YODLEE

YODLEE

A Survey of WAP Security Architecture

Neil Daswani

neil@yodlee.com

Overview

- Security Basics
- Wireless Security
- WTLS & SSL
- WAP Security Models
- WIM, WMLScript, Access Control
- Summary
- References

Security Basics

- **Security Goals**
  - **Authentication**
  - **Confidentiality**
  - **Integrity**
  - **Authorization**
  - **Non-Repudiation**

Security Basics

- Cryptography
  - Symmetric: 3DES, RC4, etc.
  - Asymmetric: RSA, ECC
- Key Exchange
- Digital Signature
- Certificates
- PKI

Wireless Security

- **Link Layer Security**
  - GSM
  - CDMA
  - CDPD
- **Application Layer Security**
  - WAP: WTLS, WML, WMLScript, & SSL
  - iMode: N/A
  - SMS: N/A

Need for App Level Security

- **Bearer Independence**

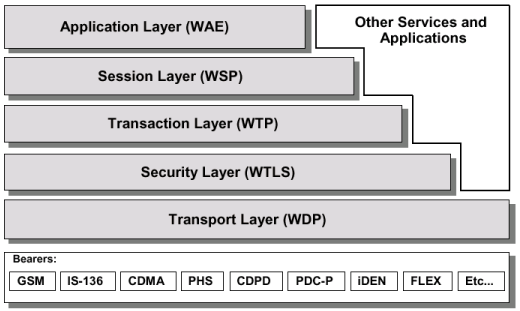
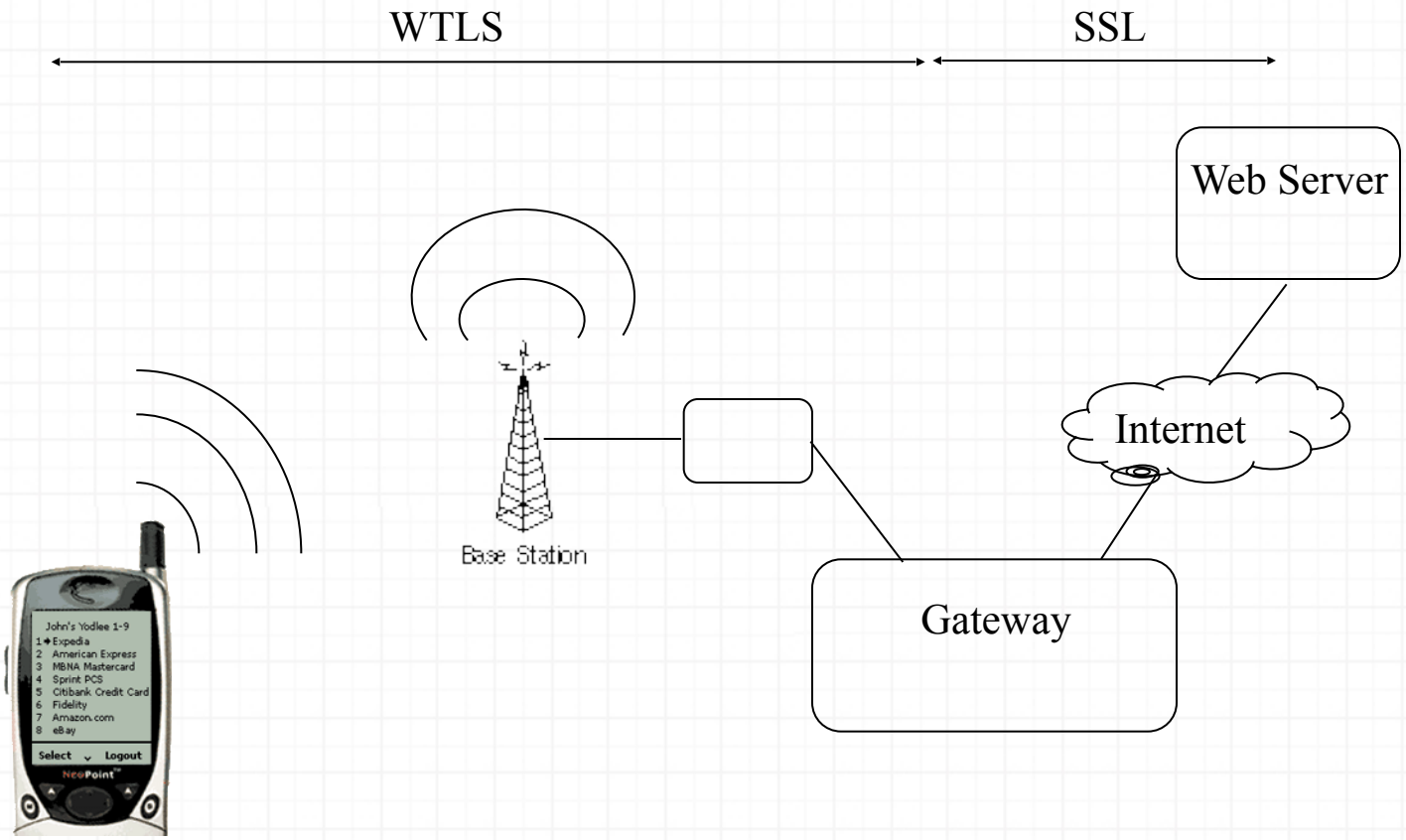


