

# 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)

TLS Server

(Scheme Initiator U)

Server Static Public Key ( $Q_{sU}$ )



Client Static Public Key ( $Q_{sV}$ )



Server Ephemeral Public Key ( $Q_{eU}$ )



Client Ephemeral Public Key ( $Q_{eV}$ )



# MQV Primitive

## Inputs

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

## Actions

- $implicitsig_U = de_U + (Qe_U \times ds_U) \pmod{n}$
- $P = h \times implicitsig_U \times (Qe_V + (Qe_V \times Qs_V))$
- if  $P = 0$  output “invalid” and stop;
- otherwise  $z = x_p$ , the x-coordinate of  $P$

# Mutually Authenticated TLS Key Exchange

Client (V)

Server (U)

$Q_{sU}$   
←

$Q_{eU}$   
←

Certificate

ServerKeyExchange

CertificateRequest

Certificate

$Q_{sV}$   
→

ClientKeyExchange

$Q_{eV}$   
→

CertificateVerify message is not sent.

# Unauthenticated Client TLS Key Exchange

Client (V)

Server (U)

$Q_{sU}$   
←

$Q_{eU}$   
←

ClientKeyExchange  
 $Q_{sV}, Q_{eV}$  →

Certificate

ServerKeyExchange

CertificateRequest\*

# Changes Since 00

- added an explanation of ECMQV--including a ladder diagram for the scheme itself
- proposed alternative wording in section 4.5



# Questions?

- Anyone want support for DSA certificates?
- Can this become a WG item?