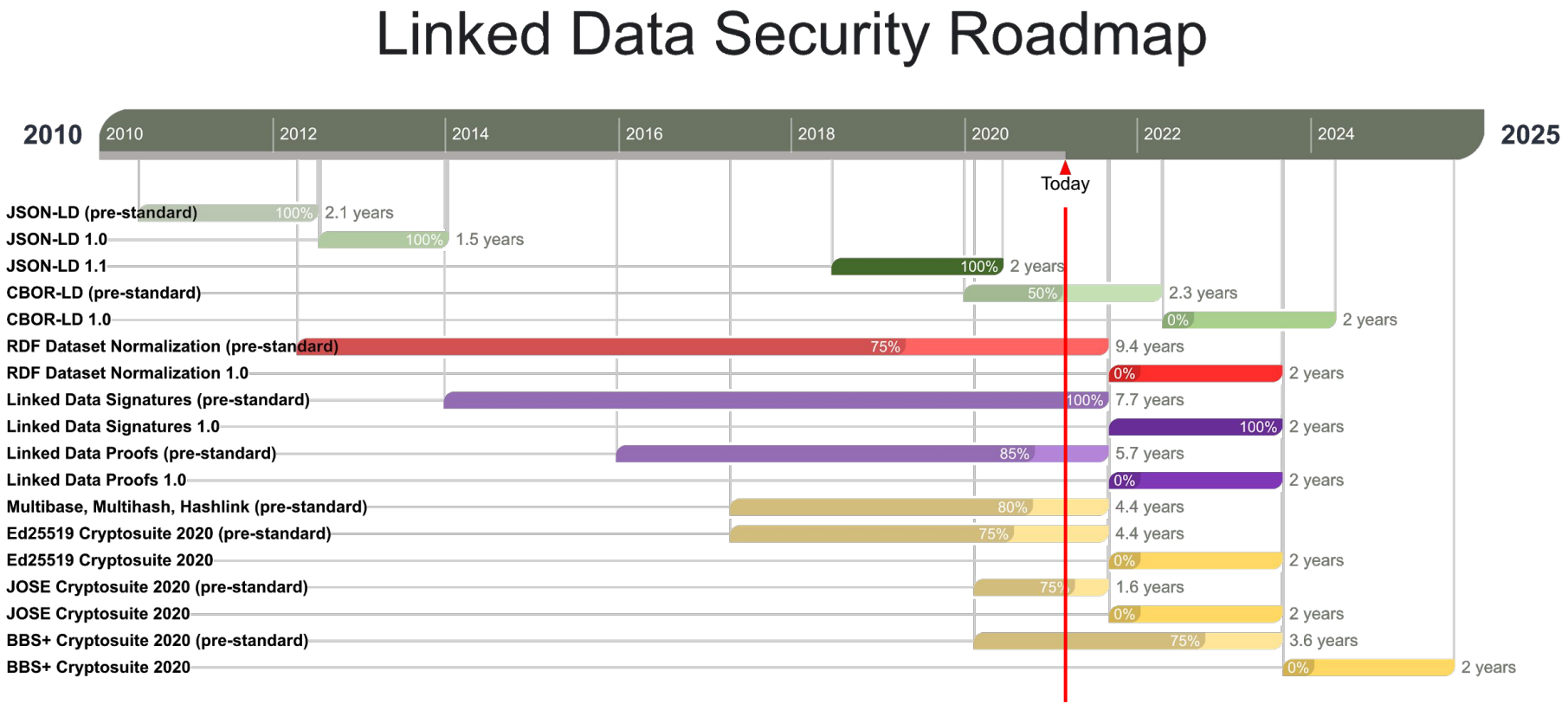
Linked Data Security

Adding digital signatures and digital proofs to existing linked data systems

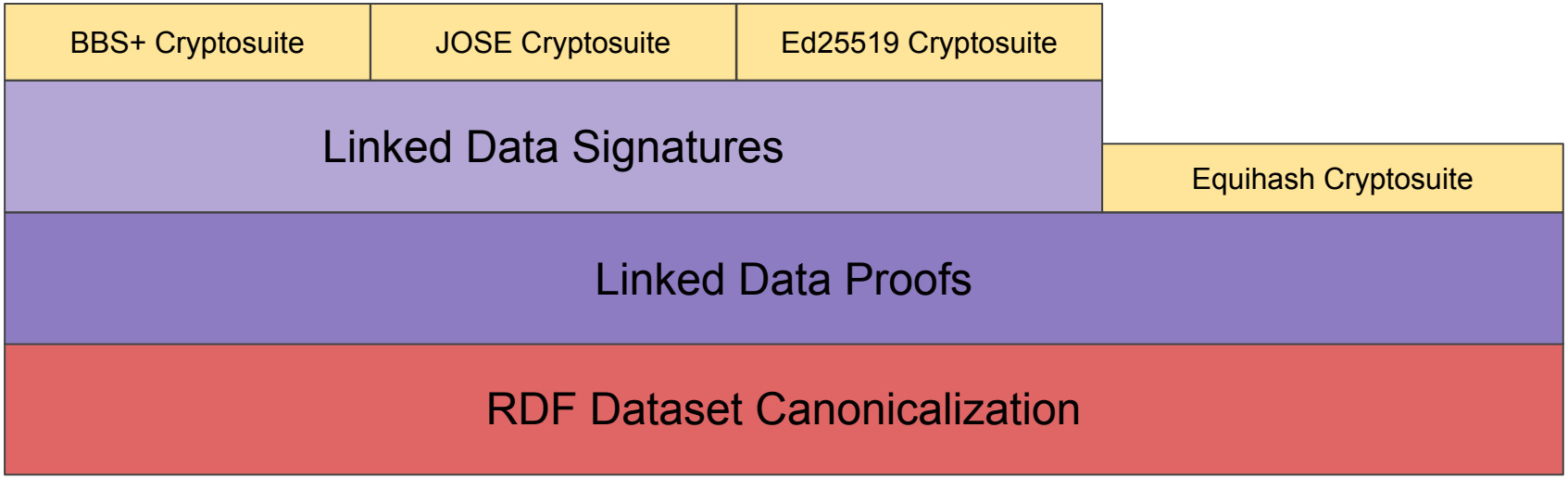
In this session, we will discuss:

- Why are we talking about this now?
- Canonicalization
- Digital Proofs
- Digital Signatures
- Next Steps

Why are we talking about this now?



The Linked Data Security Stack (excerpt)



What can we do with this stack?

RDF Dataset Canonicalization (c14n)

- Transforms input to deterministic output (useful for digital signatures)
- 2 mathematical proofs with peer review

RDF Dataset Canonicalization Example

```
{
  "@context": "http://schema.org/",
  "@type": "Person",
  "name": "Jane Doe",
  "jobTitle": "Professor",
  "telephone": "(425) 123-4567",
  "url": "http://www.janedoe.com"
}
```

```
{"@context":"http://schema.org/","@type
":"Person","name":"Jane Doe","jobTitle"
:"Professor","telephone":"(425) 123-456
7","url":"http://www.janedoe.com"}
```

```
_:c14n0 <http://schema.org/jobTitle> "Professor" .
