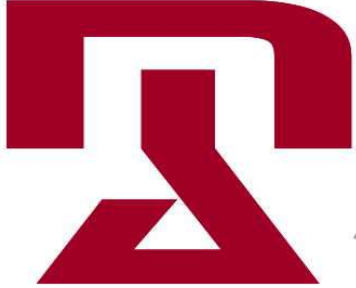
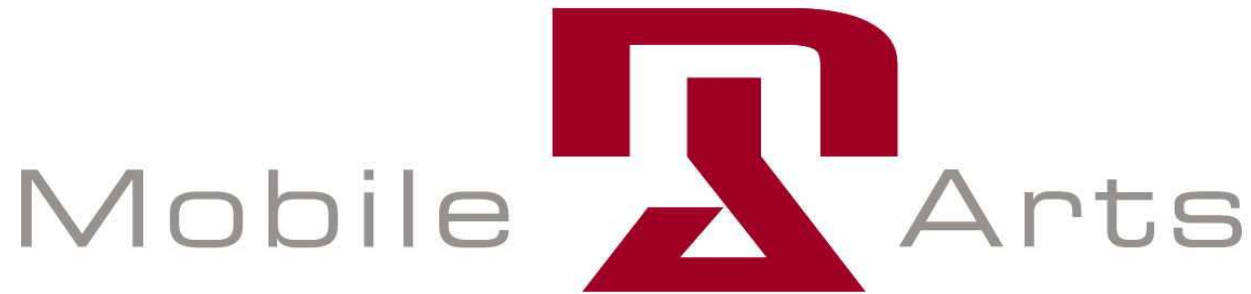


Mobile  Arts



An Erlang WTLS Implementation

Göran Oettinger

Erlang User Conference 2004

Introduction

▶ Master thesis

- Extending the SoWap WAP gateway to support Wireless Transport Layer Security



ROYAL INSTITUTE
OF TECHNOLOGY



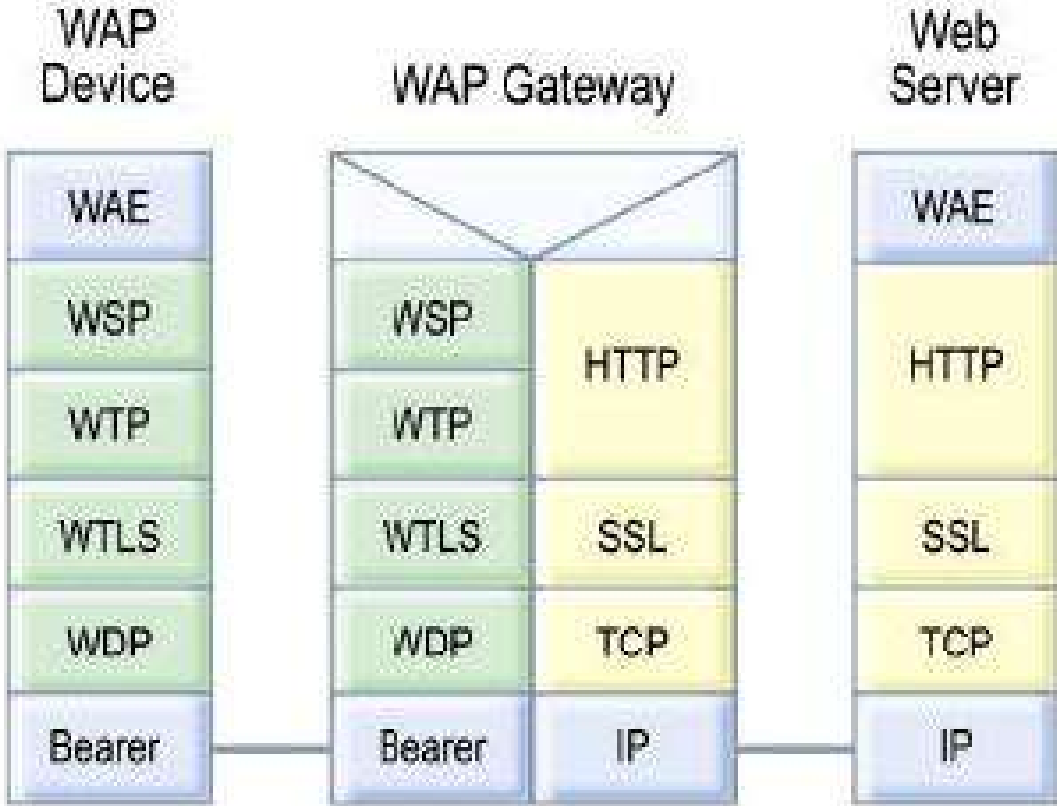
▶ Implementing WTLS

▶ Extending Erlang cypto library support

Background

- ▶ WAP – Wireless Application Protocol
- ▶ SoWap – Erlang Open Source WAP Gateway
 - History
 - Future

WAP Gateway



Wireless Transport Layer Security

- ▶ Security goals

 - Privacy

 - Integrity

 - Authentication

- ▶ WTLS vs TLS

 - Processor speed

 - Bandwidth

Wireless Transport Layer Security

▶ Cryptographic standards

Symmetric ciphers (bulk ciphers)

- DES, 3DES, RC5, IDEA

Asymmetric key exchange algorithms

- RSA, Diffie-Hellman, ECDH

Keyed hash algorithms (MAC)

