Wireless Public-Key Infrastructure

Abstract

The WAP protocol enables M-Commerce by defining the standards by which internet data moves to and from wireless devices. This paper provides an overview of the WAP environment and its relation to the Internet, the security standards specified for WAP and how PKI standards and technologies have been adapted to meet M-Commerce security requirements.

CONTENTS

Overview

Wireless communications provide convenience over traditional wired communications in terms of demands for the user's physical location and size of the access device. This is because wireless-access devices (e.g. cellular telephones, pagers, personal-digital assistants) need not be tethered to networks via physical wires and are small enough to be carried on one's person, allowing their users to be mobile. Until recently, wireless devices have mainly been used for sending/receiving person-to-person voice conversations and text messages. Now, due to their convenience and widespread use, there is significant demand to use wireless devices on the Internet. Meeting this demand are the *Wireless Application Protocol (WAP)* standards as specified by the *WAP Forum*. WAP standards define a wireless-application framework and networking protocols for personal wireless devices. The purpose of the WAP standards is to bring more advanced data services such as Internet content and transactions to wireless devices. Because WAP defines the standards by which Internet data moves to and from a wireless device, it makes e-commerce possible from wireless devices. The term "Mobile Commerce" or m-commerce refers to e-commerce transactions involving a wireless device. M-commerce and e-commerce have their own specific requirements for security. These security requirements are best met with cryptographic technology and Public-Key Infrastructure (PKI) services. PKI encompasses the necessary cryptographic technology and a set of security management standards that are widely recognized and accepted for meeting the security needs of e-commerce. (For more information on security requirements of e/m-commerce refer to *Certicom: Public-Key Infrastructure Technology and Concepts, November 2000.*)

The WAP Environment

The best analogy for the WAP environment is the *World Wide Web (Web)* environment. The Web environment consists of three primary components: a *Web Client*, an *Internet Protocol (IP)* network, and a *Web Server*. Web components communicate over IP networks like the Internet using HyperText Markup Language (HTML) data, as in Fig. 1:

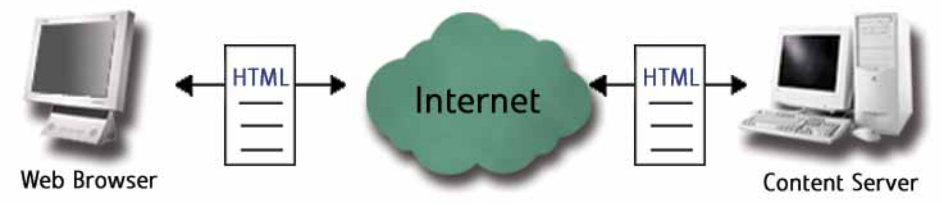

Fig. 1. Components of the Web environment.

There are three primary differences between the WAP and Web environments:

(1) Wireless end-user devices have significantly less processing power as compared to the common Web end-user device (a personal computer) wireless devices have much

- less powerful CPUs
- less memory
- less storage for data and programs
- less network bandwidth
- smaller displays

(2) Limited processing power in wireless devices means that services and software in the WAP environment must be extremely efficient, requiring minimal CPU cycles, memory, and storage. Likewise data objects and transactions must be compact, requiring only small amounts of storage, memory, and processing cycles. Therefore, WAP protocols are much more efficient than Web-based protocols and the two are not naturally interoperable.

(3) Since Web-based and WAP-based protocols are not directly interoperable, a component known as the WAP Gateway is needed in order to translate Web-based protocols to/from WAP-based protocols.

Wireless-to-Internet

WAP extends the reach of the Internet to the wireless environment. The WAP-Internet environment consists of a *WAP Client*, a *Wireless Network*, a *WAP Gateway*, an *IP network* and a *Content (Web) Server*. The WAP Client communicates with the WAP Gateway using Wireless Markup Language (WML) data transmitted over a wireless network. The WAP Gateway translates WML data to/from HTML data and also relays the data between the wireless and wired network and communicates with the Web Server. The primary components and general data flow in the WAP-Internet environment are shown in Fig. 2.

