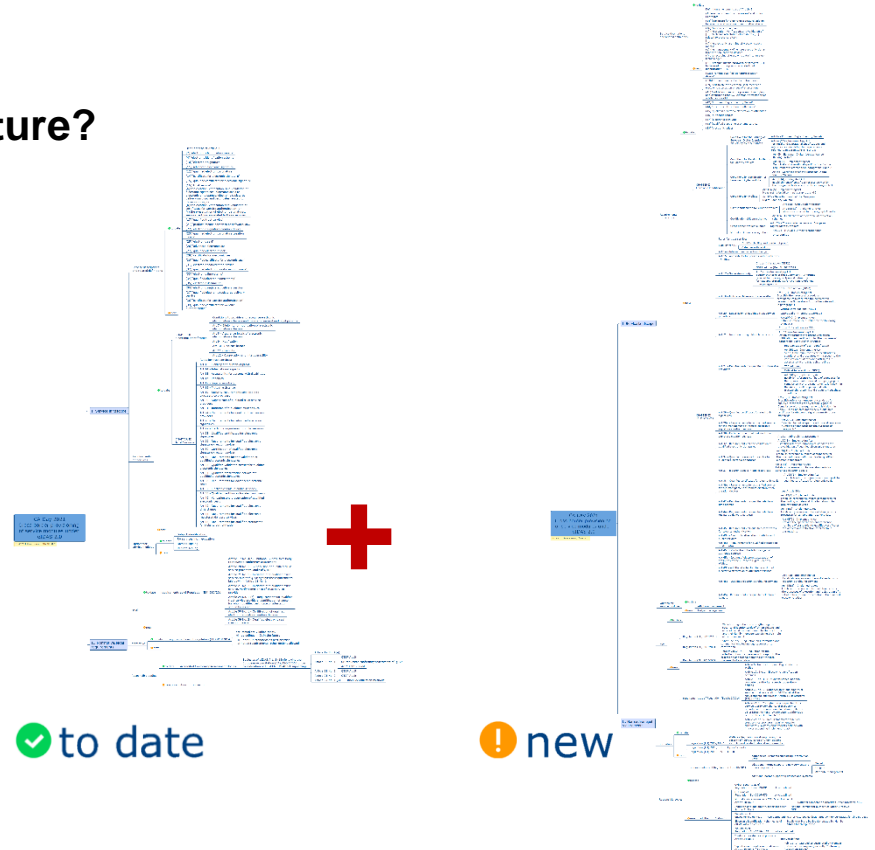
✅ to date   ❗ new

III. eIDAS Regulation 2.0 – what's the future?

- New level of complexity
- Revised eIDAS Regulation 2.0
  draft as of June 3rd, 2021

Really good news (1):

amended set of Services

- European Digital Identity Wallet
- electronic archiving
- electronic attestation of attributes
- management of remote electronic signature and seal creation devices
- electronic ledgers

own TS = may replace Service Modules!
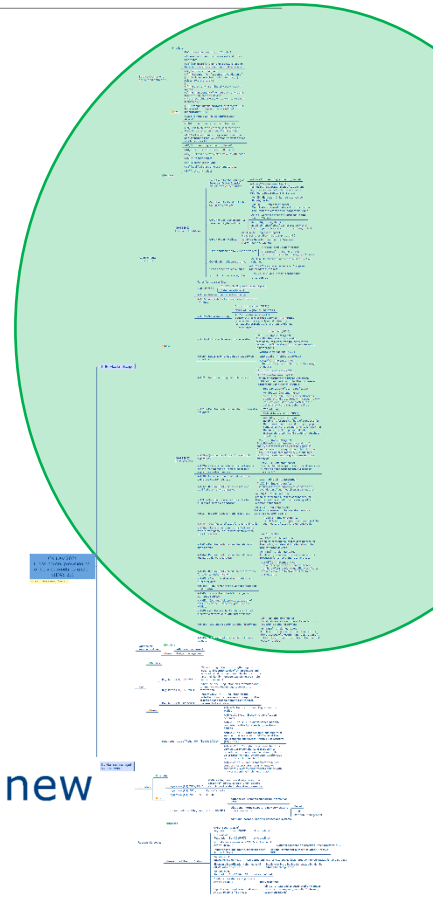
⚠ new