- MD5, SHA

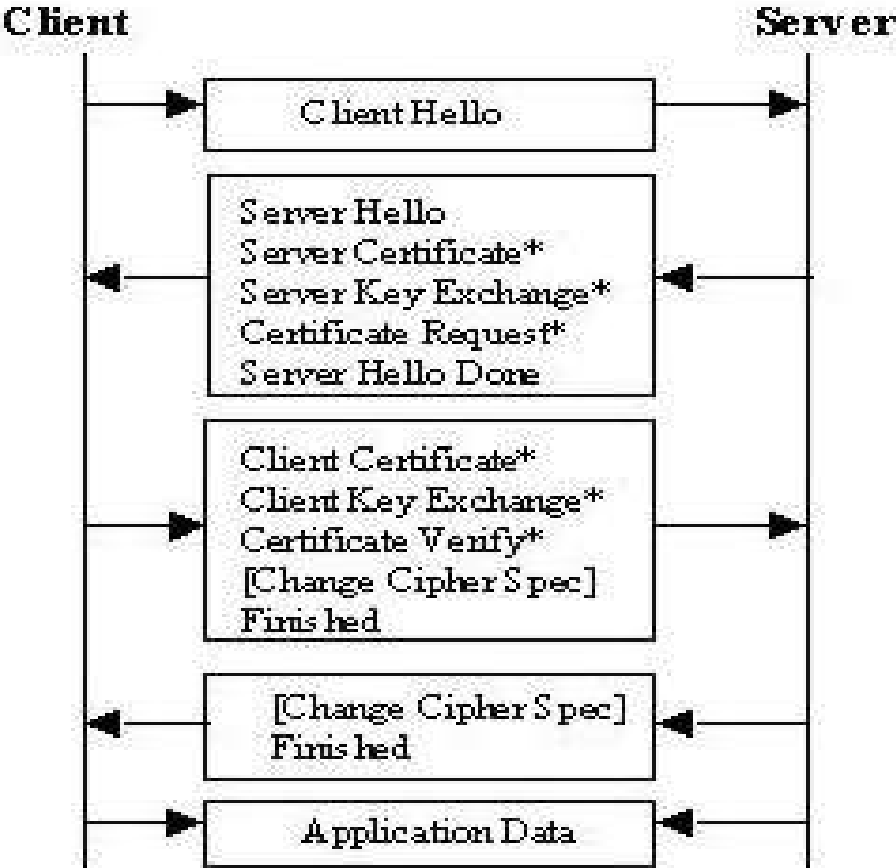
Certificates

- X.509, X9.68, WTLS Certificate

WTLS Handshake

- ▶ Negotiate security algorithms
- ▶ Exchange random values and security settings
- ▶ Exchange certificates
- ▶ Calculate secret

WTLS Handshake



WTLS in Erlang

- ▶ Advantages

 - Concurrency – many connections running
 - WTLS engine is a state machine - `gen_fsm`

- ▶ Disadvantages

 - Not enough crypto support

Erlang Crypto Library

▶ Supports

Bulk ciphers

- DES, 3DES

Keyed hash algorithms

- SHA, MD5

▶ WTLS also specifies

Bulk ciphers

- RC5, IDEA

Key exchange algorithms

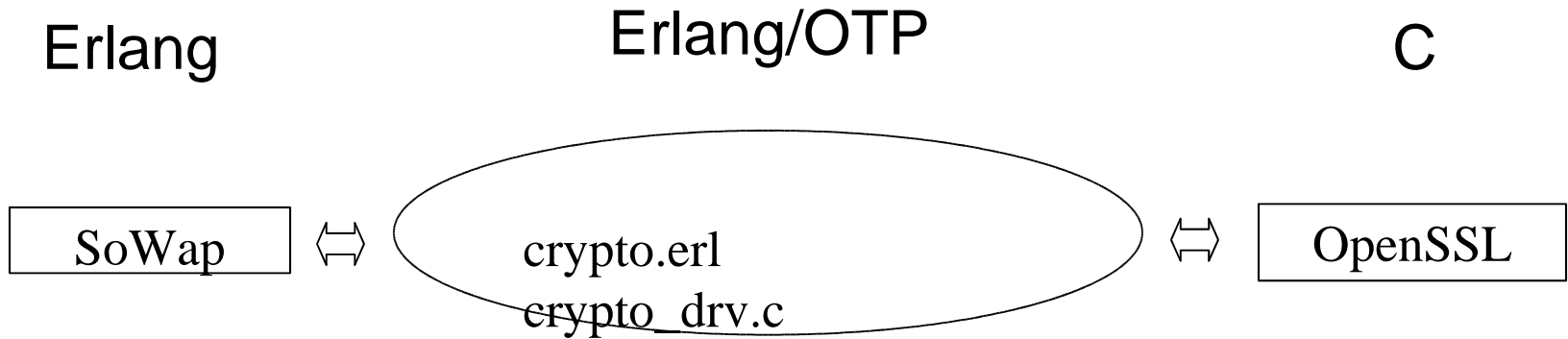
- RSA, Diffe-Hellman, ECDH

Erlang Crypto Library

- ▶ Extensions needed
 - RC5
 - RSA, Diffie-Hellman

- ▶ Overlooked algorithms
 - IDEA
 - ECDH

Erlang Crypto Library



OpenSSL

- ▶ Open Source Toolkit for SSL/TLS

 - Command line tool

 - SSL/TLS API

 - Crypto library

- ▶ OpenSSL Crypto Library

 - Blowfish, **DES**, IDEA, CAST, RC2, RC4, **RC5**

 - DSA, **RSA**, **DH**

 - MD2, MD4, **MD5**, MDC-2, RIPE-MD, **SHA**

Future

▶ To do:

- Certificate support
- Extensive testing with mobile devices
- Installation at TS Lab

▶ Further academic lab use?

Conclusion

- ▶ SoWap now supports WTLS
- ▶ Erlang crypto library extended