Sequence Diagrams

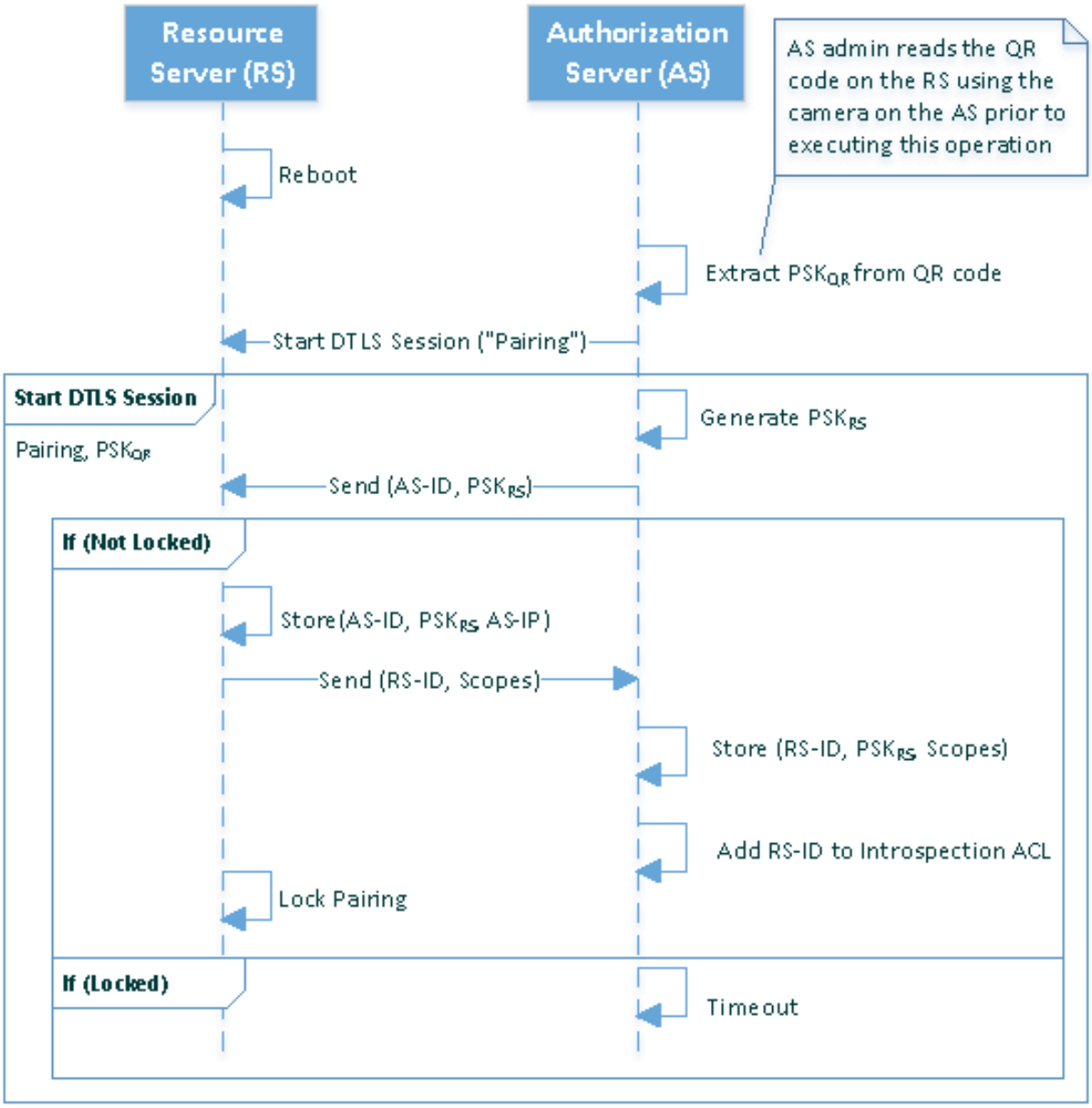
The sequence diagrams below represent the four main operations that take place in the system: RS-AS Pairing, Resource Access, RS Introspection, and Client Introspection. We assume that the pairing procedure between the Client and the AS will take place as described in our previous work (using a USB or Bluetooth connection to exchange PSKs).