Figure 4. WAP Architecture

- **Security out to Gateway**
- **Advanced Security Goals (ie. Non-Repudiation)**

Basic WAP Architecture



WTLS & SSL

- **WTLS Goals**
  - **Authentication: Asymmetric Key Crypto**
    - **Class 1: No Authentication**
    - **Class 2: Server Authentication**
    - **Class 3: Mutual Authentication**
  - **Privacy: Symmetric Key Crypto**
  - **Data Integrity: MACs**

WTLS: Class 1

- **No Authentication**

```
ClientHello                 ---------->
                                                ServerHello
                            <----------         ServerHelloDone

ClientKeyExchange
ChangeCipherSpec
Finished                    ---------->

                            <----------         Finished

Application Data            <---------->        Application Data
```

WTLS: Class 2

- **Server-Authentication Only**

```
ClientHello                 ---------->
                                                ServerHello
                                                Certificate
                            <----------         ServerHelloDone
```

1. Verify Server Certificate

```
ClientKeyExchange
ChangeCipherSpec
Finished                    ---------->
```

2. Establish Session Key

```
                            <----------         Finished

Application Data            <---------->        Application Data
```

WTLS: Class 3

- **Mutual-Authentication**

```
Client Hello                ---------->
                                                ServerHello
                                                Certificate
                                                CertificateRequest
                            <----------         ServerHelloDone
Certificate
ClientKeyExchange  (only for RSA)
CertificateVerify
ChangeCipherSpec
Finished                    ---------->

                            <----------         Finished

Application Data            <---------->        Application Data
```

