COSE Struct Choose your own adventure

One document or multiple documents

- One Document
  - Single document with everything current is considered a benefit.
  - Time to full standard is going to be slowed down
- Multiple documents
  - Base document can move to full standard much sooner
  - Easier to focus just on the question of countersignature support when moving to full standard
  - Still can reference as one STD number

- One document goto slide 3, multiple documents goto slide 5

Treatment of countersignature version 1

- Where should the countersignature v1 algorithm be placed?
- In the main text?
  - Easier to find?
- In an appendix?
  - Maps better to some that is deprecated than in the main text
- In RFC 8152
  - Document references the existence of the algorithm, points to where it is in RFC 8152 and discusses the fact that it is deprecated. (Could be in introduction or section on countersigning)
- Goto slide 4

New structure names?

- Do we keep the same structure name or should the name reflect the algorithm version?
- Is there any reason to have standalone tags for the old version. I cannot think of any given that it is deprecated.

- Goto Next presentation

Treatment of Countersign version 1

- Where should it go?
  - Main text of new document
  - Appendix of new document
  - Leave behind in RFC 8152
    - Reference the existence and discuss the deprecation and why

- Goto slide 4

New Countersign Algorithm

Body structure and build of Countersign TBS

[Protected Attributes,

Unprotected Attributes,

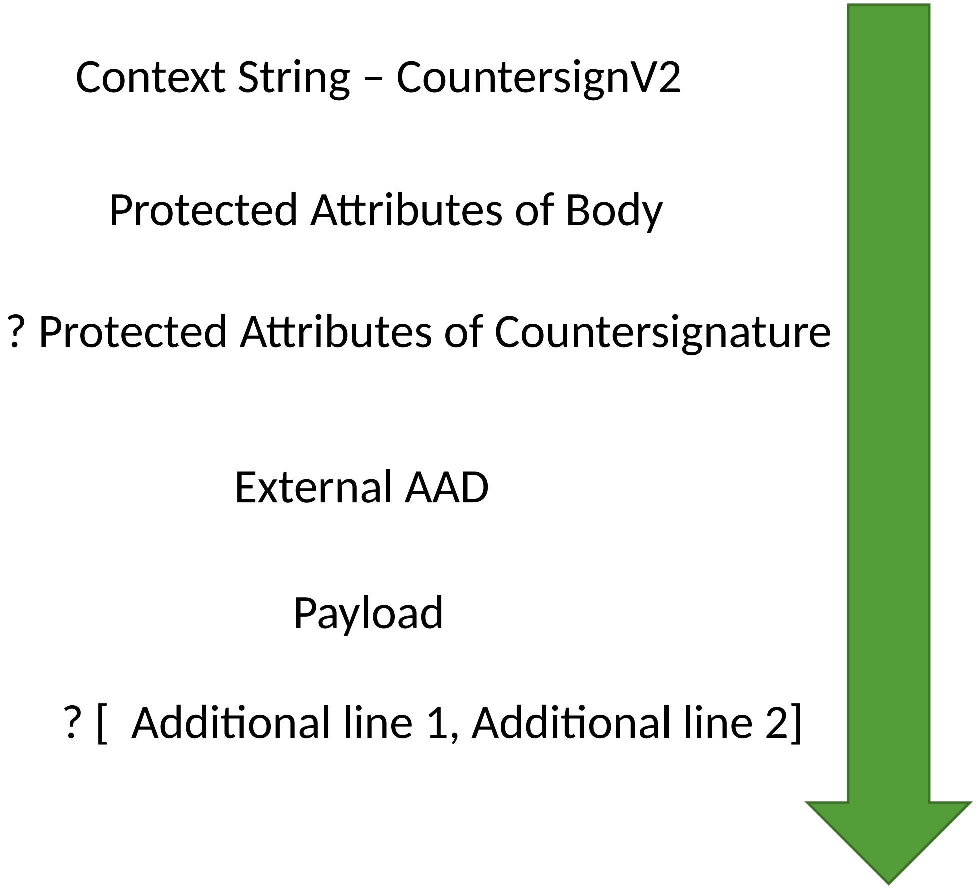
Payload

Additional Line 1

Additional Line 2

6.TBD(Additional Line 3)

]



Context String – CountersignV2

Protected Attributes of Body

? Protected Attributes of Countersignature

External AAD

Payload

? [Additional line 1, Additional line 2]

Tag 6.TBD – Ignore this tag

- Tag is defined as
  - Only apply this to a bstr. Behavior is not really defined anyplace else.
  - Parser – mark where this tag occurs in the output
  - Tag makes no changes to the behavior of the wrapped object
  - If tag exists then the countersignature algorithm ignores the tagged field.

- Do we define the tag even though we have no use for it and don't for see one coming soon
  - Carsten "Tags are cheap."
  - Tag range to ask for?