Doc. A/96
3 February 2004

ATSC Standard:
ATSC Interaction Channel Protocols

Advanced Television Systems Committee
1750 K Street, N.W.
Suite 1200
Washington, D.C. 20006
www.atsc.org

The Advanced Television Systems Committee, Inc., is an international, non-profit organization developing voluntary standards for digital television. The ATSC member organizations represent the broadcast, broadcast equipment, motion picture, consumer electronics, computer, cable, satellite, and semiconductor industries.

Specifically, ATSC is working to coordinate television standards among different communications media focusing on digital television, interactive systems, and broadband multimedia communications. ATSC is also developing digital television implementation strategies and presenting educational seminars on the ATSC standards.

ATSC was formed in 1982 by the member organizations of the Joint Committee on InterSociety Coordination (JCIC): the Electronic Industries Association (EIA), the Institute of Electrical and Electronic Engineers (IEEE), the National Association of Broadcasters (NAB), the National Cable Television Association (NCTA), and the Society of Motion Picture and Television Engineers (SMPTE). Currently, there are approximately 140 members representing the broadcast, broadcast equipment, motion picture, consumer electronics, computer, cable, satellite, and semiconductor industries.

ATSC Digital TV Standards include digital high definition television (HDTV), standard definition television (SDTV), data broadcasting, multichannel surround-sound audio, and satellite direct-to-home broadcasting.

Table of Contents

Listing of Figures and Tables

ATSC Standard:
ATSC Interaction Channel Protocols

1. SCOPE

1.1 Purpose

This standard defines a core suite of protocols to enable remote interactivity in television environments. Remote interactivity requires the use of a two-way interaction channel that enables communications between the client device and remote servers. Examples of remote interactivity include E-commerce transactions during commercials, electronic banking, polling, email services, or other services yet to be defined.

1.2 Organization

The document is organized as follows:

Section 1: Describes the purpose and the organization of the document.

Section 2: Lists references and applicable documents.

Section 3: Provides definitions of terms, acronyms, abbreviations, syntax format, and code points.

Section 4: Provides an architectural overview and an introduction to the Interaction Channel Protocols.

Section 5: Describes the physical and data-link layer of the Interaction Channel Protocols.

Section 6: Specifies the network and transport layers of the Interaction Channel Protocols.

Section 7: Specifies the application layer of the Interaction Channel Protocols.

Section 8: Specifies a profile for certificates and certificate revocation lists.

Section 9: Specifies a protocol suite for establishing secure channels.

Annex A: Provides additional information on access technologies.

2. REFERENCES

2.1 Normative References

[RFC 791] Internet Protocol , RFC 791, IETF

[RFC 768] User Datagram Protocol, RFC 768, IETF

[RFC 793] Transmission Control Protocol, RFC 793, IETF

[RFC 2246] The TLS Protocol Version 1.0, RFC 2246, IETF

[HTTP1.1] Hypertext Transfer Protocol – HTTP/1.1, RFC 2616, IETF

[HTTP-AUTH] HTTP Authentication: Basic and Digest Access Authentication, RFC 2617, IETF

[HTTP-STATE] HTTP State Management Mechanism, RFC 2965, IETF

[RFC 2818] HTTP over TLS, RFC 2818, IETF

[RFC 1034] Domain Names – Concepts and Facilities, RFC 1034, IETF

[RFC 1035] Domain Names – Implementation and Specifications, RFC 1035, IETF

[RFC 2535] Domain Name System Security Extensions, RFC 2535, IETF

[RFC 2560] X.509 Internet Public Key Infrastructure Online Certificate Status Protocol, RFC 2560, IETF.

[RFC 2929] Domain Name System (DNS) IANA Considerations, RFC 2929, IETF

[PKIX] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 3280, IETF

[PKIXALGS] Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 3279, IETF

[URI] IETF RFC 2396, Uniform Resource Identifiers (URI). Generic Syntax. 1998.

[URI-LID] Declarative Data Essence - The Local Identifier (lid:) URI Scheme, SMPTE 343M, SMPTE

[UTF-8] UTF-8, A Transformation Format of ISO 10646, RFC 2279, IETF.

2.2 Informative References

[DBCAST] ATSC Standard A/90 (2000), Data Broadcast Standard.

[PSIP] ATSC Standard A/65 (1997), Program and System Information Protocol for Terrestrial Broadcast and Cable.

[FIPS 180-1] FIPS PUB 180-1, Secure Hash Standard, Federal Information Processing Standards

[PKCS#1] PKCS #1: RSA Encryption Version 1.5, RFC 2313, IETF.

[TRANSP] ATSC Standard A/53 (1995), ATSC Digital Television Standard.

[PPP] RFC 1662 “PPP in HDLC-like Framing”, W. Simpson, 21.07.1994.

[NTP] Network Time Protocol (Version 3) Specification, RFC 1305, IETF.

