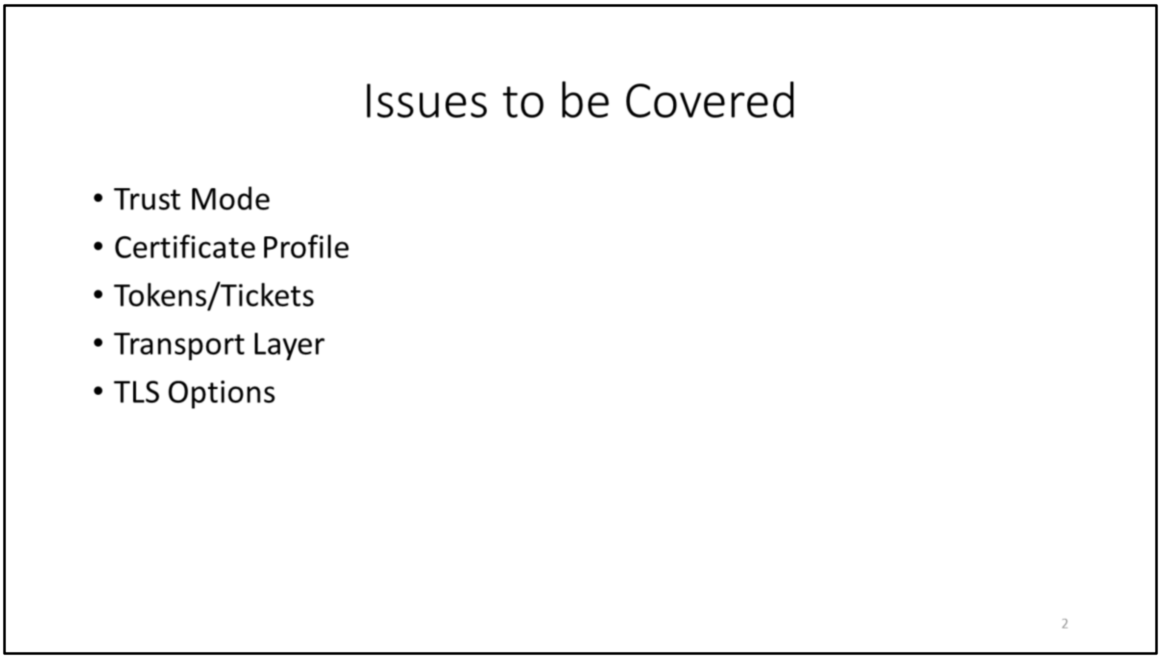
TLS 1.3 & RADEXT

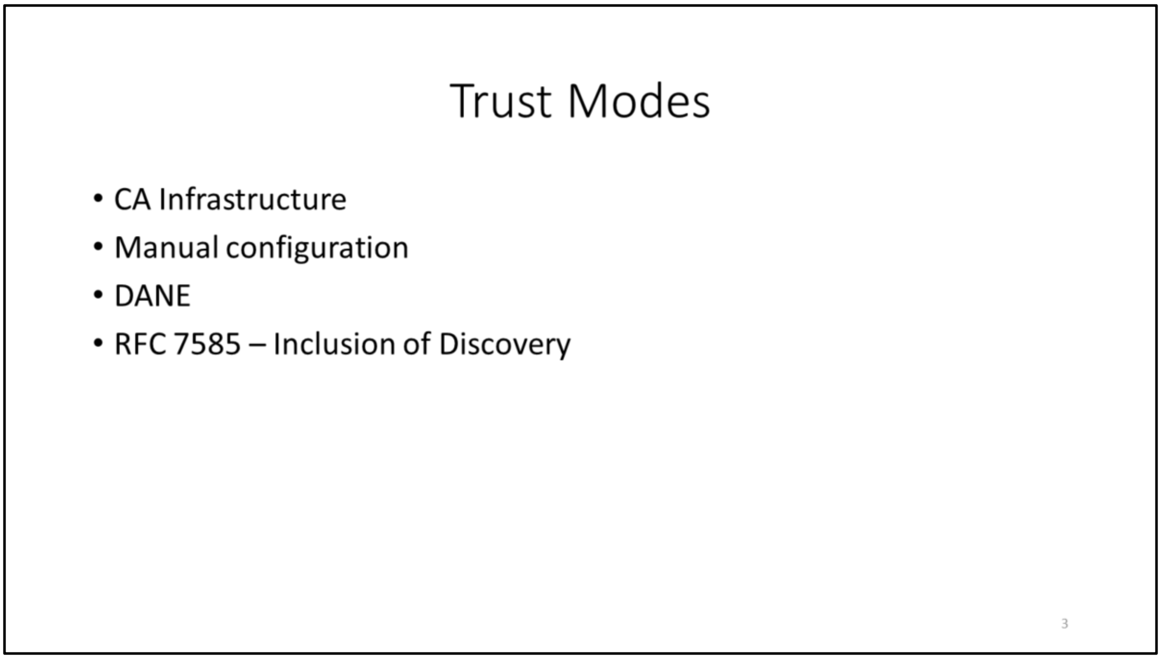
Jim Schaad
August Cellars



Issues to be Covered

- Trust Mode
- Certificate Profile
- Tokens/Tickets
- Transport Layer
- TLS Options

What do I say here?
