Security

Description of the different security related aspects of the protocol

Security model in the Bit Repository Architecture

For authentication purposes, messages are signed by the senders (clients/pillars/...) using their private key.

Messages may optionally be encrypted using the SLA public key. Encryption does not ensure authenticity.

client -> pillar(s): message signed by client private key, encrypted by SLA-specific public key
pillar -> client: message signed by pillar private key, encrypted by SLA-specific public key

The SLA public and private keys are distributed between SLA partners.
The client and pillar message signing certificates (ie users) are assigned by their respective organisations.

Clarifying Questions

- Will the clients be in charge of setting up their own users?
- Will the authorization be role-based?
- Assuming that we use a certificate solution, will the individual pillars check the certificates?
- Will xmldsig work for us?

Operation permissions

Describes how messages requesting operation on a collection is are checked against the permission model.

Encryption

To prevent anybody from eavesdropping on the bit repository data and messages exchanged, all communication is encrypted. Two levels of PKI are used.

Authorization

Authorization management is necessary because all clients/systems operating within a given SLA may not be allowed to have equal access to data.

Confidentiality

Information about the Bitrepository confidentiality considerations