certicom™

Complete WAP Security

from Certicom

Abstract

The Wireless Application Protocol (WAP) is a leading technology for companies trying to unlock the value of the Mobile Internet.

Certicom products and services provide complete WAP security solutions today for all of those players involved in bringing the Internet to the mobile end-user — including content providers, equipment manufacturers, network operators, application service providers and enterprises.

Contents

WAP

The WAP (Wireless Application Protocol) is a suite of specifications that enable wireless Internet applications; these specifications can be found at http://www.wapforum.org). WAP provides the framework to enable targeted Web access, mobile e-commerce, corporate intranet access, and other advanced services to digital wireless devices, including mobile phones, PDAs, two-way pagers, and other wireless devices. The suite of WAP specifications allows manufacturers, network operators, content providers and application developers to offer compatible products and services that work across varying types of digital devices and networks. Even for companies wary of WAP, individual elements of the WAP standards can prove useful by providing industry-standard wireless protocols and data formats.

The WAP architecture is based on the realization that for the near future, networks and client devices (e.g., mobile phones) will have limited capabilities. The networks will have bandwidth and latency limitations, and client devices will have limited processing, memory, power, display and user interaction capabilities. Therefore, Internet protocols cannot be processed as is; an adaptation for wireless environments is required. The entire suite of WAP specifications are derived from equivalent IETF specifications used on the Internet, modified for use within the limited capabilities in the wireless world.

Furthermore, the WAP model introduces a Gateway that translates between WAP and Internet protocols. This Gateway is typically located at the site of the mobile operator, although sometimes it may be run by an application service provider or enterprise. The two architectural models can be seen in Figures 1 and 2 below.

Security Solutions for WAP

As the Mobile Internet market is being formed, new value chains and players are emerging. These players include the mobile operator, enterprises, content providers, wireless application service providers and end-users.

Certicom offers complete security solutions for all of the players involved in the value chain from content to end-user. Certicom products are fully compliant with WAP specifications.

Authentication
The property that the identity of a communicating party is known. This ensures that the source or the destination of the data is trusted.

Confidentiality
The property that data is readable only by the sender and the intended recipient. This is achieved by encrypting all data being transferred.

Message Integrity
The property that the data received is guaranteed to be indentical to the data that was sent. This prevents a third party from modifying the data during transmission.

Non-repudiation

The property that the sender of a given piece of data cannot later dey having sent it.

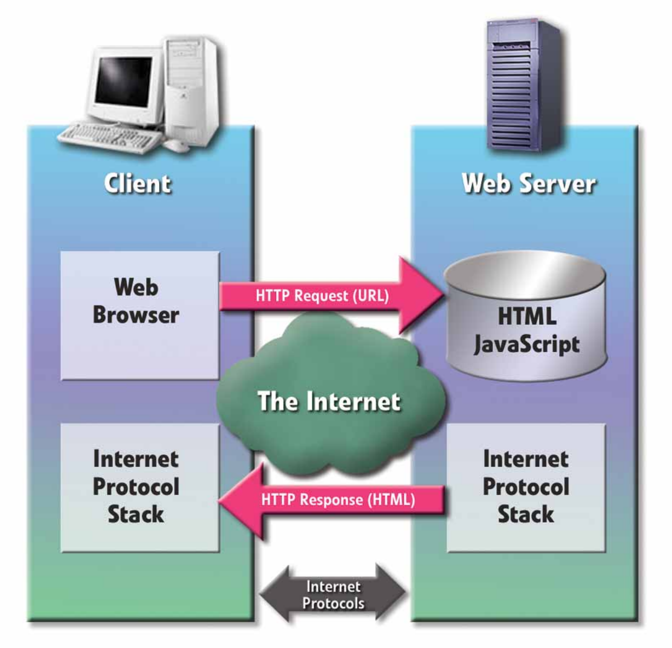

Figure 1. The Internet Architecture

There are two primary components of WAP security: transport level security and application level security.

- Transport level security, also called "channel security" since the focus is on the point-to-point communications channels, is provided via WTLS (Wireless Transport Layer Security) and SSL (Secure Sockets Layer).
- End-to-end transactional security is provided via application-level security functions (digital signatures and field-level encryption) and the associated Public Key Infrastructure (PKI).