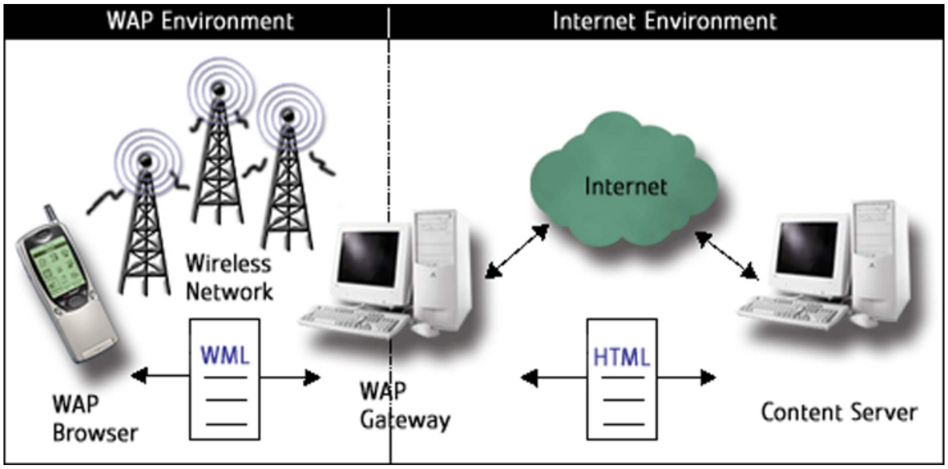

Fig. 2. Components in the WAP-Internet environment

WAP Security

WAP encompasses four standards that apply security at the application, transport and management levels in the wireless environment. These standards are known as

- the *WAP Identity Module (WIM)*
- the *WML Script Crypto API (WMLSCrypt)*
- the *Wireless Transport Layer Security (WTLS)*
- the *Wireless Application Protocol PKI (WPKI)*

WIM

The WAP Identity Module is a tamper resistant computer chip that optionally resides in the WAP device (the cellular phone, PDA, etc.). It can store key material (like the PKI root public key and the user's private key). WIMs are most commonly implemented using smart card chips. Smart card chips have memory and storage for data and programs.

WMLSCrypt

WML Script Crypto API (WMLSCrypt) is an application programming interface that allows access to basic security functions in the WML Script Crypto Library (WMLSCLib), such as key pair generation, digital signatures and the functions that process objects commonly found in the PKI (e.g., keys and public-key certificates). WMLSCrypt allows WAP applications to access and use the security objects and basic security services used and managed by the other WAP security standards. The basic functions in the WMLSCrypt and WMLSCLib include

- generate key pairs
- store keys and other personal data
- control access to stored keys and data
- generate and verifying digital signatures
- encrypt and decrypt data

WML Script can utilize an underlying WIM Module to provide the crypto functionality.

WTLS

Wireless Transport Layer Security is a transport-level security protocol based on the Internet security protocol known as Transport Layer Security (TLS). WTLS can authenticate communicating parties and encrypt and check the integrity of the WML data when it is in transit. WTLS has been optimized for use in wireless devices that rely on narrow bandwidth wireless networks. WTLS is a cryptograpy-based, PKI-enabled protocol that provides the following security services to WAP applications:

- **Authentication:** verify the identity of an entity prior to an online exchange, transaction, or allowing access to resources. Since WTLS is PKI-enabled it may use *digital signatures* and *public-key certificates* to authenticate individuals, servers or nodes.
- **Privacy:** prevents eavesdropping or unauthorized access. WTLS is capable of encrypting the WAP data between communicating parties and because it is PKI-enabled it can support one-to-many communication encryptions using an authenticated and different encryption key for each communicating party.
- **Integrity:** prevents data tampering, ensures that data is not altered, either by accident or on purpose, while in transit or in storage. WTLS employs data fingerprints using a cryptographic technique called hashing that detects data modifications.

- **Denial of Service Protection:** makes typical service denial attacks harder to accomplish. WTLS contains services that detect and reject data that has been replayed or not successfully verified.

