GetChecksums

Operation to get checksums from one or more pillars in a given collection.

One or all files

Checksums can be requested either for a single file or for all files in a collection.

Requesting checksums for all files in a collection may yield a large set of results. Due to this the protocol supports a method of limiting which files are listed, which can be used for implementing a paging mechanism.

Paging

To be able to page through a large number of checksums the GetChecksums request supports limitations on the checksum time.

The limitations are:

- Minimum timestamp
- Maximum timestamp
- Maximum number of results

Pillars responding to a GetChecksums request should adhere to the following:

- The returned checksums should be ordered by their date oldest first.
- No more than the maximum number of results specified in the request should be delivered.
- If the pillar itself only allows for transmitting fewer results than specified in the request the pillar should keep to its own maximum.
- If the pillar has more checksums than could be sent in the response, then the response should be marked as a PartialResult.
- If limitations by minimum or maximum timestamp is present, the results should be inclusive.
    - If a minimum timestamp is in place, then first result should match the minimum limitation.
    - If a maximum timetamp is in place, then the last result should not be after the limitation. If the number of results is larger than the allowed maximum, the response should be marked as a PartialResult.

Checksum specification

As part of the GetChecksums request, the type of checksum is specified. The protocol specifies a set of known hash algorithms, but is also open for extensions.

Directly specified in the protocol are:

- MD5
- SHA-family of hash algorithms.

When it comes to salted checksums HMAC is in conjunction with the algorithm. I.e. HMAC_MD5 or HMAC_SHA256.

The Checksum specification is per request and for all files that it pertains (a single file, or all).

A client should expect that checksum pillars will reject a GetChecksums request if the checksum type does not match the one that the pillar has stored.