TLS 1.3 Encrypted SNI

ekr: ekr@rtfm.com dkg: dkg@aclu.org

DISCLAIMER: THIS IS NOT FULLY-BAKED

We just fleshed out this idea yesterday, so it's hand-wavy. Insufficient analysis has been done.

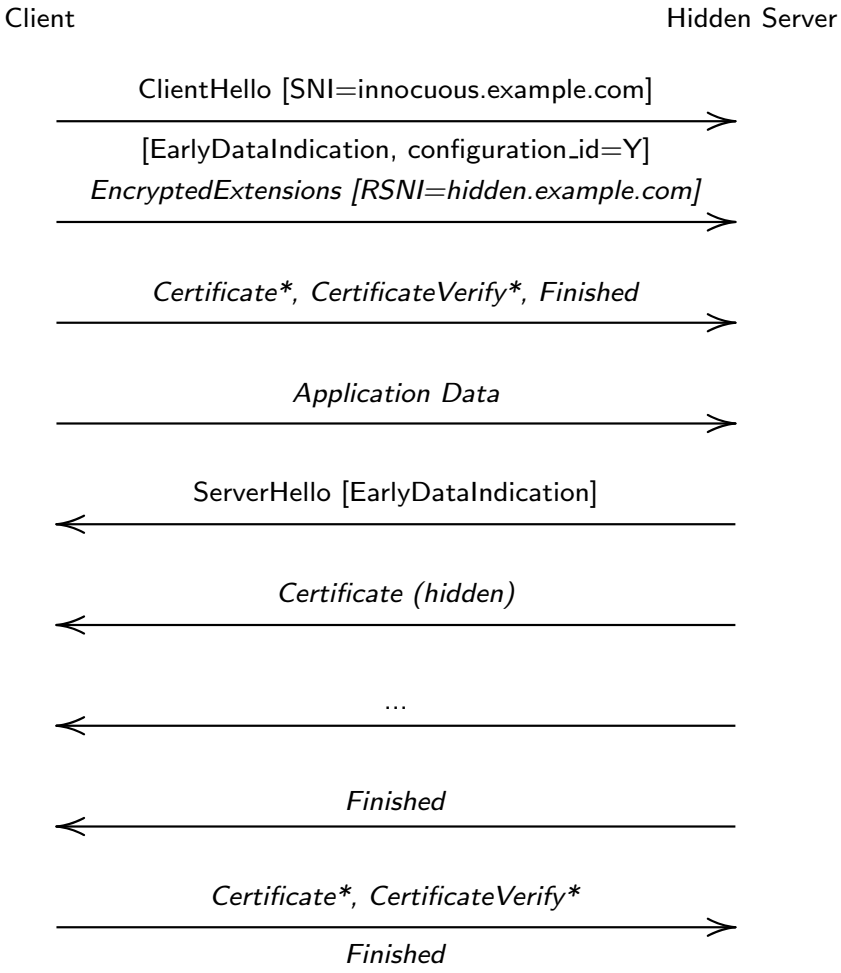
Desired security properties

1. If you connect to the hidden site, you can learn that someone is covering for it and how to connect to the covering site.
2. If you connect to the covering site, you don't learn that it is covering for anyone or who that list is. However, you can *verify* that is covering for someone if you suspect that it is.
3. Observation of traffic between the client and gateway/covering site does not allow attackers to determine whether the connection is to the the covering site or the hidden site.
4. Client's first connection to hidden server need not be protected.

Operational Modes

- Co-tenanted sites with wildcard certificate
  - Client just needs to know it can omit SNI
- Co-tenanted sites with SAN certificate
  - Need encrypted SNI only
- Gateway server with separate origin server
  - The origin server shouldn't see any application-layer traffic
  - Need something fancier

