‘Simple’ is a feature.
What’s new in -06?

Format change:
- Added hash of Issuer-signed part and Disclosures in KB-JWT

Clarifications and restructuring:
- Restructured sections around data formats and Example 1
- More precise wording around storing artifacts with sensitive data
- Ensured claims that control validity are checked after decoding payload
- The claim name _sd or ... must not be used in a disclosure

Other changes:
- Fixed minor issues in some examples
- Added IANA media type registration request for the JSON Serialization
- Added JWT claims registration requests to IANA
- Updated JSON Serialization to remove the kb_jwt member and allow for the disclosures to be conveyed elsewhere
- Expanded the Enveloping SD-JWTs section to also discuss enveloping JSON serialized SD-JWTs
Hash in KB-JWT
Issuer

Issuance

End-User (Holder)

Presentation

Verifier

**SD-JWT**

plain-text claims + hashed Disclosures

✓ signed by Issuer

**Disclosures**

salt + claim name + claim value

**Selected Disclosures**

salt + claim name + claim value

Holder-Binding JWT

nonce audience etc.

✓ signed by Holder

Holder's public key
Issuer

Issuance

End-User (Holder)

Presentation

Verifier

SD-JWT
plain-text claims + hashed Disclosures

✓ signed by Issuer

Disclosures
salt + claim name + claim value

+ hashed Disclosures

✓ signed by Issuer

Selected Disclosures
salt + claim name + claim value

Nonce
Audience
_sd_hash
etc.

New: _sd_hash, a hash over the Issuer-signed JWT and the selected Disclosures (REQUIRED)

Holder-Binding JWT

nonce

.sd_hash

signed by Holder

holder's public key

✓ signed by Issuer
Key-Binding JWT Body:

```json
{
  "nonce": "1234567890",
  "aud": "https://verifier.example.org",
  "iat": 169807790,
  "_sd_hash": "34t8vCC_c_VLnnOd4twh4vBErS19zK0wam6ihT_U"
}
```
Next Steps
Next Steps

- Neil’s comments on cryptography — will address (#359, #360, TBD)
- More issues on issue tracker but nothing major
- Approaching Working Group Last Call?
  - Format (mostly) stable for some time now
  - No expected breaking changes
  - At least nine implementations