DNSSD Privacy

Stuart Cheshire
Presenting on behalf of Christian Huitema

102nd IETF, Montréal, July 2018

Drafts

Privacy Extensions for DNS-SD	draft-ietf-dnssd-privacy-04
Device Pairing Using Short Authentication Strings	draft-ietf-dnssd-pairing-04
Device Pairing Design Issues	draft-ietf-dnssd-pairing-info-01
DNS-SD Privacy and Security Requirements	draft-huitema-dnssd-prireq-00
DNS-SD Privacy Scaling Tradeoffs	draft-huitema-dnssd-privacyscaling-01

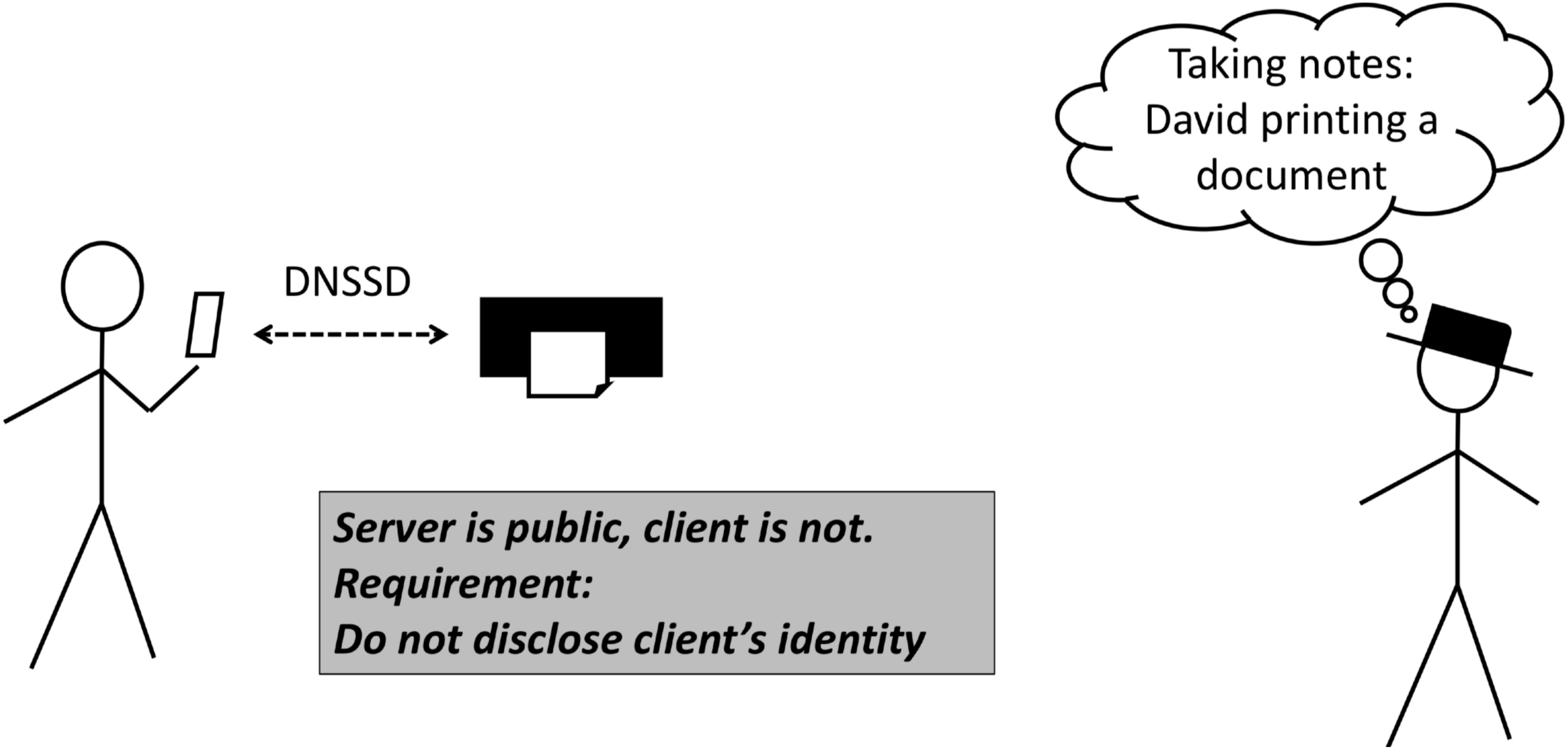
Initial Solution

- Drafts by Christian Huitema and Daniel Kaiser
- Symmetric key solution with pairing
- Scalability issues

