



WAP Transport Layer End-to-end Security

Approved Version 28-June-2001

Wireless Application Protocol
WAP-187-TLE2E-20010628-a

A list of errata and updates to this document is available from the WAP Forum™ Web site, <http://www.wapforum.org/>, in the form of SIN documents, which are subject to revision or removal without notice.

© 2001, Wireless Application Protocol Forum, Ltd. All Rights Reserved. Terms and conditions of use are available from the WAP Forum™ Web site (<http://www.wapforum.org/what/copyright.htm>).

© 2001, Wireless Application Protocol Forum, Ltd. All rights reserved.

Terms and conditions of use are available from the WAP Forum™ Web site at <http://www.wapforum.org/what/copyright.htm>.

You may use this document or any part of the document for internal or educational purposes only, provided you do not modify, edit or take out of context the information in this document in any manner. You may not use this document in any other manner without the prior written permission of the WAP Forum™. The WAP Forum authorises you to copy this document, provided that you retain all copyright and other proprietary notices contained in the original materials on any copies of the materials and that you comply strictly with these terms. This copyright permission does not constitute an endorsement of the products or services offered by you.

The WAP Forum™ assumes no responsibility for errors or omissions in this document. In no event shall the WAP Forum be liable for any special, indirect or consequential damages or any damages whatsoever arising out of or in connection with the use of this information.

WAP Forum™ members have agreed to use reasonable endeavors to disclose in a timely manner to the WAP Forum the existence of all intellectual property rights (IPR's) essential to the present document. The members do not have an obligation to conduct IPR searches. This information is publicly available to members and non-members of the WAP Forum and may be found on the "WAP IPR Declarations" list at <http://www.wapforum.org/what/ipr.htm>. Essential IPR is available for license on the basis set out in the schedule to the WAP Forum Application Form.

No representations or warranties (whether express or implied) are made by the WAP Forum™ or any WAP Forum member or its affiliates regarding any of the IPR's represented on this list, including but not limited to the accuracy, completeness, validity or relevance of the information or whether or not such rights are essential or non-essential.

This document is available online in PDF format at <http://www.wapforum.org/>.

Known problems associated with this document are published at <http://www.wapforum.org/>.

Comments regarding this document can be submitted to the WAP Forum™ in the manner published at <http://www.wapforum.org/>.

Document History	
WAP-187-TLE2E-20010628-a	Current
WAP-187_100-TLE2E-20010330-a	Class 3 SIN
WAP-187-TLE2E-20010628-a	Initial Version

Contents

1. SCOPE	4
2. REFERENCES	5
2.1. NORMATIVE REFERENCES	5
2.2. INFORMATIVE REFERENCES	5
3. TERMINOLOGY AND CONVENTIONS	6
3.1. CONVENTIONS	6
3.2. DEFINITIONS	6
3.3. ABBREVIATIONS	7
4. INTRODUCTION	8
5. SEQUENCE DIAGRAM	10
6. MASTER PULL PROXY DEFINITION	12
7. NAVIGATION DOCUMENT DEFINITION	13
8. MASTER PULL PROXY BASIC BEHAVIOUR	14
8.1. HANDLING THE STATUS 300 HTTP RESPONSES	14
8.1.1. Navigation Document Content Validation	14
8.1.2. Navigation Document Origination Validation.....	15
8.2. NAVIGATION DOCUMENT LIFECYCLE ENFORCEMENT	15
9. USER AGENT BEHAVIOUR	16
9.1. USER AGENT SUPPORT OF THE NAVIGATION DOCUMENT	16
9.2. HANDLING OF THE NAVIGATION DOCUMENT ON RECEPTION	16
9.3. THE PROXY SELECTION MECHANISM	16
9.3.1. Selecting a Proxy	16
9.3.2. Adding a Proxy Definition	17
9.3.3. Removing a Proxy Definition.....	17
9.4. SUBORDINATE PULL PROXY COMMUNICATION ESTABLISHMENT	17
9.5. CLOSING THE SUBORDINATE PROXY COMMUNICATION	18
9.6. NAVIGATION DOCUMENT LIFECYCLE	18
10. CONTENT PROVIDER RECOMMENDATIONS	19
APPENDIX A. STATIC CONFORMANCE REQUIREMENTS (NORMATIVE)	20
A.1. CLIENT FEATURES	20
A.2. MASTER PULL PROXY FEATURES	22
APPENDIX B. IMPLEMENTATION NOTES	23
B.1. CLIENT RECOMMENDATIONS	23
B.1.1. Recommendations for Managing Navigation Documents	23
B.1.1.1. Using HTTP Caches for Navigation Document Storage	23
B.1.2. User Agent Behaviour when Using WTLS for End to End Security	23
B.1.3. User Agent Behaviour for NAPDEF Navigation Documents.....	23
APPENDIX C. CHANGE HISTORY (INFORMATIVE)	24

1. Scope

Wireless Application Protocol (WAPTM) is a result of continuous work to define an industry wide specification for developing applications that operate over wireless communication networks. The scope for the WAP Forum is to define a set of specifications to be used by service applications. The wireless market is growing very quickly and reaching new customers and providing new services. To enable operators and manufacturers to meet the challenges in advanced services, differentiation, and fast/flexible service creation, WAP defines a set of protocols in transport, session and application layers. For additional information on the WAP architecture, refer to “*Wireless Application Protocol Architecture Specification*” [WAP].

