

# Chipping flakes from "TLS 1.2 is still frozen"

**Rich Salz, Nimrod Aviram**

## Remove duplicates from UTA WG use-tls-13 draft

- Remove the bullet list from the introduction
- Remove the security considerations
- Add text that says “nothing here applies to DTLS 1.3”

This would make the draft about 1.5 pages and boilerplate keeping the IANA instructions.

# What remains?

```
# IANA Considerations {#iana}
```

```
IANA will stop accepting registrations for any TLS parameters  
{{TLS13REG}} except for the following:
```

- TLS Exporter Labels
- TLS Application-Layer Protocol Negotiation (ALPN) Protocol IDs

```
Entries in any other TLS protocol registry should have an  
indication like "For TLS 1.3 or later" in their entry
```

# PQ also

(NIST, IETF, etc., introduction)

For TLS it is important to note that the focus of these efforts is TLS 1.3 or later.

Bluntly, post-quantum cryptography for TLS 1.2 WILL NOT be supported (see `iana`).