Solution Requirements

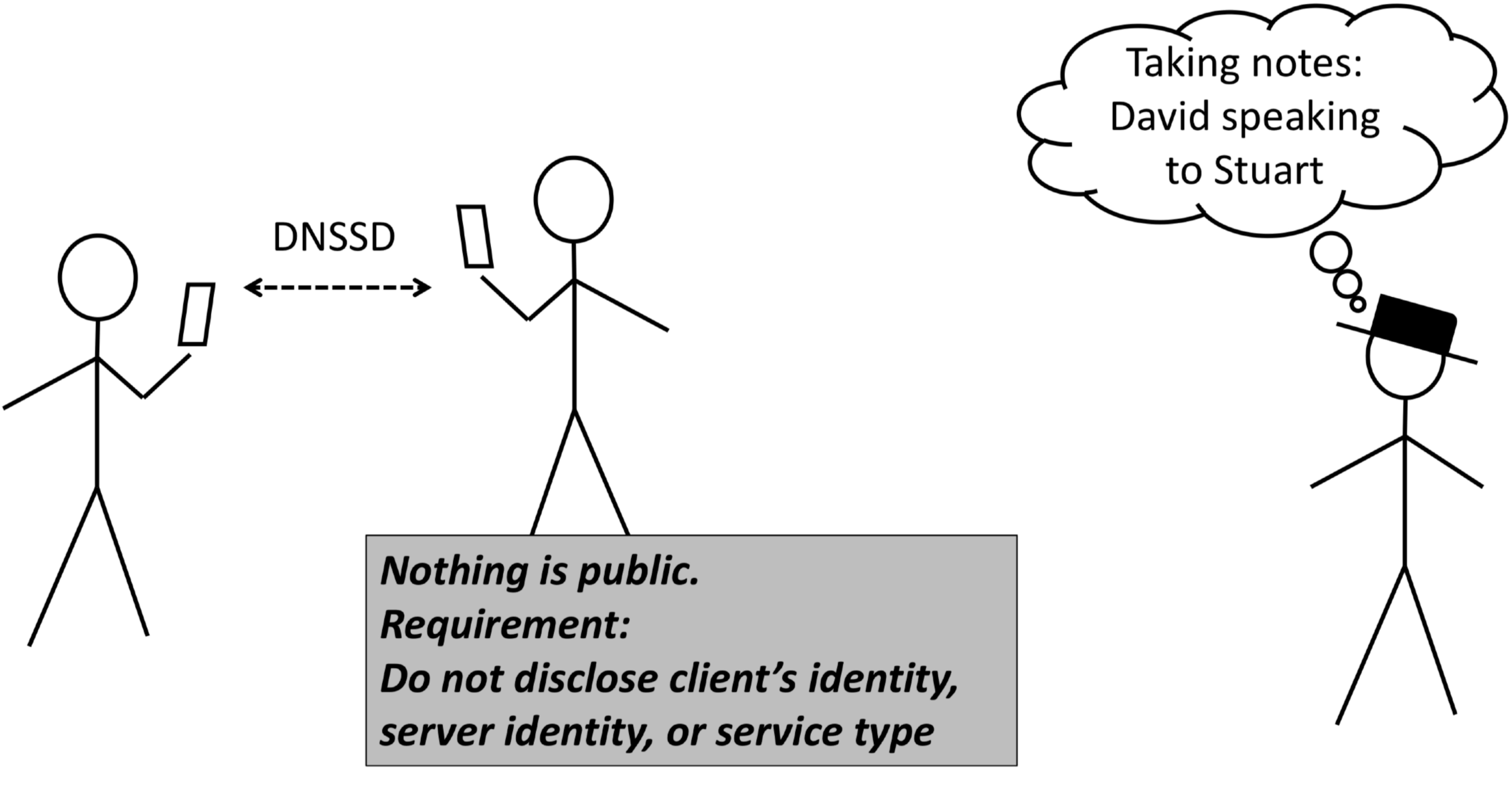
- New draft by Christian Huitema
  draft-huitema-dnssd-prireq
- Discusses discovery scenarios, privacy considerations, and requirements

