FollowMe

Security Integration

Laurence Jordan

Context

- Addition of security to FlexiNet/FollowMe
  - Decision to use SSL
  - Supplies authentication in FollowMe
  - Other aspects of security
    - Access control
    - Secured objects
- Follows on from work previously done by Ugai Tackanori

SSL

- Key Exchange Algorithm
- Certificate
- Certificate Verify Option
- Encryption Algorithm
- Message Authentication Algorithm

- Key Exchange Algorithm
- Certificate Option
- Certificate Verify Option
- Encryption Algorithm
- Message Authentication Algorithm

Configuration Support

- Certificates
  - From file
- Algorithm triples
  - By selection of required algorithms
  - By selection of specific triples
- Check for trusted root in certificate chain
  - Option for client and server
- Client certificate requirement
  - Server access option

SSL and Security

- Communication
  - Message authentication codes (signing) provides integrity.
  - Message encryption provides confidetiality.
- Certificates
  - Based on an idea of a “hierarchy of trust”.
  - Given a copy of the X509 certificate for an authority, an SSL certificate can checked as having been issued by the authority by another via delegation from the authority.

Binder (Crimson)

Server (generator)

protocol:
"sslrrp" *or*
"rrp"

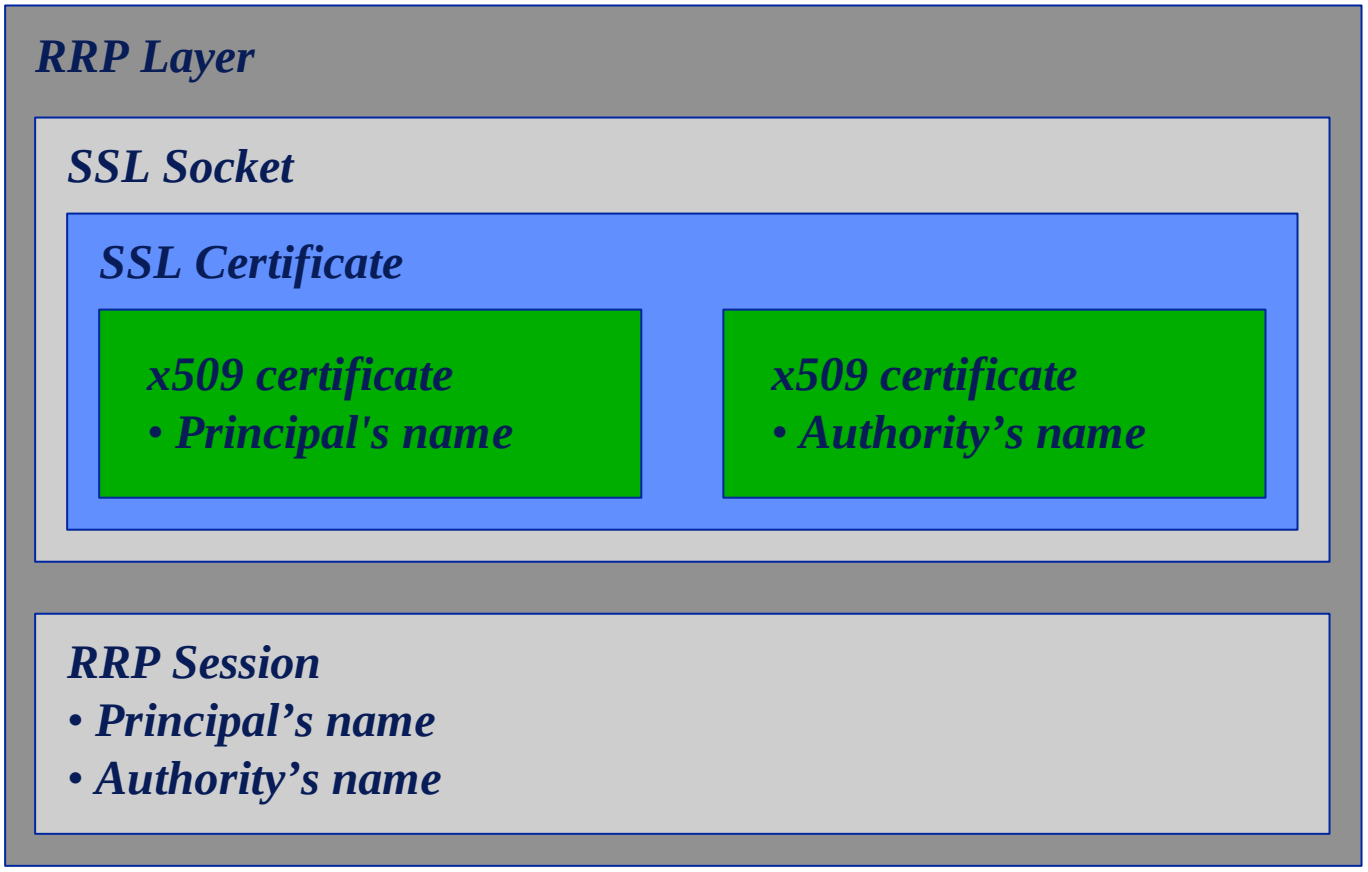
Server Socket
Client Sockets

Client (resolver)

protocol:
"sslrrp" *or*
"rrp"

Client Sockets

User Authentication



Access Control