TLS Extension Definitions

draft-ietf-tls-rfc4366-bis-06

Status

- Waiting for revised draft
- Issues with Server Name
  - Multiple Server Names
  - Session Resumption
  - Renegotiation
- Justify SHA-1 without algorithm agility

Multiple Server Names

- Client hello can contain more than one server name
  - Apparently, existing clients only send one, and some servers ignore everything except the first one
- Proposed Resolution
  - forbid more than one name of same "name_type"

Session Resumption

- The document should be clearer about how server_name and session resumption interact
- Proposed clarification of existing behavior

“The "server_name" is completely ignored when resuming a session.”

Renegotiation and Server Name

- Possible that server name changes upon renegotiation
- Proposed resolution
  - Add the following to the security considerations for server name:

"Since it is possible for a client to present a different server_name during renegotiation, application server implementations that rely upon these names being the same MUST check to make sure the client did not present a different name during renegotiation. "

Use of SHA-1 without algorithm agility

- SHA-1 is used for trusted_CA_Keys and client_certificate_URL
- Proposed resolution

  Describe that the usage does not rely upon the cryptographic properties of SHA-1 in the security considerations section. The two cases probably need to be treated differently.

  "The usage of SHA-1 in the trusted_CA_Keys extensions in this document does not rely upon the properties of a cryptographic hash function. Algorithm agility is not provided because a cryptographic hash function is not required."

  Need text for client_certificate_URL