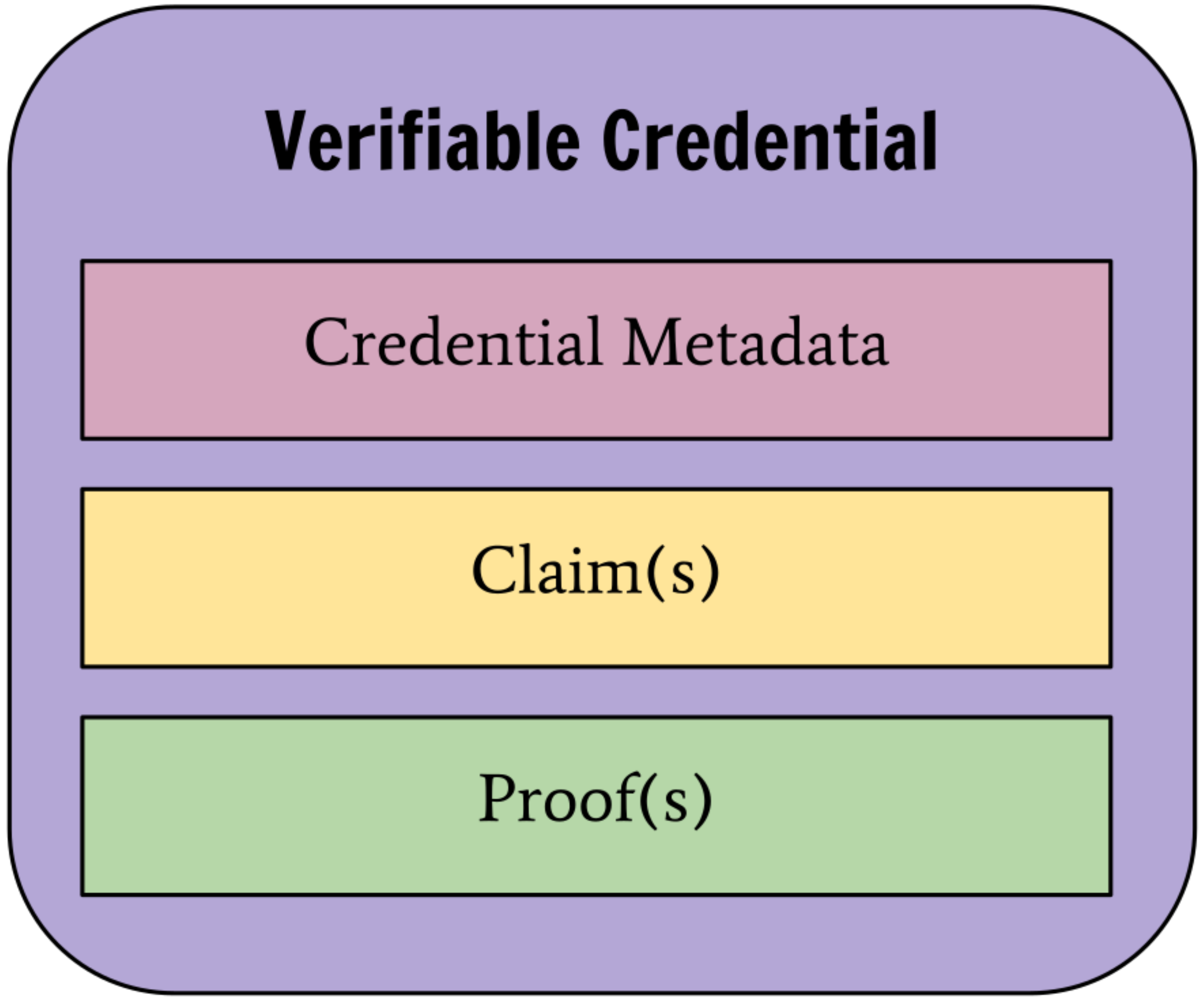
What is a (W3C) Verifiable Credential?