[RFC 1321] The MD5 Message-Digest Algorithm, RFC 1321, IETF

[SSL] The SSL Protocol Version 3.0, Internet Draft, IETF

[X9.42] ANSI X9.42 Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Algorithm Keys Using Diffie-Hellman.

2.3 Reference Acquisition

2.3.1 ATSC Standards

Advanced Television Systems Committee (ATSC), www.atsc.org, 1750 K Street N.W., Suite 1200 Washington, DC 20006 USA; Phone: +1 202 872-9160; Fax: +1 202 872-9161.

2.3.2 IETF Standards

Internet Engineering Task Force (IETF), www.ietf.org, c/o Corporation for National Research Initiatives, 1895 Preston White Drive, Suite 100, Reston, VA 20191-5434, USA; Phone: +1 703 620 8990; Fax: +1 703 758 5913.

2.3.3 ISO Standards

International Organization for Standardization (ISO), www.iso.ch, 1, rue de Varembé, Case postale 56, CH-1211 Geneva 20, Switzerland; Phone: +41 22 749 01 11; Fax: +41 22 733 34 30.

2.3.4 ITU Standards

International Telecommunication Union (ITU), www.itu.ch, Place des Nations, CH-1211 Geneva 20, Switzerland; Phone: +41 22 730 51 11; Fax: +41 22 733 72 56.

2.3.5 SMPTE Standards

Society of Motion Picture and Television Engineers, www.smpte.org, 595 W. Hartsdale Avenue, White Plains, NY 10607-1824, USA; Phone: +1 914 761 1100; Fax: +1 914 761 3115.

2.3.6 W3C Standards

World Wide Web Consortium (W3C), www.w3.org, Massachusetts Institute of Technology, Laboratory for Computer Science, 200 Technology Square, Cambridge, MA 02139, USA; Phone: +1 617 253 2613; Fax: +1 617 258 5999.

3. DEFINITIONS AND STRUCTURE

3.1 Compliance Notation

As used in this document, “shall” denotes a mandatory provision of the standard. “Should” denotes a provision that is recommended but not mandatory. “May” denotes a feature whose presence does not preclude compliance that may or may not be present at the option of the implementer.

3.2 Acronyms and Abbreviations

The following acronyms and abbreviations are used within this Standard:

ARM Application Reference Model
ATSC Advanced Television Systems Committee
CBC Cipher Block Chaining
CRL Certificate Revocation List
DASE DTV Applications Software Environment
DES Data Encryption Standard
DH Diffie-Hellman
DHCP Dynamic Host Configuration Protocol
DNS Domain Name Services
DOCSIS Data Over Cable Service Interface Specification
DSM-CC Digital Storage Media Command and Control
DSL Digital Subscriber Line
DTV Digital Television
EDE Encryption, Decryption, Encryption

HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol – Secure
ICMP	Internet Control Message Protocol
ICP	Interaction Channel Provider
ICSP	Interactive Content Service Provider
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPM	IP Multicast
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITV	Interactive Television
ITU	International Telecommunication Union
LAN	Local Area Network
MD5	Message Digest 5
MIP	Minimal Implementation Profile
MPEG	Moving Picture Experts Group
NIC	Network Interface Card
NTP	Network Time Protocol
OCSP	On-Line Certificate Status Protocol
OSI	Open System Interconnection
PKI	Public Key Infrastructure
POTS	Plain Old Telephone Service
PSIP	Program and System Information Protocol
RFC	Request For Comments
RSA	Rivest, Shamir, Aldeman
SCTE	Society of Cable Telecommunications Engineers
SHA-1	Secure Hash Standard 1
SSL	Secure Socket Layer
STB	Set-top Box
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSFS	Transport Stream File System
URI	Universal Resource Identifier
UDP	User Datagram Protocol
WAN	Wide Area Network

3.3 Global Terms

The following global terms are used within this Standard:

communication channel A digital medium that transports a digital stream. A communication channel can be uni-directional or bi-directional.

data carousel The scenario of the DSM-CC User-to-Network Download protocol that embodies the cyclic transmission of data.

datagram A datagram is the fundamental protocol data unit in a packet-oriented data delivery protocol. Typically, a datagram is divided into header and data areas, where the header contains full addressing information (source and destination addresses) with each data unit. Datagrams are most often associated with connectionless network and transport layer services.

interaction channel A digital medium that transports digital data from servers to clients and vice versa. An interaction channel is a logical construct built on top of physical channels.

Interaction Channel Provider The entity that provides access to inter-network connectivity to ITV clients. An Internet Service Provider may serve as an Interaction Channel Provider.

Interactive Content Service Provider The entity that provides services to ITV clients using a two-way communication channel.

ITV client A software or hardware entity capable of establishing a two-way communication channel with remote servers for the purpose of exchanging data and performing interactive transactions.

network A data carriage medium or a collection of data carriage media links used to exchange information between a service provider and one or more client agents or devices.

receiver Any device capable of receiving and consuming data carried on either broadband or narrowband network.

