Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Département fédéral de justice et police DFJP

Bundesamt für Justiz BJ
Office fédéral de la justice OFJ

Technical Advisory Circle

Meeting II

16.10.2023

Create maximum value

- Shared thoughts – shared reasoning
- Use «your» tongue
- Also mention basic assumptions
- No need to defend – but challenge!

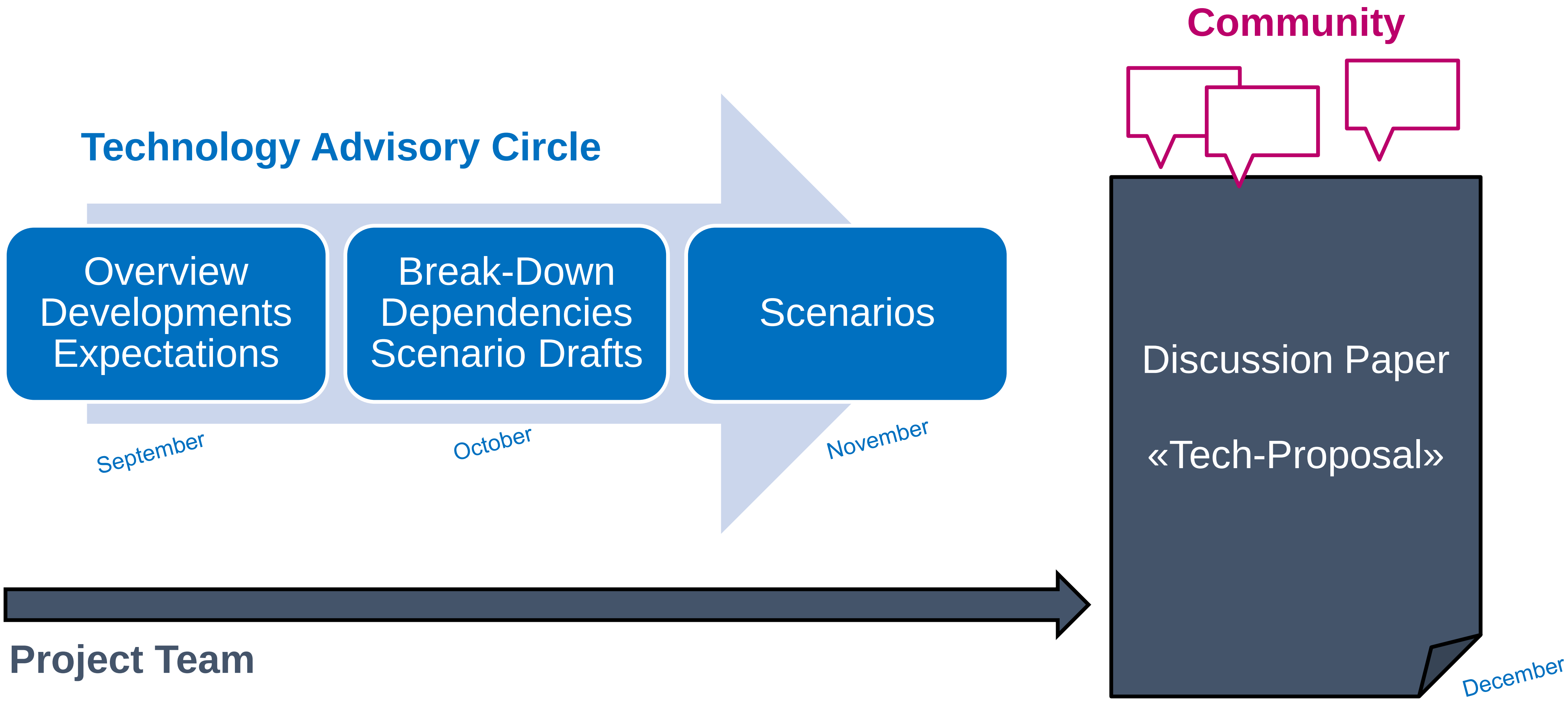
Role of Federal Representants

«We ask and listen»

Disclaimer

- Protocol without attributions
- Session is recorded to create the protocol, not for public distribution
- Name credits mentioned as «Participant of Meeting» & «Part of TAC»

What are we doing?



Community

Technology Advisory Circle

Overview Developments Expectations

Break-Down Dependencies Scenario Drafts

Scenarios

September

October

November

Discussion Paper

«Tech-Proposal»

December

Project Team

How does the Techical Advisory Circle work?

