

DRAFT Open Auto-DR Communication Standards (OpenADR)

Peter Palensky
Demand Response Research Center
Lawrence Berkeley National Laboratory
<http://drrc.lbl.gov/dras>

Agenda

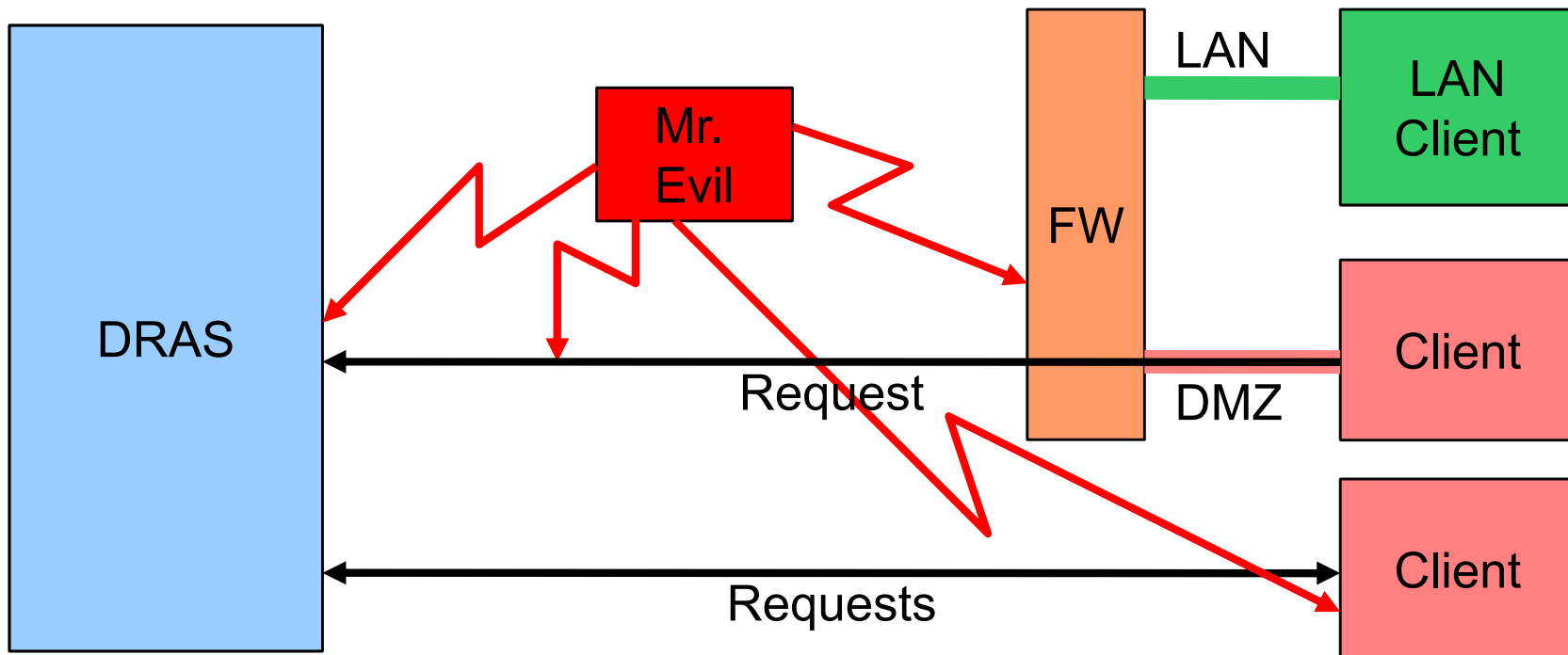
- Introduction, use cases and requirements
- Data models
- Utility Interface
- Participant Operator Interface
- DRAS Client Interface
- DRAS - BACnet Web Services
- Web Services and Security

IT Security

- Communication Paradigm
 - Client-Server m2m communication
- Design rules
 - Use existing standards wherever possible
 - Keep things simple
 - Be prepared for the future
- Interoperability vs. Flexibility
 - DRAS interface specification
 - Standard only describes WS interfaces
 - Rest of system implementation specific

Security Issues

- Auto-DR Server & Client Security
- No topology assumptions
 - -> end2end security for API interfaces

