ECMQV Cipher Suites for TLS

draft-dugal-tls-ecmqv-00

Robert Dugal
and
Brian Minard
Draft Overview

- Full MQV Scheme [X9.63:2001]
- Authenticated and Unauthenticated Clients
- No Explicit Signature Generation
- ECDSA and RSA Certificate Support
- AES and 3DES Ciphersuites with SHA-1
Approach

- Use X9.63’s implicit signature to avoid explicit signatures
- Use ECC Cipher Suites for TLS for point compression and curve negotiation
- Use an ephemeral key instead of a static key for unauthenticated clients
Full MQV Scheme

TLS Client
(Scheme Responder V)

Server Static Public Key (QsU)

Client Static Public Key (QsV)

Server Ephemeral Public Key (QeU)

Client Ephemeral Public Key (QeV)

TLS Server
(Scheme Initiator U)
MQV Primitive

Inputs

- 2 Local Key-Pairs: \((ds_U, Qs_U), (de_U, Qe_U)\)
- 2 Remote Public Keys \(Qs_V, Qe_V\)

Actions

- \(\text{implicitsig}_U = de_U + (Qe_U \times ds_U) \pmod{n}\)
- \(P = h \times \text{implicitsig}_U \times (Qe_V + (Qe_V \times Qs_V))\)
- if \(P = 0\) output "invalid" and stop;
- otherwise \(z = xp\), the \(x\)-coordinate of \(P\)
Mutually Authenticated TLS Key Exchange

Client (V)
- Certificate
- ClientKeyExchange

QsU
QeU

Server (U)
- Certificate
- ServerKeyExchange
- CertificateRequest

QsV
QeV

CertificateVerify message is not sent.
Unauthenticated Client
TLS Key Exchange

Client (V)

Server (U)

QsU

QeU

QsV, QeV

Certificate

ServerKeyExchange

CertificateRequest*

ClientKeyExchange
Changes Since 00

- added an explanation of ECMQV--including a ladder diagram for the scheme itself
- proposed alternative wording in section 4.5
Anyone want support for DSA certificates?

Can this become a WG item?