4. SYSTEM OVERVIEW AND INTRODUCTION

4.1 Architecture

This standard specifies protocols to enable interactive television applications using an interaction two-way channel possibly in combination with forward broadcast download channels from terrestrial, cable, and satellite networks. A typical topology for interactive television involves a client (for example a STB or a DTV unit) using a modem to exchange data with an Interactive Content Service Provider (ICSP). As Figure 4.1 illustrates, in order to communicate with the ICSP, the client may need to establish contact first with an Interaction Channel Provider (ICP), a role that may be fulfilled by a conventional Internet Service Provider (ISP).

A more complex but similarly likely access topology is shown in Figure 4.2. In this case, the interactive television client becomes part of a home LAN that may incorporate other elements such as hubs, switches, routers, servers, firewalls, CE devices, and other related data network devices and systems. The LAN communicates with the Interaction Channel Provider (ICP) typically through broadband access lines such as DSL, cable modems, ISDN, T1 lines, and others.

Data exchanged between the Interactive Content Service Provider (ICSP) and the ITV client may include for example application data related to a certain television program, news on-

demand extracted from a web server, or credit card information uploaded during some e-commerce transaction. It is assumed that content could be delivered from a service provider to a client by one or more delivery systems such as a terrestrial or cable broadcast channel and an interaction channel.

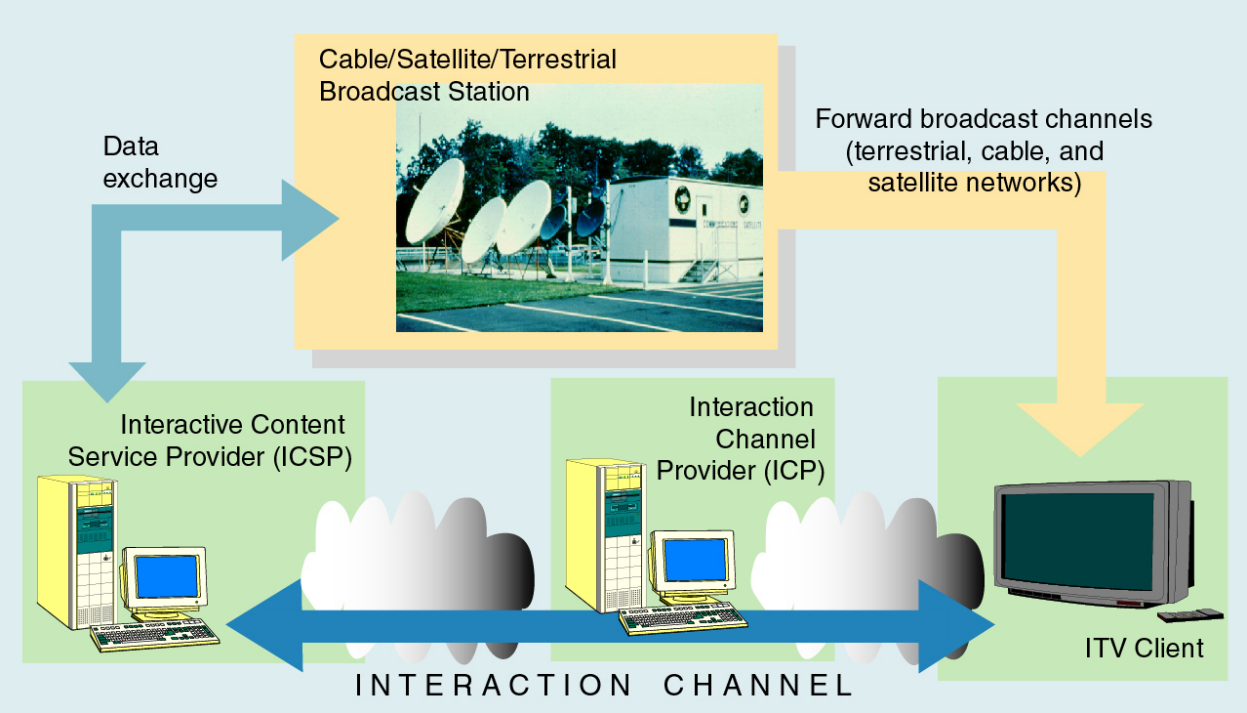

Figure 4.1 Architecture to provide ITV services over the interactive channel.

