DID Doc/metadata/etc. Properties

Please don't bikeshed names of these properties! Goal is to capture the potential new use cases and requirements, not to specify them or require their use.

These were discussed (briefly) at W3C DID WG F2F Amsterdam 31 Jan 2020

1. UNNAMED #1: A timestamp at which a DID was resolved
    a. For: cache invalidation
    b. From: the resolution process
    c. Ganesh
2. UNNAMED #2: A self-attested timestamp at which the DID controller created it
    a. For: Contributes to validation of temporal flow
    b. From: DID controller (software agent)
    c. Ganesh and Joe
3. UNNAMED #3: Document serialization format (representation)
    a. For: parser/code dispatch—programmatically recognizing the type of representation
    b. From: output of resolution
    c. Justin
4. UNNAMED #4:Capability invocation
    a. For: key material used to invoke an object capability, i.e., the public key associated with the private key that an entity uses to invoke an object capability. For example, if a car key had a fingerprint reader before it could be used.
    b. From: DID Controller (some entity)
    c. Manu
5. UNNAMED #5: Capability delegation
    a. For: key material used to delegate a capability
    b. From: DID Controller (some entity)
    c. Manu

    d. CLARIFICATION TO #4-#5: These are both assertions by the DID controller about which verification methods are authorized to invoke or delegate a capability on behalf of the DID subject
6. UNNAMED #6: Controller Version Identifier of a DID document
    a. For: A version identifier for relying parties to know that a DID document changed. It may be different that a date provided by the resolution process.
    b. From: DID Controller (software agent, but not a blockchain)
    c. Christopher Allen
7. UNNAMED #7: Redacted Property Value or Flag
    a. For: Allows a controlled to redact information in a DID document
    b. From: DID Controller (person or agent)
    c. Christopher Allen
8. UNNAMED #8: Anti-Sybil / Reputation Information
    a. For: Allows the verifier to evaluate trust based on various anti-sybil mechanisms
    b. From: the Verified Data Registry
    c. Christopher Allen
9. UNNAMED #9: Retired Keys
    a. For: Key validation, i.e., for checking proofs from older keys that should not be considered invalid, but are not the current keys
    b. From: DID controller (any)
    c. Joe
10. UNNAMED #10: DID Created (Timestamp)
    a. For: The timestamp at which the Verifiable Data Registry finished the Create Operation. Finished is defined by when the DID can be resolved with its new changes applied.
    b. From: Verifiable Data Registry
    c. Markus and Ganesh
11. UNNAMED #11: DID Updated (Timestamp)
    a. For: The timestamp at which the Verifiable Data Registry finished the Update Operation. Finished is defined by when the

DID can be resolved with its new changes applied.
    b. From: Verifiable Data Registry
    c. Markus and Ganesh
12. UNNAMED #12: DID Deactivated (Timestamp)
    a. For: The timestamp at which the Verifiable Data Registry finished the Deactivate Operation. Finished is defined by when the DID can be resolved with its new changes applied.
    b. From: Verifiable data registry
    c. Markus and Ganesh
13. UNNAMED #13: Version Identifier of DID Document
    a. For: Cache invalidation, contribute to verification
    b. From: verifiable data registry
    c. Markus
14. UNNAMED #14: DID Document Cached Flag
    a. For: Making trust decisions about the DID document
    b. From: Resolver
    c. Markus
15. UNNAMED #15: Resolver Method Spec Version Identifier
    a. For: Security—knowing which version has been implemented
    b. From: Resolver
    c. Oliver
16. UNNAMED #16: Resolver Method Code Version Identifier
    a. For: Security—knowing which version has been implemented
    b. From: Resolver
    c. Oliver
17. UNNAMED #17: Resolver Engine Code Version Identifier
    a. For: Security—knowing which version has been implemented
    b. From: Resolver
    c. Oliver
18. UNNAMED #18: Verifiable Proof of Control Authority (Full Proof)
    a. For: cryptographically establishing control authority over the DID. It means the root control over the DID, from which all other forms of control derive. It can be attenuated from there. It’s a

proof that proves the set of root keys that have control authority for a DID. It is proof of ultimate control authority. This also gives you any keys that have been retired.
    b. From: DID Controller (it is a cryptographic proof, could come from an agent)
    c. Sam Smith
19. UNNAMED #19: Verifiable Proof of Control Authority (Hash and a Reference)
    a. For: Same as above
    b. For: Same as above
    c. Sam Smith
20. UNNAMED #20: Requested Content Type
    a. For: Requester expressing to a DID resolver for the representation type of a DID document requested
    b. From: DID client or requester
    c. Tobias
21. UNNAMED #21: Assertion (incomplete name)
    a. For: a DID controller to express verification methods that are authorized to assert things on behalf of the DID subject
    b. From: DID controller
    c. Tobias
22. UNNAMED #22: Controller
    a. For: For expressing the entity that is in control of the DID. This is an indirection to another entity, which is what makes it different from Verifiable Proof of Control Authority.
    b. From: DID controller
    c. Manu
23. UNNAMED #23: Key Agreement Key
    a. For: establishing a key for the purposes of establishing another key for encrypted communication
    b. From: DID controller
    c. Manu
24. UNNAMED #24: DID URL method VDR identifier

    a. For: identifying VDR
    b. From: DID controller
    c. Joe
25. UNNAMED #25: Target Verifiable Data Registry Identifier
    a. For: Identifying the VDR intended for the registration
    b. From: DID Controller
    c. Christopher Allen
26. UNNAMED #26: Actual Verifiable Data Registry Identifier
    a. For: Verifying the VDR
    b. From: Resolver
    c. Christopher Allen

The following did not have group discussion at F2F

27. UNNAMED #27: Arbitrary claims about the DID subject (phone number, country, etc.)
    a. For: Making trust decisions about the DID subject from the DID document alone
    b. From: DID controller
    c. Markus Sabadello
28. UNNAMED #28: Optional multisig flag on keys “multisig list”, “singlesig’ “multisig aggregated”
    a. For: as we move to a multisig world, some signatures types (Schnoor) the multisig can look like single sig (and thus are not-accountable/aggregate). In same cases the controller may want to inform the verifier it explicitly is multisig.
    b. From: DID controller
    c. Christopher Allen
29. UNNAMED #29: Select * from DID Core JSON-LD Context
    a. For: Defining Properties of a DID Subject
    b. From: DID Controller
    c. Posted by: Orie Steele
30. UNNAMED #30: Select * from HTTP Headers

    a. For: Defining Properties of a DID Document Representation
    b. From: DID Method Resolver
    c. Posted by: Orie Steele
31. UNNAMED #31: <Property description>
    a. For:
    b. From:
    c. Posted by: