draft-wei-paws-framework-00

Xinpeng Wei

Zhu Lei

Peter McCann

Comparison with draft-das

	draft-das	**draft-wei**
Data Model	similar	similar
Messages	INIT-REQ/RESP REG-REQ/RESP DBQUERY-REQ/RESP DBNOTIF-REQ/RESP DEVVALID-REQ/RESP	REG-REQ/RESP AVAILWS-REQ/RESP CHUSAGE-REQ/RESP DEVVALID-REQ/RESP
Security	Server certificate & client Digest based on shared secret	Server & client certificate validated during TLS
Encoding	Suggests JSON	Defines XML schema
Usage of HTTP	POST in both directions	PUT (registration, chusage); GET (query, validation) Responses are in HTTP Responses (200 OK)

Security Discussion

- The Digest in draft-das is not HTTP Digest
  - It is a re-implementation of Digest at the application layer
- Digest is subject to Asokan-style attacks
  - Need a secure binding between the TLS authentication and the Digest authentication
- Digest requires a shared symmetric key
  - Key distribution is difficult to do securely
  - If the master device changes database providers, key re-distribution would be required
- Suggestion: add option for client certs
- More on security later from Yang Cui

Encoding Discussion

- XML Schema vs. JSON
  - XML schema is more rigorously defined

HTTP Usage Discussion

- Responses more appropriate than server-to-client POST method
  - Can be 200 OK with body

Messages Discussion

- To support Digest-style authentication, would need to add one more XML message type to convey the server nonce