draft-huitema-dnssd-privacy

DNS-SD Privacy Extensions

Christian Huitema, Daniel Kaiser

July 20, 2016

Published Resource Records

```
 _presence._tcp.local:  type PTR,
alice@Alice's Notebook._presence._tcp.local
```

Published Resource Records

```
 _presence._tcp.local:  type PTR,
alice@Alice's Notebook._presence._tcp.local
```

```
 alice@Alice's Notebook._presence._tcp.local:
type SRV, port 5298,
target Alice's Notebook.local
```

Published Resource Records

```
 _presence._tcp.local:  type PTR,
alice@Alice's Notebook._presence._tcp.local
```

```
 alice@Alice's Notebook._presence._tcp.local:
type SRV, port 5298,
target Alice's Notebook.local
```

```
 alice@Alice's Notebook._presence._tcp.local:
type TXT,
vc=!  ver=2.10.6 node=libpurple
port.p2pj=5298 txtvers=1
status=gaming
last=Wonderland
1st=Alice
```

Published Resource Records

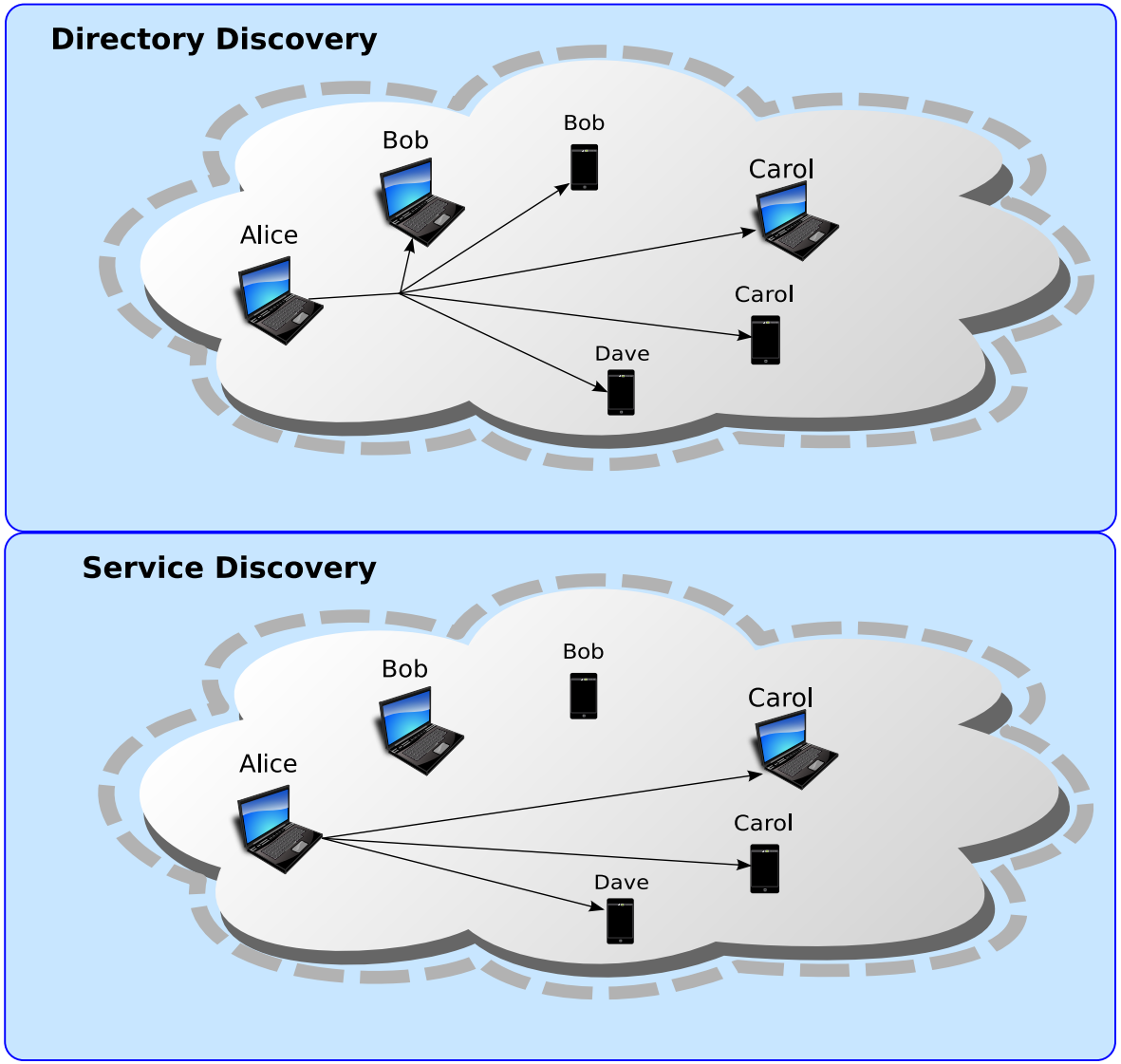
```
 _presence._tcp.local:  type PTR,
alice@Alice's Notebook._presence._tcp.local
```

```
 alice@Alice's Notebook._presence._tcp.local:
type SRV, port 5298,
target Alice's Notebook.local
```

