SyncCloud Data Transfer Pipeline.

# Step 1. Client authentication with global service.

Diagram

Description automatically generated with medium confidence

Client connects to the global service endpoint via HTTPS and supplies authentication request information: project GUID, project username, and password.

# Step 2. Conduit server ping

Diagram

Description automatically generatedDiagram

Description automatically generated

On successful authentication of user in the project, global service connects to the endpoint of the conduit server linked to the project. If successful, conduit server generates a transaction ID (or TID) - a short-lived unique token used by the conduit server to identify this transaction session.

# Step 3. Global service returns transaction metadata to the client

Diagram

Description automatically generated

Transaction metadata consists of:

* Conduit server URI
* Transaction ID (TID) token
* Project metadata such as scripts

# Step 4. Creation of transaction session between client and conduit server

Diagram

Description automatically generatedDiagram

Description automatically generated

Client generates a pair of **asynchronous** encryption keys then transfers the TID token and public key directly to the conduit server.

Note, at this point the global server **is not** participating in any further communication between the client and the conduit server.

Conduit server makes sure that TID token is valid and not expired. Then generates a synchronous encryption key. Encrypts this key using the public key supplied by the client, and sends it back to the client

# Step 5. Data transfer

Diagram

Description automatically generated

Client decrypts the synchronous session key it received from the server using its own private asynchronous key it generated earlier. Then starts sending data to the server, encrypted with the server session key.

Note, packages consist of header and body. Header is an XML formatted package metadata and does not contain any data that originates from the client device. Headers are stored unencrypted in the conduit server cache. All actual data is stored in the body of the package. Body data is always encrypted, is stored encrypted in the conduit server cache and never decrypted by the conduit server.