A need to provide end-to-end secure applications for e-commerce, corporate access, etc has emerged in WAP. It is generally recognised that the end-to-end problem as defined in section 5 below can be solved either at the transport layer or at the application layer. This specification is only concerned with the transport layer end-to-end security solution.

2. References

2.1. Normative References

- [CREQ] “Specification of WAP Conformance Requirements”. WAP Forum™.
WAP-221-CREQ-20010425-a. [URL:http://www.wapforum.org/](http://www.wapforum.org/)
- [RFC2119] “Key words for use in RFCs to Indicate Requirement Levels”. S. Bradner. March 1997.
[URL:http://www.ietf.org/rfc/rfc2119.txt](http://www.ietf.org/rfc/rfc2119.txt)
- [RFC2234] “Augmented BNF for Syntax Specifications: ABNF”. D. Crocker, Ed., P. Overell.
November 1997. [URL:http://www.ietf.org/rfc/rfc2234.txt](http://www.ietf.org/rfc/rfc2234.txt)
- [HTTP] “Hypertext Transfer Protocol – HTTP/1.1”, R. Fielding, et al. June 1999, URL:
<http://www.ietf.org/rfc/rfc2616.txt>
- [ProvCont] “WAP Provisioning Content”. WAP Forum™.
WAP-183-PROVCONT-20010314-a. . [URL:http://www.wapforum.org/](http://www.wapforum.org/)
- [ProvUAB] “WAP Provisioning User Agent Behaviour Specification”. WAP Forum™.
WAP-185-PROVUAB-20010314-a. . [URL:http://www.wapforum.org/](http://www.wapforum.org/)
- [ProvArch] “WAP Provisioning Architecture Overview”. WAP Forum™.
WAP-182-PROVARCH-20010314-a. . [URL:http://www.wapforum.org/](http://www.wapforum.org/)
- [RFC2396] “Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997, URL:
<http://www.ietf.org/rfc/rfc2119.txt>
- [WBXML] “WAP Binary XML Content Format”, WAP Forum™.
WAP-192-WBXML-20000306-a.
- [WSP] “WAP Wireless Session Protocol. WAP Forum™.
WAP-230-WSP-20010118-a. [URL:http://www.wapforum.org/](http://www.wapforum.org/)
- [WTLS] “WAP Transport Layer Security Protocol Specification”. WAP Forum™.
WAP-199-WTLS-20000218-a. [URL:http://www.wapforum.org/](http://www.wapforum.org/)
- [XML] “Extensible Markup Language (XML)”, W3C Recommendation 10-February-1998,
REC-xml-19980210”, T. Bray, et al, February 10, 1998, URL: <http://www.w3.org/TR/REC-xml>

2.2. Informative References

- [PushArch] “WAP Push Architectural Overview”. WAP Forum™.
WAP-165-PushArch-19991108-a. [URL:http://www.wapforum.org/](http://www.wapforum.org/)
- [TLS] “The TLS Protocol”, Dierks, T. and Allen, C., January 1999, URL: <ftp://ftp.isi.edu/in-notes/rfc2246.txt>
- [WAE] “Wireless Application Environment Overview”. WAP Forum™.
WAP-195-WAEOverview-20000329-a. [URL:http://www.wapforum.org/](http://www.wapforum.org/)
- [WAP] “Wireless Application Protocol Architecture Specification”. WAP Forum™.
WAP-100-WAPArch-19980430-a. [URL:http://www.wapforum.org/](http://www.wapforum.org/)

3. Terminology and Conventions

3.1. Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

3.2. Definitions

Active Configuration Context - contains the collection of available proxies from which the proxy selection mechanism can select a proxy to route a specific request. Please refer to [ProvArch].

Application - A value-added data service provided to a WAP Client. The application may utilise both push and pull data transfer to deliver content.

Bearer Network - a network used to carry the messages of a transport-layer protocol between physical devices. Multiple bearer networks may be used over the life of a single push session.

Content - subject matter (data) stored or generated at an origin server. Content is typically displayed or interpreted by a user agent on a client. Content can both be returned in response to a user request, or be pushed directly to a client.

Default Pull Proxy - or home proxy, defines the preferred proxy of the device.

Device - is a network entity that is capable of sending and/or receiving packets of information and has a unique device address. A device can act as either a client or a server within a given context or across multiple contexts. For example, a device can service a number of clients (as a server) while being a client to another server.

Master Pull Proxy - is a trusted entity with regards to the transmission of a subordinate pull proxy navigation document. The master pull proxy is defined by the trusted provisioning entity.

Navigation document - is a XML document containing the necessary information to reach a subordinate pull proxy. It is a restricted subset of the connectivity document defined in [ProvCont]. The connectivity document defines proxies and access points to be used by the mobile device to access applications.

Pre-arranged trust agreement - refers to an agreement passed between a subordinate pull proxy owner and a master pull proxy owner establishing certain access rules for the subordinate pull proxy owner.

Connectivity document - is a XML document containing the necessary information to reach the default and/or master pull proxy. It is defined in [ProvCont].

Proxy Discovery Mechanism – refers to the mechanism used to inform the client device that it should use another proxy to access the requested information. Configuration information for proxies discovered using this mechanism is part of the active configuration context as defined in [ProvArch] until the expiration of the navigation document.

