# Requirements for HyperText Transfer Protocol Security

Internet Draft: <draft-bossert-httpsec-req-00.txt>
Expires: August 1995

Abstract:

This document specifies the requirements for the provision of security services to the HyperText Transport Protocol. These services include confidentiality, integrity, user authentication, and certification of servers/services, including proxied or gatewayed services. Such services may be provided as extensions to HTTP, or as an encapsulating security protocol. Secondary requirements include ease of integration and support of multiple mechanisms for providing these services.

Authors:

Greg Bossert <bossert@noc.rutgers.edu>
Simon Cooper <scooper@noc.rutgers.edu>
Walt Drummond <drummond@noc.rutgers.edu>
Network Services, Telecommunications Division,
Rutgers University Computing Services
Hill Center, Brett Road, Bush Campus
Piscataway, New Jersey 08855-0879 USA

## Terminology

WTS:

Web Transaction Security protocol.

Transaction:

A complete HTTP action, consisting of a request from the client and a response from the server.

Gatewayed Service:

A service accessed, via HTTP or an alternate protocol, by the HTTP server on behalf of the client.

Mechanism:

An specific implementation of a protocol or related subset of features of a protocol.

## General Requirements

WTS must provide the following services. These services must be provided independently of each other.:

- Confidentiality of the HTTP transaction.
- Authentication of the server/service.
- Authentication of the client/user.
- Integrity of the HTTP transaction.

In addition, WTS should conform to a number of secondary requirements:

- Ease of integration with other features of HTTP.
- Support of multiple mechanisms for the above services.

## Confidentiality

WTS must provide confidentiality of the HTTP transaction, via encryption of the HTTP messages. The entire HTTP transaction must be considered private; thus, the HTTP headers and data objects of client requests and server responses must be confidential.

Note: because the identity of the object being requested is potentially sensitive, the URI/URL of the request should be confidential; this is particularly critical in the common case of form data or other user input being passed in the URL.

## Service Authentication

WTS should support the authentication of gatewayed services to the client.

WTS should support the authentication of the origin HTTP server or gatewayed services regardless of intermediary proxy or caching servers.

To allow user privacy, WTS must support service authentication without user authentication.

Because the identity of the object being requested is potentially sensitive, service authentication should occur before any part of the request, including the URI of the requested object, is passed. In cases where the authentication process depends on the URI (or other header data) of the request, such as gatewayed services, the minimum necessary information to identify the entity to be authenticated should be passed.

## User Authentication

WTS must support the authentication of the user to the server.

WTS should support the authentication of the client to gatewayed services.

WTS should support the authentication of the client to the origin HTTP server regardless of intermediary proxy servers.

## Integrity

WTS must provide assurance of the integrity of the HTTP transaction, including the HTTP headers and data objects of both client requests and server responses.

## Integration

In order to support integration with current and future versions of HTTP, and to provide extendibility and independence of development, the secure services provided by WTS must be orthogonal to and independent of other services provided by HTTP.

In accordance with the layered model of network protocols, WTS must be:

- independent of the content or nature of data objects being transported.
- implementable over a variety of connection schemes and underlying transport protocols

## Multiple Mechanisms

WTS must be compatible with multiple mechanisms for authentication and encryption. Support for multiple mechanisms is required for a number of reasons:

- Accommodation of variations in site policies, including those due to external restrictions on the availability of cryptographic technologies.
- Support for a variety of applications and gatewayed services.
- Support for parallel implementations within and across administrative domains.

To allow interoperability across domains, and to support the transition to new/upgraded mechanisms, WTS should provide negotiation of authentication and encryption mechanisms.

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

**IETF Stockholm Summer 95 WTS Working Group**

**Requirements for Hypertext Transfer Protocol Security**

**G. Bossert, S. Cooper, W. Drummond**

**Rutgers University Computing Services · Telecommunications Division · Network Services**