Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

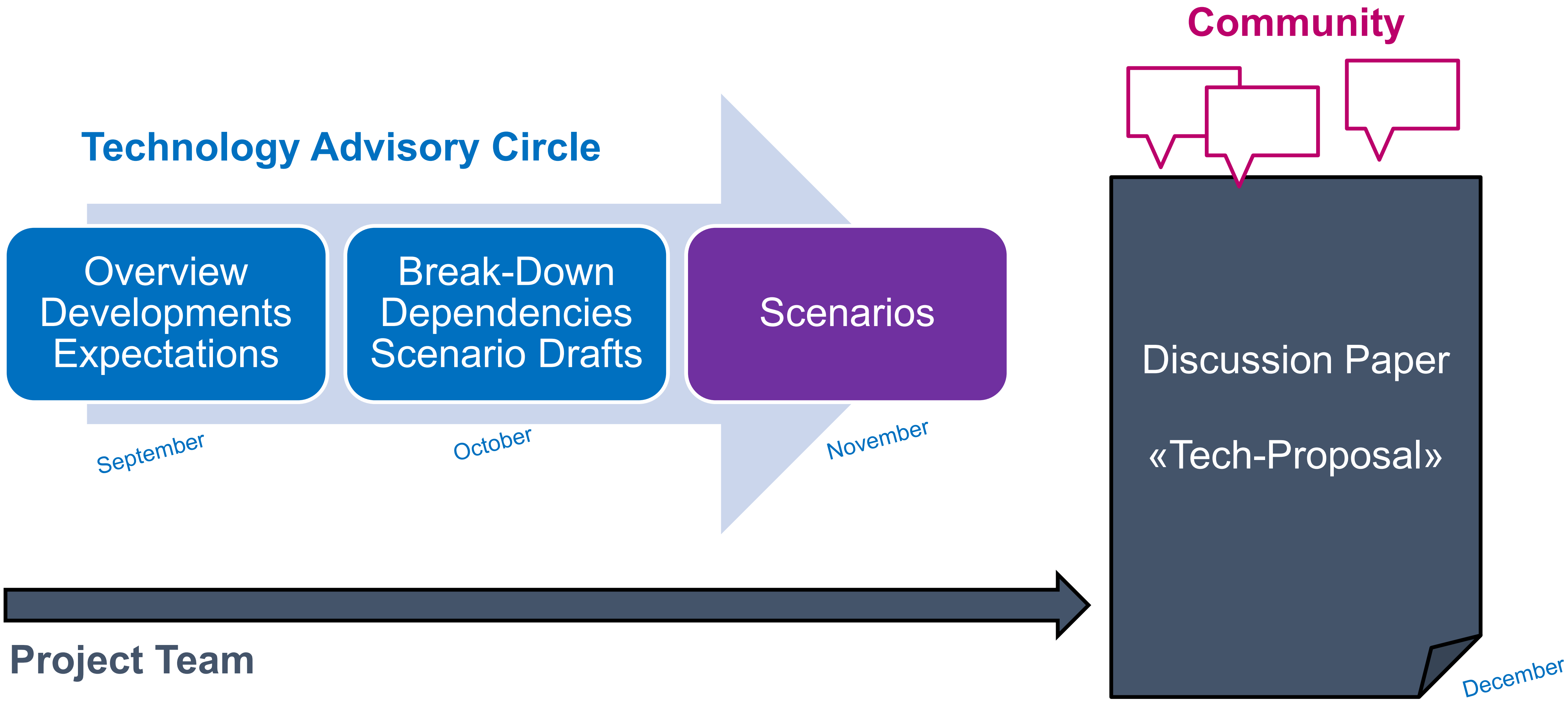
Bundesamt für Justiz BJ
Office fédéral de la justice OFJ

Technical Advisory Circle

Meeting III

09.11.2023

Welcome at our 3rd Meeting



Community

Technology Advisory Circle

Overview Developments Expectations

Break-Down Dependencies Scenario Drafts

Scenarios

September

October

November

Discussion Paper

«Tech-Proposal»