Abbreviations and terms used in the sequence diagrams are:

- ACL: Access Control List maintained by AS (there is one for RSs and one for Clients)
- AS-ID: Authorization Server ID
- AS-IP: Authorization Server IP Address
- Audience: Access token claim that indicates the audience that the token is intended for, which in our case is a specific resource server
- C-ID: Client ID
- Claims: Information carried in an access token
- PoP-Key: Proof of Possession (PoP) Key generated by the AS for access to a specific RS
- PoP-Key-ID: ID for a PoP-Key
- PSK_C: PSK used by the Client to communicate with the AS.
- PSK_{QR}: PSK encoded in QR code associated to the RS
- PSK_{RS}: PSK used by RS to communicate with AS
- Resource Name: Unique name given to a resource managed by the RS.
- RS-ID: Resource Server ID
- Scopes: Parameter that indicates what an access token actually authorizes, such as "read", "write", "open", "close." In our case, we use the operation and the name of the resource provided. For example "r_temperature" would indicate that the token can be used by a client can "read temperature." Scopes are shared between the RS and AS during the pairing process.

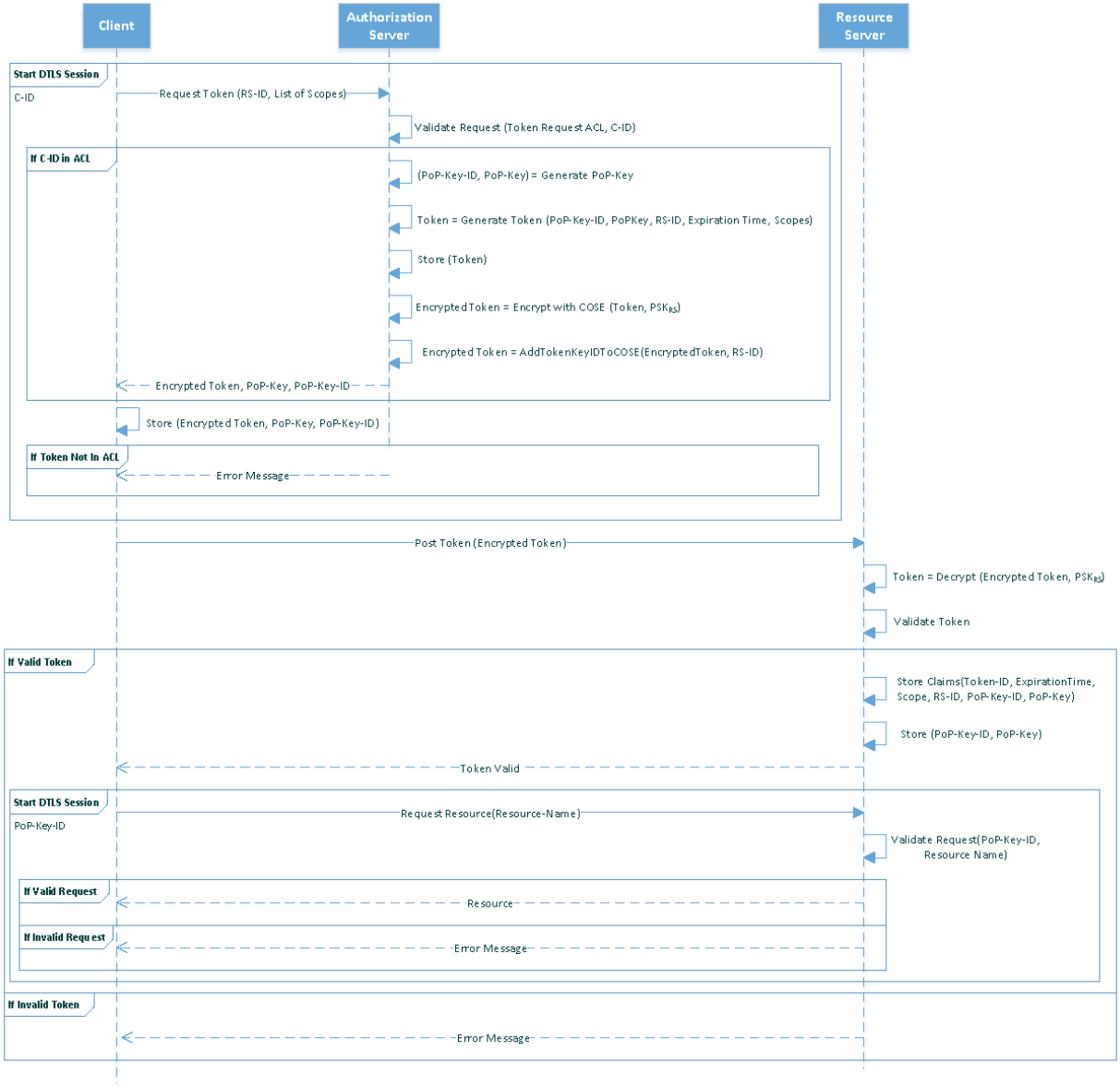
RS-AS Pairing

The sequence diagram below contains the high-level operations to pair a Resource Server (RS) to the Authentication Server (AS). Of particular note is that an RS can only be paired to one AS at a time. Pairing to a different AS would require to reboot the RS.