These two levels of security together address the concerns that any security model will have, including authentication, confidentiality, message integrity, and non-repudiation.

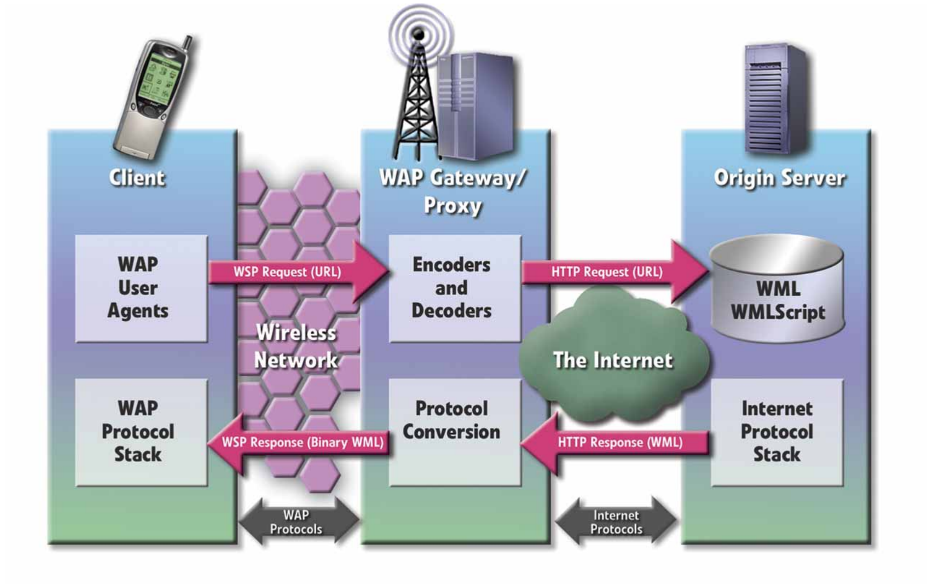

Figure 2. The WAP Architecture

Channel Security

Channel security in a typical WAP architecture is illustrated in Figure 3. The transport layer from the client to the content server is split into two sections by the WAP Gateway, with WAP protocols on one side, and Internet protocols on the other. The transport layers are WDP on the WAP side and TCP on the Internet side; the respective transport layer security protocols are WTLS and SSL (or its IETF sibling, TLS).

TLS is the IETF standard for transport layer security on the Internet. WTLS is a variation of this Internet standard designed specifically for low bandwidth, high latency and connectionless networks. Several changes to TLS were made, such as adding highly efficient cryptographic algorithms such as elliptic curve cryptography (ECC) and the definition of a compact public key certificate format. There are three modes of operation of WTLS, corresponding to three ascending levels of authentication. Class I WTLS includes no authentication, Class II WTLS includes authentication of the server to the client, and Class III WTLS includes mutual authentication, i.e., authentication of both the server and the client to each other.

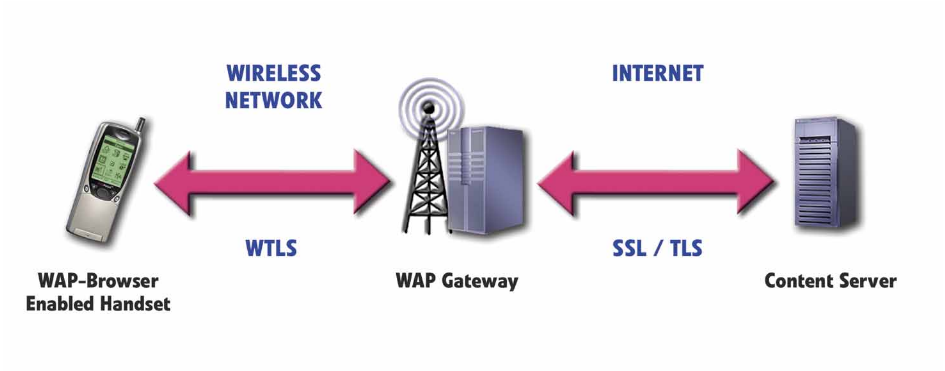

Figure 3. WAP Channel Security

Certicom enables transport level security on the channel between the WAP client and WAP Gateway via the WTLS Plus™ toolkit, and on the channel between the WAP Gateway and the Internet servers via the SSL Plus™ toolkit. By using WTLS Plus™ and SSL Plus™, a sequence of two secure channels are established between the client and the content server; a WAP Gateway is responsible for bridging the two secure connections.