WPKI

Wireless Application Protocol PKI (WPKI) is not an entirely new set of standards for PKI; it is an optimized extension of traditional PKI for the wireless environment. To learn more about traditional PKI, see: *Certicom: Public-Key Infrastructure Technology and Concepts, November 2000.* WPKIs, like all PKIs, enforce m-commerce business policies by managing relationships, keys and certificates. WPKI is concerned primarily with the policies that are used to manage E-Business and security services provided by WTLS and WMLSCrypt in the wireless application environment. In the case of wired networks, IETF PKI standards are the most commonly used; for wireless networks, WAP Forum WPKI standards are the most commonly used.

WPKI Architecture and Data Flow

Say a user not yet registered with a PKI attempts to connect to a service provider (content server). Since the service provider requires digital signatures on its transactions and/or secure communications, it notifies the user that it must contact a PKI Portal (and provides PKI ID information - e.g. URL, CA-service name, etc.). The diagram in Fig. 3 indicates the flow starting from the next step in the process.

Primary WPKI Components

As shown here, WPKI requires the same components used in traditional PKI:

- End-Entity Application (EE)
- Registration Authority (RA)
- Certification Authority (CA)
- PKI Directory

However, in WPKI, the EE and RA are implemented a bit differently, and a new component referred to as the *PKI Portal* is also required.

- **The EE in WPKI** is implemented as optimized software that runs in the WAP device. It relies on the WMLSCrypt API for key services and cryptographic operations. It is responsible for the same functions as the EE in traditional PKI including

- generate, store and allow access to a user’s public key pair
- complete, sign and submit first-time certificate applications
- complete, sign and submit certificate-renewal requests
- complete, sign and submit certificate-revocation requests
- search for and retrieve certificates and revocation information
- validate certificates and read the certificate contents
- generate and verify digital signatures

- **The PKI Portal** is a networked server, like the WAP Gateway, it logically functions as the RA and is responsible for translating requests made by the WAP client to the RA and CA in the PKI. The PKI Portal will typically embed the RA functions and interoperate with the WAP devices on the wireless network and the CA on the wired network.

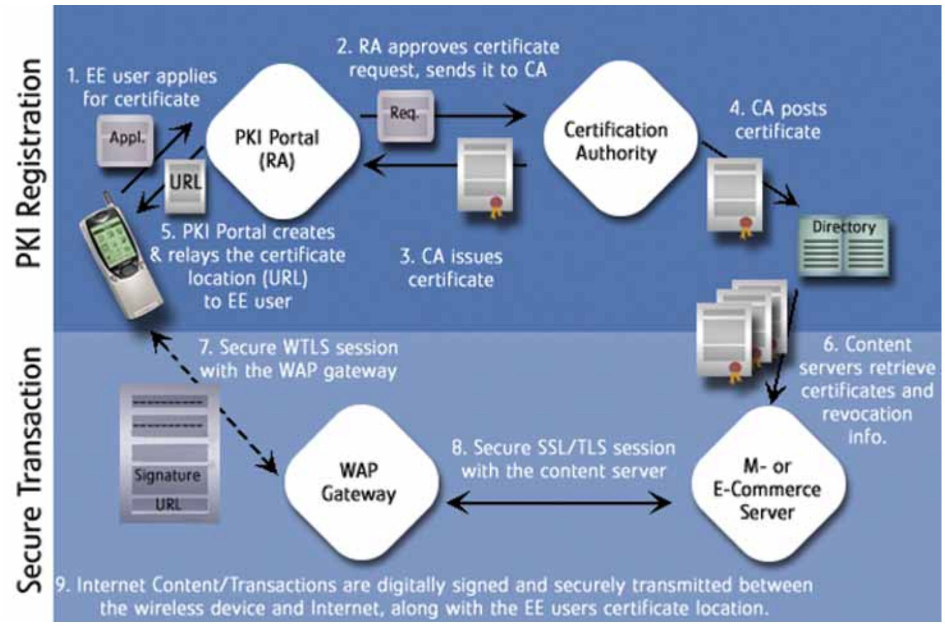
PKI Registration
Secure Transaction
1. EE user applies for certificate
Appl.
URL
PKI Portal (RA)
2. RA approves certificate request, sends it to CA
Req.
Certification Authority
4. CA posts certificate
Directory
5. PKI Portal creates & relays the certificate location (URL) to EE user
3. CA issues certificate
7. Secure WTLS session with the WAP gateway
6. Content servers retrieve certificates and revocation info.
Signature
URL
WAP Gateway
8. Secure SSL/TLS session with the content server
M- or E-Commerce Server
9. Internet Content/Transactions are digitally signed and securely transmitted between the wireless device and Internet, along with the EE users certificate location.

