PRESENTED BY :

Nick Sullivan

TLS WG
IETF 123

ECH
SIGNED CONFIG

PROBLEM **STATEMENT**

INCIDENTAL FINDING

Clients must validate the server’s certificate against the **public_name** when ECH is rejected. This highlights why outer SNI must equal the public name for fallback to succeed under current rules.

PROBLEM

Only two ways of updating an out-of-date ECH configuration

- Inside a TLS connection where public_name is the trusted name
- Re-querying DNS

Goal: To make it easier for clients to obtain updated ECH configs without limiting server choices.

PREVIOUS **DISCUSSIONS**

MASQUERADE

- Martin Thomson's Public Name Masquerade for ECH draft – notes that a new approach can allow fallback authentication without a valid certificate for the public name by using a ***known public key*** instead

IMPLICIT ECH

- PR from Dennis Jackson on Implicit ECH draft (https://github.com/grittygrease/draft-sullivan-tls-implicit-ech/pull/9/files) expands on this to define a signed ECH configuration.

DNSSEC DISCUSSION

- Paul Wouters during the DNSOP/TLS list discussion of the SVCB-ECH draft in October 2024.suggested DNSSEC signing as a way to mitigate downgrade issues. (https://mailarchive.ietf.org/arch/msg/dnsop/boF_qejma2MRkdo4WsjpDmmQILA/)

PROPOSED **SOLUTION**

KEY FEATURES

- **Augmented ECH configuration**: Add some additional values to the ECH configuration structure around expiration.
- **Signature Format**: Key identifier and canonical signature format.
- **Potential Trust Mechanisms**:
  - TOFU public key
  - Certificate auth
  - DNSSEC or Succinct ZKP (https://dl.acm.org/doi/10.1145/3694715.3695962)

BENEFITS

- **Guaranteed trust for retry_config**: No need to rely on the live signature of the TLS connection.
- **Out-of-band updates**: ECH can be fetched from unauthenticated locations, including well-known URI
- **Implicit ECH works**: No more conflicts when sending in-band updates on a connection with client-chosen outer SNI.

PRESENTED BY :

Nick Sullivan

TLS WG
IETF 123

ECH
SIGNED CONFIG