SLOVENSKI STANDARD
SIST-TS TS 101 321 V2.1.1:2004

01-april-2004

Harmonizacija telekomunikacij in internetnega protokola prek omrežij (TIPHON) - Protokol odprtega dogovora (OSP) za meddomensko izmenjavo zaračunavanja, avtorizacije in uporabe

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Open Settlement Protocol (OSP) for Inter-Domain pricing, authorization, and usage exchange

Ta slovenski standard je istoveten z: **ETSI TS 101 321 V2.1.1 (2000-08)**

ICS:

33.040.30	Komutacijski in signalizacijski sistem	Switching and signalling systems

SIST-TS TS 101 321 V2.1.1:2004 **en**

ETSI TS 101 321 V2.1.1 (2000-08)

Technical Specification

Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Open Settlement Protocol (OSP) for Inter-Domain pricing, authorization, and usage exchange

Reference
RTS/TIPHON-03004.2

Keywords
internet, network, interoperability, protocol,
telephony, IP

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at http://www.etsi.org/tb/status/

If you find errors in the present document, send your comment to:
editor@etsi.fr

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Project Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON).

Introduction

The contents of the present document are the result of contributions and discussions in Working Group 3.

1 Scope

The present document shall be called the Open Settlement Protocol (OSP). The present document specifies a set of protocols and associated profiles to permit the exchange of inter-domain pricing, authorization, and settlement information between internet telephony operators. The protocols specified fulfil the essential requirements of such services, by providing appropriate functionality between multiple administrative domains in a secure manner. The specification also provides for non-standard extensions that permit co-operating parties to augment or replace the basic functionality.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] American National Standards Institute. Accredited Standards Committee X9 Working Draft: American National Standard X9.42-1993: Public Key Cryptography for the Financial Services Industry: Management of Symmetric Algorithm Keys Using Diffie-Hellman. American Bankers Association, September 21, 1994.

[2] RFC 1945 (1996): Hypertext Transfer Protocol - HTTP/1.0. Berners Lee, T., R. Fielding, and H. Frystyk.

[3] Bray, Tim, Jean Paoli, and C. M. Sperberg-McQueen. Extensible Markup Language (XML) 1.0. World Wide Web Consortium (W3C): 10 February 1998. [http://www.w3.org/TR/REC-xml].

[4] RFC 2068 (1997): Hypertext Transfer Protocol - HTTP/1.1. Fielding R., J. Gettys, J. Mogul, H. Frystyk, and T. Berners-Lee.

[5] RFC 2045 (1996): Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies. Freed, N. and N. Borenstein.

[6] Freier, Alan O., Philip Karlton, and Paul C. Kocher. The SSL Protocol Version 3.0 [http://www.netscape.com/eng/ssl3/ssl-toc.html]. Netscape Communications Corporation: March 1996. As amended by SSL 3.0 Errata of August 26, 1996 [http://www.netscape.com/eng/ssl3/ssl-errata.html].

[7] ISO 4217 (1995): "Codes for the representation of currencies and funds".

[8] ISO 8601 (1988): "Data elements and interchange formats -- Information interchange -- Representation of dates and times".

[9] ITU-T Recommendation H.225.0 (1998): "Call signalling protocols and media stream packetization for packet-based multimedia communication systems".

[10] ITU-T Recommendation H.245 (1998): "Control protocol for multimedia communication".

[11] ITU-T Recommendation X.691 (1995): "Information technology - ASN.1 encoding rules - Specification of Packed Encoding Rules (PER)".

[12] ITU-T Recommendation E.164 (1997): "The international public telecommunication numbering plan".

[13] ITU-T Recommendation H.323 (1998): "Packet-based multimedia communications systems".

[14] ITU-T Recommendation H.235 (1998): "Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals".

[15] National Institute of Standards and Technology, U.S. Department of Commerce NIST FIPS PUB 46-1 (January 1988): "Data Encryption Standard".