Proxy selection - is a user agent behaviour for selecting a proxy from a set of available proxies before making a network request.

Secure Domain – is a network domain environment protected from external intrusion by means such as firewall, proxy, access control device, etc. Within a secure domain it is assumed that the origin server(s) can establish the source of a request to ensure it is coming from a trusted source.

Service provider - is an entity that wants to provide end-to-end secure services to WAP clients.

Subordinate Pull Proxy - is a proxy which serves part of the content space. The subordinate pull proxy is granted control on its portion of the content space by the master pull proxy. The client becomes aware of the subordinate pull proxy dynamically by using WAP facilities defined in this specification.

Trusted Provisioning Proxy - is a trusted entity with regards to the transmission of a client connectivity content document.

User - a user is a person who interacts with a user agent to view, hear, or otherwise use a rendered content. Also referred to as end-user.

User agent - a user agent (or content interpreter) is any software or device that interprets resources. This may include textual browsers, voice browsers, search engines, etc.

XML – the Extensible Markup Language is a World Wide Web Consortium (W3C) standard for Internet markup language, of which WML is one such language.

3.3. Abbreviations

CN	Common Name
DNS	Domain Name System
E2E	End-to-end
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
NAP	Network Access Point
OS	Origin Server
RFC	Request For Comments
SCR	Static Conformance Requirements
SSL	Secure Socket Layer
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
WAP	Wireless Application Protocol
WDP	Wireless Datagram Protocol
WPP	Wireless Port Proxy
WSP	Wireless Session Protocol
WTLS	Wireless Transport Layer Security
XML	Extensible Mark-up Language

4. Introduction

The security problem is well known and is usually defined by the following four areas:

- Privacy: no one can see the content transferred on the network. This is usually solved by encrypting.
- Integrity: no one can tamper with the content transferred on the network. This is usually solved by signing content.
- Authentication: both parties in a transaction are really the one they say they are. This can be solved in multiple ways including simple password scheme, certificates, etc.
- Non-repudiation: a user or a provider can not deny having done a transaction. This can be solved by the use of digital signature mechanism.

To create an environment where transactions can be made freely with minimal disruptions those four items need to be addressed.

Figure 1 shows the network elements of the transport layer end-to-end architecture.

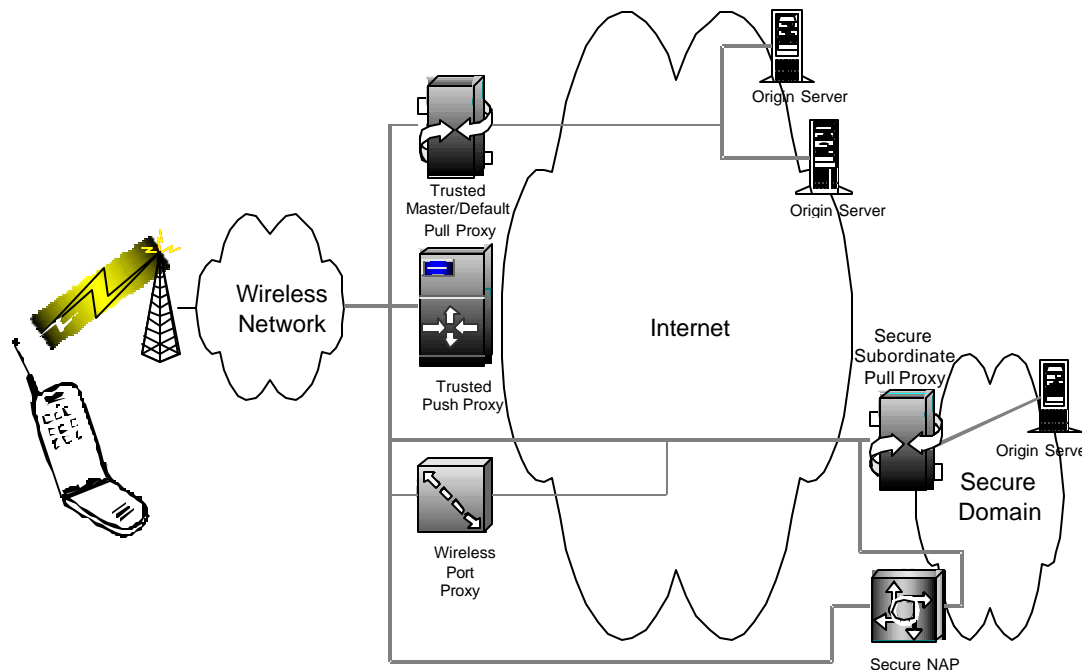


Figure 1: Transport Layer End-to-end Security Architecture

Please note that the network elements shown are functional elements. They might be combined into one or more physical elements as appropriate. The *default pull proxy* defines the preferred proxy of the device. The *default pull proxy* may contain the *master pull proxy* functionality. The *master pull proxy* is a trusted entity with regard to the transmission of a navigation document. The *trusted push proxy* provides push services to the device. WAP service provider and end user trust the push proxy to perform access control on pushed information. The *wireless port proxy* provides a gateway between WDP and UDP, and UDP tunnelling. The *secure domain* is a trusted network environment run by an entity (service provider) that wants to provide end-to-end secure services to WAP clients. The *secure subordinate pull proxy* is a pull proxy run within the secure domain of the service provider. The *secure NAP* is a network access point run within the secure domain of the service provider. The *origin servers* are providing WAP services.