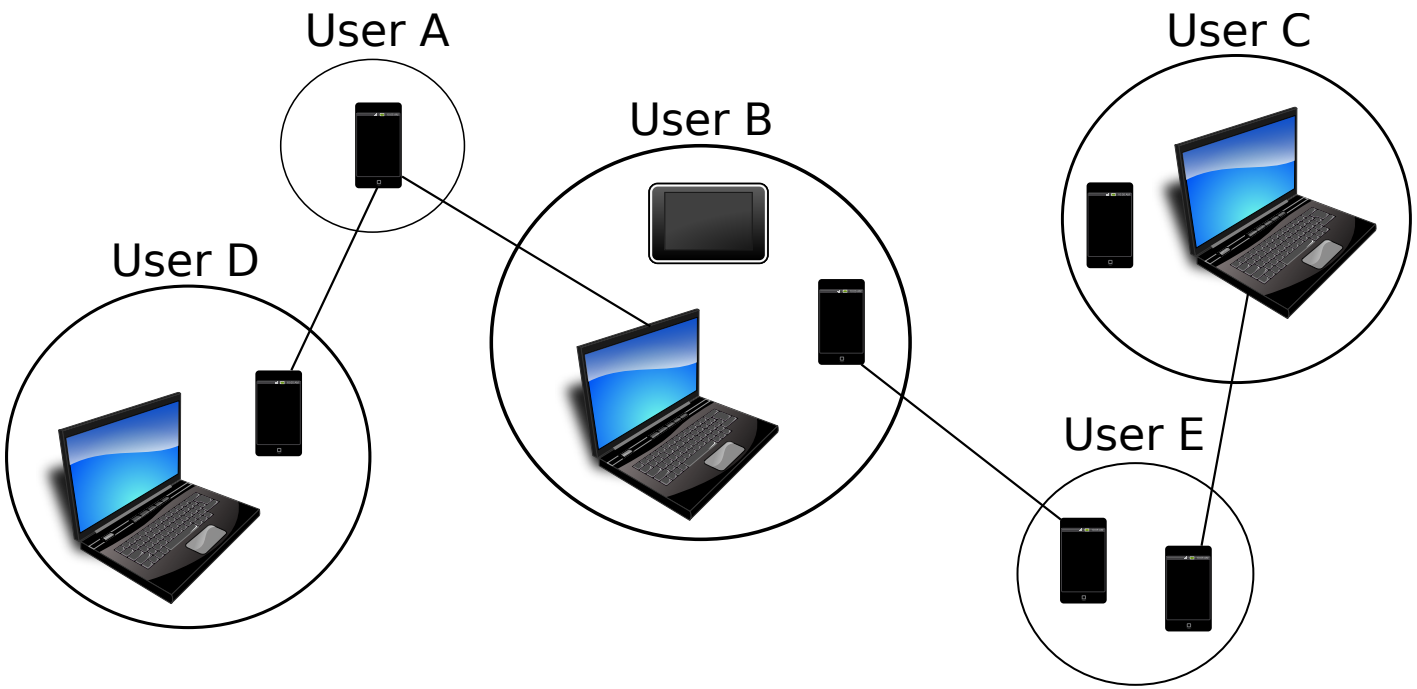
```
 alice@Alice's Notebook._presence._tcp.local:
type TXT,
vc=!  ver=2.10.6 node=libpurple
port.p2pj=5298 txtvers=1
status=gaming
last=Wonderland
1st=Alice
```

```
 Alice's Notebook.local:  type A, addr 134.34.10.36
```

Two-stage Approach



Pairing



Obfuscated Instance Name

Algorithm 1: Create a multi hint _psds instance.