1. Verify Server Certificate

2. Establish Session Key

3. Generate Signature

TLS/SSL vs. WTLS

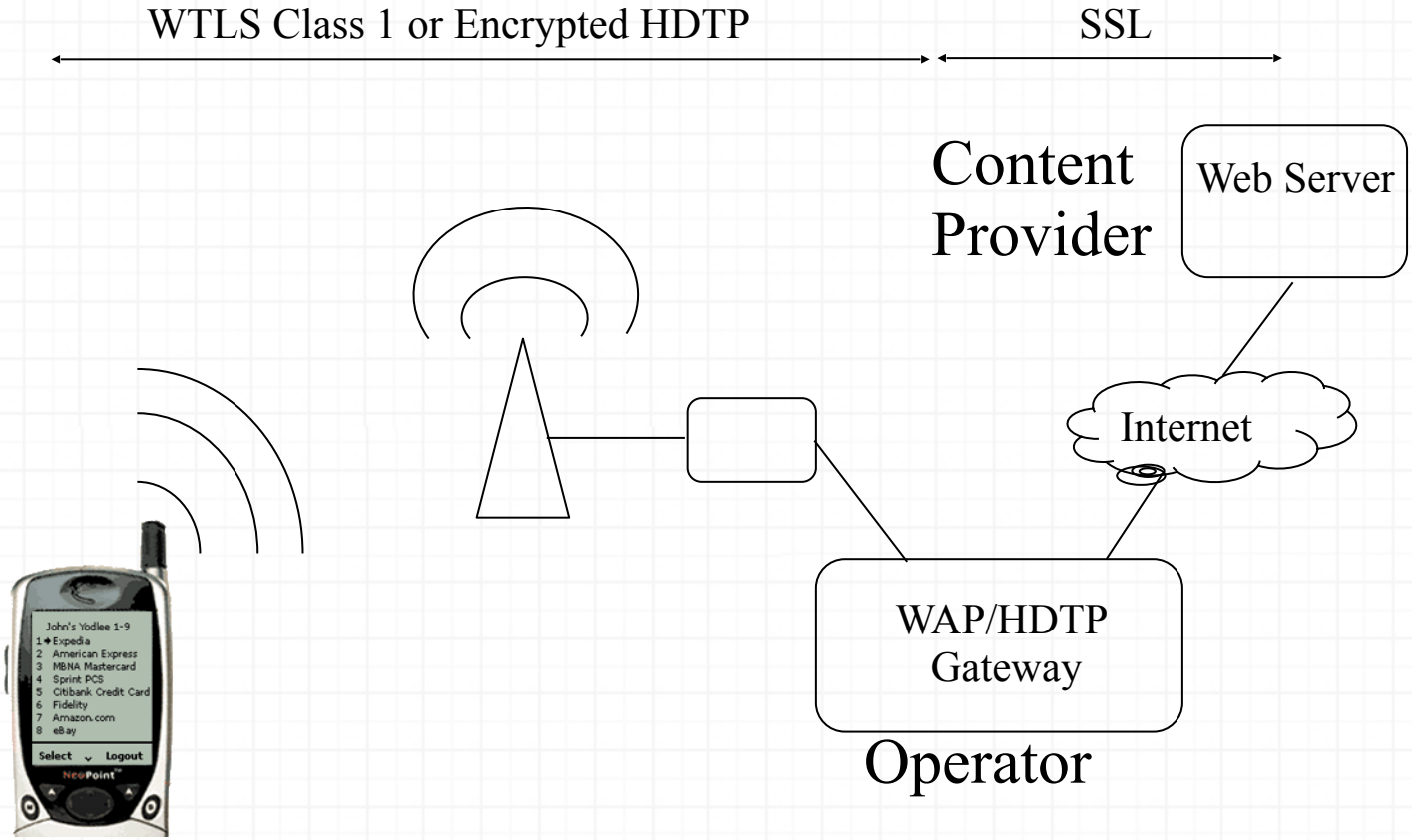
- WTLS supports ECC
- WTLS over WDP
  TLS over TCP
- Premaster secret is 20 bytes
  (vs. 48 in TLS/SSL)

WAP Security Models

- Operator Hosts Gateway
  - Without PKI
  - With PKI
- Content Provider Hosts Gateway
  - Static Gateway Connection
  - Dynamic Gateway Connection