III. eIDAS Regulation 2.0 – what's the future?

- New level of complexity
- Revised eIDAS Regulation 2.0
  draft as of June 3rd, 2021

Really good news (2):

- outsourcing and
- subcontracting (e.g. Art. 24 (2b))
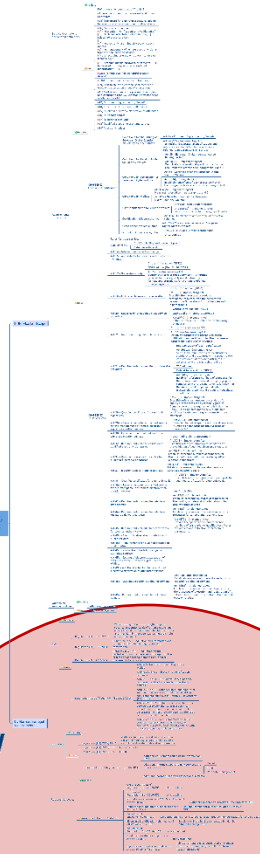
are supported!

= Modules for Trust Services

⚠ new

III. eIDAS Regulation 2.0 – what's the future?

- New level of complexity
- Revised eIDAS Regulation 2.0
  draft as of June 3rd, 2021

Not so good news, really:

services (all) map to more complex set of

    a. responsible bodies and

    b. requirements

⚠ new

I. What are „Modules" and why are they a good idea?

II. eIDAS Regulation (EU) 910/2014 – what's the state of play?
- Requirements for Module Operators
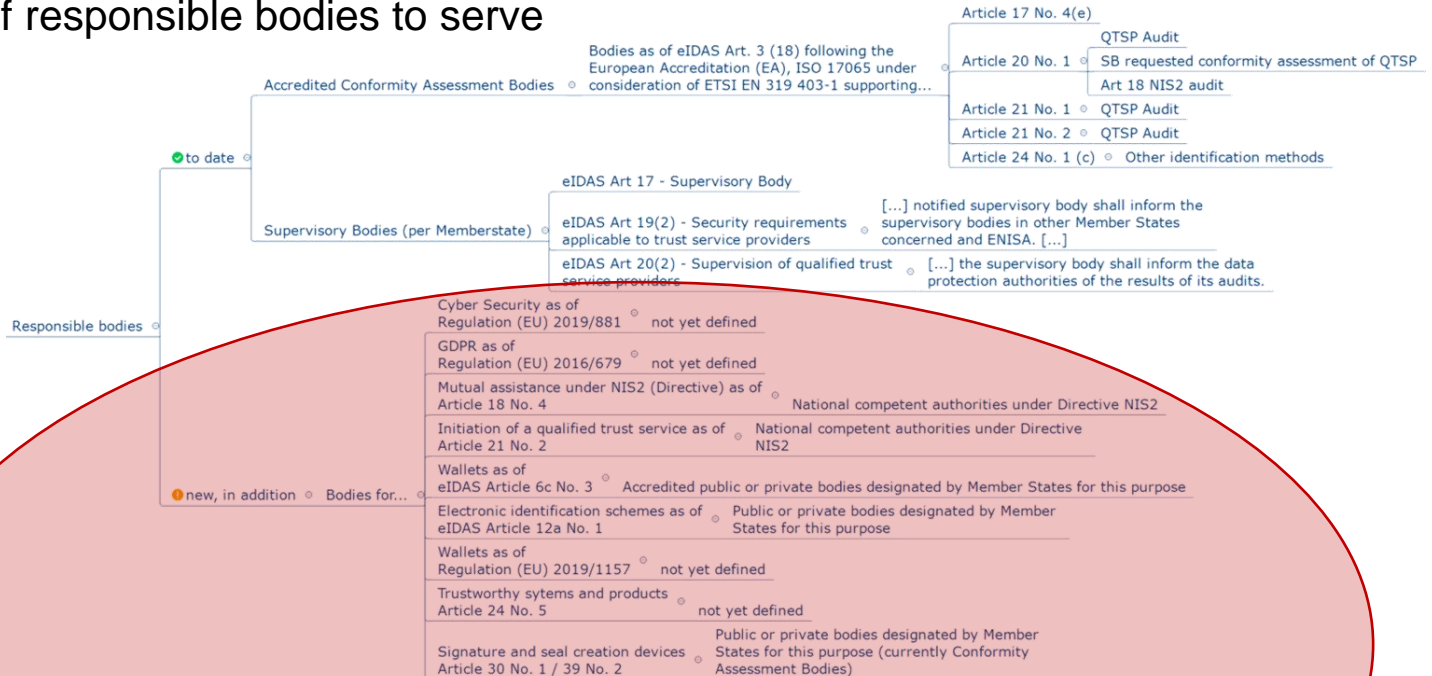
III. eIDAS Regulation 2.0* – what's the future?
- New level of complexity
- Variety of responsible bodies to serve

