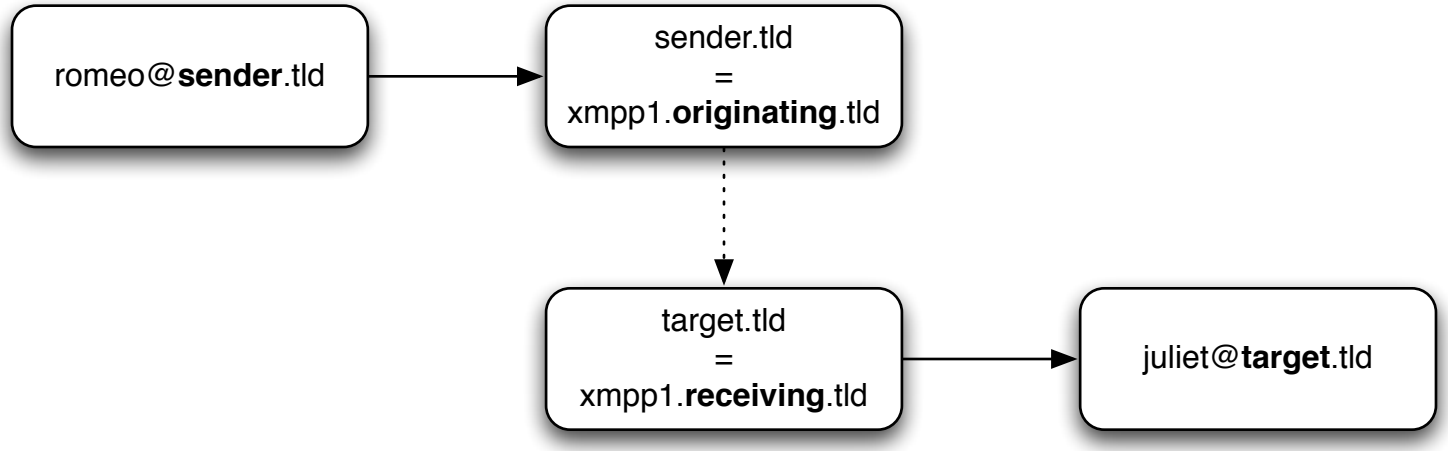
Domain Name Assertions

Richard Barnes
Jonas Lindberg
XMPP @ IETF80

Reminder: The Problem



- When XMPP services are delegated…
- How do you verify that a server is authorized to represent a domain?
- How can the providers in the middle re-use connections for many different customers?

High-level solution

- Authentication:
  - Use DNSSEC to verify SRV records
  - Keep an list of authorized domains per server
- Connection Sharing:
  - Keep a routing table that maps domain pairs to connections
  - Add some signaling to the XMPP stream to update this routing table

DNSSEC

```
_xmpp-server._tcp.target.tld. 400 IN SRV
                    20 0 5269 xmpp1.receiving.tld

_xmpp-server._tcp.target.tld. 400 IN RRSIG
```

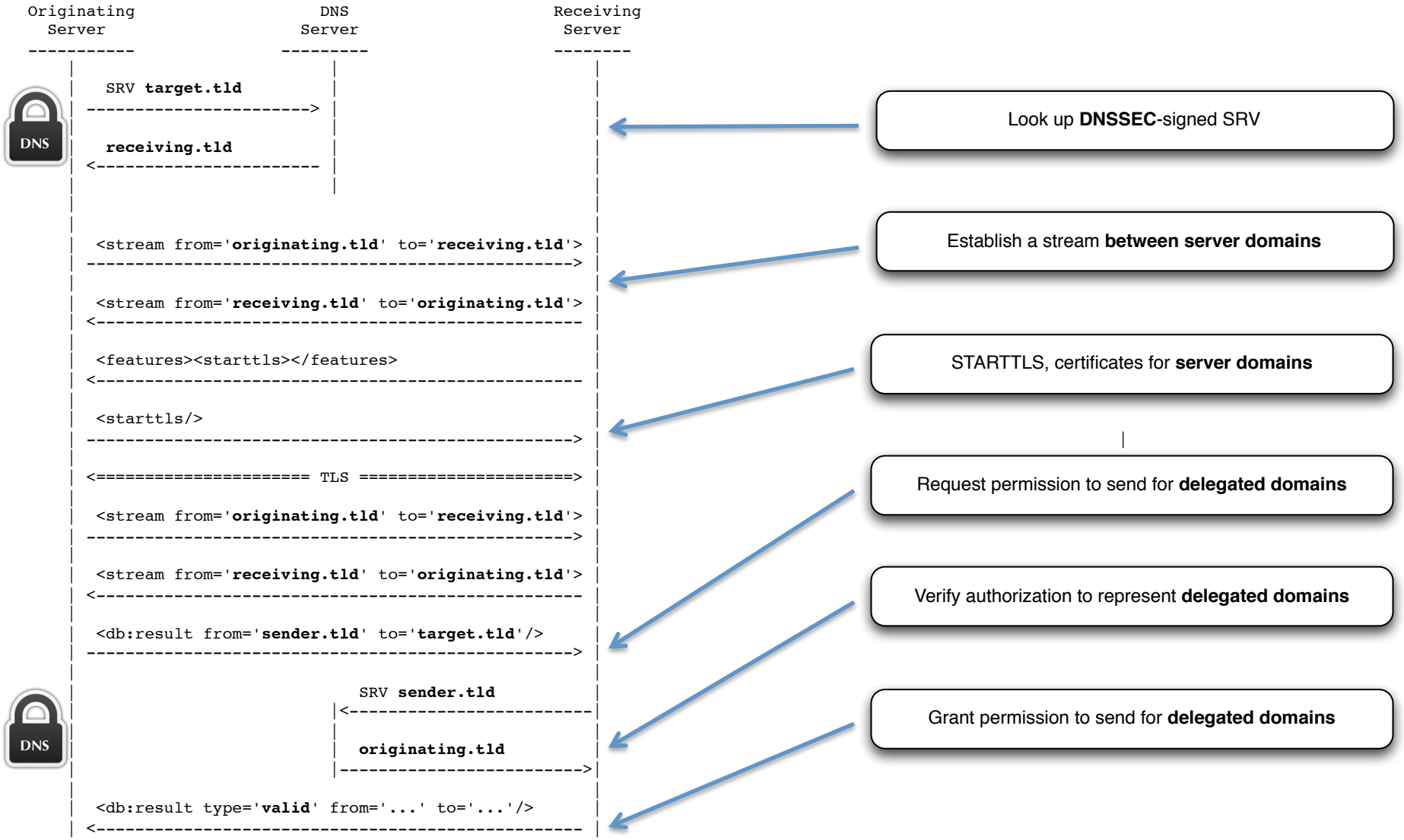
Connection	Server Domain Names	Delegated Domain Names
XXX	xmpp1.receiving.tld	target.tld
YYY	xmpp2.receiving.tld	target.tld
AAA	paris.example	paris.example

Routing Table

```
I: <db:result from='sender.tld' to='target.tld' />
R: <db:result type='valid'
              from='sender.tld' to='target.tld' />
```

Local	Remote	Connections
sender.tld	target.tld	XXX, YYY
laurence.example	capulet.example	AAA
laurence.example	paris.example	YYY, AAA

Overall Flow



Status

- The current document is incomplete …
  - Needs Security Considerations
  - Needs IANA Considerations
  - Needs Operational Considerations
- … but we think the protocol spec is pretty much there
- Is this the right path?
  - Implementability?
  - Backward Compatibility?