Operator Hosts Gateway

- **Without PKI**

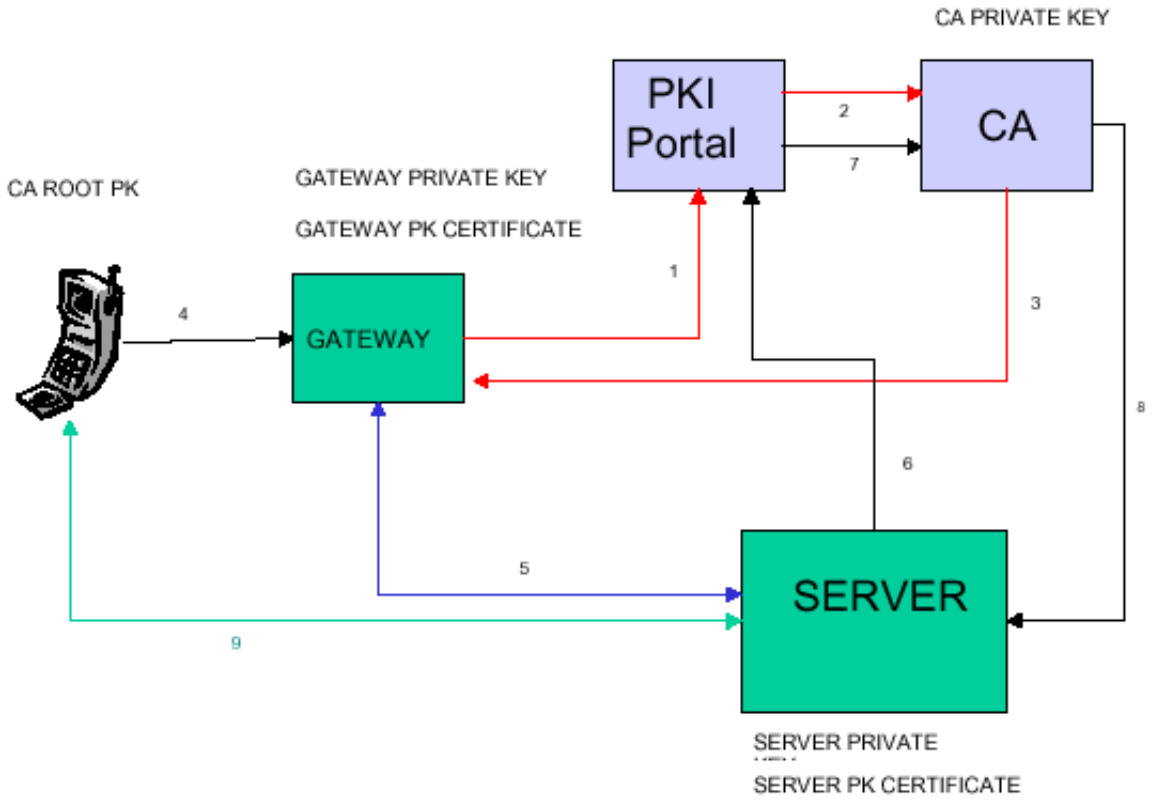


Operator Hosts Gateway

- **Without PKI:**
  - **Advantages**
    - **No extra work for Content Provider**
    - **No extra work for user**
    - **System only requires one logical gateway**
  - **Disadvantages**
    - **Content Provider must trust Operator (NDA)**
    - **Operator can control home deck**
    - **Operator can introduce advertising**