The proposed architecture allows for a variety of network configurations to enable transport level end-to-end security. For example, when the client is aware of the service provider proxy:

- A UDP-enabled client can communicate and establish a WTLS session with the subordinate pull proxy directly.
- A WDP-enabled client can communicate and establish a WTLS session with the subordinate pull proxy either directly or via the wireless port proxy.
- A UDP over circuit data enabled client can establish a circuit directly with the secure NAP and access the secure domain at the network level. Once the circuit is established, the client communicates with the secure pull proxy via the secure NAP.

The underlying assumptions of this transport layer end-to-end security solution are as follows:

- WTLS is used to establish a secured link between the handset and the secure domain pull proxy (the subordinate pull proxy). This ensures end-to-end privacy and integrity.
- WTLS server authentication is used
- Client authentication can be performed if needed with the existing authentication mechanisms (i.e.: HTTP Proxy Authentication, WTLS Shared Secret, simple ID/Password scheme at the application level, etc).
- Non-Repudiation can be handle by the application.
- Push access control is handle by the trusted push proxy. This framework only provides for secure pull end-to-end functionality.

This specification describes the relationships between the entities listed above.

5. Sequence Diagram

The following figure illustrates a typical general sequence required to establish a transport layer end-to-end security communication with a service provider proxy (the subordinate pull proxy).

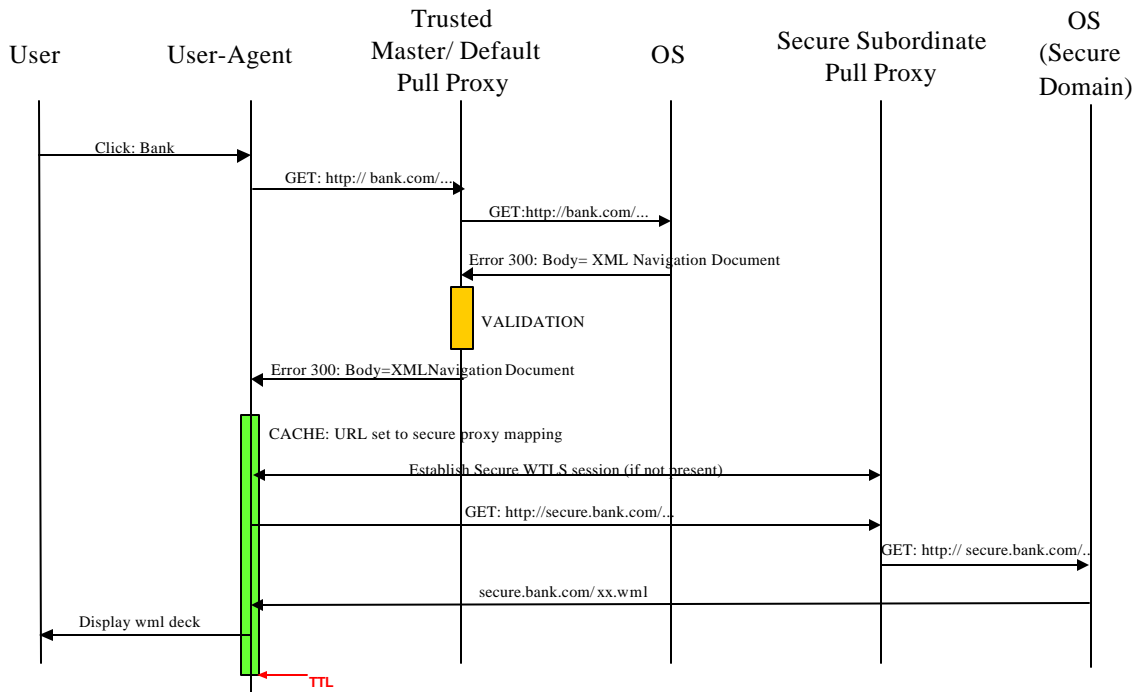


Figure 2: Sequence Diagram

- Below is a step by step description of the mechanism shown on figure 2.
- The user selects his service provider (i.e.: a bank) on the client;
- The client user agent sends a WSP method requesting the selected URL (via its default pull proxy);
- The default pull proxy forwards the method request to the origin server;
- The origin server sends back an HTTP status 300 response to the default pull proxy. A XML navigation document is included in the body section of the reply;
- The master pull proxy functionality of the default pull proxy gets the error reply and analyses the navigation document to make sure it contains valid parameters in accordance with the policies defined in this document and the master pull proxy owner policies. The master pull proxy also analyses cache control headers and directives for the document;
- Once validated the navigation document is forwarded to the handset user agent (using an HTTP 300 error);
- Once accepted by the user agent, the navigation document is cached according to the cache control headers and directives specified for each document and the related configuration data is made available to the proxy selection mechanism;
- When the user subsequently requests a URL, the user agent uses the proxy selection mechanism, as defined in [ProvUAB], to determine which subordinate pull proxy it should use to complete the request;

-
- If no secure session exists between the user agent and the selected subordinate pull proxy, the user agent establishes a WTLS session with the selected proxy;
 - The user agent informs the user that the session is secure. It also shows the information available in the certificate;
 - The originally requested method is sent to the selected subordinate pull proxy;
 - The subordinate pull proxy forwards the request to the origin server;
 - The origin server replies to the user agent via the subordinate pull proxy;

The navigation document and its associated configuration data (if any) are invalidated when the document expires.