I missed the TLS Options



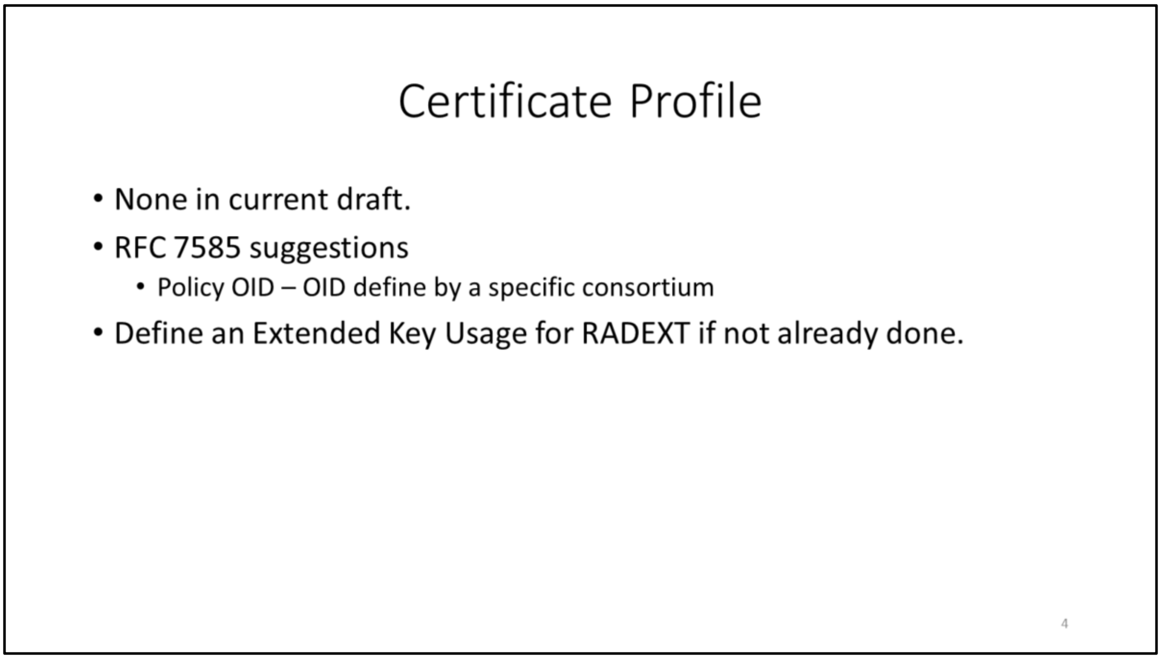
Trust Modes

- CA Infrastructure
- Manual configuration
- DANE
- RFC 7585 – Inclusion of Discovery

3

Several different things that can be done for dealing with trust models.

