Herd Privacy and DIDs

Issues #199, #373, #539; PRs #457, #460, #480

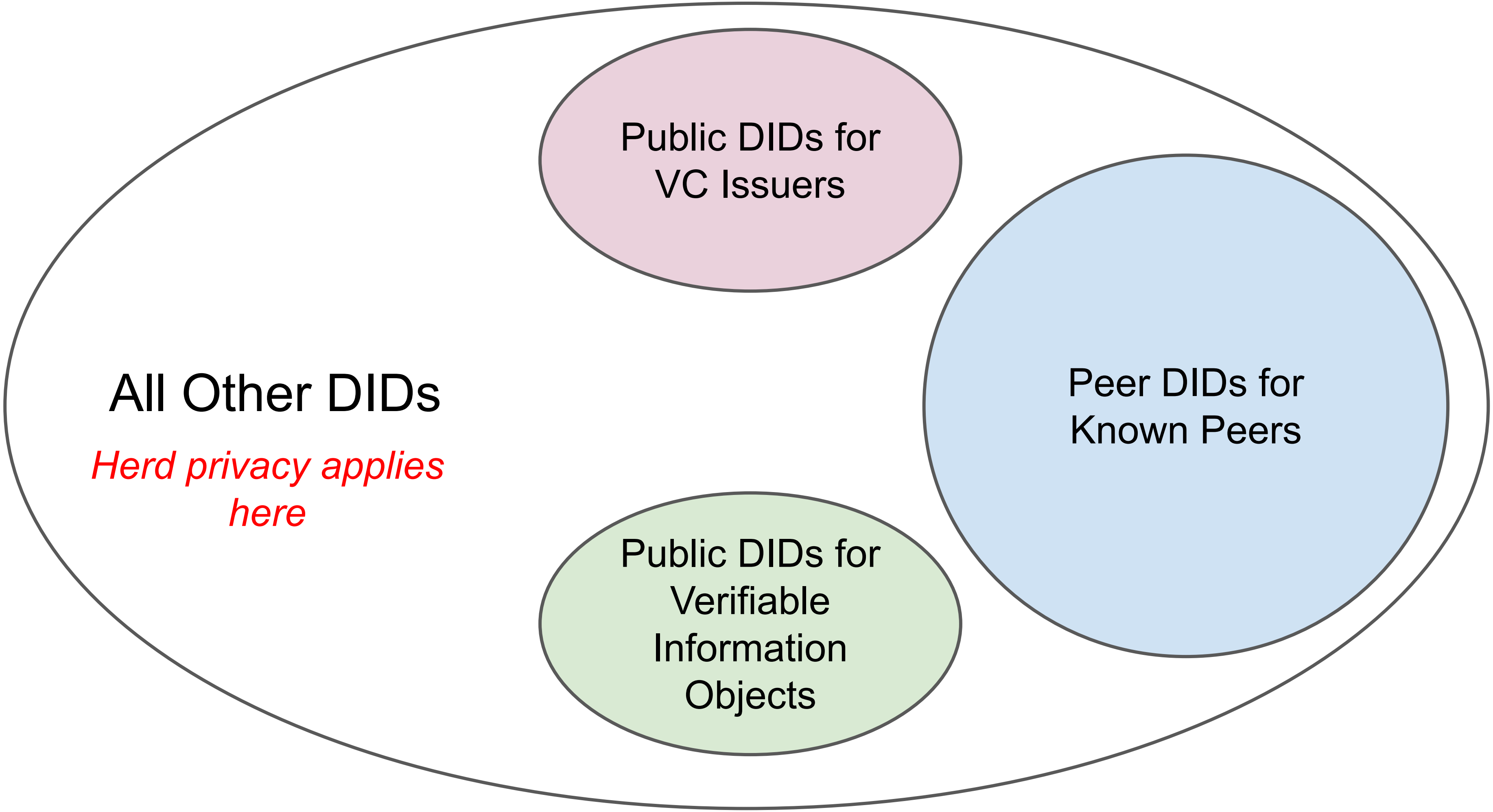
W3C DID Working Group Discussion Document
2020-01-14

10.5 Herd Privacy

When a DID subject is indistinguishable from others in the herd, privacy is available. When the act of engaging privately with another party is by itself a recognizable flag, privacy is greatly diminished. DIDs and DID methods need to work to improve herd privacy, particularly for those who legitimately need it most. Choose technologies and human interfaces that default to preserving anonymity and pseudonymity. To reduce digital fingerprints, share common settings across requesting party implementations, keep negotiated options to a minimum on wire protocols, use encrypted transport layers, and pad messages to standard lengths.