_:c14n0 <http://schema.org/name> "Jane Doe" .
_:c14n0 <http://schema.org/telephone> "(425) 123-4567" .
_:c14n0 <http://schema.org/url> <http://www.janedoe.com> .
_:c14n0 <http://www.w3.org/1999/02/22-rdf-syntax-ns#type> <http://schema.org/Person> .
```

Linked Data Proofs

Used to express various types of digital proofs such as:

- Proof of Work
- Proof of Existence
- Proof of Elapsed Time
- Digital Signatures

LD Proof Example

```
"proof": {
  "type": "EquihashProofOfWork2018",
  "created": "2020-09-16T15:22:02Z",
  "domain": "blockchain.example",
  "proofPurpose": "capabilityInvocation",
  "proofValue": "z8je...0al9E",
  "nonce": "fdfe1d4d"
}
```

Linked Data Signatures

- A type of Linked Data Proof
- Used to express Digital Signatures

LD Signature Example

```
"proof": {
  "type": "Ed25519Signature2020",
  "created": "2021-03-16T15:22:02Z",
  "verificationMethod": "did:example:123#key1",
  "domain": "website.example",
  "nonce": "fjpqi43io"
  "proofPurpose": "authentication",
  "proofValue": "zj902k...lY7dhH",
}
```