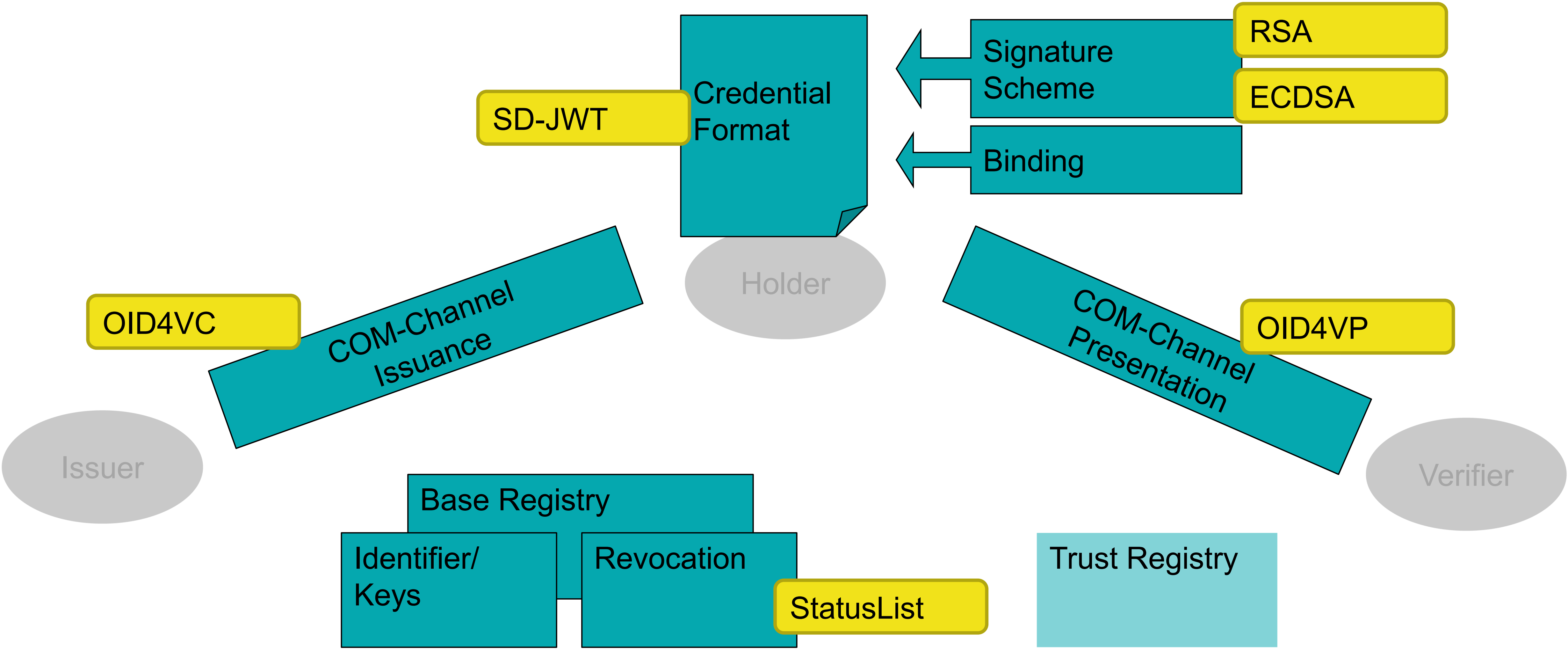
December

Project Team

Inputs from everybody – current thoughts

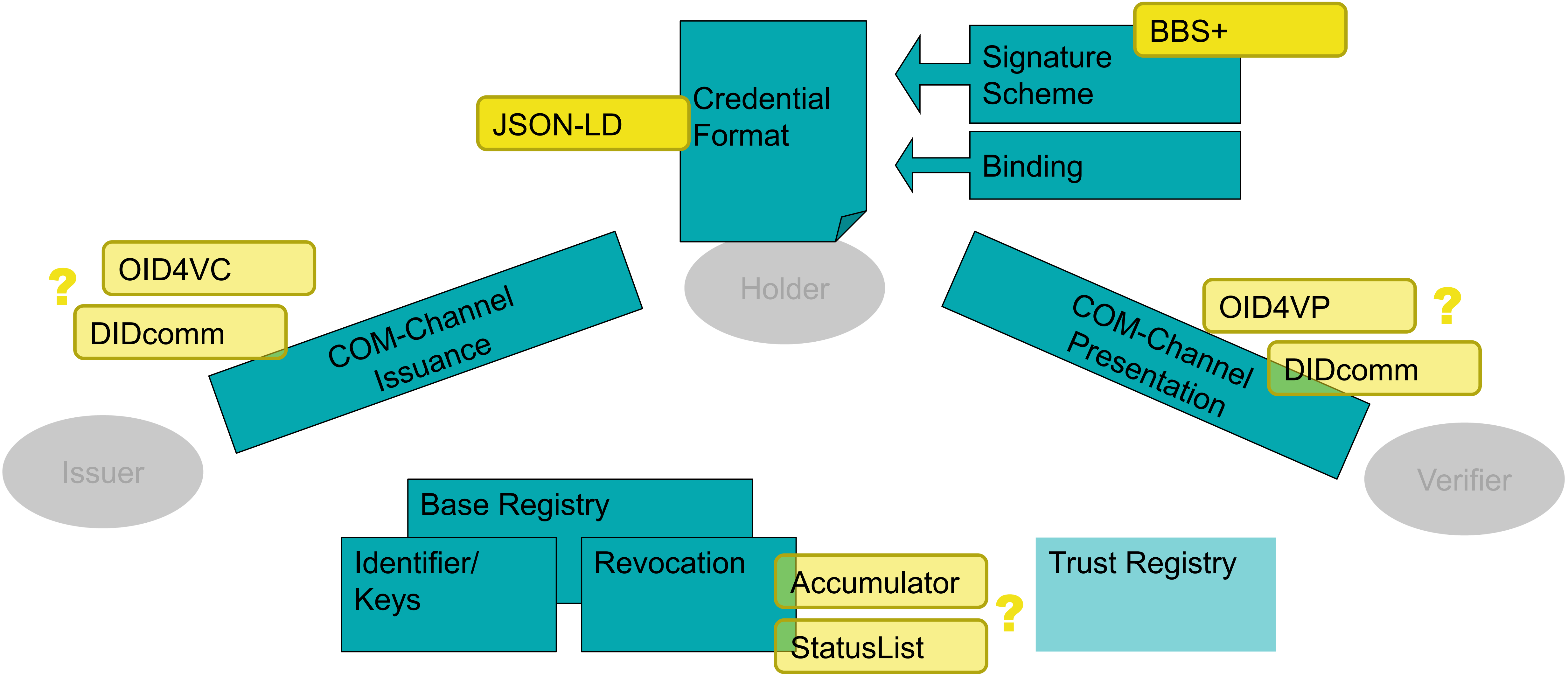
SCENARIO A

„Direct interoperability with the EU“



SCENARIO B

„Following a privacy path“



Q#1: News from topic “Interoperability Profiles”?

- no inputs

Q#2: Holder-Binding for JSON-LD/BBS+: experiences?

- BFH investigates on that topic. BBS and BBS+ are the same. Are doing the Holder-Binding. The Papers discribing the cryptographic concepts seems to have missing part in the presentation. Maybe it is simple, but not clear now.
- Base Signatures Schemes basics are not approved yet; advanced cases even are «more in the air».
- Learning from DAA! Long story, many difficulties even with dedicated hardware.

Q#3: Revocation-check through verifier vs. non-revocation proof: Pros & Cons? Accumulator vs. StatusList?

- No production ready accumulator today
- Accumulators need a communication from holder with the issuer (to get delta)
- 3rd Method beside Accumulator and StatusList: Short living Issued «Validity Credentials» (trade-off: issuer knows about this issuance; can be «masquaraded»
- Qualified Signature Certificates: Revocation Lists are used accross EU, since a long time
- StatusList: No call home, simple Download possible (privacy exists)
- StatusList do easily scale and use it «offline» (in risk appetite…)
- How can all Credentials of a Holder be revoked at the same time?
- Malicious Issuers using StatusLists when in its hand

Q#4: Communication standards OID(4VC/4VP) vs. DIDcomm: Matching the criteria of maturity, operational aspects, ease of implementation…?