6. Master Pull Proxy Definition

The master pull proxy is a trusted entity with regard to the transmission of navigation document. It can be the same entity as the trusted provisioning proxy but does not need to be. The master pull proxy trust can be established by using WTLS with server authentication between the client and the master pull proxy or by any other means which the master proxy owner consider trustworthy (for example trust could be established using wireless network architecture).

The initial master pull proxy is identified to the user agent by setting the MASTER parameter contained in the connectivity content document received from the trusted provisioning authority. There MAY be multiple master pull proxies defined simultaneously. In that case, the selection of the master pull proxy for a specific request is defined in [ProvUAB].

7. Navigation Document Definition

The navigation document definition is equal to the connectivity content document defined in [ProvCont]. This section defines restrictions on the data model defined in [ProvCont]. A navigation document that does not obey these restrictions is considered malformed.

MIME-type of the textual navigation document is *text/vnd.wap.connectivity-xml*. MIME-type for the tokenised navigation document is *application/vnd.wap.connectivity-wbxml*: the WBXML tokenisation is defined in [ProvCont].

A navigation document **MUST** contain exactly one PX-LOGICAL definition. A navigation document **MAY** contain zero or more NAPDEF characteristic definitions.

If PXLOGICAL.DOMAIN definition is included in the document, it **MUST** define exactly one full or partial authority definition and it **MAY** include a path definition. A navigation document **MUST NOT** contain more than one PXLOGICAL.DOMAIN parameter. Note that the PXLOGICAL.DOMAIN parameter in the navigation document can either apply to a specific domain (bank.com) or to a range of sub-domains (.bank.com) but not both due to the proxy selection rules defined in [ProvUAB]. According to that rule *x.y.com* domain matches *.y.COM* but does not match *y.com*.

A navigation document **MUST NOT** contain the following characteristic definitions:

- BOOTSTRAP
- CLIENTIDENTITY

A navigation document **MUST NOT** contain the TRUST parameter.

If there are no NAPDEF characteristics definitions in the navigation document, the user agent **MUST** use the same NAPDEF characteristics definitions that was used when navigation document was accessed. If content defines multiple network access points (NAP), user agent **MAY** choose the appropriate one to use. If a PXPHYSICAL.TONAPID parameter has the value INTERNET user agent **SHOULD** use a previously defined NAPDEF with INTERNET parameter defined.

8. Master Pull Proxy Basic Behaviour

8.1. Handling the Status 300 HTTP Responses

The navigation document is sent to the master pull proxy as an HTTP response with status 300. No other 300 series status codes are valid to transmit navigation document.

The master pull proxy **MUST** verify the navigation document content format to be a valid format as defined in section 7.

The master pull proxy **MUST** forward any HTTP response with error code 300 to the user agent including the body of the response if:

- the user agent has indicated to the master pull proxy that it was supporting the navigation document type using the accept header; AND
- the navigation document meets the master pull proxy owner policies (if any); AND
- the navigation document content format validation (if any) was successful.

In the event the master pull proxy refuses to forward the navigation document for policy reason or because the master pull proxy did not received the accept header for the navigation document content type, an HTTP status 403 **MUST** be returned. Explanatory text **SHOULD** also be provided.

If the navigation document is in textual format and client accepts only tokenised documents, the master pull proxy **MUST** encode the document as defined in [ProvCont]. If encoding fails due to an error in the content, the master pull proxy **MUST** return HTTP status 502 to the client.

The master pull proxy **MAY** change the content of the navigation document according to its policies.

The master pull proxy **MAY** also modify or add HTTP response headers according to its policies.

8.1.1. Navigation Document Content Validation

While this specification does not specify any detailed interfaces for filtering, it is recommended that, at a minimum, the master pull proxy implementation allows the administrator to achieve the following:

- Filter any field in the navigation document;
- Disable or enable navigation documents which specify an empty DOMAIN entry;
- Disable or enable navigation documents which specify “MASTER” proxies; AND
- Disable or enable navigation documents which specify “NAPDEF” clauses.

As a default policy it is recommended that:

- navigation documents with an empty DOMAIN entry are REJECTED;
- navigation documents with a NAPDEF characteristics defined are REJECTED; AND
- navigation documents with the MASTER parameter set are REJECTED.

While it is not the place for these recommendations to **REQUIRE** certain product features, they are included with the hopes of ensuring that the default operation of a master pull proxy does not leave the user open to potentially unexpected security breaches.

8.1.2. Navigation Document Origination Validation

Navigation document origination validation is required to ensure that no malicious organisation is capable of redirecting users to their own subordinate pull proxy by using the identity of another subordinate pull proxy (slamming).