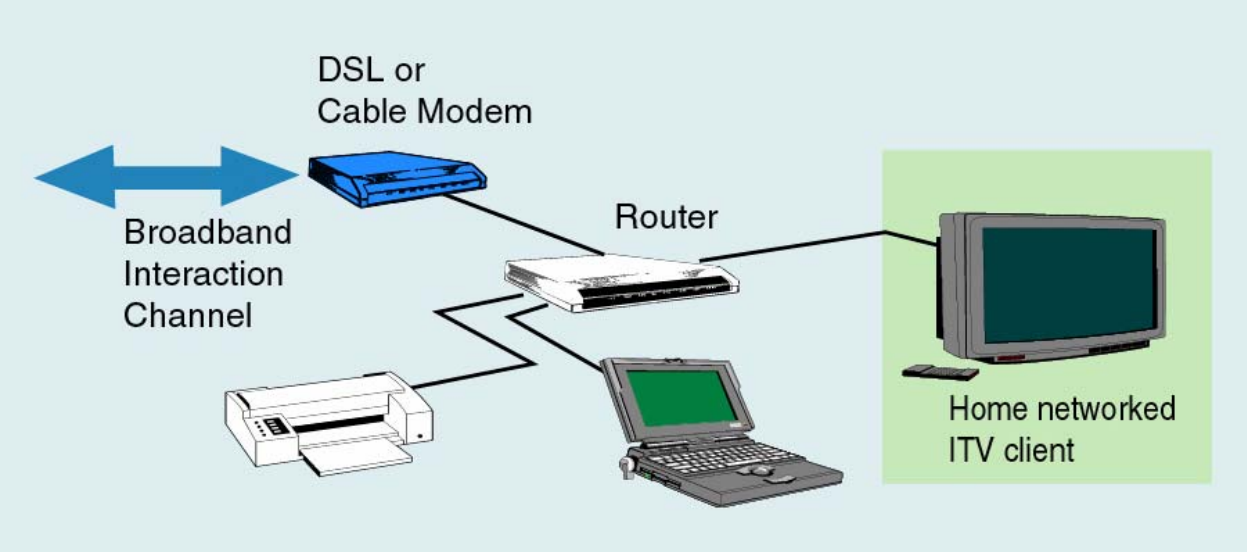

Figure 4.2 Architecture where the ITV client constitutes an element of a home LAN.

4.2 Remote Interactivity

Interactive television services are those that allow a certain degree of interaction between a user and an application running on the DTV unit or STB, or on a remote server. One way of providing interactivity is by using carousel data which after demultiplexing and decoding, is stored locally as shown in Figure 4.3*a*. In this case, a user will run application software based on data and code stored locally. A second manner to provide interactivity occurs when users access data or software located in remote servers using an interaction channel as shown in Figure 4.3*b*. This second manner is referred to as "remote interactivity". The protocols required for enabling remote interactivity constitute the purpose of this specification.

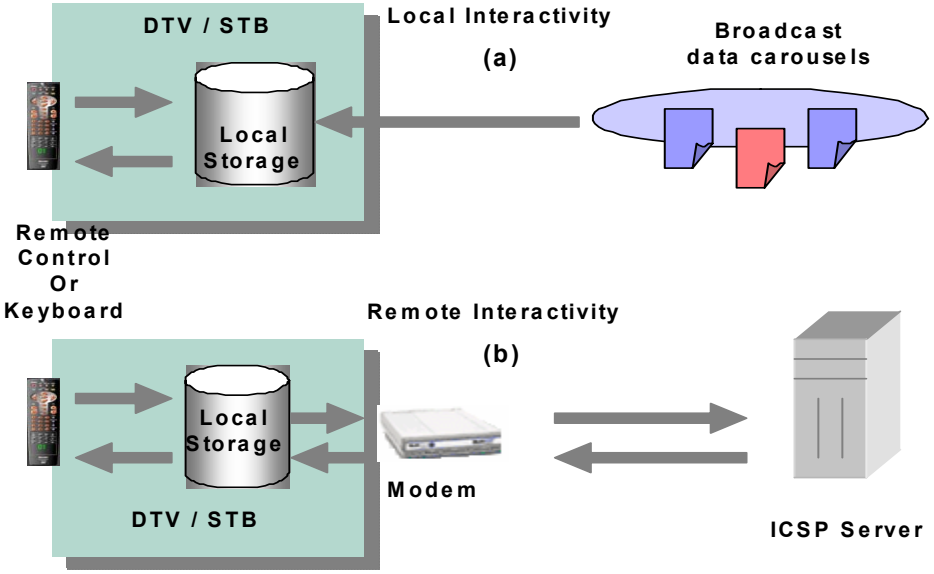

Figure 4.3 Local interactivity (*a*) compared to remote interactivity (*b*).

4.3 Service and Channel Providers

An Interaction Channel Provider (ICP) is the entity that provides network access for ITV clients that include an interaction channel. Notice that the interaction channel may be deployed using a narrow-band telephone modem, a high-speed T1 line, a cable modem, DSL, and others. Consequently, Internet Service Providers (ISP), telephone companies, T1 leasing companies, and others may act as Interaction Channel Providers. An Interactive Content Service Provider (ICSP) generates and manages remote applications and software to provide interactive television sessions once a communication channel has been established. An ITV client typically connects to a cluster of networks (including possibly the Internet) via an ICP. One of the networks in the cluster will include the ICSP remote server that hosts ITV applications. Communications between the ITV client and an ICSP remote server occur through a series of layered protocols as described and defined in subsequent sections of this document.