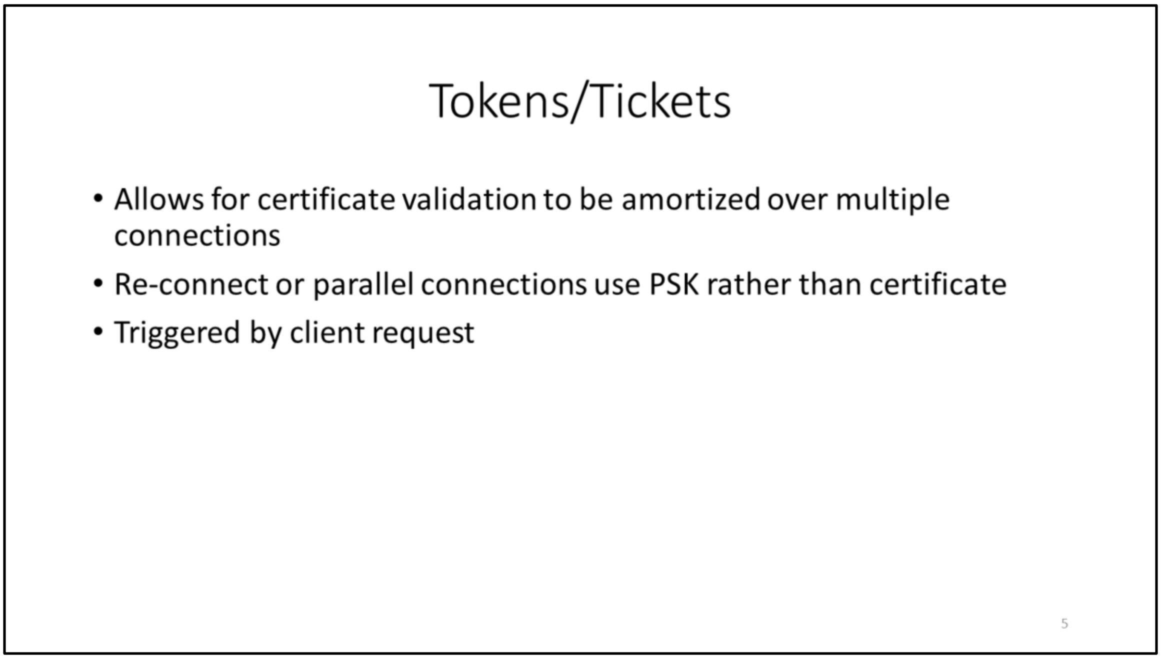
- CA infrastructure – problem is getting a single group to deal with this in some cases. Also may need to determine the infrastructure that you are using before talking to the server so that you know if you are going to be able to supply a client certificate to do mutual auth.
- Manual configuration – scale problems
- DANE lookups – need to do more than the simple is this the right certificate, still need to additionally look at is this someplace where I trust results that are going to come back.
- Discovery is documented in RFC 7585 – should we wrap it in here or keep it separate. Preference for refer to it but don't include it.
- If do lookup in DNS ala 7585, need to be sure that the trust decisions are based on the original DNS address and not on the final one. Different keys/client certs may apply based on the starting DNS point even if they resolve to the same AAA address.