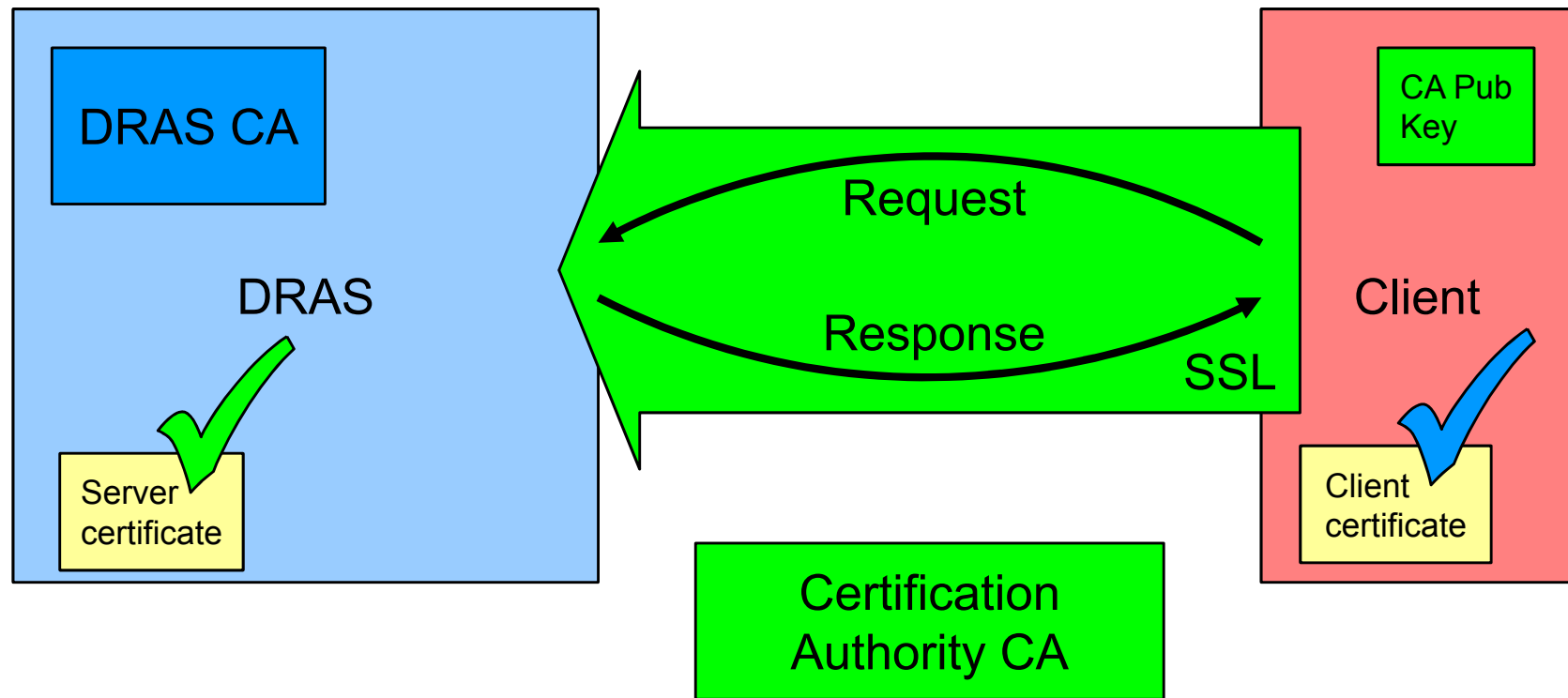


DRAS Interface Security

- Three Choices:
- TLS 1.0 + Server Cert. + HTTP BASIC
 - Easy handling, lightweight
- TLS 1.0 + Server Cert. + Client Cert.
 - Increased Security
- Web Services Security
 - Full fledged power of WS Security

Mutual Cert. Example

- Client pulls information from DRAS
 - WS exchange encapsulated in TLS 1.0
 - Use of mutual certificates