*draft as of June 3rd, 2021

III. eIDAS Regulation 2.0 – what's the future?

- Variety of responsible bodies to serve

III. eIDAS Regulation 2.0 – what's the future?

- Additional responsible bodies…

Bodies for…

Cyber Security as of
Regulation (EU) 2019/881

GDPR as of
Regulation (EU) 2016/679

Mutual assistance under NIS2 (Directive) as of
Article 18 No. 4

Initiation of a qualified trust service as of
Article 21 No. 2

Wallets as of
eIDAS Article 6c No. 3

Electronic identification schemes as of
eIDAS Article 12a No. 1

Wallets as of
Regulation (EU) 2019/1157

Trustworthy sytems and products
Article 24 No. 5

Signature and seal creation devices
Article 30 No. 1 / 39 No. 2

EU level? (process related)
responsible bodies (eIDAS) not yet appointed

National/MS level (process related)
responsible bodies:
- National comp. authorities as of Directive NIS2
  for critical infrastructures
- Public or private bodies designated by memberstates for
  this purpose

Mixed EU or National/MS level (tech. related)
responsible bodies:
- Public or private bodies designated by memberstates for
  this purpose, currently CABs
- or not yet appointed for eIDAS

II. eIDAS Regulation (EU) 910/2014 – what's the state of play?

- <u>New requirement set</u> – also for Module Operators

(1) eIDAS Regulation (EU) 910/2014 (update)

(2) Regulation (EU) 2019/881 (Cyber Security)

(3) Regulation (EU) 2016/679 (GDPR)

(4) Technical/process related for TSP

(5) Technical/process related for wallets as of Regulation (EU) 2019/1157

(6) Technical/process trustworthy systems and products (eIDAS Article 24 No. 5)

Per EU memberstate:

(5) National law and regulations on Trust Services = memberstate specifics

(6) NIS 2 National competent authorities

…plus others, depending on the specific service provided.

Entity responsible for compliance and matters of harmonized implementation?

Upon successful assessment…
…by whom?
…of what exactly?

And the final compliance decision is taken by…?

Today

II. eIDAS Regulation (EU) 910/2014 – what's the state of play?

- Requirements for Module Operators <u>as of today</u>

(1)   eIDAS Regulation (EU) 910/2014

(2)   Technical/process related for TSP

Per EU memberstate:

(3)   National law and regulations on Trust Services = memberstate specifics

Upon successful assessment

- Issuance of CAR for the Module SP
- National SB takes final compliance decision based upon CAR

Conclusion

I. What are „Modules" and why are they a good idea?

II. eIDAS Regulation (EU) 910/2014 – what's the state of play?
- Requirements for Module Operators

III. eIDAS Regulation 2.0* – what's the future?
- New level of complexity
- Variety of responsible bodies to serve

*draft as of June 3rd, 2021

Service Modules for Qualified Trust Services under eIDAS 2.0

Cross border provisioning of Trust Service Modules

Conclusion
eIDAS 2.0, draft as of June 3rd, 2021

Rising demand for Service Modules under eIDAS 2.0
(Subject identification; RA services incl. revocation; attribute management; …)

Services facing higher compliance complexity level
(eIDAS Regulation (EU) 910/2014 (update); Regulation (EU) 2019/881 (Cyber Security);
Regulation (EU) 2016/679 (GDPR); NIS 2 Directive; …)

Multiple additional responsible bodies to serve (also nationals)
(Cyber Security; GDPR; NIS2; systems and devices; …)

Assessing service elements in form of Modules (Components) is preserved

But: Clear set of requirements and resp. bodies necessary to be defined!

Established Conformity Assessment Bodies (CAB) are ready to implement

But: CAB need to be mandated by EU Commission!