Conveying a Certificate Signing Request (CSR) in a SZTP Bootstrapping Request

draft-kwatsen-netconf-sztp-csr-01

Kent Watsen
Russ Housley
Sean Turner

NETCONF WG
IETF 108 (Virtual)

Motivation

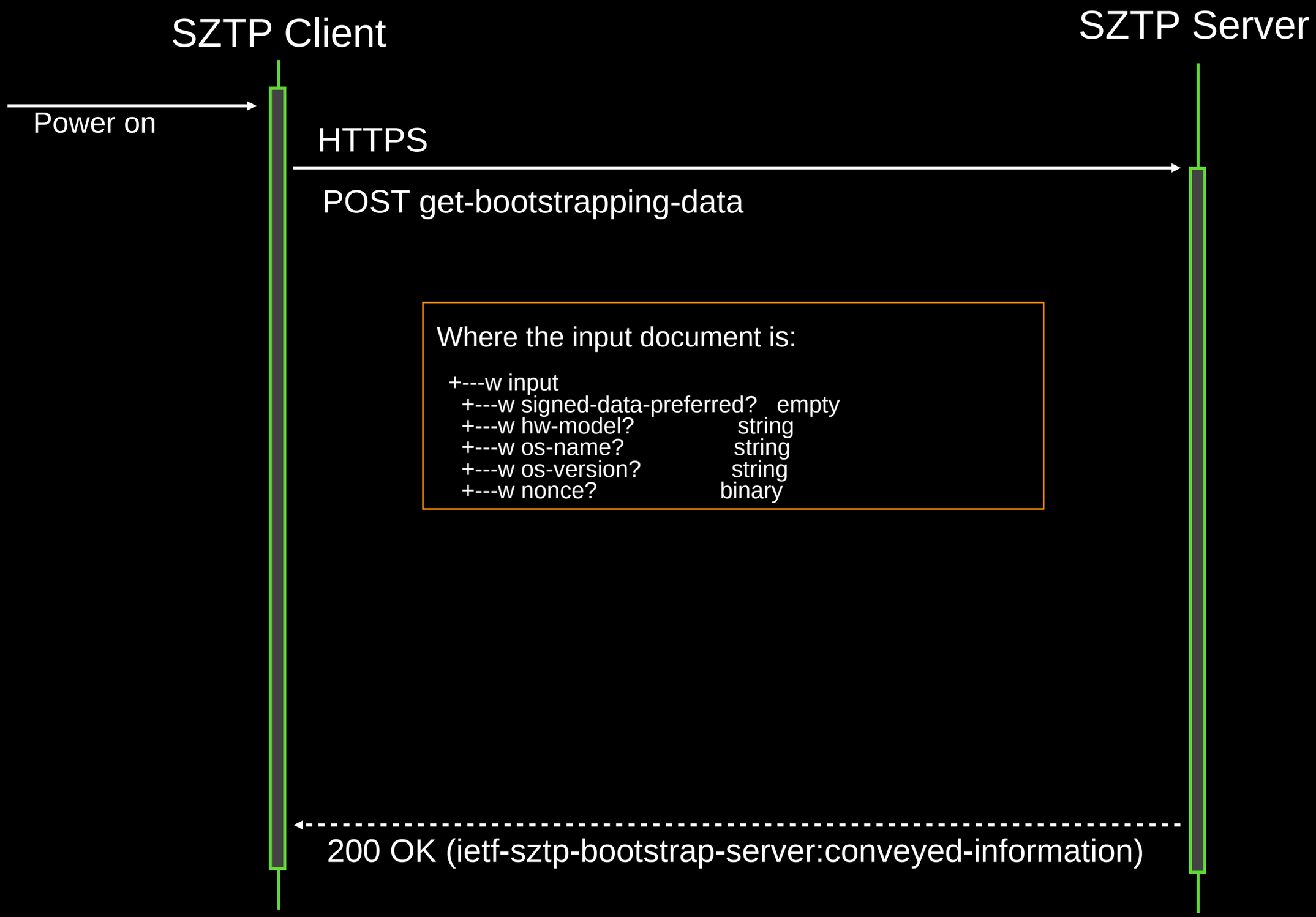
- RFC 8572 is being adopted by vendors, telecoms, established infrastructure providers, and startups.

- One feature missing is the ability for the bootstrapping device (i.e., the SZTP-client) to be issued an LDevID certificate from the bootstrap server (i.e., the SZTP server).