[16] National Institute of Standards and Technology, U.S. Department of Commerce NIST FIPS PUB 186 (18 May 1994): "Digital Signature Standard"

[17] National Institute of Standards and Technology, U.S. Department of Commerce NIST FIPS PUB 180-1 (31 May 1994): "Secure Hash Standard".

[18] RFC 2311 (1998): S/MIME Version 2 Message Specification. S. Dusse, P. Hoffman, B. Ramsdell, L. Lundblade, and L. Repka.

[19] RFC 2268 (1998): Description of the RC2® Encryption Algorithm. R. Rivest.

[20] RFC 1321 (1992): The MD5 Message-Digest Algorithm. R. Rivest.

[21] RSA Laboratories. PKCS #1: RSA Encryption Standard. Version 1.5, November 1993.

[22] RSA Laboratories. PKCS #7: Cryptographic Message Syntax Standard. Version 1.5, November 1993.

[23] The Unicode Consortium. The Unicode Standard. Version 2.0.

[24] Dierks, Tim and Christopher Allen. The TLS Protocol Version 1.0. Work in progress.

[25] The Open Trading Protocol Consortium. Internet Open Trading Protocol Part 2: Specification. Version 0.9, 12 January 1998.

[26] ISO/IEC 9646-7 (1995): "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 7: Implementation Conformance Statements".

[27] ISO/IEC 10646 (1993): "Information technology -- Universal Multiple-Octet Coded Character Set (UCS)".

[28] RFC 2630 (1999): Cryptographic Message Syntax. Housley, R.

[29] WAP-154, Binary XML Content Format Specification

[30] ISO/IEC 7812-1: "Identification cards -- Identification of issuers -- Part 1: Numbering system".

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CMS	Cryptographic Message Syntax
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DTD	Document Type Definition
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSEC	Internet Protocol Security
MD5	Message Digest 5
MIME	Multipurpose Internet Mail Extensions
OSP	Open Settlement Protocol
PIN	Personal Identification Number (e.g. for automated teller machines)
PKCS	Public Key Cryptography Standard

RAS	Registration Admission and Status
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator
UTC	Universal Time Co-ordinated
UTF	Universal Text Format
XML	Extensible Markup Language

4 Open Settlement Protocol Architecture

This clause introduces the protocol architecture for the OSP specification. It identifies the major protocols used by communicating parties, and it outlines their relationship to each other. The clause also describes the overall format of messages exchanged by the protocols. The intent of this clause is to outline the framework for the standard's protocols and message formats; later clauses detail specific profiles for these protocols and the specific message content.

4.1 Communication Protocols

As figure 1 shows, systems conforming to the OSP specification use a combination of the Hypertext Transfer Protocol (HTTP), and either the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to transfer pricing, authorization, and usage information. As the figure indicates, these protocols are layered on top of the Transmission Control Protocol (TCP) for communication across Internet Protocol (IP) networks.

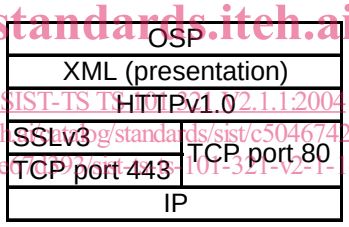

Figure 1: Open Settlement Protocol Architecture for Pricing, Authorization, and Usage Exchange

4.1.1 Secure Sockets Layer/Transport Layer Security

The Secure Sockets Layer and Transport Layer Security protocols add authentication and privacy to TCP connections. SSL is the standard protocol for securing web browsing. As such, it is widely deployed on the Internet and is distinguished by considerable operational experience. SSL also enjoys near universal support from firewalls and proxy servers. TLS is an updated version of SSL currently being developed within the Internet Engineering Task Force (IETF). TLS is heavily based on SSL and, although it is not strictly backwards compatible with SSL, systems supporting both TLS and SSL can automatically recognize either protocol and adapt as required to ensure interoperability.