Herd privacy is a valuable feature for many DIDs. However, it **cannot** apply to all DIDs. Forcing herd privacy requirements to apply all DIDs is counter-productive.

A fundamental design principle for DIDs is that they can serve as **contextual identifiers**. Some contexts cannot use herd privacy.


Public DIDs for VC Issuers
All Other DIDs
Herd privacy applies here
Peer DIDs for Known Peers
Public DIDs for Verifiable Information Objects

Contexts in which herd privacy does not apply

1. Public DIDs for VC Issuers
   - Companies, universities, NGOs, governments
   - World-verifiable correlation is a **requirement**
2. Public DIDs for Verifiable Information Objects
   - Schemas, revocation registries, governance frameworks, etc.
   - World-verifiable correlation is a **requirement**
3. Peer DIDs for Known Peers
   - There is no “herd”—the peers are known to each other

Proposal

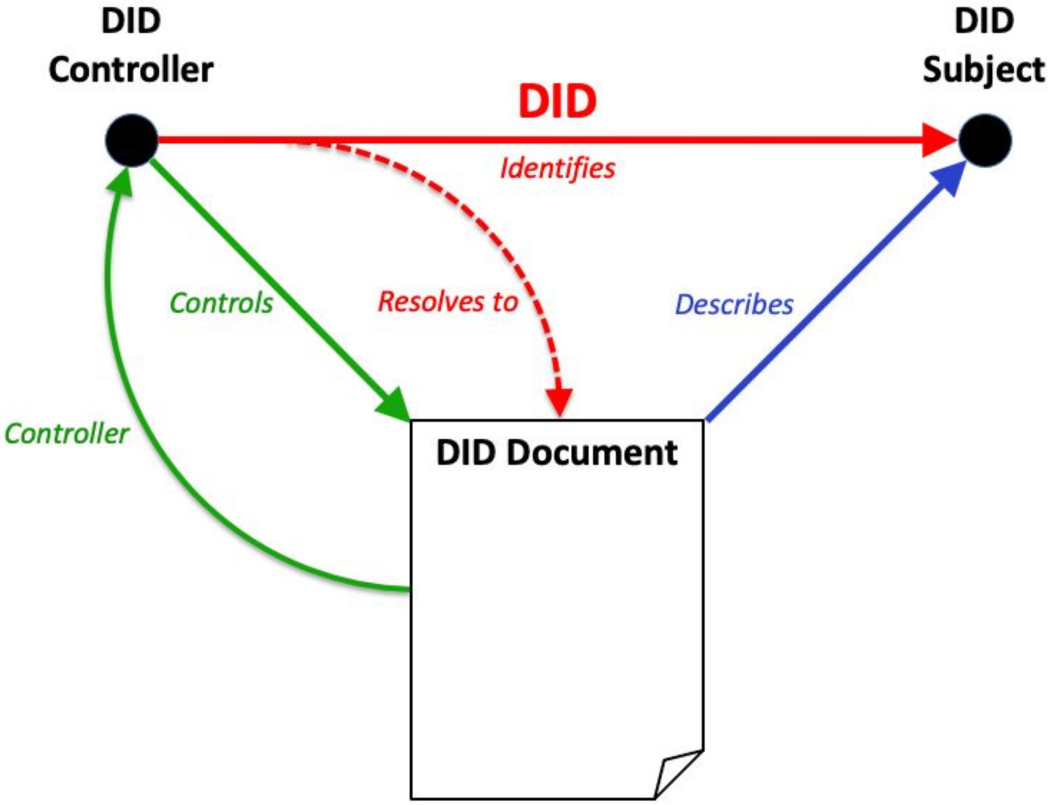
The DID Core Specification shall include editorial text specifying that:

1. Herd privacy is valuable for some but not all uses of DIDs.
2. Herd privacy is strongly recommended for DIDs identifying individuals in contexts where they wish to be anonymous or pseudonymous.
3. Herd privacy does not apply in contexts when DIDs identify:
    a. Entities that are already known to each other.
    b. Entities that must be well-known in order to achieve trust.

What Does a DID Identify?

Issues #199, #373; PRs #457, #460

Does anyone disagree with this diagram?



Proposals

1. The DID Core Specification shall include editorial text specifying that DIDs are URIs and identify resources as defined in RFC 3986.
2. The DID Core Specification Appendices shall clarify that a DID identifies a DID subject and resolves to a DID document. It does NOT identify the DID document as a separate resource. The DID document is an artifact of DID resolution that serves as a descriptor of the DID subject and potentially of related resources (e.g., AlsoKnownAs).