- Sharing current knowledge, oppinions, expectations
- Collecting valuable sources (pointers to other relevant papers, PoCs, activities…)
- Outlining potential contributions «of Switzerland» to an SSI-world
- **Get stuff done:** Having two scenarios defined at the third meeting

Input creation for the Discussion Paper «Tech-Proposal»

Will the TAC continue after the announced meetings? Most probably.

Inputs from 37th Internet Identity Week (IIW)

R|EVOLUTION
The First 2000 Years of Computing
N
The First 2000 Years of Computing

Discussion Paper «Tech-Proposal»: Structure

Discussion Paper – Structure:

0 References/Sources
1 Purpose of the document
2 Background
3 Design Principles & Criteria
4 Lessons learned
5 Scenarios
6 Public discussion of the "how to"

Structure on GitHub: Discussion paper content collection · e-id-admin/open-source-community · Discussion #25 (github.com)
References/Source-Collection on GitHub: https://github.com/e-id-admin/open-source-community/discussions/25#discussioncomment-7292021

- A Working Group of the E-ID Team is in charge of writing
- Inputs from TAC and Dev-Team E-ID is taken into account
- Goal is to have a paper which allows a public consultation regarding the technology decision and the potential compromises it brings regarding the fulfilment of requirements.

Discussion Paper «Tech-Proposal»: Planned next steps

- Third TAC meeting: November 9, 2023
- Public discussion paper: December 1, 2023
- Informal public consultation process until end December 2023
- Analysis of feedbacks
- Decision by the confederation beginning 2024

Requirements: The principles as in the six motions and proposed law (Gesetzesvorentwurf)

- **Privacy by Design**
  - “A holder can present a verifiable credential to a verifier without the issuer being informed.”
- **Data Minimization**
  - “A holder can define which credential, which parts of a credentials (selective disclosure) or which derived information of a credential shall be transmitted.”
- **Decentral Storage of eID**
  - The credential is sent from the issuer to the holder and from there presented to verifiers.
  - The choice of the technical means of storage is up to the holder.
  - No credential information resides in the base registry except revocation information.
- **Governance**
  - The system is run by the Confederation

Let’s talk about «Unlinkability»

Input from the public consultation (Vernehmlassung): «Overidentification», misuse of unnecessarily collected data, risk of tying need to be better addressed

- Misuse linkability? Issuer and verifier collude; different verifiers collude; verifier colludes different use-cases. Countermeasures?
- On what data can correlations be made?
  - Attribute value/content (e.g. Social security number)
  - Hashes (SD-JWT)
  - Public keys (Key binding verification)
  - Revocation (StatusList Index)
  - Context-Data (Browser fingerprint …)
- Mitigation possibilities for the user?
- Unlinkability as a risk for the verifier? (Hello Proxy!?)

Criteria cluster(s)