- DIDcomm and OID4VC: Thinkable Joining soon (working group IDunion)
- DIDcomm practical asynchronous communication; scalability not an issue anymore
- DIDcomm and OID4VC have different paradigmes.
- Depending on the Use Case! Not vs., its an OR.
- Adoption on Verifier-side OID4VP is easier. E-ID also would be the mean for authentication.

Scenario A: Pros, Cons, Uncertainties & Risks

Let's brainstorm again!

Privacy preservation* | *Security* | *Ease of Use* | *Readiness for the future* | *Interoperability & Standardization* | *Maturity* | *Operability & Integration

Pros

- a

Uncertainties

- a

Cons

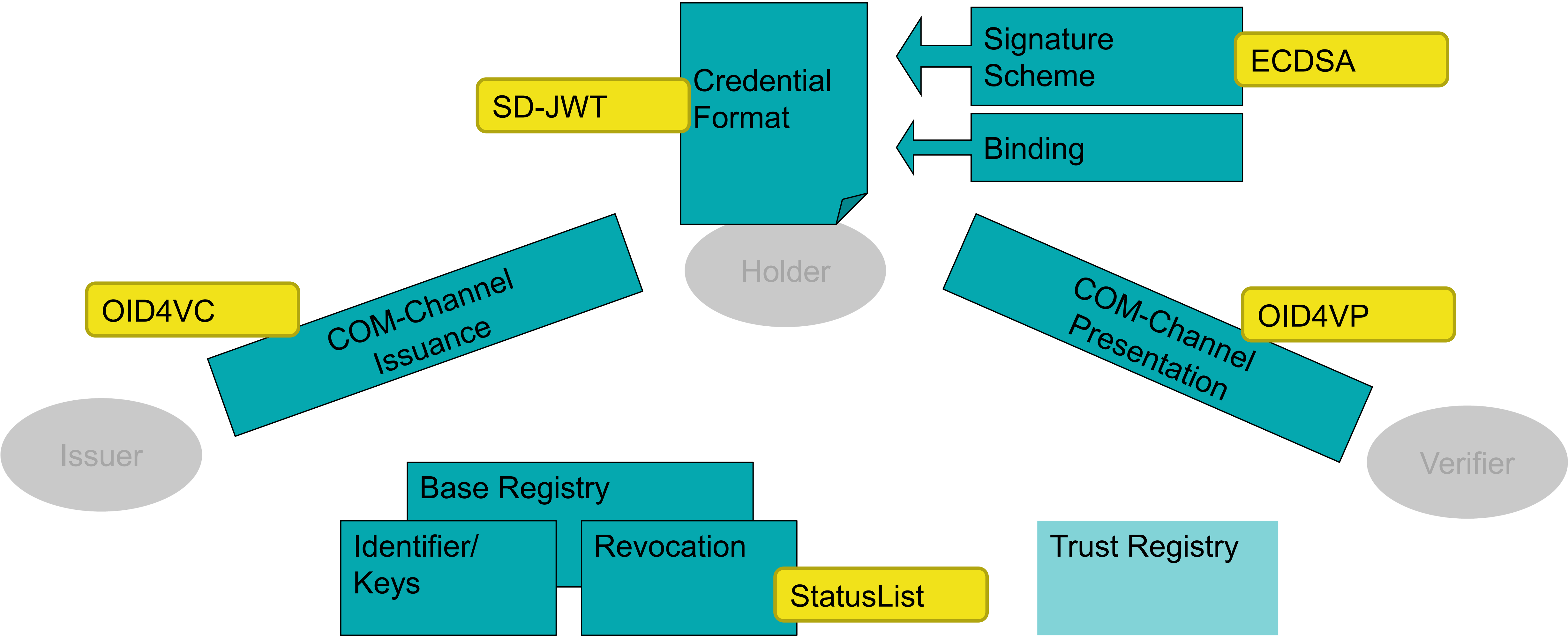
- a

Risks

- a

SCENARIO A

„Direct interoperability with the EU“



Scenario B: Pros, Cons, Uncertainties & Risks

Let's brainstorm again!