When there is no pre-arranged trust agreement between the master pull proxy owner and the subordinate pull proxy owner, the master pull proxy **SHOULD** authenticate the server originating the navigation document to deter denial of service attack. This could be done either by using some network facilities (VPN, lease line, etc) or by using SSL/TLS server authentication between the master pull proxy and the origin server originating the navigation document. The following domain parameter check **MUST** be performed:

- The master pull proxy **MUST** ensure that:
- the authority portion of the requested URL is included as a whole in the authority portion of the PXLOGICAL.DOMAIN entry of the navigation document; and
- the path portion (if any) of the PXLOGICAL.DOMAIN is included as a whole in the path portion of the requested URL.
- When SSL/TLS is used, the master pull proxy **MUST** also ensure that the CN parameter contained in the SSL/TLS server certificates as defined in [TLS] is included as a whole in the authority portion of the PXLOGICAL.DOMAIN entry of the navigation document.

For example a CN equal to x.y.com is included in the following PXLOGICAL.DOMAIN:

- a.x.y.com
- .x.y.com
- x.y.com

but that CN is not included in the following PXLOGICAL.DOMAIN:

- .y.com
- y.com
- .com
- *

While it is permitted to use an alternate mechanism for establishing trust verification, the recommended mechanism is SSL/TLS. Though an administrator may configure the master pull proxy to do otherwise, implementations **SHOULD** support SSL/TLS as the preferred trust verification mechanism.

When a pre-arranged trust agreement is in place between the master pull proxy owner and the subordinate pull proxy owner, the master pull proxy **SHOULD** authenticate the origin server originating the navigation document and it **SHOULD** perform the domain parameter check according to the policies in place between the master pull proxy owner and the subordinate pull proxy owner.

8.2. Navigation Document Lifecycle Enforcement

The master pull proxy **MUST** use Cache-Control header and the max-age directive for modifying the navigation validity period to a different value than the origin server has proposed with the Expires header.

9. User Agent Behaviour

9.1. User Agent Support of the Navigation Document

If a user agent is capable and willing to receive a navigation document, it **MUST** inform the master pull proxy that it accepts connectivity media type. This **MUST** be done using the HTTP Accept header with content type *application/vnd.wap.connectivity-wbxml*. A user agent that supports connectivity document media type **MUST** be capable of receiving a tokenised navigation document.

9.2. Handling of the Navigation Document on Reception

Navigation documents are included in the body of an HTTP status code 300 response.

The user agent **MUST** be capable of recovering the body of any HTTP response having a 300 status code.

The user agent **MUST** only accept navigation documents received from the master pull proxy. Other navigation documents **MUST** be rejected.

User agent **MUST** assure that the navigation document conforms to the definitions found in section 7 of this specification. User agent **MAY** apply its own validation policies on the navigation document.

In the event that the user agent rejects the navigation document, the user agent **SHOULD** treat the response as if the request had returned HTTP status code 403. User agent **MUST** be able to interpret navigation documents according to this specification.

If the user agent accepts the navigation document content, it **MUST** make the PXLOGICAL definition available to the active configuration context as defined in this specification.

If the user agent rejects the navigation document or if it receives a 403 error, it **SHOULD** inform the user.

9.3. The Proxy Selection Mechanism

The proxy selection mechanism defines a user agent behaviour for selecting a proxy before making a network request among the proxies the user agent has local knowledge.

Some rules to manage the proxy definitions are required to ensure that the proxy discovery sequence is complete and that the behaviour is consistent on all user agents. This section describes those rules.

9.3.1. Selecting a Proxy

For each URL request the user agent **MUST** apply the proxy selection mechanism as defined in [ProvUAB] to identify which subordinate pull proxy should handle that specific request. If two or more configurations in the same active configuration context have equal value in PXLOGICAL.DOMAIN when using a case-insensitive match, precedence **MUST** be given to the configuration received via proxy discovery mechanism.

9.3.2. Adding a Proxy Definition

When a navigation document that defines a proxy (A) is received and accepted it **MUST** be added to the active configuration context. This **MAY** cause removal of another subordinate proxy definition due to e.g. limited amount of memory for subordinate proxy definitions.

If the active configuration context contains a proxy definition (B) where B.PXLOGICAL.DOMAIN is equal to the A.PXLOGICAL.DOMAIN when using a case insensitive match and the proxy (B) definition was received via proxy discovery mechanism, the proxy (B) definition **MUST** be deleted.

9.3.3. Removing a Proxy Definition

When a subordinate proxy definition expires it **MUST** be removed from the active configuration context. Subordinate proxy definition **MUST** be removed from the active configuration context when requested by the subordinate proxy as defined in section 9.5.

9.4. Subordinate Pull Proxy Communication Establishment

Once the selected subordinate pull proxy has been identified, the user agent **MUST** contact the proxy defined in the PXLOGICAL portion of the selected configuration using the associated PXPHYSICAL and NAPDEF characteristics and either:

- establish a WTLS secure session with that proxy; or
- use an existing WTLS session established between the user agent and the proxy defined in the PXLOGICAL portion of the selected configuration.

WAP client **MAY** keep existing WSP sessions, WTLS secure sessions and WTLS secure connections while connecting to the new proxy.

User agent **MAY** use an existing WSP session with the proxy that is compatible with the PXLOGICAL specified in the selected configuration if such a session exists. User agent **MAY** use an existing WTLS secure session that is compatible with the PXLOGICAL specified in the selected configuration if such a WTLS secure session exists.