Privacy preservation

- Resilience
- Unlinkability

Security

- Protocol security
- Cryptographic primitives

Ease of Use

- *User centered*
- *Understanding*

Readiness for the future

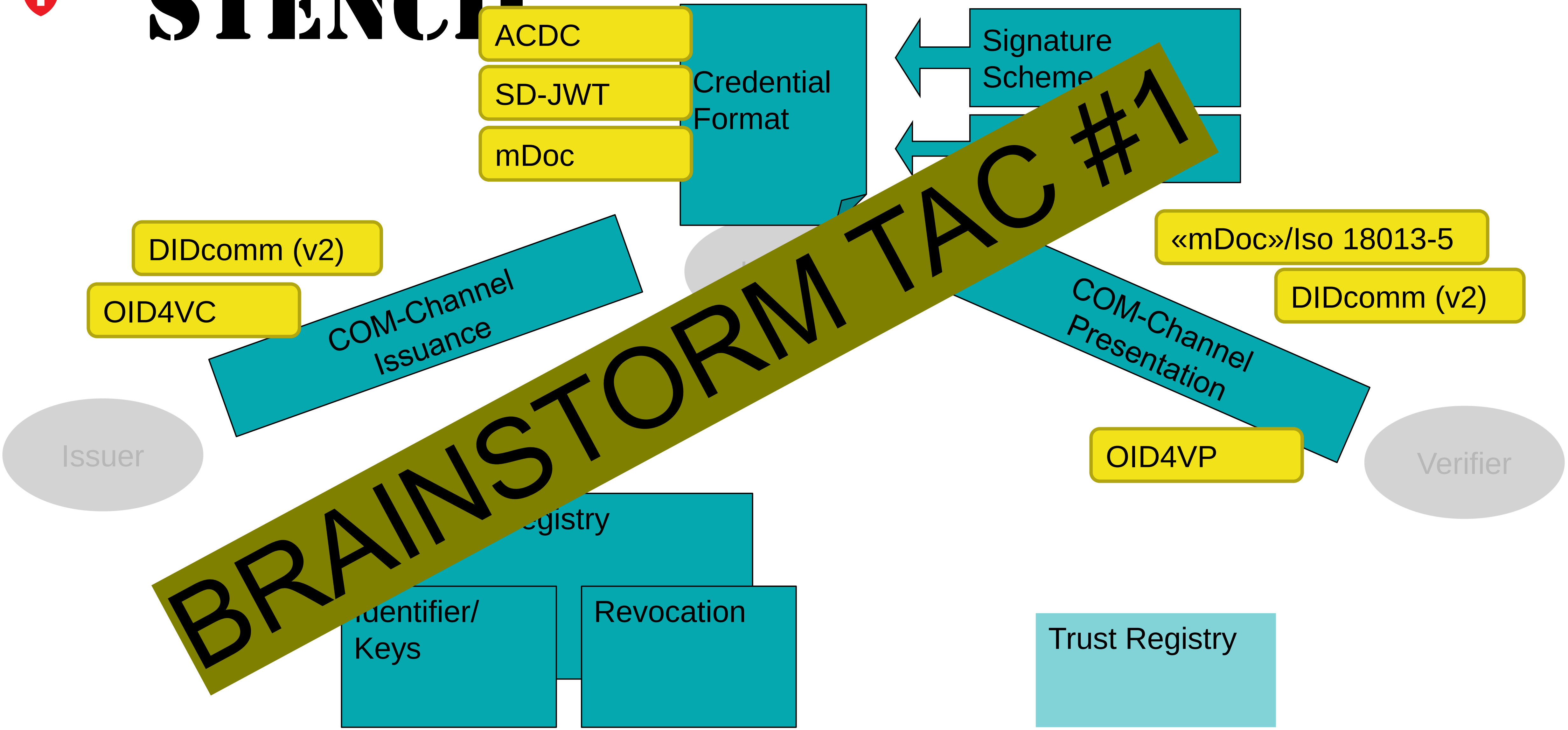
- Crypto agility
- Modularity

Interoperability & Standardization

Maturity

Operability & Integration

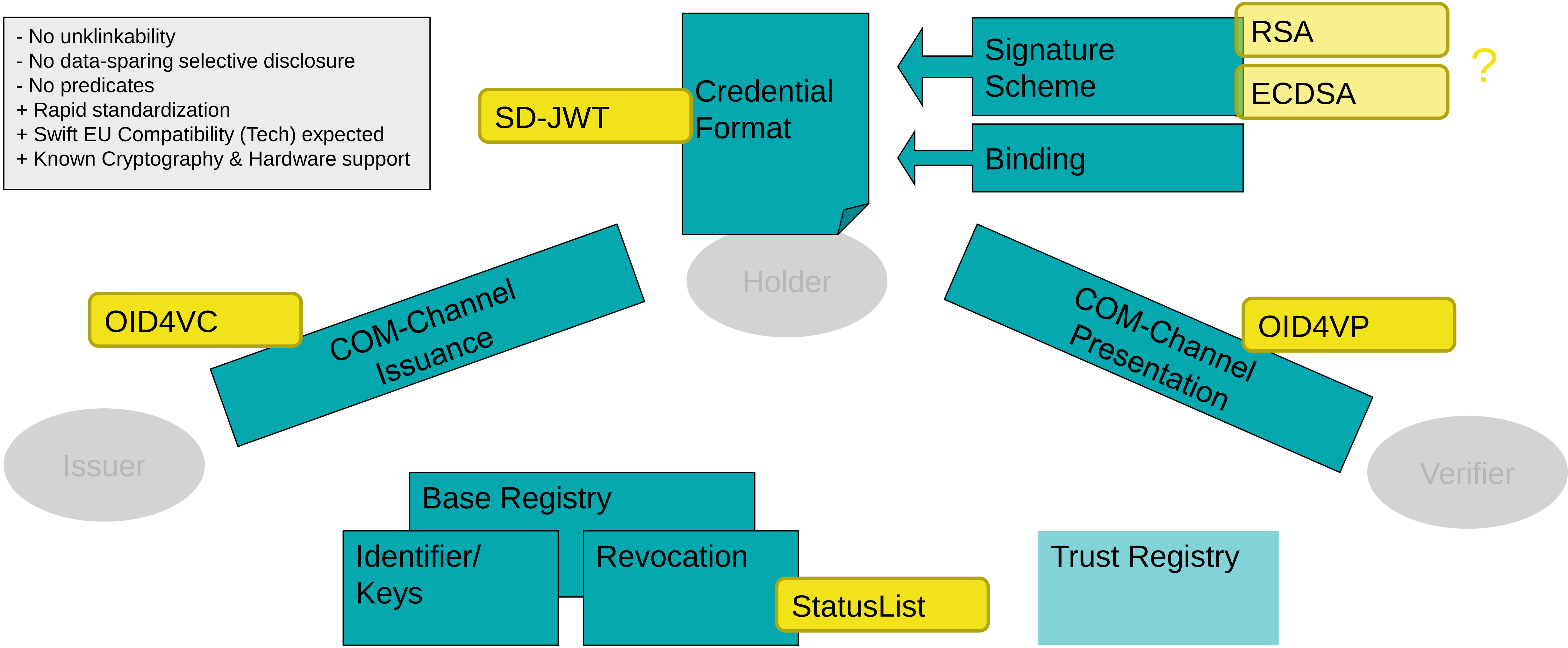
STENCH


ACDC
SD-JWT
mDoc
Credential Format
Signature Scheme
DIDcomm (v2)