Fig. 3. The major technical components and operational flow of WPKI.

Optimization in WPKI

Just as WML is in reality optimized HTML and WTLS is optimized TLS, WPKI is an optimization of the traditional IETF PKIX standards for the wireless environment. In particular, it has optimized the

- PKI protocols
- certificate format
- cryptographic algorithms and keys

WPKI Protocols

The traditional method used to handle PKI service requests relies on the ASN.1 Basic Encoding Rules (BER) and Distinguished Encoding Rules (DER). BER/DER require more processing resources than a WAP device should effectively have to handle. WPKI protocols are implemented using WML and the WML Script Crypto API (WMLSCrypt). WML and the *signText* function in WMLSCrypt provide for significant savings when encoding and submitting PKI service requests as compared to the methods used in traditional PKI.

WPKI Certificate Format

The authors of the WPKI certificate format specification sought to reduce the amount of storage required for a public-key certificate. One of the mechnisms was to define a new certificate format (WTLS Certificate format) for server side certificates, which significantly reduce the size as compared to a standard X.509 certificate. Another significant reduction in the WPKI certificate can be attributed to *Elliptic Curve Cryptography (ECC).* With ECC, the savings in the overall size of the certificate is typically more than 100 bytes due to the smaller keys needed for ECC vs. other signature schemes. WPKI has also limited the size of some of the data fields of the IETF PKIX certificate format. Because the WPKI certificate format is a sub-profile of the PKIX certificate format, it is possible to maintain interoperability between standard PKIs.

WPKI Cryptographic Algorithms and Keys

While traditional signature schemes are optionally supported by the WAP security standards, they are viewed as impractical to implement in the wireless environment from a performance and resource viewpoint. Traditional signature schemes demand much more processing, memory, and storage resources in the WAP device when compared to the resource requirements of more efficient cryptography–ECC. ECC techniques are recognized as the most optimized, and therefore the best suited for supporting security in the wireless environment. As previously mentioned, the keys for elliptic curve are typically on the order of six (6) times smaller (163 bits vs. 1024 bits) than equivalent keys in other signature schemes. This creates great efficiencies in key storage, certificate size, memory usage and digital signature processing. ECC is fully supported by the WAP security standards and has been widely accepted by WAP device manufacturers.

Conclusions

Wireless communications play an increasingly important role in e-commerce. The wireless environment is no longer isolated; the WAP standards have made it possible to extend Internet content and transactions to wireless devices. Security requirements of e-commerce remain the same in both the wired and wireless environment and PKI plays an important role in meeting those requirements. WPKI is an extension of, and includes most of the technologies and concepts that are present in traditional PKI. WPKI, like all security and application services within the WAP environment, must be optimized using more efficient cryptography and data transport techniques in order to work with personal wireless devices and the narrow band wireless networks.

WPKI-Related Standards

ANSI X9.62 Elliptic Curve Digital Signature Algorithm (ECDSA) is the Financial Services Industry's latest standard for digital signatures. This standard defines techniques for generating and validating digital signatures. It is the Elliptic Curve analog of the original ANSI Digital Signature Algorithm (DSA) (ANSI X9.30 Part 1). Elliptic Curve systems are public-key (asymmetric) cryptographic algorithms that are typically used to create digital signatures (in conjunction with a hash algorithm), and to establish secret keys securely for use in symmetric-key cryptosystems. http://www.ansi.org