4.4 ITV Clients

Digital television devices, set-top boxes, PCs become ITV clients once they implement a wired or wireless connection with an ICP and support the protocols that enable remote interactivity.

Client devices are assumed to vary greatly in the number of services they are capable of presenting and their ability to store data or process it in some meaningful way. Some may decode and present several audio/video broadcasts along with multiple data services. Others may be designed to perform a single function (such as delivering a stock ticker or providing email services) as inexpensively as possible.

4.5 Protocol Layered Architecture

This Standard defines protocols to establish communications between the ICSP server and the ITV client. The chosen data communication protocols are based on conventional practices for Internet-based communication technologies.

Throughout this document, a five-layer reference model for system interconnections will be used to describe protocols. As Figure 4.4 illustrates, the proposed model defines a physical layer, a data-link layer, a network layer, a transport layer and an application protocol layer; a model that is consistent with Internet practice For comparison, the Open Systems Interconnection (OSI) model defines seven layers but in practice, the three top OSI layers (session, presentation, and application) are normally bundled tightly in a single layer (called the application layer in this document).

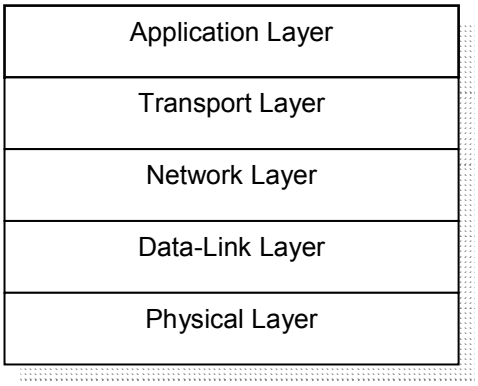

Figure 4.4 The five-layer model for client/server communication protocols.

4.6 Relation with other ATSC Standards

These specifications define a new communication channel between service providers and the user's home device (e.g., DTV, STB). As such, transport, multiplexing, and networking protocols do not use the predefined ATSC standards for those functions. Instead, the Interaction Channel Protocols rely on established Internet protocols. Figure 4.5 illustrates the parallel infrastructure defined by this specification and the manner in which it relates to other ATSC standards that exist at the time of writing.

Data exchanged over the interaction channel will be typically related to audiovisual or data services transmitted in broadcast channels, such as in e-commerce transactions during the commercial intervals of an sporting event. However, it is also possible to have service-independent data as well. An example of the latter would be the implementation of email services for DTV receivers or STBs.

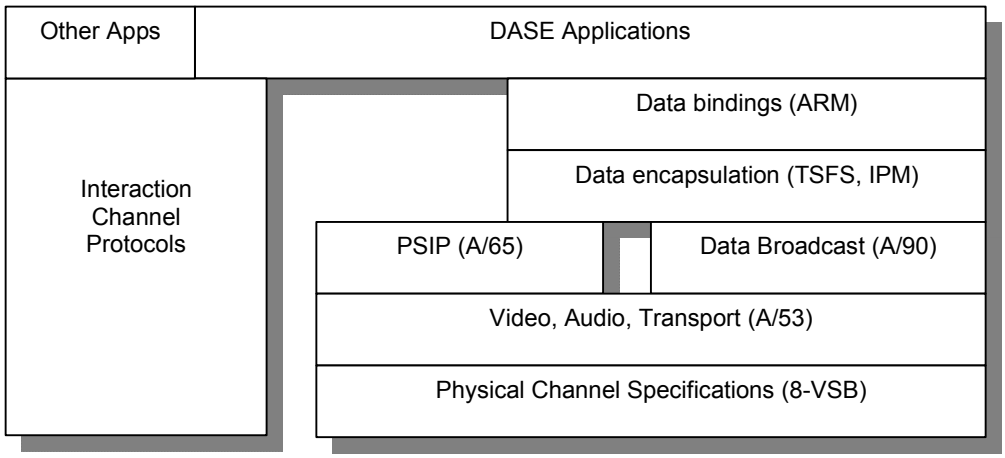

Figure 4.5 Relation of Interaction Channel Protocols and other ATSC standards.

An application in the form of files carrying code and data could be delivered using forward broadcast protocols. For ATSC, the broadcast files could include DASE content [DASE] carried using the multiple layers of ATSC data transport protocols [ARM, TSFS, IPM, DBCAST, TRANSP], and announcement protocol [PSIP]. Upon execution, the application may invoke Interaction Channel Protocols to communicate with ICSP remote servers and provide the remote interactivity experience. Figure 4.5 illustrates this case by showing a DASE protocol layer on top of both, forward broadcast and Interaction Channel protocols.

Other applications such as e-mail, games with remote interactivity, or web services could be deployed separately from broadcast facilities using the standardized Interaction Channel Protocols. Figure 4.5 also illustrates this case by showing the block 'Other Apps' independently structured on top of Interaction Channel protocols.