Operator Hosts Gateway

- **With PKI**

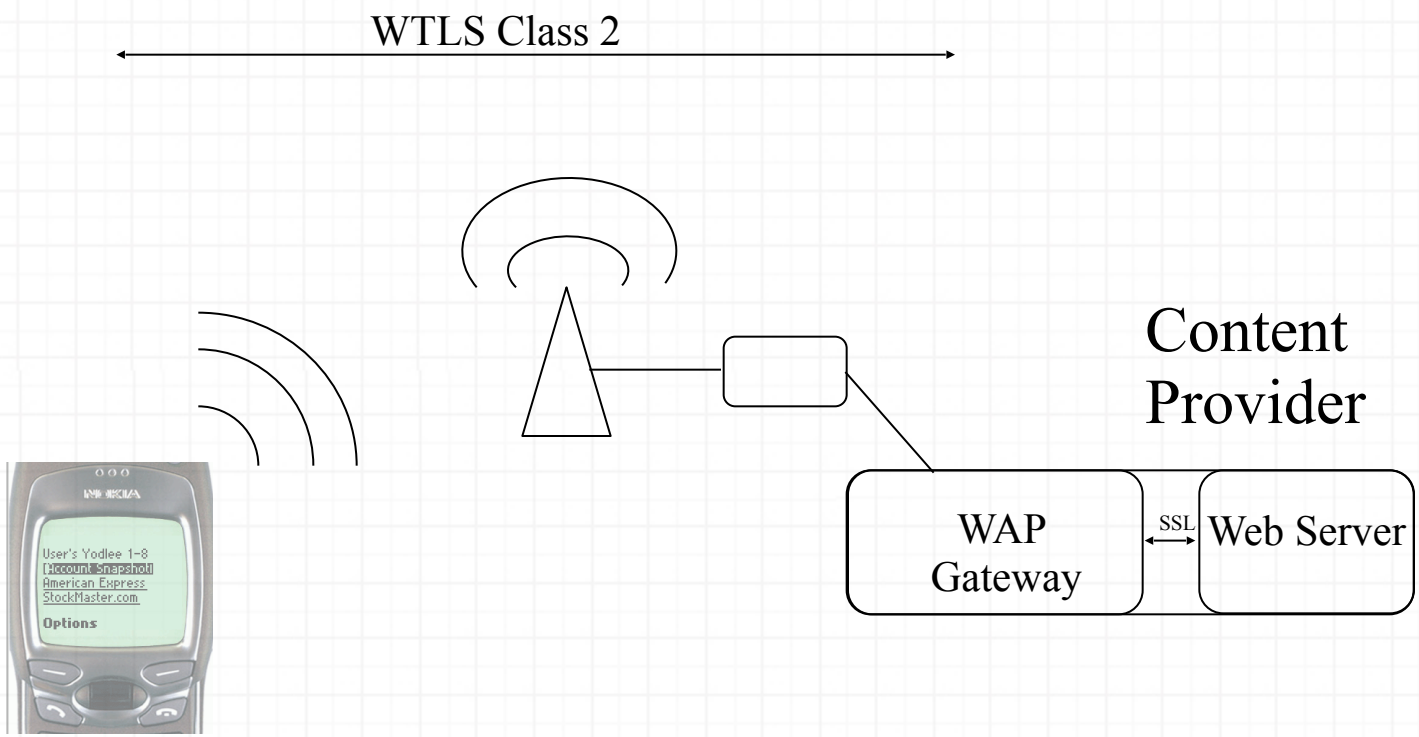


Operator Hosts Gateway

- With PKI:
  - Advantages
    - Content providers does not need to trust Operator.
  - Disadvantages
    - PKI Infrastructure must be in place.

