draft-nharper-tokbind-tls13

Nick Harper
IETF 100

Section 2: Token Binding TLS Extension

```
ClientHello
+ token_binding
```

TLS 1.2

```
ServerHello
+ token_binding
```

TLS 1.3

```
ServerHello
EncryptedExtensions
+ token_binding
```

Allowed

```
ClientHello
+ token_binding
+ early_data
```

Forbidden

```
EncryptedExtensions
+ token_binding
+ early_data
```

Section 4: Clarification of TokenBinding.signature

Uses the exporter defined in TLS 1.3 §7.5, the replacement for the RFC 5705 EKM.

“[The exporter value is] computed with the following parameters:

- Secret: exporter_master_secret.
- label: The ASCII string "EXPORTER-Token-Binding" with no terminating NUL.
- context_value: No context value is supplied.
- key_length: 32 bytes.”

(These are the same inputs as in TBPROTO)