

Binding Properties for draft-fossati-seat-expat

Muhammad Usama Sardar^{1,2}

¹TU Dresden, Germany

²Co-chair, Trusted Research Environment (TRE) Open Suite,
Global Alliance for Genomics and Health (GA4GH)

July 21, 2026

Thanks to [ULISSY s.r.l.](#) for travel sponsorship!



Binding Levels

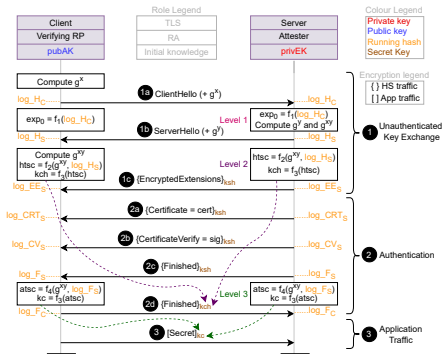
Level	Secret	Handshake state
1	DH shared secret (g^{xy})	g^x from ClientHello and g^y from ServerHello
2	Client's handshake traffic key ($htsc$)	complete ClientHello and ServerHello
3	Client's application traffic key ($atsc$)	ClientHello up to ServerFinished

- Increasingly **stronger** binding to the connection

$$G_3 \Rightarrow G_2 \Rightarrow G_1 \quad (1)$$

Binding to Client Handshake Traffic Secret is Not Sufficient

Devil is in the Details!



- $htsc$: used for encryption of clientFinished message (2d).
 - Irrelevant for security goals
 - Server **not yet authenticated** at this point
- $atasc$: used for encryption of application data (client's secret, e.g., decryption key)
 - Relevant for security goals