While establishing the WTLS session, user agent **MUST** validate the subordinate pull proxy certificate by verifying that the PROXY-PROVIDER-ID parameter of the navigation document is the same as the 4th field in server_cert. (place for commonName). Subordinate pull proxy validation failure **MUST** result in either a prompt to the user to make a decision or an abort of the WTLS session establishment. The subordinate pull proxy **MAY** perform client authentication using one of the different mechanisms offered by the WAP Architecture (HTTP Proxy Authentication, WTLS shared secret, application layer ID/Password, Client certificates, etc).

After a WSP session has been established or if connectionless WSP services are used, user agent **MUST** make a request to the subordinate pull proxy. Request headers, method and request data **MUST** be the same as in the original request. If the navigation document defines a PXLOGICAL.STARTPAGE then the request **MUST** use that URL instead of the original URL. If PXLOGICAL.STARTPAGE parameter is not defined in the navigation document then the original URL **MUST** be used.

If the subordinate pull proxy can not be contacted due to errors at WTLS, WTP or WSP level, user agent **MAY** indicate an appropriate error and user agent **SHOULD** return to the state it had before requesting the URL that returned the navigation document.

9.5. Closing the Subordinate Proxy Communication

User agent can be explicitly instructed by the subordinate proxy to stop using the proxy. This helps the application to create more deterministic behaviour of terminal and reduce the possibility of navigation documents expiring during a service usage. Terminal and subordinate proxy implementations MAY use this information to manage and optimize WTLS connection lifetimes. This improves security by ensuring that no idle WTLS connections are left hanging.

Explicit instruction to stop using a subordinate proxy is indicated by a specific HTTP response header. The response header that defines the instruction for this purpose is "x-wap-security" and value is "close-subordinate". Upon reception of this instruction user agent MUST remove the subordinate proxy definition that returned the instruction from the active configuration context as specified in section 9.3.3. Upon reception of this instruction, user agent MUST treat the previously retrieved resources as defined in section 9.6 for the case when subordinate proxy definition has expired.

9.6. Navigation Document Lifecycle

User agent MUST store the navigation document according to the HTTP Cache-related headers and directives returned with the entity.

When the navigation document has expired, the user agent MUST NOT:

- use the navigation document and its associated configuration data (if any); AND
- use the proxy identified in the expired navigation document in the proxy selection mechanism.

The WTLS session with the subordinate pull proxy does not need to be disconnected.

Special care has to be given to the case when the navigation document expires to avoid leaking private information to proxies outside of the secure domain.

Although content provider are instructed not to do so (refer to section 10), any URLs received from a secure subordinate pull proxy (secure URLs) might contain private information which neither the service provider nor the user wants to see going out to a third party proxy. To prevent any of those secure URLs requests to be sent to the wrong pull proxy an additional security match MUST be performed.

This match MUST be performed as defined by the proxy selection matching rules specified in [ProvUAB] with the additional restriction that there MUST NOT be more than one domain label difference for a successful security match. Host names are defined as a sequence of domain labels separated by "." (i.e.: x.y.com). If the authority portion of a URL to be requested contains N labels then a successful security match can only be done with a PXLOGICAL.DOMAIN definition that contains N or N-1 labels.

For example, given a secure URL request of <http://a.x.y.com/buy/something> the following PXLOGICAL.DOMAIN would match:

- a.x.y.com
- .x.y.com

While these PXLOGICAL.DOMAIN would not match because there is more than one domain label difference:

- .y.com
- .com
- *

A failure of the security match MUST be considered as a proxy selection failure. In that case the user agent SHOULD behave as described in 0.

10. Content Provider Recommendations

This solution allows the establishment of a secure WTLS session to a secure service provider domain. To ensure proper protection of application data the following recommendations are proposed.

Origin servers **SHOULD** only deliver navigation document when the Accept header of the request includes the navigation document content type.

WML and WMLScript content (part of the secure application) **SHOULD** be located in the secure domain or the Service Provider.

WMLScript content (part of a secure application) **SHOULD** only invoke URL in the same secure domain.

Sensitive application parameters intended for another secure domain than the one where the application resides **SHOULD** be encrypted.

When not following the previous rule, content provider **SHOULD** be cautious when deploying navigation document as the algorithm defined in section 9.6 might lead to a leakage of URLs. This can happen when the PXLOGICAL.DOMAIN parameter of a navigation document overlap the PXLOGICAL.DOMAIN parameter of another navigation document (i.e.: a.x.y.com and .x.y.com).

Appendix A. Static Conformance Requirements (Normative)

The notation used in this appendix is specified in [CREQ].

A.1. Client Features

Item	Function	Reference	Status	Requirement
E2E-C-001	Support for the WAP-PROVISIONINGDOC DTD.	7	M	ProvCont:MCF
E2E-C-002	Support for WAP-PROVISIONINGDOC in textual form (text/vnd.wap.connectivity-xml).	7	O	ProvCont:MCF
E2E-C-003	Support for WAP-PROVISIONINGDOC in tokenised form (application/vnd.wap.connectivity-wbxml).	7	M	ProvCont:MCF
E2E-C-004	Use of the Accept header to indicate support for the navigation document.	9.1	M	
E2E-C-005	Accept 300 error code with a response content.	9.2	M	
E2E-C-006	Only accept navigation document from Master pull proxy.	9.2	M	
E2E-C-007	Validate navigation document format.	9.2	M	ProvCont:MCF
E2E-C-008	Request each URL through the proxy selection mechanism.	9.3.1	M	ProvUAB-U-C-002
E2E-C-009	Add a subordinate proxy definition to the active configuration context.	9.3.2	M	E2E-C-019
E2E-C-010	Remove a subordinate proxy definition from the active configuration context.	9.3.3	M	E2E-C-020
E2E-C-011	Establish WTLS secure session with subordinate pull proxy.	9.4	M	WTLS:MCF
E2E-C-012	Validate subordinate pull proxy certificate.	9.4	M	WTLS:MCF AND