5. PHYSICAL AND DATA-LINK LAYER PROTOCOLS

This specification does not define the physical and data-link layer protocols that ITV clients may use to communicate with ICP servers or home network devices. Implementers should use the access technologies they consider adequate according to the environment in which the ITV client operates, and according to their own marketing and business plans for network integration.

Annex A provides some informative notes regarding physical and data-link layer protocols for common access technologies.

6. NETWORK AND TRANSPORT-LAYER PROTOCOLS

Network layer protocols enable communications (including addressing) between a remote server and the interactive television client over an interconnected system of networks. Transport-layer protocols deployed on top of network-layer protocols are used for end-to-end data exchange between servers and clients.

6.1 Network-Layer Support

Network devices that follow this specification such as ITV clients, ICSP servers and proxy servers require a minimal set of network-layer protocols for end-to-end communications.

Implementers should realize that for the insertion of ITV clients in a LAN, these devices should support other relevant protocols pertaining to LAN interconnections as defined in practice.

6.1.1 IP

Version 4 of the Internet Protocol defined in [RFC 791] shall be used as the baseline network-layer protocol for communications between ITV clients and servers from Interaction Channel Providers (ICP) and Interactive Content Service Providers (ICSP).

6.1.2 ICMP

In addition to the baseline IP protocols, ITV clients communicating with ICP or ICSP servers shall support the Internet Control Message Protocol (ICMP) defined in [RFC 792]. ITV clients shall implement the behavior associated with ICMP clients; implying that they will not generate messages designed for servers or proxies but they may decode and process those messages.

6.2 Transport-Layer Support

Network devices that follow this specification such as ITV clients, ICP and ICSP servers, and proxy servers, require a minimal set of transport-layer protocols (TCP and UDP) for end-to-end communications. Implementers should realize that for the insertion of ITV clients in a LAN, these devices should support other relevant protocols pertaining to LAN interconnections as defined in practice.

6.2.1 UDP

For transport-layer communications, interactive television clients, ICP servers, and ICSP servers shall support the User Datagram Protocol (UDP) defined in [RFC 768].

6.2.2 TCP

For transport-layer communications, interactive television clients, ICP servers, and ICSP servers shall support the Transmission Control Protocol (TCP) defined in [RFC 793].

7. APPLICATION LAYER PROTOCOLS

Network devices that follow this specification such as ITV clients, ICSP and ICP servers, and proxy servers, require a minimal set of application-layer protocols (HTTP, DNS) for end-to-end communications. Implementers should realize that for the insertion of ITV clients in a LAN, these devices may require other relevant TCP/IP applications.

7.1 HTTP

For communications at the application layer, ITV clients, ICP servers, ICSP servers, and proxy servers, shall support at least the mandatory portions of HTTP 1.1 as specified in [HTTP1.1] with the additional constraints defined in this section.

7.1.1 Role definitions

This section defines and describes the roles of the users of this standard. The following definitions were adapted from section 1.3 of [HTTP1.1].

7.1.1.1 Client

A client terminal or receiver communicates a request with one of the protocols specified in this section. The client may be in direct contact with a server or may be connected to the server through a proxy server. The client terminal will then receive a response to its request from the destination server.

7.1.1.2 Server

A server listens for client requests that are received directly from the client or via a proxy server. The server communicates its response back to the client directly or via a proxy server.

7.1.1.3 Proxy Server

A proxy server receives a request from a client intended for another server and passes the request on to the destination server or to the next proxy server in the route to the destination server. The proxy server receives a response from the destination server intended for the client and passes the response to the client or to the next proxy server in the route to the client.

7.1.2 HTTP Profiles

This section describes the additional constraints on HTTP 1.1 for clients, servers, and proxy servers.

7.1.2.1 Client Profile

An ITV client device supporting this standard shall implement the client portion of [HTTP1.1] with the additional constraints described herein.

7.1.2.1.1 Mandatory features

7.1.2.1.1.1 Closing Connections

A client that does not wish to maintain a persistent connection with a server or that is unable to do so shall send the “Connection: close” request header. See Section 8.1 of [HTTP1.1].

7.1.2.1.1.2 User Agent identification

A User-Agent request header, as defined in [HTTP1.1], shall be present in all HTTP requests.

7.1.2.1.2 Recommendations

The following subsections are recommended features or best practices from [HTTP1.1] that this standard wishes to emphasize.

7.1.2.1.2.1 Cache control and time source

A client should synchronize its clock to the application delivery system derived timing data or some other source of accurate timing data. If a client has reason to believe its clock is inaccurate, then it should perform conditional requests prior to reuse of a locally cached entity.

7.1.2.1.2.2 Support for HTTP/1.0 responses

A client should be able to parse a HTTP/1.0 response line; however, a client may treat response as if a 505 HTTP Version Not Supported status were returned in response to the request, and may subsequently close the connection on which the response was received. If a response is received without a status line, then it is likely emitted by a HTTP/1.0 server as a "simple response". In this case, it should be treated as if a HTTP/1.0 response line was received, and the same procedure described above applies.