Certificate Profile

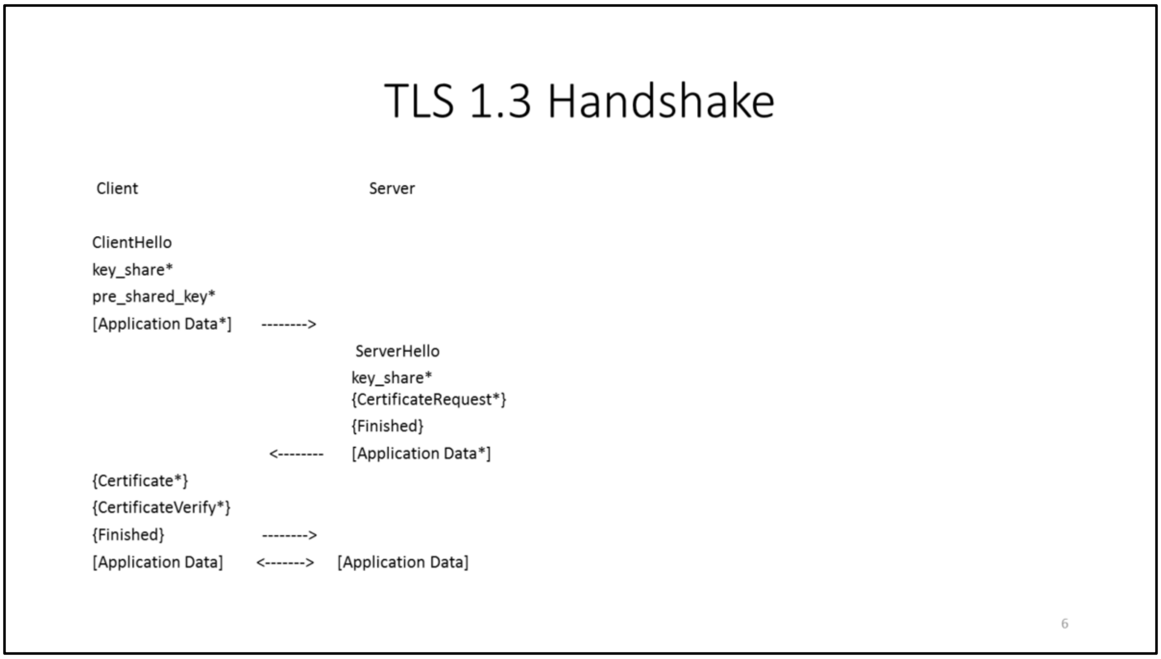
- None in current draft.
- RFC 7585 suggestions
  - Policy OID – OID define by a specific consortium
- Define an Extended Key Usage for RADEXT if not already done.

4



Tokens/Tickets

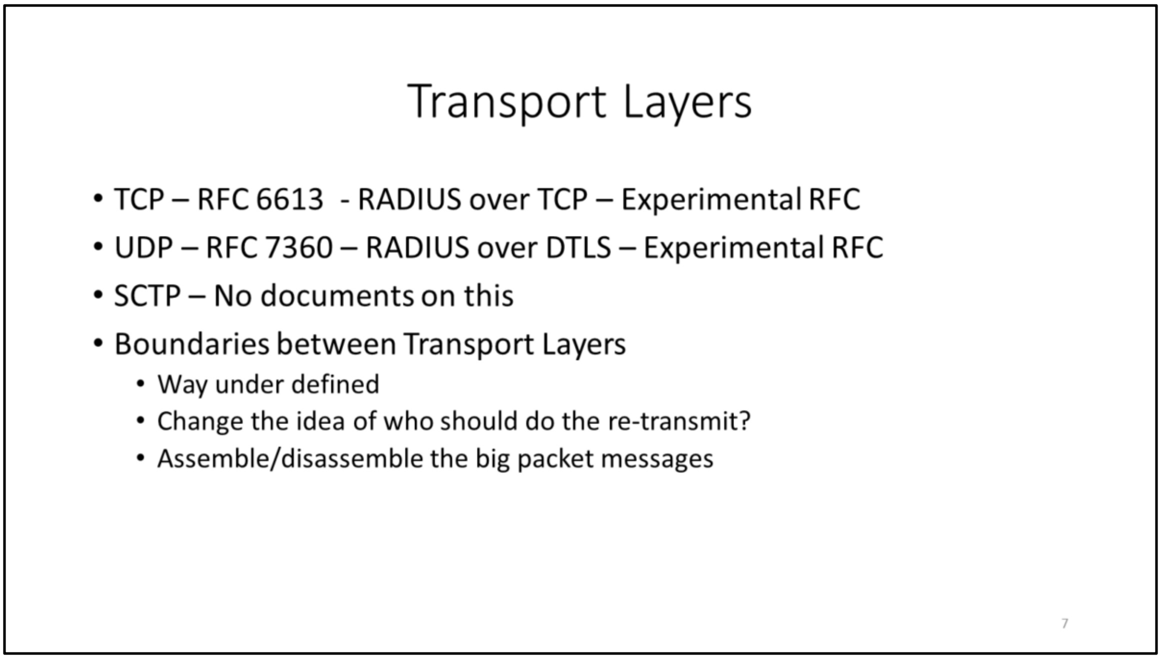
- Allows for certificate validation to be amortized over multiple connections
- Re-connect or parallel connections use PSK rather than certificate
- Triggered by client request