Item	Function	Reference	Status	Requirement
				WTLS-C191
E2E-C-013	Initial request to subordinate pull proxy using PXLOGICAL.STARTPAGE or original request.	9.4	M	
E2E-C-014	Remove the subordinate proxy definition from the active configuration context when receiving the x-wap-security header with a value of "close-subordinate".	9.5	M	
E2E-C-015	Treat previously received resources from a subordinate proxy as if the navigation document had expired upon receiving the x-wap-security header with a value of "close-subordinate".	9.5	M	
E2E-C-016	Do not use an expired navigation document.	9.6	M	E2E-C-020
E2E-C-017	Do not use the proxy identified in the expired navigation document in the proxy selection mechanism.	9.6	M	
E2E-C-018	Perform the additional security match as specified.	9.6	M	
E2E-C-019	The client has a HTTP cache that can hold at least one navigation document.	9	M	
E2E-C-020	The client has a time of day clock or a delta-second timer.	9	M	

A.2. Master Pull Proxy Features

Item	Function	Reference	Status	Requirement
E2E-S-001	Support for WAP-PROVISIONINGDOC in textual form (text/vnd.wap.connectivity-xml).	7	M	ProvCont:MSF
E2E-S-002	Support for encoding an WAP-PROVISIONINGDOC into tokenised form (application/vnd.wap.connectivity-wbxml).	7	M	ProvCont:MSF
E2E-S-003	Support for the WAP-PROVISIONINGDOC token table.	7	M	ProvCont:MSF
E2E-S-004	Navigation document format verification.	7,8.1	M	
E2E-S-005	Handling of HTTP error 300.	8.1	M	
E2E-S-006	Navigation document content validation.	8.1.1	O	
E2E-S-007	Basic DOMAIN parameter check (when no pre-arranged trust agreement exists).	8.1.2	M	
E2E-S-008	Extra DOMAIN parameter check when SSL/TLS is used (when no pre-arranged trust agreement exists).	8.1.2	O	
E2E-S-009	Navigation document lifecycle enforcement.	8.2	M	
E2E-S-010	The Master Pull Proxy uses SSL or TLS connections when requesting navigation document from Origin Server.	-	O	E2E-S-008

Appendix B. Implementation Notes

The following implementation notes are provided to identify areas where implementation choices may impact the performance and effectiveness of the overall transport layer end-to-end solution. These notes provide guidance to implementers of the protocols.

B.1. Client Recommendations

B.1.1. Recommendations for Managing Navigation Documents

B.1.1.1. Using HTTP Caches for Navigation Document Storage

If an implementation chooses to store navigation documents in the http content cache, it should use caution when clearing cached items. Removing or deleting a navigation document may cause an interruption in service for user access to sites which depend on that navigation document.

B.1.1.2. Navigation Document Deleted Failure Case

Through the course of device operation, space constraints, power cycles or other unforeseen events may result in navigation documents being removed from the store.

In this case, an attempt to navigate to a URI from history or bookmark may not be possible. At a minimum, the user agent should display an informative message to the user that the security information has expired.

Beyond the minimum an implementation is encouraged to provide more information such as the main site for the domain, a link to that main site, or any other information which might help the user. However, these enhancements are not required nor specified in this specification and are left up to the implementation.

B.1.2. User Agent Behaviour when Using WTLS for End to End Security

Currently, there is no normative specification for user agent behaviour which describes communicating security parameters such as server certificate identification or cipher strength to the user.

It is recommended that when using WTLS, the user agent should allow the security session to be within easy reach of the user. This may be manifested as the familiar “lock icon” in desktop browsers which can be clicked on to reveal details, it may be a context menu from an info key, a voice or sound indication, a UI popup temporarily displayed, or any other mechanism. The authors recommend that implementers provide some level of security indication while making appropriate product usability tradeoffs, as appropriate, with the goal of allowing the user to verify end-to-end security.

B.1.3. User Agent Behaviour for NAPDEF Navigation Documents

It is recommended that the default preference setting for navigation documents which contain a NAPDEF are to be confirmed by the user via some appropriate method.

While it is not the place for these recommendations to REQUIRE certain product features, they are included with the hopes of ensuring that the default operation of a implementation does not leave the user open to potentially unexpected security breaches or abuse.

A simple example of the danger of allowing NAPDEF navigation documents to be used with out user confirmation is the threat of automatically placing a call to a long distance or otherwise prohibitively expensive phone number.

Appendix C. Change History (Informative)

Type of Change	Date	Section	Description
Class 3	28-June-2001	All	New WAP Spec template
Class 3	30-March-2001	Section 7 Appendix A	New SCR format + clarification in section 7 (WAP-187_100-TLE2E SIN)
Class 0	28-June-2001		The initial version of this document.