The recommendation above does not preclude a proxy server from rewriting an upstream HTTP/1.0 response to be a valid HTTP/1.1 response to be received by a client.

7.1.2.1.2.3 Use of Referrer request header

The Referrer request header has many privacy issues associated with its use. See section 15.1.2 of [HTTP1.1] for further information.

7.1.2.1.2.4 From request header

The 'From' request header has many privacy issues associated with its use. See section 15.1.2 of [HTTP1.1] for further information.

7.1.2.1.2.5 GET and POST usage in form submissions

For the submission of form data, it is recommended that an application environment use the POST request method instead of the GET request method. See section 15.1.3 of [HTTP1.1] for further information.

7.1.2.1.2.6 HTTP Basic Authentication use

Reliance on HTTP Basic Authentication as defined in [HTTP-AUTH] is strongly discouraged. See Section 4 of [HTTP-AUTH] for a discussion of the limitations and pitfalls of HTTP Basic Authentication.

7.1.2.1.2.7 Use of Accept Request headers

A client should send the appropriate Accept* request headers. These headers include: Accept, Accept-Charset, Accept-Encoding, Accept-Language, and Accept-Ranges. The use of the Accept-Language header is particularly encouraged if a client has prior knowledge that the response body is or is expected to be language sensitive.

7.1.2.2 Server Profile

7.1.2.2.1 HTTP version requirement

The immediate proxy server or, in absence of any proxy server, the origin server shall support the server portion of HTTP/1.1.

7.1.2.2.2 Mandatory features

7.1.2.2.2.1 Entity Body and Content-Type

Any HTTP/1.1 message containing an entity-body shall include a Content-Type header field defining the media type of that body.

7.1.2.2.3 Recommendations

The following subsections are recommended features or best practices from [HTTP1.1] that this standard wishes to emphasize.

7.1.2.2.3.1 Range Requests

A server should support range requests as defined in [HTTP1.1].

7.1.2.3 Proxy Server Profile

7.1.2.3.1 HTTP version requirement

A proxy server that is the immediate proxy server for a client of this standard shall support the proxy server portion of HTTP/1.1.

7.1.3 HTTP State Management

7.1.3.1 Sending Cookies

The client shall send cookies as specified in [HTTP-STATE].

7.1.3.2 Receiving Cookies

The client shall accept cookies as specified in [HTTP-STATE].

7.2 DNS

The Domain Name Service (DNS) provides network hosts with the means to convert text-based domain names into destination IP addresses for generating TCP/IP traffic (forward conversion), as well as reverse translation from IP addresses to domain names.

For domain name resolution, ITV clients shall implement at least the DNS resolver protocols that enable forward translation of fully qualified domain names to IP addresses, as defined by [RFC 1034], [RFC 1035] and [RFC 2929].

The network that hosts the ITV client (e.g., the ICP network) shall provide the DNS database and the name servers defined in the specifications. In addition, ITV clients may implement the forward DNS resolver protocols for security-aware clients in accordance to the secure DNS specifications [RFC 2535].

7.3 Configuration Services

This specification does not define any particular method required by ITV clients to acquire the initial network configuration parameters, several of which depend on the network type. Some parameters, however, apply to any type of networks. In particular, the network that hosts the ITV client (e.g., the ICP network) shall provide ITV clients with the means to obtain at least the following configuration parameters:

- A unique temporary or permanent IP address for every network interface in an ITV client for the purpose of enabling IP-based communications between the ITV client and remote ICP and ICSP servers.
- One or more DNS server addresses which the ITV client uses for domain name resolution according to the DNS protocol.

- The address of a default gateway which the ITV client uses as a router in the local network to access other networks.

The configuration process may be performed manually, through private protocols, or using automatic configuration services such as DHCP [RFC 2131].

8. CERTIFICATES AND CERTIFICATE REVOCATION LISTS

8.1 Generalities

The syntax and semantics for Certificates and Certificate Revocation Lists (CRL) are derived from [PKIX]. However, from the large functional space defined by [PKIX], this standard defines a subset called the Minimal Implementation Profile (MIP) which determines the basic functionality that shall be supported by ITV clients. While performing secure electronic transactions, servers, proxies, and other clients shall assume that the target ITV client supports the MIP.

ITV clients shall implement the MIP. An implementation of the MIP results in a PKIX-compliant implementation. Implementations may choose to support additional features from [PKIX].

8.2 Minimal Implementation Profile for Certificates

Table 8.1 lists all the certificate fields and extensions defined by [PKIX] and it specifies their inclusion and support in the context of the Minimal Implementation Profile.