NIST FIPS PUB 186-2 is the US Digital Signature Standard (DSS). This standard now recognizes different cryptographic subsystems the original Digital Signature Algorithm (DSA) and the Elliptic Curve Digital Signature Algorithm (ECDSA) as defined in ANSI X9.62. http://www.nist.gov

IETF RFC 2459 is the standard that provides the Internet profile of X.509 Certificate and CRL formats. http://www.ietf.org

IETF RFC 2510 is the Internet X.509 Public-Key Infrastructure Certificate Management Protocols (CMP) standard. http://www.ietf.org

IETF RFC 2511 is the Internet X.509 Certificate Request Message Format (CRMF) standard. http://www.ietf.org

IETF RFC 2527 is the Internet X.509 PKI Certificate Policy and Certification Practice Framework. Presents a framework for Certificate Policies (CP) and Certification Practice Statements (CPS). In particular, the framework provides a comprehensive list of topics that may need to be covered in policy definition. http://www.ietf.org

ISO/IEC 9594-8/ITU-T Recommendation X.509 provides the generalized public-key certificate and CRL formats, a public-key trust model and security framework, as well as some of the first formal descriptions of public-key based entity authentication protocols.

ISO/IEC 9594-8 on Certificate Extensions, Final Text of Draft Amendment DAM 1 provides one of the earliest comprehensive lists of extensions and descriptions in ASN.1 of X.509 v3 certificate extensions.

JCE: Java Cryptographic Extensions from JDK v1.2 are the cryptographic libraries provided to Java application developers that allow access to cryptographic serves such as key generation, encryption/decryption, digital signature generation and verification and X.509 certificate and CRL processing.

SEC 1: Elliptic Curve Cryptography specifies public-key schemes based on Elliptic Curve Cryptography, in particular signature schemes, encryption schemes and key management schemes. http://www.secg.org

SEC 2: Recommended Elliptic Curve Domain Parameters help insure interoperation among PKI-enabled applications that use elliptic curve cryptography (ECC) and specifies profiles for standard domain parameters for those implementing elliptic curve according to SEC 1, ANSI X9.62 or FIPS PUB 186-2. http://www.secg.org

Wireless Application Environment Overview: WAP-195-WAE Overview provides an overview of the elements in the WAP architecture with a focus on client-side components. http://www.wapforum.org

WAP Architecture defines a technical architecture for wireless networking and applications and relates this architecture to the Internet networking and application environment. http://www.wapforum.org

WAP Certificate and CRL Profiles: WAP-211-X.509. Specifies the contents, formats and encoding rules for WAP certificate and CRL objects. http://www.wapforum.org

WAP Identity Module: WAP-198-WIM. Defines WIM requirements both functional and physical. http://www.wapforum.org

WAP Public Key Infrastructure: WAP-217-WPKI profiles the existing IETF PKIX PKI standards for the specific requirements of the wireless application environment. http://www.wapforum.org

List of Acronyms Used

ANSI	The American National Standards Institute
ASN.1	Abstract Syntax Notation 1
BER	Basic Encoding Rules
CA	Certification Authority
CRL	Certificate Revocation List
DAM	Draft Amendment
DER	Distinguished Encoding Rules
DSS	Digital Signature Standard
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
E-Commerce	Electronic Commerce
EE	End Entity
FIPS	Federal Information Processing Standard
HTML	HyperText Markup Language
IEC	International Electro-technical Commission
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Standarization Organization
ITU	International Telecommunications Union
JCE	Java Cryptographic Extensions
JDK	Java Developers Kit
M-Commerce	Mobile Commerce
NIST	National Institute of Standards and Technology
PKI	Public-Key Infrastructure
RA	Registration Authority
RFC	Request For Comment
SEC	Standards for Efficient Cryptography http://www.secg.org
SSL	Secure Sockets Layer
TLS	Transport Layer Security
WAE	Wireless Application Environment

WAP	Wireless Application Protocol
WIM	WAP Identity Module
WML	Wireless Markup Language (Script)
WPKI	Wireless Application Protocol Public Key Infrastructure
WTLS	Wireless Transport Layer Security

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

tp wp 002-1