The Gap in WAP

The bridging of two secure connections at the WAP Gateway, where the WAP Gateway is run by the operator, has been termed “the gap in WAP” by some media, since the data is decrypted for a brief period at the WAP Gateway. Whether this is a security concern depends upon two factors: the security policies implemented by the operator for access to the WAP Gateway and the sensitivity of the information being transferred. Most operators run secure facilities, since authentication of a cellular call requires storage of secret keys and a reputable operator is aware of the importance of keeping such information secure. However, there may still be some data that is highly sensitive to the content provider, and the operator doesn’t want the liability associated with access to the plaintext.

In some cases, this security gap can be addressed at the transport level if the content originator operates its own “enterprise” WAP Gateway, so that WTLS packets can be routed through or around the wireless carrier’s Gateway to the enterprise Gateway. In other cases, however, the security needs can only be met by using application-level security.

Application-Level Security

There are two main situations where application-level security is needed in addition to transport-level security. First, security might need to be carried beyond the endpoint of the transport-level protocols, for example to carry a signed transaction to a financial institution's back-end legacy system. Second, the architecture of the wireless network might include one or more intermediate nodes that need to process the presentation layer without access to confidential application information; for example, there may be a translation server converting between HTML and WML, to which unencrypted account numbers should not be exposed. The solution in all these cases is application-level security.

WAP enables such capability via use of a crypto API, referred to as the WMLScript Crypto API. WMLScript is a simple script language that allows client-side processing, and instructs the client device to invoke application-level functions. Digital signatures are created by the client using the WMLScript *signText* function. To use *signText*, each client must have a private-public key pair, which implies the presence of a PKI to support issuance and management of public key certificates. Although *signText* is currently the only function in the Crypto API, the future addition of encryption functionality will likely follow; then data such as bank account information, can be encrypted end-to-end between the client and the content provider.

Certicom supports end-to-end transactional security by providing the following products and services:

- Digital signature creation/verification, encryption/decryption, and management of keys and certificates on client devices via the Trustpoint Client.
- Signature verification and encryption/decryption capability on the application server via the Security Builder™ SDK and the Trustpoint/Java toolkit.
- Wireless PKI support via the Trustpoint™ PKI Portal/Registration Authority and the Trustpoint Certificate Authority.
- Certificates for wireless clients, WAP Gateways, and content servers via the MobileTrust service.

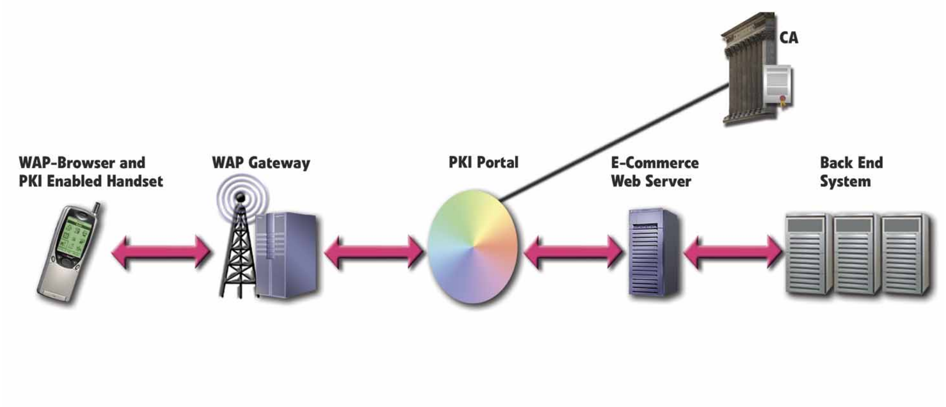

Figure 4. WAP Network with PKI and Client Authentication

WAP PKI

WAP has introduced a number of innovations to tailor PKI for a wireless environment:

- Certificate formats : The general WAP PKI model is adaptable to many certificate types including X.509v3, X9.68 (currently in draft) and the newly defined WTLS certificate format.
- Certificate request protocols: The request for a short-lived certificate is a simple HTTP GET to a URL which was supplied by the CA.
- WAP profiles of X.509 certificates
- Use of certificate URL's: Rather than pass client certificates over-the-air, the new approach is to pass certificate URL's over-the-air, which saves bandwidth and still allows the client certificate to be retrieved by all relying parties.