NOTE: As other industry standard mechanisms for IP-based security (for example, IPSEC) reach maturity, later revisions to the present document may incorporate support for those mechanisms in addition to SSL/TLS. Such revisions to the security mechanisms may also permit the use of an unreliable transport such as UDP.

4.1.2 Hypertext Transfer Protocol

The Hypertext Transfer Protocol (HTTP) is the standard protocol for web-based communications. HTTP has been adopted for a wide variety of purposes including proxy services, bi-directional content delivery, database access, network management, and metering information. HTTP is by far the most widely used application protocol on the Internet, and is supported by all significant firewalls and proxy servers.

4.2 Message Format

To illustrate the overall format of OSP messages, figure 2 shows an example message. As the figure indicates, the content within the HTTP message is formatted according to the standard for Multipurpose Internet Mail Extensions (MIME). The individual components of the message are a document conforming to the Extensible Markup Language (XML) specification and a Secure MIME (S/MIME) digital signature.

NOTE: The digital signature is optional and, if omitted, the message content consists solely of a XML document.

HTTP Header

```
POST scripts/settlements HTTP/1.0
content-type: multipart/signed;
    protocol="application/pkcs7-signature";
    micalg=sha1;
    boundary=bar
content-length: 844
```

Message Content

```
--bar
Content-Type: text/plain
Content-Length: 524

<?xml version='1.0'?>
<Message messageId="123454321" random="12345678">
    <AuthorizationRequest componentId="9876567890">
        <Timestamp>
            1998-04-24T17:03:00Z
        </Timestamp>
        <CallId>
            1234432198766789
        </CallId>
        <SourceInfo type="e164">
            81458811202
        </SourceInfo>
        <DestinationInfo type="e164">
            4766841360
        </DestinationInfo>
        <Service/>
        <MaximumDestinations>
            5
        </MaximumDestinations>
    </AuthorizationRequest>
</Message>
```


Digital Signature

```
--bar
Content-Type: application/pkcs7-signature
Content-Length: 191

GhyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIG
fHfYT64VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756t
bB9HGTrfvbnjn8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfH
fYT6ghyHhHUujpfyF47GhIGfHfYT64VQbnj756

--bar--
```

Figure 2: Example Message Showing Overall Format

4.2.1 Multipurpose Internet Mail Extensions

All messages exchanged as part of this OSP specification conform to the Multipurpose Internet Mail Extensions (MIME) specification. The MIME specification defines mechanisms to combine individual components of arbitrary format (e.g. text, graphics, audio information, binary data, etc.) into a single message. Originally designed for electronic mail, the MIME specification has been adapted for a variety of communication applications, including web browsing. MIME format is widely supported by existing firewalls and proxy servers.

4.2.2 Extensible Markup Language

The first part of each MIME message is a document conforming to the Extensible Markup Language (XML) standard. As an extension of the widely deployed Hypertext Markup Language (HTML), XML can be readily parsed by firewalls and proxy servers. Unlike HTML, though, XML is readily extensible and can easily support rich, structured data such as pricing and usage information.

4.2.3 Secure MIME

The second part of each MIME message, if present, is a digital signature conforming to the Secure Multipurpose Internet Mail Extensions (S/MIME). S/MIME format includes support for multiple digest and signing algorithms and for variable cryptographic strength (e.g. key lengths). S/MIME format is also self-identifying with respect to these parameters, so that a recipient can derive the necessary information for verifying the signature from the signature data.

NOTE: This does not imply that the recipient is guaranteed to be able to verify the signature, only that the recipient can tell what it needs to perform the verification. (So that, for example, the recipient may identify a signing algorithm that it does not support).