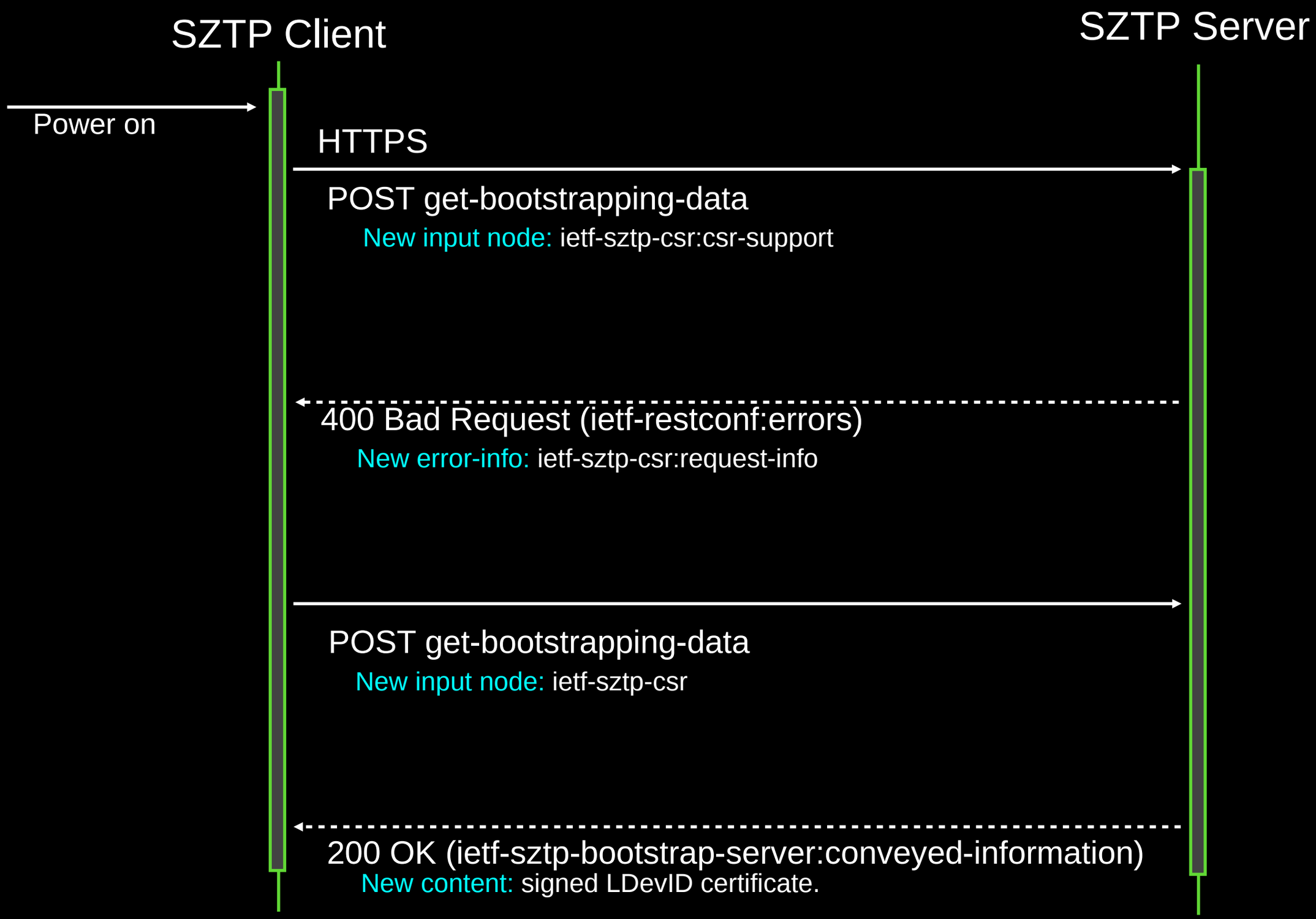
- The ability to issue an LDevID during bootstrapping is critical when the LDevID is needed to establish post-bootstrap network connectivity (e.g., a dynamically-provisioned network slice).

- This I-D updates RFC 8572 to fill-in this missing piece.

Per RFC 8572


SZTP Client
SZTP Server
Power on
HTTPS
POST get-bootstrapping-data
Where the input document is:
+---w input
+---w signed-data-preferred? empty
+---w hw-model? string
+---w os-name? string
+---w os-version? string
+---w nonce? binary
200 OK (ietf-sztp-bootstrap-server:conveyed-information)

Proposed Update



ietf-sztp-csr:csr-support

```
---- csr-support!
 +---- key-generation!
 |  +---- supported-algorithms
 |     +---- algorithm-identifier*   binary     (An “AlgorithmIdentifier” structure, RFC 2986)
 +---- csr-generation
    +---- supported-formats
       +---- format-identifier*   identityref  (Base: certificate-request-format)
```

This input parameter:

1) Enables the SZTP-client to indicate if it supports generating a new key and, if so, which algorithms it supports.
2) Enables the SZTP-client to specify what CSR formats it supports (p10, cmc, cms).