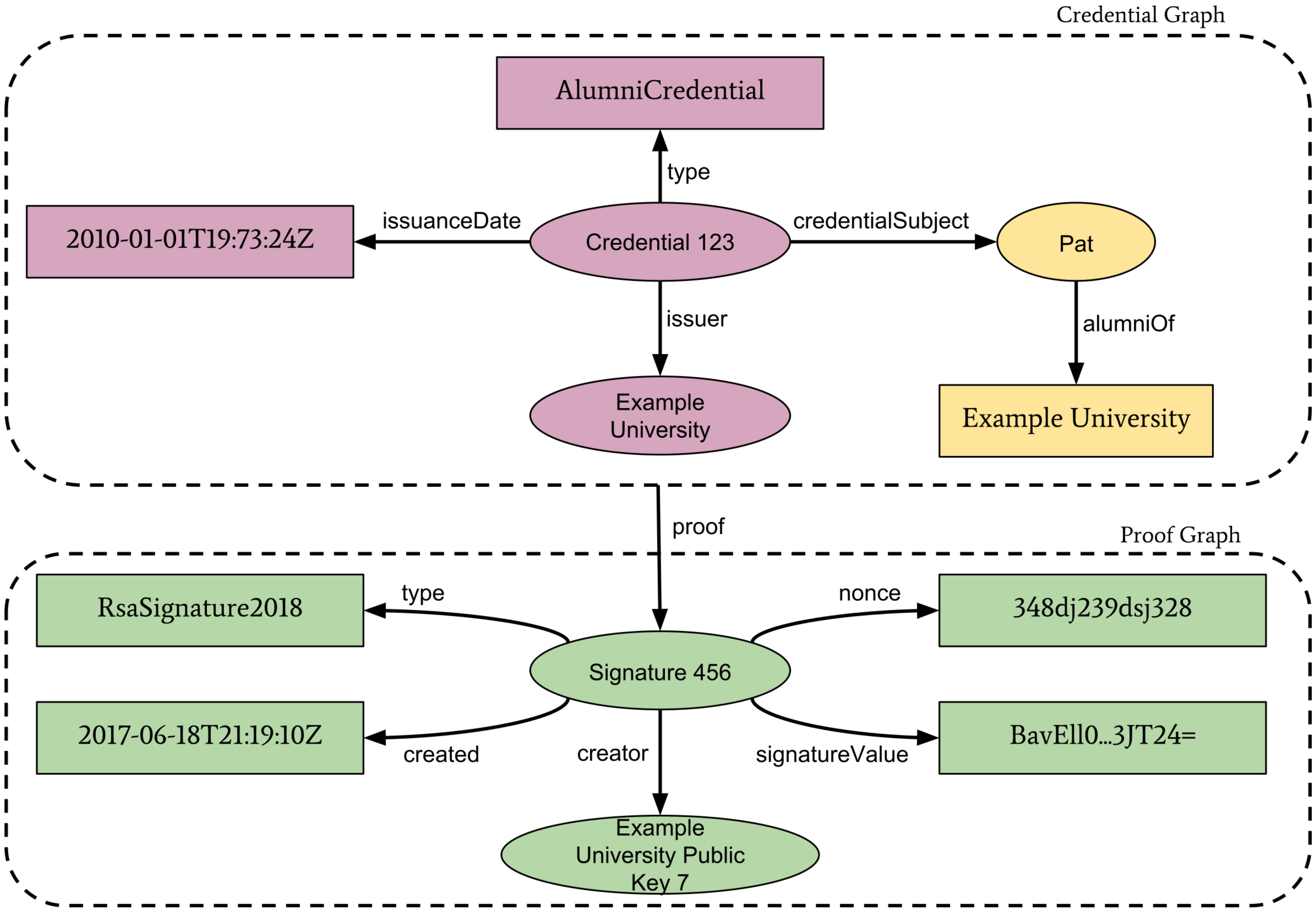
- A digital resource that can hold the same credential data as a physical credential (driving license, university diploma, medical information)
- The resource also includes cryptographic data to make the credential tamper evident and trustworthy (e.g., digital signature)
- It uses digital identifiers to refer to the ”subject”, the ”issuer”, or the “holder” of the credential

Simple View of a Verifiable Credential



- Metadata: contain expiry dates, representative image, identification of the issuer and the subject, etc.
- Proof(s): contain the cryptographic data for, e.g., signatures (keys, signature values, etc.)

Simple View of a Verifiable Credential



Representation of Verifiable Credentials

- The abstract model can be “expressed” in JSON, JSON-LD, CBOR,…
  - can then be encoded in, say, a QR code
- The cryptographic data can be expressed in various formats, e.g., JWT, JSON-LD Proofs and Signatures,…
- The standard does not specify the “higher level” functionalities, e.g., the behavior of specialized wallets
  - this is left to implementers and to market forces

The standard defines a *framework*

- The The Recommendation itself standardizes terms like "`issuanceDate`" or "`proof`"
- The final application defines the terms like "`alumniOf`" or "`AlumniCredential`"
  - there is a registry to refer to such application-dependent vocabularies
- *This extension mechanism is at the heart of Verifiable Credentials*

Some further points

- The extension model is applicable to the proof mechanism
  - new proof methods can be registered
- There is an extra layer to separate the “presentation” of (part of) the credential from the credentials themselves. This “presentation” can be checked separately via cryptographic means
  - e.g., *it is possible to provide a selective disclosure of the data*

Current status

- The specification has been a Web Standard for 2 years
- A discussion is starting for the renewal of the charter adding some new features
  - current ideas under discussion:
    - broader range of serializations
    - additional proof types for various serializations
    - formalize the registry mechanism to make it more precise