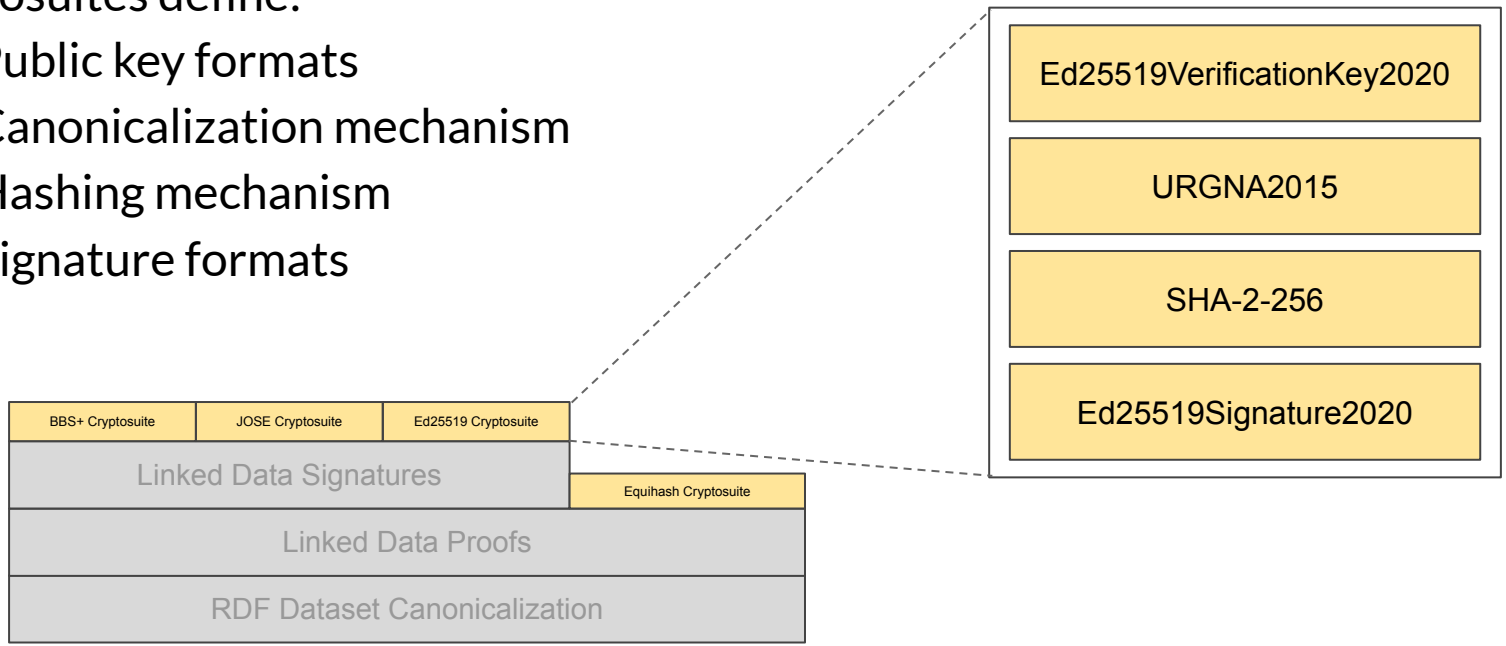
Linked Data Cryptosuites

- Provide approved / pre-packaged cryptography suites.
- Typically bundle Canonicalization algorithm, hashing algorithm, and signature algorithm

Linked Data Cryptosuite

Cryptosuites define:

- Public key formats
- Canonicalization mechanism
- Hashing mechanism
- Signature formats



Next Steps?

Proposed Linked Data Signatures Working Group Charter

DRAFT

This is a *draft* text, under development by the community. The W3C Advisory Committee has not yet been informed on the development this draft. The goal is to, eventually, submit this draft charter proposal to an official W3C AC review.

Any text rendered like this refers to content that must be finalized before the charter is sent to AC review, preferably before the advance notice on the charter is sent to the AC.

Any text rendered like this refers to content that must be updated when the final charter is published at the latest (e.g., adjusting hyperlinks).

This proposed charter is available on GitHub. Feel free to raise issues.

The **mission** of the Linked Data Signatures Working Group is to define a standard for *digital signatures* or a unique identification of RDF Datasets.

Start date	*[30 September 2021] (date of the "Call for Participation", when the charter is approved)*
End date	*[30 September 2023]* The duration of the WG must be decided.
Charter extension	See Change History. n/a.
Chairs	*[chair name] (affiliation)*
Team Contacts	Ivan Herman (0.1 FTE)
Meeting Schedule	**Teleconferences:** 1 hour calls to be held weekly; extra topic-specific calls may also be held. **Face-to-face:** we will meet during the W3C's annual Technical Plenary week; additional face-to-face meetings may be scheduled by consent of the participants, usually no more than 3 per year.

Discussion

- When should you use a Linked Data Signature instead of a JWT? What is the difference? [Benefits of JWTs] [Benefits of Linked Data Signatures]
- What's an example of an easy-to-understand signature suite? [Edwards 2020 Cryptosuite]
- When would you want to define a new one, and what are the key ingredients to that?
- What are work items or tools that could help in someone's journey?