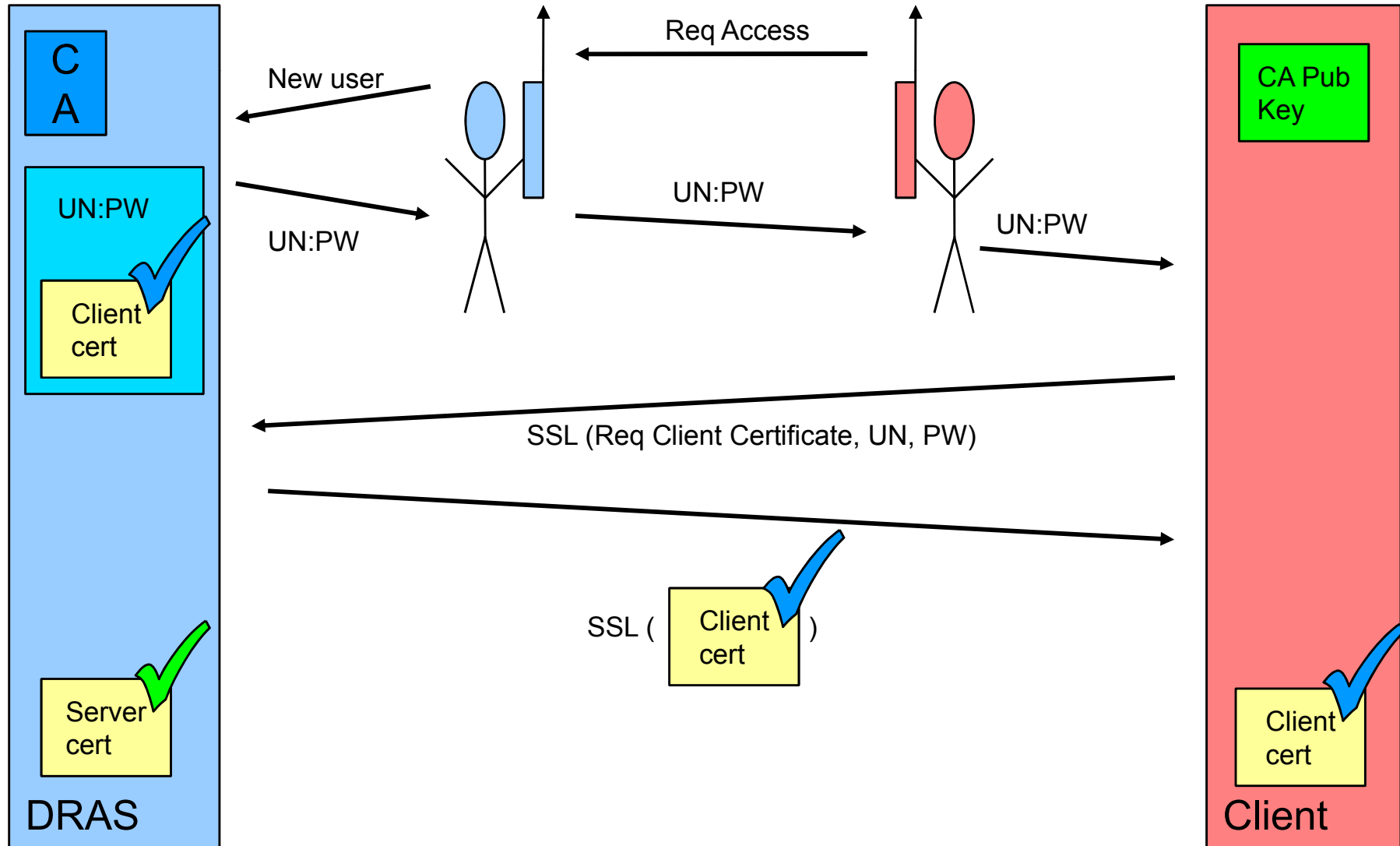
Implementation

- Non-API interfaces/functions
- Not part of Standard
- Recommendations given
- E.g.: Client Certificate/Key exchange
 - Pre-programmed/configured clients,
 - SIM card,
 - Trained and trusted installation team,
 - Temporary one-time pad,
 - User gets envelope with key,
 - Etc.

Cipher Choice

- Embedded environment
- Most interoperable = not really new
- Most secure = no embedded support
- Selection:
 - Key exchange: RSA1024
 - Data Encryption: 3DES, AES128
 - MIC: SHA1
 - MAC: HMAC-SHA1
- Stronger/updated ciphers explicitly allowed!

Akuacom Client Cert



Security Summary

- DRAS WS Interfaces protected
- 3 different standard flavors
- State-of-the-art 2008 Security
- Not covered by standard because implementation dependent
 - Optional DRAS Firewall
 - Credential/Certificate distribution
 - LBNL/Akuacom Reference Implementation
 - Combine easy logistics with mutual certificates