Content Provider Hosts Gateway

- **Static Gateway Connection**

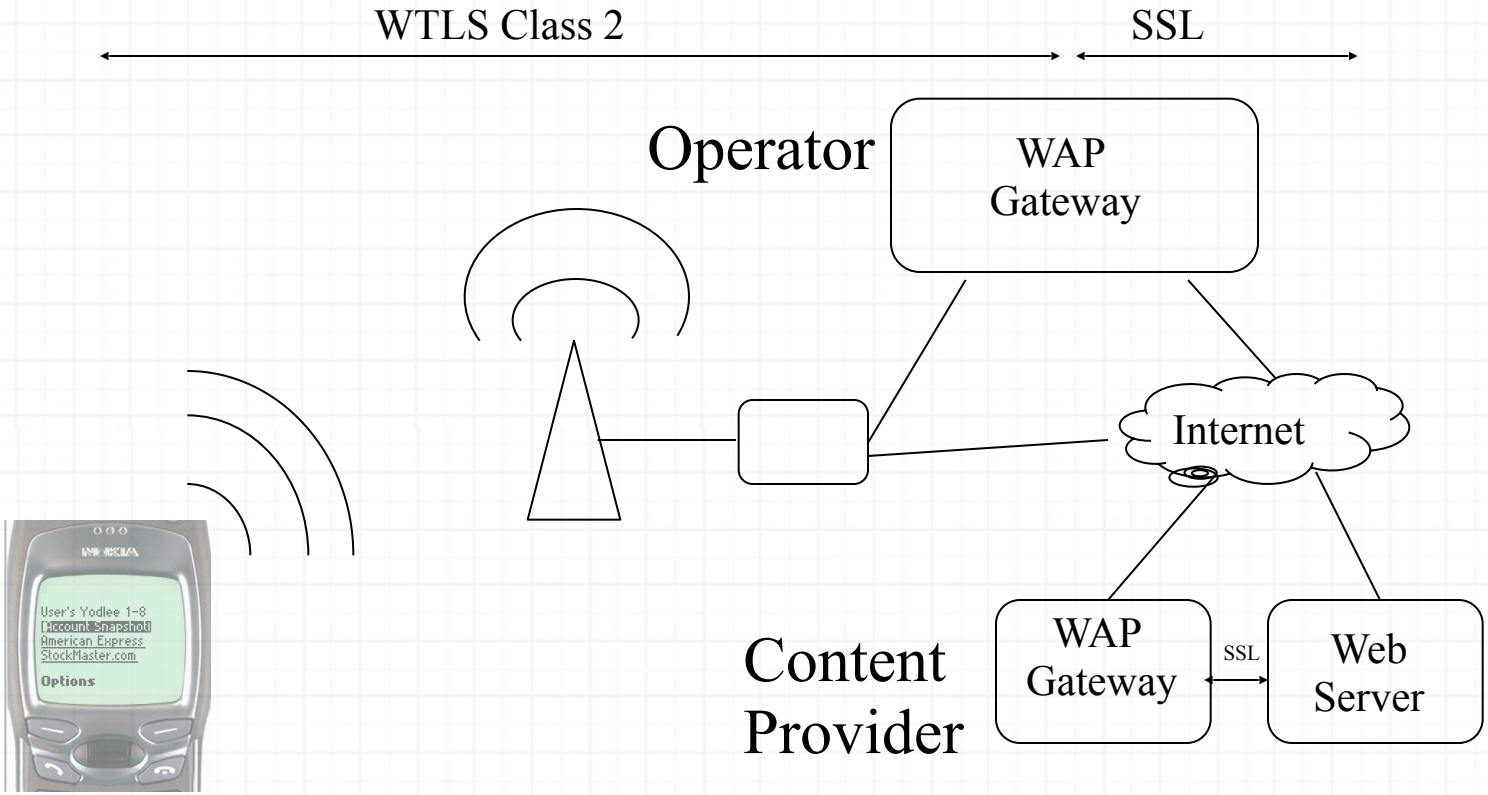


Content Provider Hosts Gateway

- **Static Gateway Connection**
  - **Advantages**
    - **Content Provider does not need to trust Operator**
    - **Content Provider can control home deck**
    - **OTA can be used to configure mobile terminal**
  - **Disadvantages**
    - **Mobile terminal may have limited number of gateway config sets (i.e., Nokia 7110 has 10)**
    - **Mobile Terminal needs to be configured.**
      - **OTA via WAP Push / SMS may not work with gateway / mobile terminal combination**
      - **Content Provider may have to pre-configure mobile terminals**

Content Provider Hosts Gateway

- **Dynamic Gateway Connection**



Content Provider Hosts Gateway

- Dynamic Gateway Connection
  - Advantages
    - Content Provider does not need to trust Operator.
    - Content Provider does not need to worry about mobile terminal config
  - Disadvantages
    - Operator needs to trust Content Provider.
    - Not deployed yet.

Restricting Gateway Access

- Consider the following attack:
  - Eve runs a “modified” WAP gateway
  - Eve fools a user into using her gateway
- Now, Eve can eavesdrop on all of the users requests and responses!
- To prevent this, check the gateway IP address in the HTTP request.

WIM: WAP Identity Module

- WIM must be tamper-resistant
- Stores Keys & Master Secrets
- Computes crypto operations
  - "unwrapping master secret"
  - client signature in WTLS Handshake
  - key exchange (ECC WTLS Handshake)
- Also:
  - Generates Keys
  - Stores Certificates (or their URLs)
    - CA & Root Certs
    - User Certs
- Can be implemented with SIM

WMLScript Crypto API

- **Non-repudiation**
- ***signedString = Crypto.signText (stringToSign, options, keyIdType, keyId)***

```
var foo = Crypto.signText("Bill of Sale\n------------------\n3
Bolognese $18.00\n1 Pepperoni  $7.00\n4 Lemonade   $6.00\n----
--------------\nTotal Price $31.00",
0, 1,
"\x37\x00\xB6\x96\x37\x75\xE3\x93\x48\x74\xD3\x98\x47\x53\x94\
x34\x58\x97\xB5\xD6");
// The application indicates the signature key
```

- **WIM can store signing key and compute signature**

WML Access Control

- **WML Deck-Level Access Control**

```
<wml>
<head>
<access domain="worldfaq.com" path = "/stats">
</head>
<card>
…
</card>
</wml>
```

- **WMLScript Access Control**

```
use access
        domain domain_name |
        path path_name |
        domain domain_name path path_name;
```

- **use access domain "worldfaq.com" path "/stats"**

Summary

- Gateway position & configuration allows for different trust models
- Security at multiple levels
  - Link Layer (depends on bearer)
  - App Layer
    - Authentication, Confidentiality, and Integrity: WTLS
    - Authorization: App-dependent, or WML <access> and WMLScript use access pragma
    - Non-Repudiation: WML signText

References

- C. Arehart, N. Chidambaram, S. Guruprasad, et. al. Professional WAP. Wrox Press, 2000. ISBN 1-861004-0-44
- D. Margrave, GSM Security and Encryption
- WAP-100, Wireless Application Protocol Architecture Specification
- WAP-191, Wireless Markup Language Specification
- WAP-193, WMLScript Language Specification
- WAP-199, Wireless Transport Layer Security Specification
- WAP-198, Wireless Identity Module
- WAP-161, WMLScript Crypto API Library
- WAP-187, WAP Transport Layer E2E Security Specification
- WAP-217, WAP Public Key Infrastructure Definition