Data: secret[ ]
Result: obfuscated_name[ ]

```
1 seed := 4 bytes rounded timestamp;
2 for i=0; i < ⌈m/10⌉; i := i+1 do
3 |   obfuscated_name[i] := BASE64(seed);
4 end
5 for i=0; i < m; i := i+1 do
6 |   long_hash := HASH(seed | secret[i]);
7 |   instance_hash := first 4 bytes of long_hash;
8 |   obfuscated_name[⌊i/10⌋] := obfuscated_name[⌊i/10⌋] |
  |   BASE64(instance_hash);
9 end
```

Two Stage Summary

Private Directory Discovery

- use obfuscated host name
- use encoded instance name
- only paired peers can identify instances

Actual Service Discovery

- only via PSDS
- use DNS-SD > TLS (DH-PSK)

Conclusion

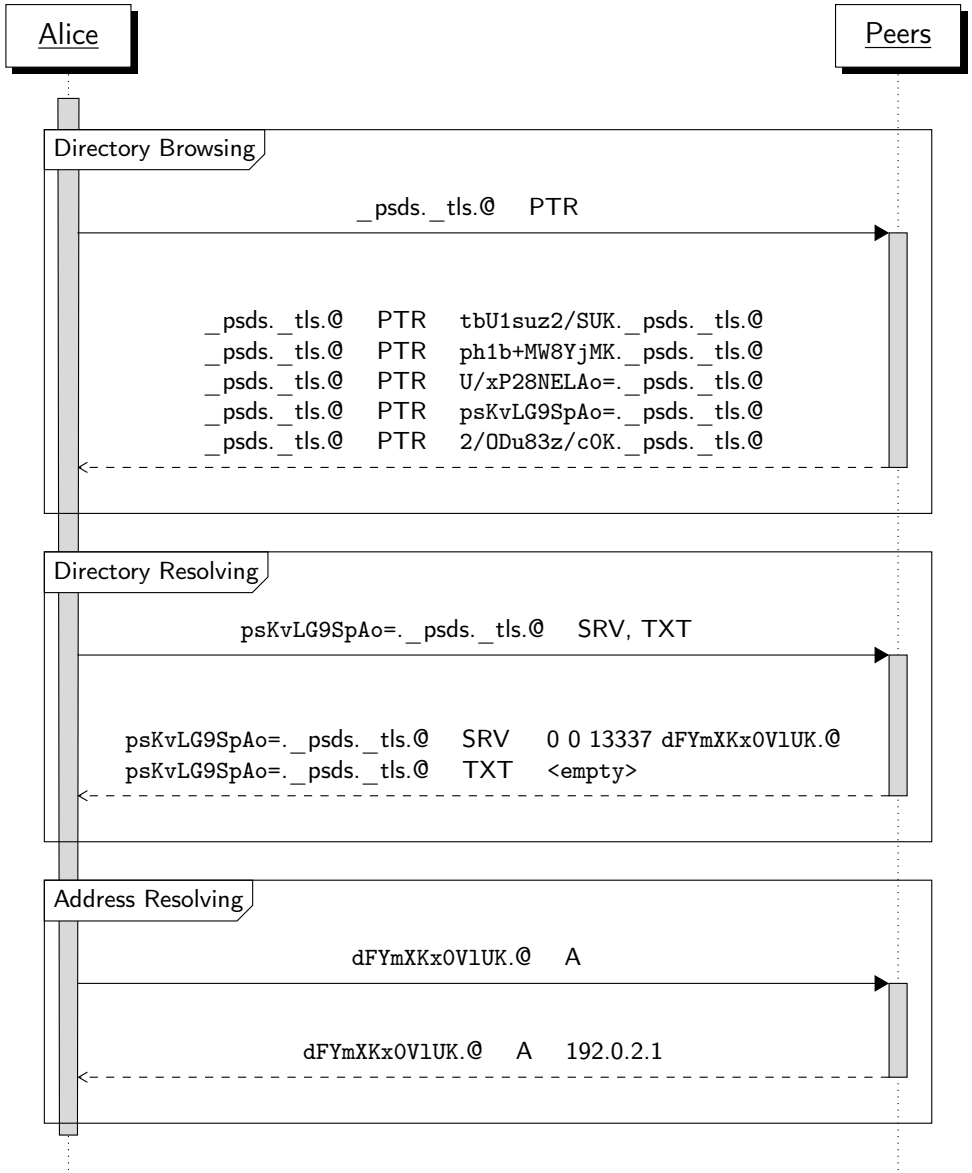
Should we adopt this draft?

