S/MIME Example Keys and Certificates

LAMPS/IETF 111
Daniel Kahn Gillmor
draft-ietf-lamps-samples-04
draft-ietf-lamps-samples-04

- Offers cross-signed verification paths
- Ordered DNs by scope
- (last several drafts included useful pointers and clarifications from several WG members)
What are the certs?

- **Alice** (signing)
  - **RSA CA** (pubkey: X)
  - **Alice** (encryption)
  - **Bob** (signing)
  - **ed25519 cross CA** (pubkey: Y)

- **Bob** (signing)
  - **RSA cross CA** (pubkey: X)

- **Carlos** (signing)
  - **ed25519 CA** (pubkey: Y)
  - **Carlos** (encryption)

- **Dana** (signing)
  - **ed25519 CA** (pubkey: Y)
  - **Dana** (encryption)
What kinds of chains?

RSA CA (pubkey: X) → Alice (signing)

ed25519 CA (pubkey: Y) → RSA cross CA (pubkey: X) → Alice (signing)
What formats?

Authority certs:
- Secret key (PEM)
- Certificate (PEM)

End-Entity certs:
- Secret key (PEM)
- Certificate (PEM)
- PKCS #12 (password-locked, includes cross-certs, PEM-encoded)
What else?

• Some MUAs can’t import some elements? Please report!

• Possible appendix: steps for specific clients:
  – Loading CA cert
  – Loading Client bundle
Next steps

• WGLC?