The Evolution of WAP Security

The current approved specification for WAP is WAP 1.2. Future revisions will address functions such as billing, WAP in 3G systems, and location-based services. Certicom is an active participant in the WAP Forum and is contributing to the development of these standards.

Certicom WAP Products and Services

WTLS Plus™

Certicom's WTLS Plus™ allows developers to build WAP communication security into their implementations. It encompasses both client and server components, enabling the deployment of a complete secure WAP communications infrastructure. Available worldwide, WTLS Plus™ can be ported to virtually any client or server platform. WTLS Plus was the first WTLS toolkit on the market and is the only commercially available WTLS to support Class III operation, which includes client authentication. WTLS Plus is also the only commercially available WTLS to support all three public-key algorithms in the standard: Diffie-Hellman, Elliptic Curve, and RSA.

SSL Plus™

Certicom's SSL Plus™ is the industry leading SSL implementation and can be easily integrated into any WAP Gateway or content server for securing the communication between the Gateway and the Internet. SSL Plus™ includes TLS, the IETF standard for transport-level security.

Security Builder™

Certicom's Security Builder™ is a software toolkit that contains a wide array of cryptographic primitives necessary to enable various security functions. For example, it enables digital signature verification, allowing content providers to verify a signed transaction received from a WAP client device. Security Builder™ can also be used by WAP Gateways and clients developing their own WTLS by adding the efficiency of ECC to legacy products and enabling mutual client and server authentication.

Trustpoint™ Client

Certicom's Trustpoint Client is a software toolkit designed to enable client-side security in the highly constrained environments of wireless devices. The toolkit allows both certificate management and basic cryptographic functionality, and follows WAP standards for both application layer security and wireless PKI.

Trustpoint™ PKI Portal/RA

The Trustpoint PKI Portal is a full registration authority (RA) that provides interoperability between wireless clients and deployed PKIs by converting the highly efficient WAP certificate request protocols to the protocols that are understood by existing PKIs. This Portal can be located with the WAP Gateway itself or as another server on the network.

Trustpoint™/Java Toolkit

Providing comprehensive computing platform coverage through Java libraries, Trustpoint™/Java includes a complete set of tools for deploying and managing a PKI, with a special focus on flexibility and the efficiencies required for deployment in a wireless infrastructure. Also containing tools for basic crypto functionality, Trustpoint /Java is fully compliant with JDK Versions 1.1.7 and 1.2.

MobileTrust™ Managed Certificate Service

Certicom's MobileTrust™ is the first outsourced Certificate Authority designed to enable PKIs for mobile devices. An operator or ASP may outsource the CA function to MobileTrust, while still operating the PKI Portal or RA. MobileTrust™ provides Certificates for WAP Gateways, content servers, and WAP client devices. MobileTrust™ certificates can optionally be branded by the operator or ASP.

WAP Identity Module (WIM) Solutions

For WIM-based WAP client implementations, Certicom provides the necessary cryptographic primitives, including those required for creating a secure WTLS connection and for end-to-end client authentication. Using Certicom's ECC, WIM implementations can enable client authenticated WAP security functions cost-effectively, including on-board key generation.

Integration Services

Certicom offers comprehensive assistance to its customers for integrating various security components that comprise a complete solution. These services include training, custom development, security analysis, and policy customization for building a PKI. In addition, Certicom offers support and maintenance packages for all its products.

certicom™

www.certicom.com

Certicom Office Locations

25801 Industrial Blvd.
Hayward, CA 94545
USA
Tel: 510.780.5400
Fax: 510.780.5401

5520 Explorer Drive 4th Floor
Mississauga, Ontario, L4W 5L1
Canada
Tel: 905.507.4220
Fax: 905.507.4230

Sales Support:
Tel: 510.780.5400
Fax: 510.780.5401
Email: **sales@certicom.com**

Application Engineering and Customer Support:
Tel: 1.800.511.8011
Fax: 1.800.474.3877
Email: **support@certicom.com**

Investor Inquiries:
Contact Starla Ackley
510-780-5404
Email: sackley@certicom.com

wap wp 001-1