Identities:

certificate-request-format
+ p10 (from RFC 2986)
+ cmc (from RFC 5272)
+ cmp (from RFC 4210)

ietf-sztp-csr:request-info

Returned in the “ietf-restconf:errors/errors-info“ field:

```
structure: request-info
  +-- key-generation!
  |  +-- selected-algorithm
  |     +-- algorithm-identifier      binary
  +-- csr-generation
  |  +-- selected-format
  |     +-- format-identifier    identityref
  +-- cert-req-info?             ct:csr-info
```

This response:

1) Enables the SZTP-server to indicate if it wants the SZTP-client to generate a new key and, if so, which algorithms to use.
2) Enables the SZTP-server to select which CSR format the SZTP-client is to generate.
3) Enables te SZTP-server to provide a fully populated (but not yet signed) CSR structure.

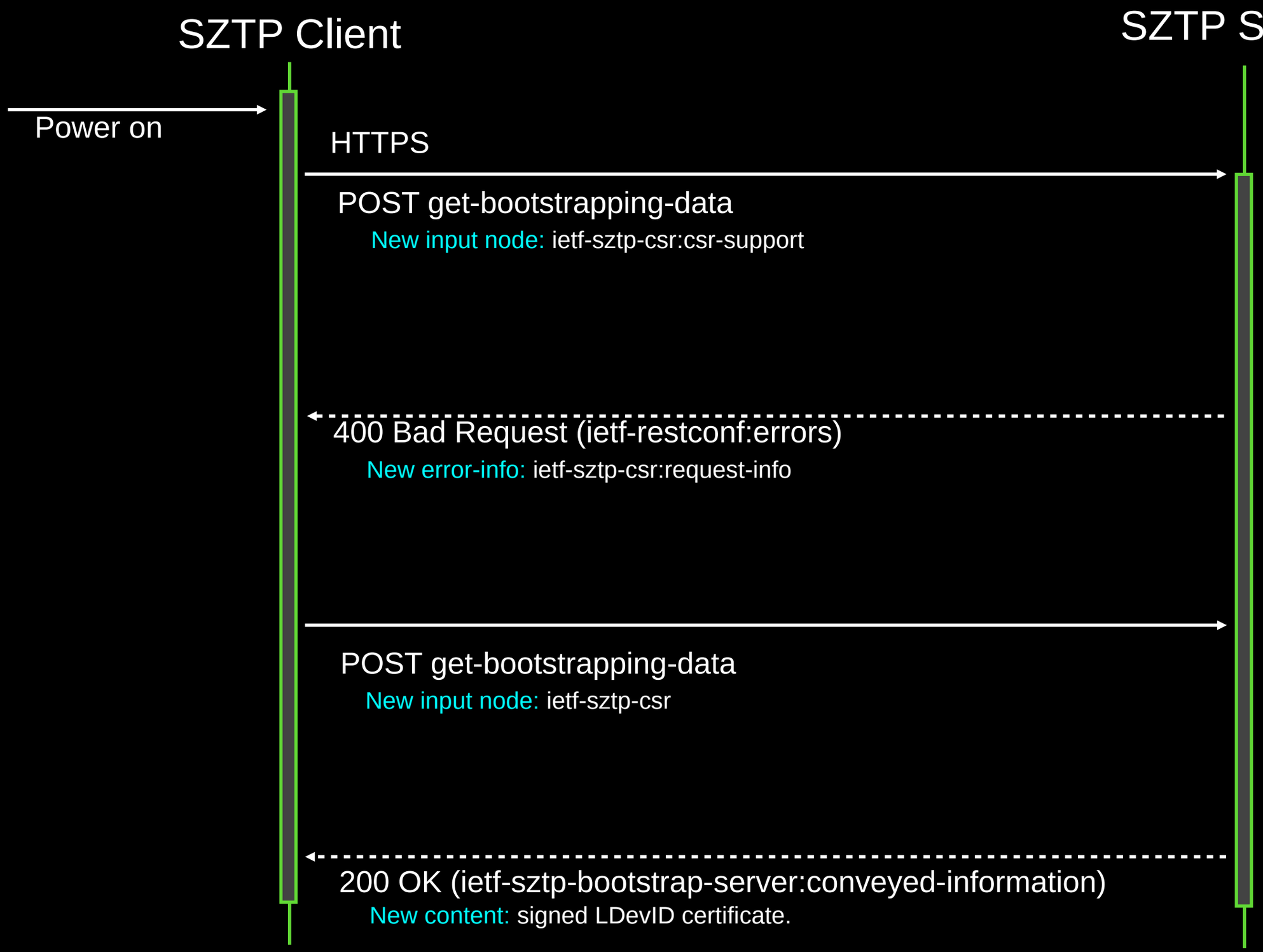
ietf-sztp-csr

```
+---- csr!
   +---- (request-type)
      +--:(p10)
      |  +---- p10?   ietf-crypto-types:csr
      +--:(cmc)
      |  +---- cmc?   binary
      +--:(cmp)
         +---- cmp?   binary
```

This input parameter:

- Enables the SZTP-client to communicate the requested CSR to the SZTP-server.

Recap: Proposed Update



Important/Requested Enhancement

Please adopt