OID4VC
COM-Channel Issuance
«mDoc»/Iso 18013-5
DIDcomm (v2)
COM-Channel Presentation
OID4VP
Issuer
Verifier
BRAINSTORM TAC #1
egistry
dentifier/ Keys
Revocation
Trust Registry

SCENARIO A

„Direct interoperability with the EU“

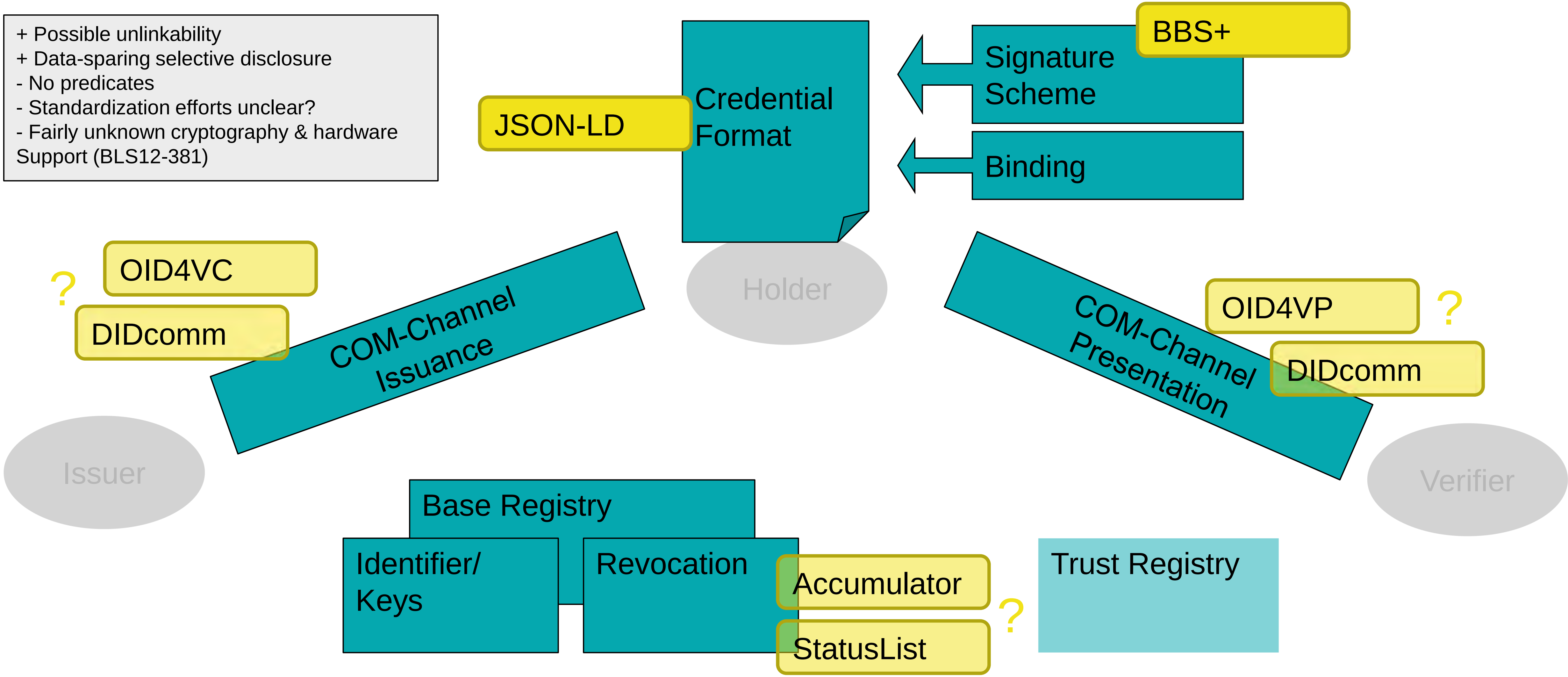
- No unklinkability
- No data-sparing selective disclosure
- No predicates
+ Rapid standardization
+ Swift EU Compatibility (Tech) expected
+ Known Cryptography & Hardware support