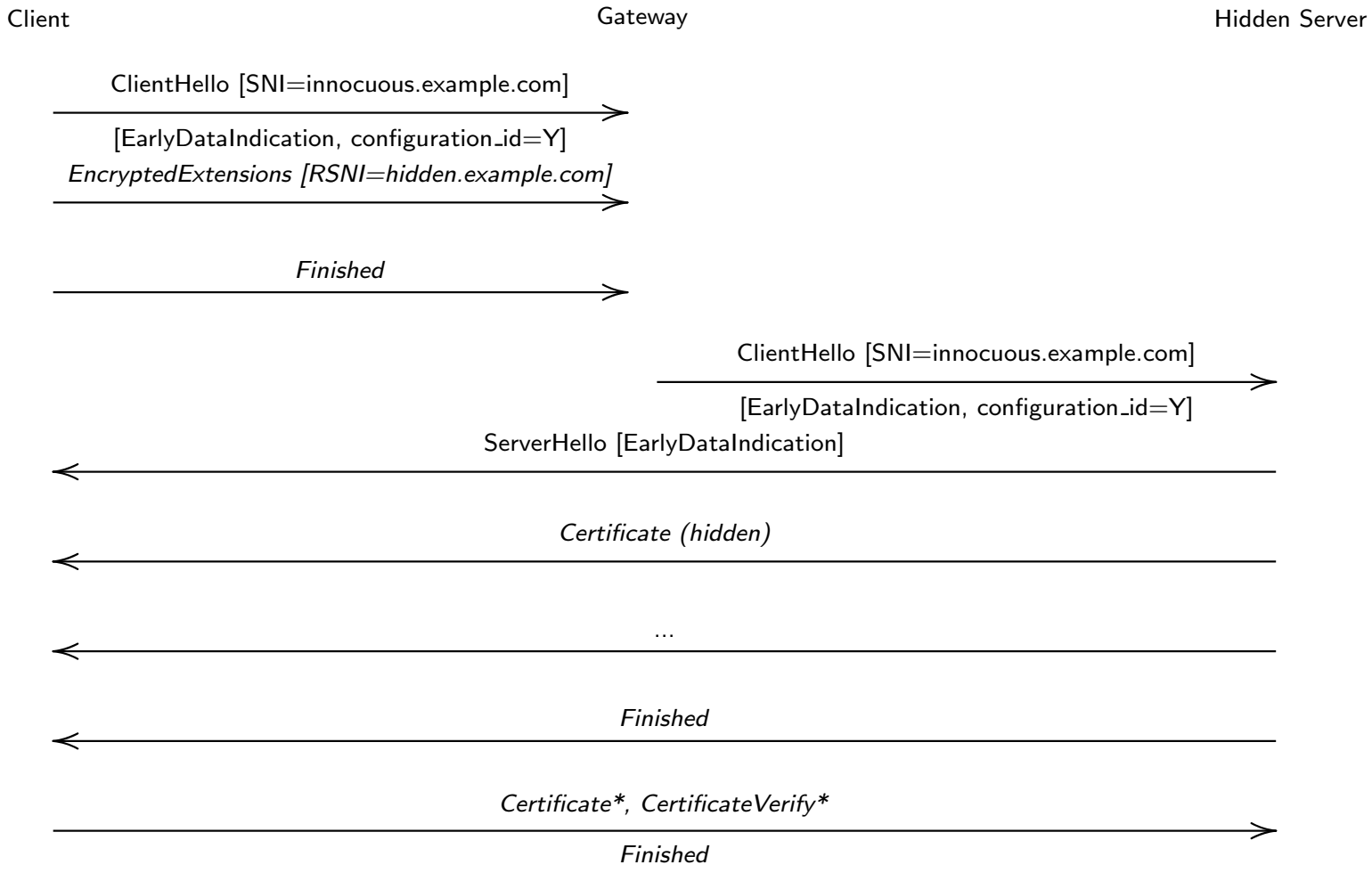
Co-tenanted Flow



Intuition

- This is just a standard 0-RTT handshake, but using the fact that the first flight is encrypted to hide the SNI.

Gateway Server Flow



Intuition

- The client *knows* that encrypted SNI is in use
  - 0-RTT data goes to the gateway *not* to the hidden server
  - Can't send any application data in 0-RTT
  - But the covering site *emph* can have 0-RTT for non-hidden servers
    - Switch-hit based on RSNI
- So what *certificate* is used to generate keys for 0-RTT?
  - Shouldn't be hidden server's certificate (would have to iterate)
  - So, the gateway's certificate
    - This makes sense since we're encrypting to the gateway
  - TLS doesn't require that these certs be the same
- Yes, this is a bit weird

How does the client learn about this?

- Client needs to know triplet [ServerConfiguration (DH_s), CSNI, GCERT]
- Traffic to hidden servers *must* use the same configuration id as traffic to other servers fronted by gateway
- Client's first connection to hidden server isn't protected.

Possible options

1. Hidden server sends unsolicited extension with CSNI and GCERT
2. Hidden server sends CSNI and GCERT in ServerConfiguration but in some other part of it that's not hashed into the keys.
3. Hidden server sends a ServerConfiguration with CSNI and GCERT but with same configuration_id as the ordinary gateway ServerConfiguration. Requires gateway server to do trial decryption.
4. Hidden server delivers the triplet in a non-TLS message (e.g., HTTP header)
5. Hidden server just delivers gateway's domain name somehow and then the client connects to the gateway server to get ServerConfiguration.

Good idea, or the best idea?