Privacy preservation* | *Security* | *Ease of Use* | *Readiness for the future* | *Interoperability & Standardization* | *Maturity* | *Operability & Integration

Pros

- a

Uncertainties

- a

Cons

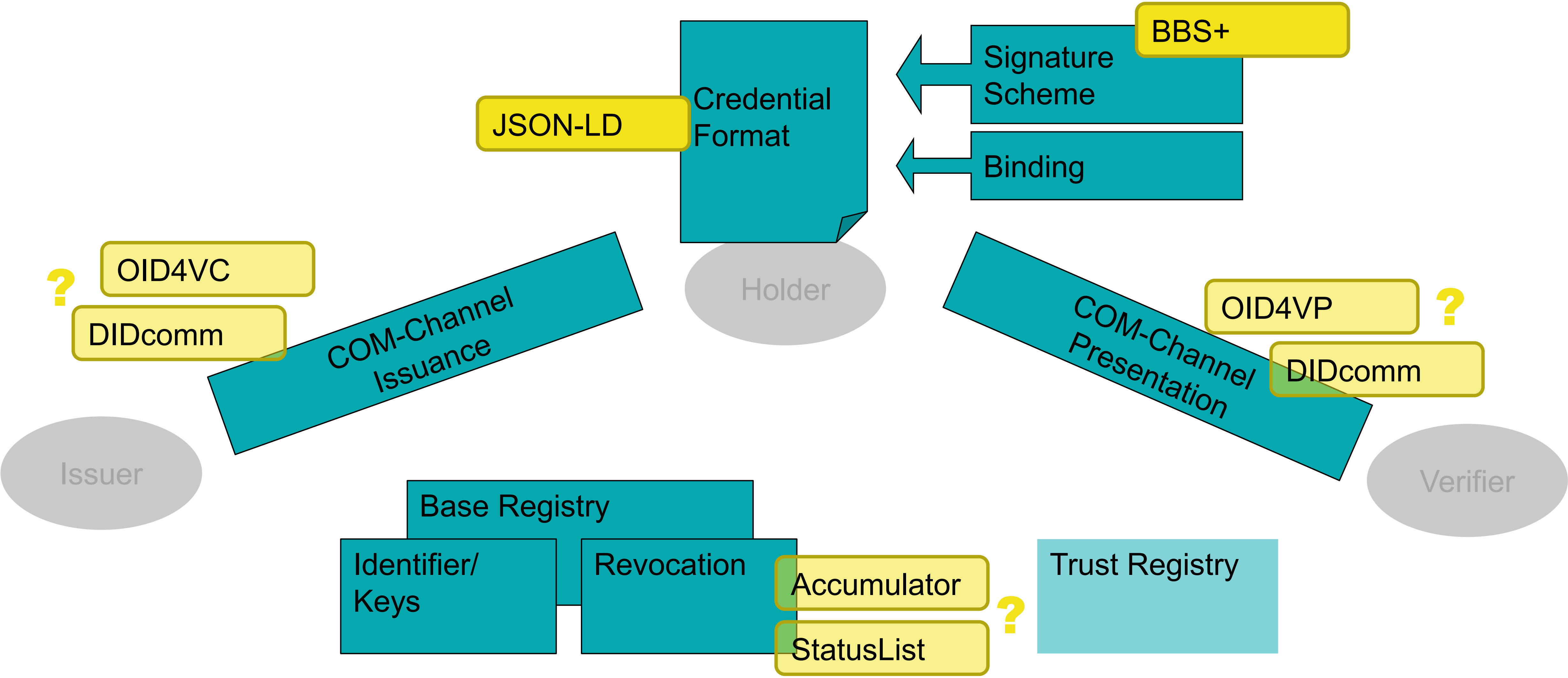
- a

Risks

- a

SCENARIO B

„Following a privacy path“



Discussion Paper «Tech-Proposal»: Planned next steps

- Finalization discussion paper E-ID Team
  and draft publication on GitHub: continuously from November 13, 2023
- Official publication of the discussion paper: December 1, 2023
- Informal public consultation process until December 31, 2023
- Analysis of feedbacks within E-ID Team
- Decision by the confederation early 2024

Any other inputs?

The TAC will most probably continue…

Please, 2 Minutes for our short survey:

- https://findmind.ch/c/HoHG-bR4e

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

Take your seat:
https://findmind.ch/c/ZYTa-thg3