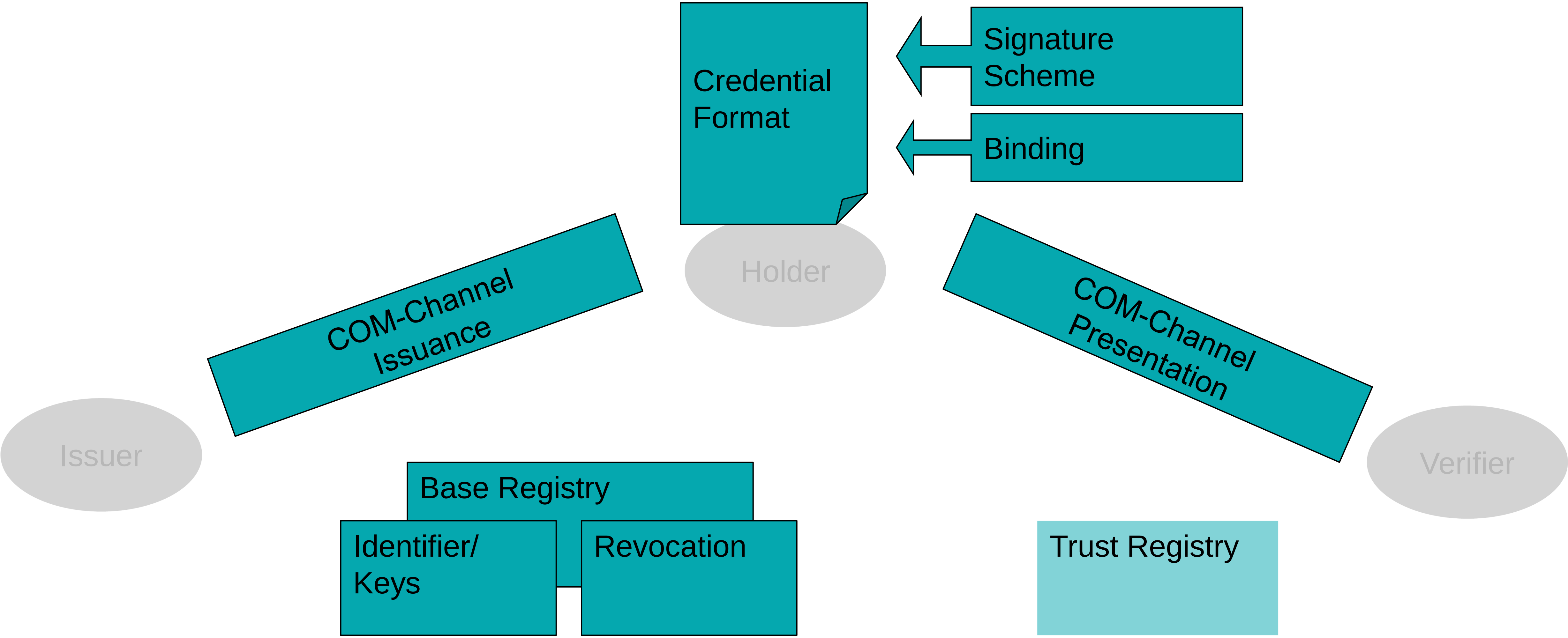
SCENARIO B

„Following a privacy path“

+ Possible unlinkability
+ Data-sparing selective disclosure
- No predicates
- Standardization efforts unclear?
- Fairly unknown cryptography & hardware Support (BLS12-381)



SCENARIO C ?


Credential Format
Signature Scheme
Binding
Holder
COM-Channel Issuance
COM-Channel Presentation
Issuer
Verifier
Base Registry
Identifier/ Keys
Revocation
Trust Registry

Any other inputs?

Next TAC: Thursday, November 9, 2023; 15:00 – 17:00

Instructions may follow.
Call-Link already sent.

Announcment: Hybride Participation Meeting: Friday, December 1, 2023 approx. 9 – 17 h