Abstract: Defines how to protect NETCONF messages with TLS 1.3

Motivation:
- Best to be explicit about TLS 1.3 profile
- Address 0-RTT and cipher suites
- EVERYTHING else is based on RFC 7589

Note: I-D purposely does NOT update RFC 7589 - we feel TLS 1.2 will be around for a while
O-RTT:

- Allows a client to send "early data" as part of the first flight of messages to a server
- O-RTT can be used when the client & server share a pre-shared key (PSK)
- PSK can be loaded from external source or derived from a previous handshake
- In the absence of an application specific profile, RFC 8447 says MUST NOT use O-RTT
- This I-D explicit says MUST NOT use O-RTT

Cipher suites:

- Algorithms are different than those in TLS 1.2
- The mandatory-to-implement algorithms are forward secure

Ask:

- Adopt as WG item