Security 2.0 Project Team

Meeting notes from 2/24/15

Features Discussed

- ObjC bindings for security – Sec 2.1
- Certificate revocation – Sec 2.1
    - Should begin design and spec interfaces
- Distribution of policy updates and membership certificates - ??
    - Dino to discuss with team
    - May be more work than time allows
- Anonymous session – Sec 2.0
- Guild equivalence – Sec 2.0
- User equivalence certificate – Sec 2.0
- Crypto agility exchange – ??
    - Put hooks in to support negotiating AES encryption modes
    - Dino to discuss with team
- Broadcast signals and multipoint sessions – Sec 2.1
    - Request if a multipoint session is requested that Sec 2.0 fail
- Manufacture certificates – Sec 2.1
    - Multiple roots of trust is supported in Sec 2.0
    - Ken to reach out to Symantec to determine use cases
- Support for signing keys and communication keys – Sec 2.0
    - Requires design
    - May move out depending on design decisions
    - QEO to document use cases
- Packet header encryption – Sec 2.0
    - May change based on crypto feedback
- Default Authlistener – Sec 2.0
- IRB Suggestions – Sec 2.0

Proposed timing (tentative)

- HLD Lock – 3/20
- Interfaces Lock – 5/1
- Feature Complete – 6/1
- Validation - 6/1 – 7/22
- 15.08 release – 8/26 (Follows Core release process)