- preserves privacy
- efficient
- reduces visual clutter
- offers services selectively

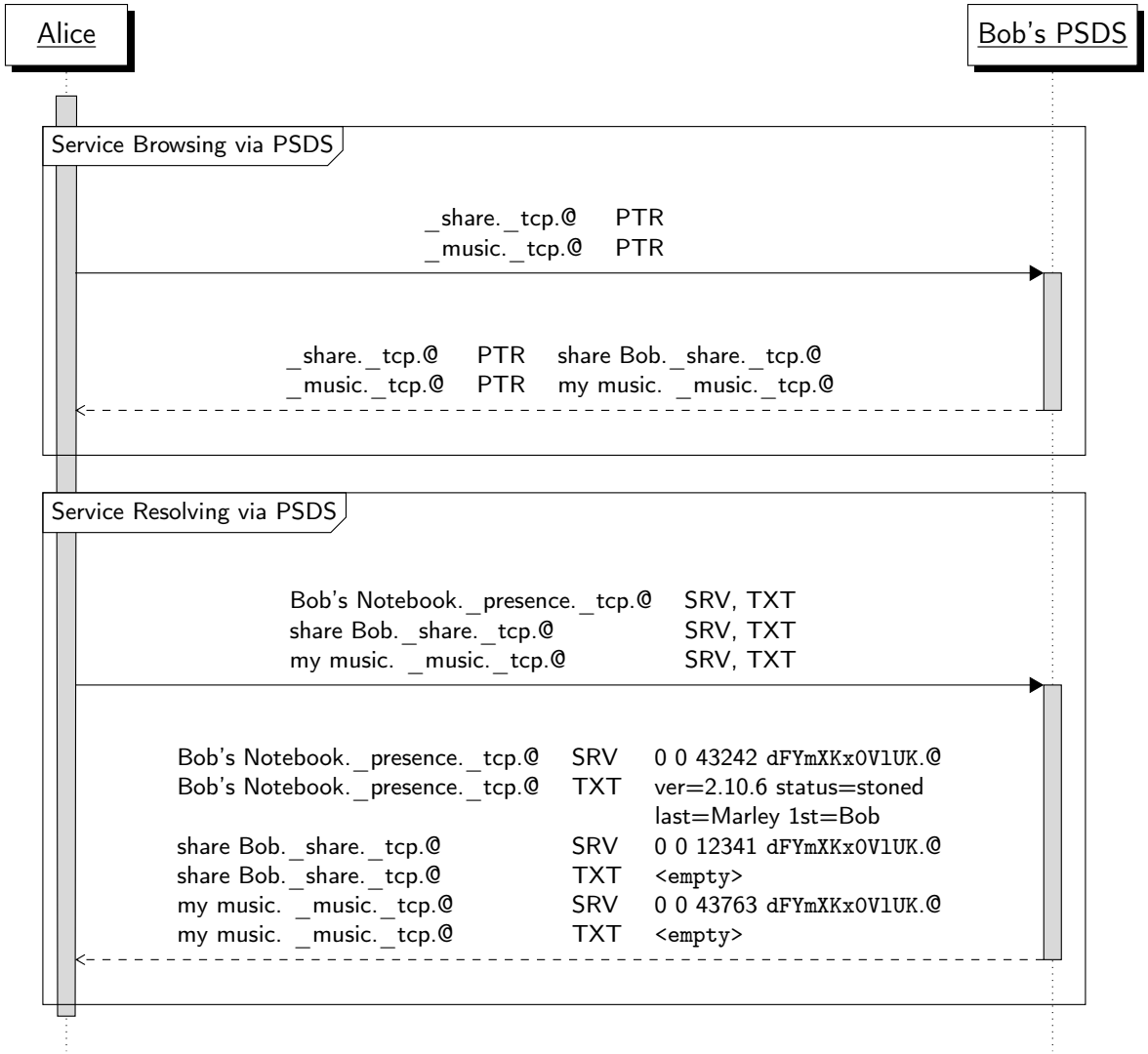
Should we work on pairing?

- essential for privacy preserving service discovery
- other applications will also benefit

Private Directory Discovery cont'



Service Discovery



Direct Resolving