5 Protocol Profiles

This clause specifies the profiles for the protocols required by this OSP specification. It identifies the normative references to those protocols, as well as the specific versions, options, and extensions that the present document requires. The specific protocols described in this clause are the Secure Sockets Layer (SSL) and Transport Layer (TLS) protocols and the Hypertext Transfer Protocol (HTTP). The clause concludes by specifying the overall format of the messages conveyed through these protocols. The following clauses describe the message content in detail.

5.1 Secure Sockets Layer/Transport Layer Security

If secure authentication of the server is desired, or if confidentiality of the information exchanged between client and server is desired, the communication between the devices shall be secured using the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) as described in this clause.

5.1.1 Protocol Version

Conforming systems shall support version 3.0 of the Secure Sockets Layer protocol [6] to secure their communications.

NOTE: As an implementation option, systems may support version 1.0 of the Transport Layer Security protocol [24] or later versions.

5.1.2 Client/Server Roles

When initiating a communication as part of the present document, the initiating system shall act as an SSL/TLS client while the responding system shall act as an SSL/TLS server.

5.1.3 CipherSuites

Annex B documents the cryptographic algorithms required and recommended by the present document, including SSL/TLS ciphersuites.

5.2 Hypertext Transfer Protocol

5.2.1 Protocol Version

Conforming systems shall support version 1.0 of the Hypertext Transfer Protocol [2] as the base transfer protocol for their messages.

NOTE: As an implementation option, systems may support HTTP version 1.1 [4].

5.2.2 Client/Server Roles

When initiating a communication as part of the present document, the initiating system shall act as an HTTP client, while the responding system shall act as an HTTP server.

5.2.3 TCP Port

Clients shall support sending their requests to TCP port 443 if SSL/TLS is being used, and to TCP port 80 otherwise. As an implementation option, communicating parties may agree to communicate via other TCP ports.

5.2.4 HTTP Methods

Requests from clients to a server shall be in the form of HTTP request messages using the POST method. Responses from a server shall consist of valid HTTP response messages.

5.2.5 Uniform Resource Identifier

The uniform resource identifier included in the POST request is not specified in the present document, but rather is subject to prior agreement between the communicating parties.

5.2.6 HTTP Headers

The HTTP header of the POST method shall minimally consist of the request-line. All request-header and general-header fields are optional. If present, they shall conform to the HTTP standard [2]. The status-line for the HTTP responses shall be present in those responses, and it shall conform to the HTTP standard, including status-code and reason-phrase values. All response-header and general-header fields are optional. If present, they shall conform to the HTTP standard.

5.2.7 HTTP Entity Body

Each message (i.e. HTTP entity body) conveyed as part of the present document shall conform to the Multipurpose Internet Mail Extensions standard [5], and shall, if signed, consist of exactly two parts, an Extensible Markup Language document and a Secure Multipurpose Internet Mail Extensions digital signature, as specified in the following two clauses. The highest level structure for each message shall conform to the multipart/signed syntax defined in S/MIME [18]. The message's media type shall be "multipart/signed" with appropriate parameters (e.g. protocol of "application/pkcs7-signature" and micalg of "sha1".) The entity shall indicate the correct content-length value, as defined in the HTTP standard [2].

If not signed, each message shall simply consist of a single, text/plain part.

6 XML Content

This clause specifies the actual message format used by the OSP to exchange pricing, authentication and authorization, and usage information. It outlines the overall XML document structure, lists the individual XML elements, and describes how those elements are combined into exchanges.

6.1 Document Structure

6.1.1 Multipurpose Internet Mail Extensions Conformance

As the first part of a Multipurpose Internet Mail Extensions (MIME) message, each message content shall conform to the MIME standard [5] as indicated below.

6.1.1.1 Content-Type

The message's content-type shall be designated text/plain.

NOTE: It is anticipated that the Internet Engineering Task Force (IETF) will eventually define a MIME content-type for XML documents (e.g. text/xml). When such a definition is available, subsequent revisions of the present document may specify the use of that content-type instead of text/plain.