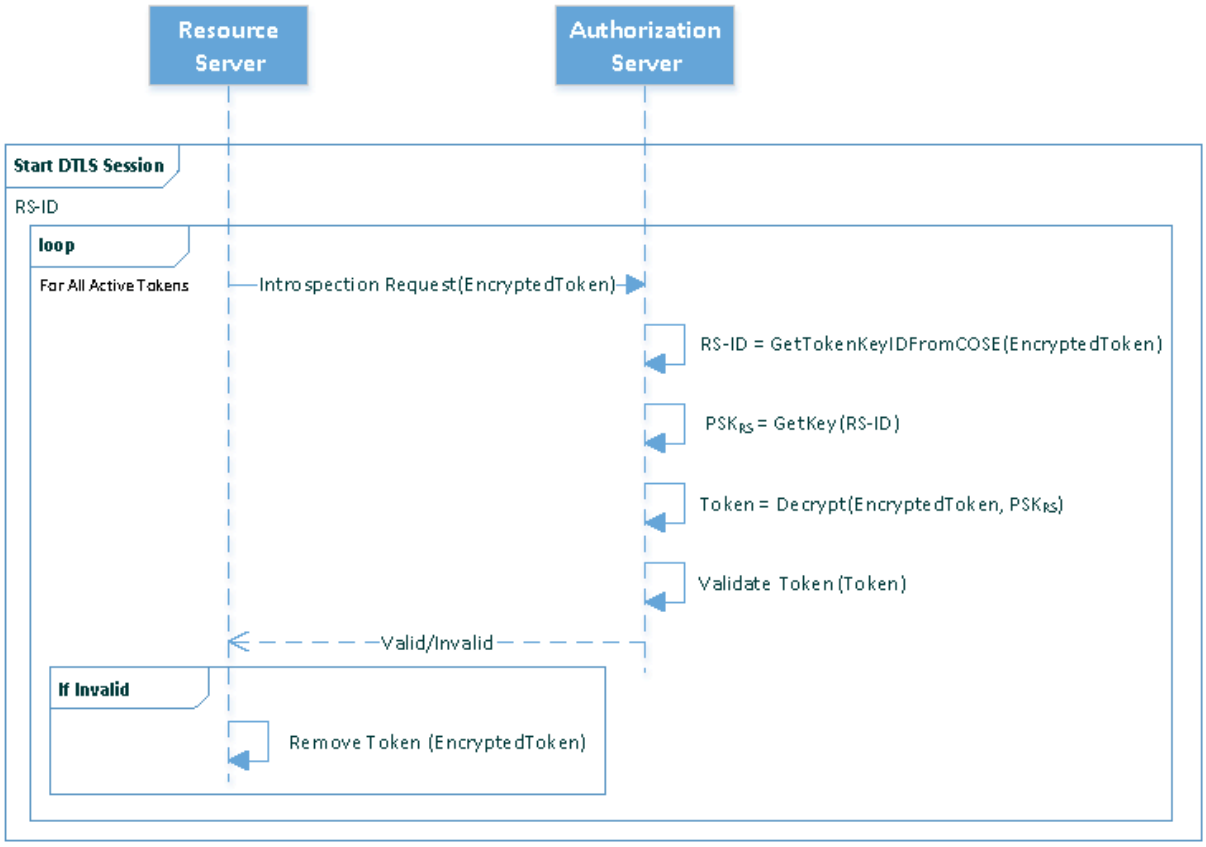
Resource Access

The sequence diagram below contains the high-level operations for a Client to access a resource exposed by a Resource Server (RS). It includes the operations executed by the Client to request the token from the Authorization Server (AS) as well as the operations used by the Client to access the RS with the provided token.



RS Introspection

The sequence diagram below contains the high-level operations for a Resource Server to perform introspection on all its active tokens (not expired). If a token has been marked as invalid in the AS, the token will be removed from the list of active tokens in the RS.



Client Introspection

The sequence diagram below contains the high-level operations for a Client to perform introspection on all its active tokens (not expired). If a token has been marked as invalid in the AS, the token will be removed from the list of active tokens in the Client.