Scenario #1



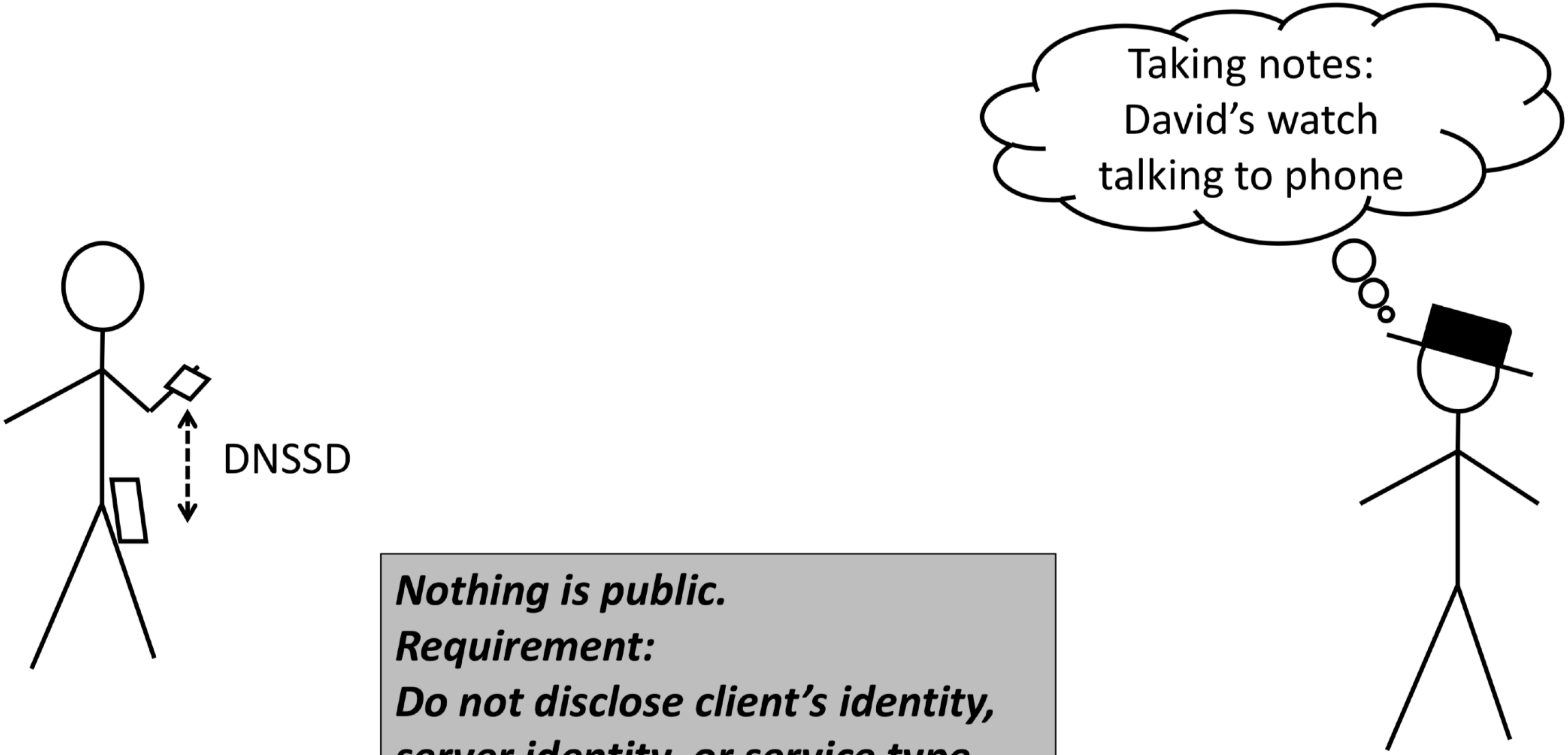
Server is public, client is not.
Requirement:
Do not disclose client's identity

Scenario #2



Nothing is public.
Requirement:
Do not disclose client’s identity, server identity, or service type

Scenario #3



Nothing is public.
Requirement:
Do not disclose client's identity, server identity, or service type

Discovery Requirements

Open issue: What requirements are mandatory for each scenario?

- Confidentiality
- Authenticity, integrity, and freshness
- Resistance to dictionary attacks
- Resistance to DoS attacks
- Resistance to sender impersonation
- Sender deniability

Three Discovery Variants

(At least) three variants:

- Shared symmetric key: draft-ietf-dnssd-privacy-04
- Shared public key: volunteers?
- Group key: volunteers?

Scaling considerations are critical