TLS 1.3 Handshake

```
Client                                    Server

ClientHello
key_share*
pre_shared_key*
[Application Data*]     -------->
                                        ServerHello
                                        key_share*
                                        {CertificateRequest*}
                                        {Finished}
                          <--------     [Application Data*]
{Certificate*}
{CertificateVerify*}
{Finished}              -------->
[Application Data]     <------->     [Application Data]
```



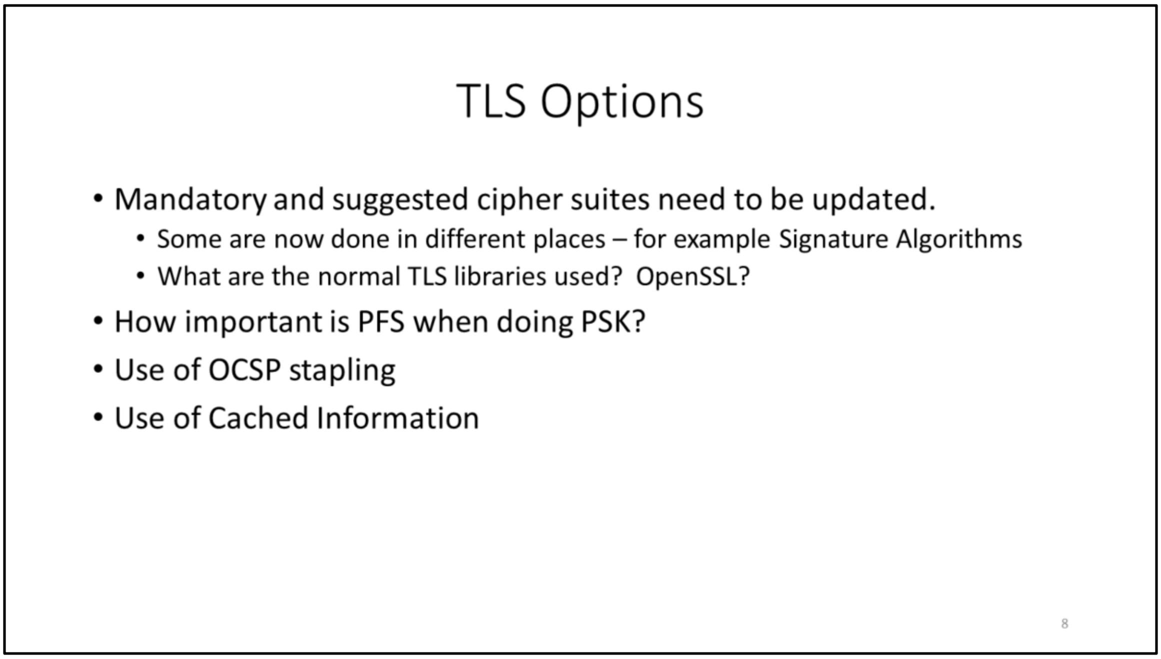
Transport Layers

- TCP – RFC 6613 - RADIUS over TCP – Experimental RFC
- UDP – RFC 7360 – RADIUS over DTLS – Experimental RFC
- SCTP – No documents on this
- Boundaries between Transport Layers
  - Way under defined
  - Change the idea of who should do the re-transmit?
  - Assemble/disassemble the big packet messages

7

Current the TCP draft is experimental status – so it would need to be updated.
DTLS – should we roll this into a single draft? Makes it easier to find and update as long as we are not trying to get new TLS versions rolled out too quickly.
*Unsure of how much DTLS exists, but does solve some problems.
*No harder to configure using PSK than current methods of configuration

TCP says don't do re-transmits, but this breaks down if you get a TCP->UDP change at some point. What does this mean if you have UDP->TCP where the NAS will re-transmit even though some portion is reliable.
Expectation is that this is going to be network boundaries – would expect to be monolithic inside of a company but might change when go outside of the company.
May be a set of well defined proxies that need to make these transitions.



TLS Options

- Mandatory and suggested cipher suites need to be updated.
  - Some are now done in different places – for example Signature Algorithms
  - What are the normal TLS libraries used? OpenSSL?
- How important is PFS when doing PSK?
- Use of OCSP stapling
- Use of Cached Information

Discussions