Table 8.1 MIP Support of PKIX Certificate Fields and Extensions

PKIX element	MIP support	Comments
Certificate Fields		
Version	Yes with constraints	Only Version 3 included in the MIP
Serial Number	Yes	
Signature	Yes with constraints	Only some selected algorithms included in the MIP
Issuer	Yes with constraints	Only some selected name encoding formats included in the MIP
Validity	Yes	
Subject	Yes with constraints	Only some selected name encoding formats included in the MIP
Subject Public Key Info	Yes with constraints	Only some selected algorithms included in the MIP
Issuer Unique ID	No	Defined as optional in [PKIX]
Subject Unique ID	No	Defined as optional in [PKIX]
Signature Algorithm	Yes with constraints	Only some selected algorithms included in the MIP
Signature Value	Yes	
Certificate Extensions		
Authority Key Identifier	Yes	
Subject Key Identifier	Yes	
Key Usage	Yes	
Private Key Usage Period	No	Use discouraged by [PKIX]
Certificate Policies	No	
Policy Mappings	No	
Subject Alternative Name	Yes with constraints	Only some selected name encoding formats included in the MIP
Issuer Alternative Name	Yes with constraints	Only some selected name encoding formats included in the MIP
Subject Directory Attributes	No	Use discouraged by [PKIX]
Basic Constraints	Yes	
Policy Constraints	No	
Extended Key Usage	Yes	
CRL Distribution Points	Yes with constraints	Only some selected access mechanisms included in the MIP
Inhibit Any-Policy	No	
Freshest CRL	No	
Authority Information Access	Yes	Only some selected access mechanisms included in the MIP
Subject Information Access	No	

8.2.1 Constraints on Certificate Fields

Reference [PKIX] defines the actual syntax and semantics for certificate fields. Constraints on certificate fields that determine the MIP profile are given below.

8.2.1.1 Constraints on Version

This field describes the protocol version for certificates. An ITV client that supports the MIP shall be capable of processing version 3 of X.509 certificates.

8.2.1.2 Constraints on Issuer and Subject

The Issuer field describes the entity that has signed and issued the certificate. The 'Subject' field describes the entity that owns the public key carried in the certificate. An ITV client that supports the MIP shall decode these fields when encoded as PrintableString, BMPString, and UTF8String.

The restrictions imposed in the previous paragraph imply that an implementation that does not include functionality beyond the MIP will not decode TeletexString or UniversalString. Reference [PKIX] deprecates the use of these encoding types for new certificates.

8.2.1.3 Supported Cryptographic Algorithms for Signature and Subject Public Key Info

The MIP subset of cryptographic algorithms for digital signatures that shall be supported by ITV clients is listed in Table 8.2.

Table 8.2 Algorithms for Digital Signatures

Algorithm	Implementation Specifications
RSA with SHA-1	The implementation shall comply with [PKIX] and [PKIXALGS].
RSA with MD5	The implementation shall comply with [PKIX] and [PKIXALGS]

Note: As defined in [PKIXALGS], the implementation of the RSA, SHA-1, and MD-5 algorithms follows respectively [PKCS#1], [FIPS 180-1], and [RFC1321].

The MIP subset of cryptographic algorithms for key agreement protocols that may be supported by ITV clients and servers is defined in Table 8.3.

Table 8.3 Algorithms for Key Agreement

Algorithm	Implementation Specifications
DH	If implemented, the implementation shall comply with [PKIX] and [PKIXALGS]

Note: As defined in [PKIXALGS], the implementation of the Diffie-Hellman algorithm follows [X9.42].

For RSA and DH (if implemented), ITV clients and servers shall be capable of processing key lengths with not less than 512 bits and as large as 4096 bits. ITV clients and servers should reject keys that exhibit lengths less than 512 bits (insecure key lengths) but they may accept key lengths larger than 4096 bits.

The key lengths described in this section apply to the US. Other countries may have different legal constraints (typically export and import policy constraints) and hence, they may define different limits.

8.2.2 Constraints on Extension Fields

Table 8.1 defines certificate extension fields that shall be supported by MIP implementations. Reference [PKIX] defines the syntax and semantics for these extension fields and it also defines whether each extension should be treated as critical or not.

Certificates Authorities that issue certificates for the ITV environment, and which carry extension fields other than the ones included under the MIP should exercise caution when marking those extensions critical. According to the rules and procedures described in [PKIX], software agents that find a critical mark in one of their unsupported list of extensions, are required to discard the certificate and fail the validation process.

The next subsections define extension field constraints applicable to the Minimal Implementation Profile (MIP).

8.2.2.1 Constraints on the Subject Alternative Name

This extension field defines the means to provide alternative names associated to the subject. From all the possible alternative name formats described in [PKIX], server and clients that implement the MIP shall be capable of decoding and processing at least the following formats:

- rfc822Name for names based on email addresses
- dNSName for names based on DNS entries
- uniformResourceIdentifier for names based on non-relative “http” URIs.
- iPAddress for names based on IP addresses

8.2.2.2 Constraints on the Issuer Alternative Name

This extension field defines the means to provide alternative names associated to the issuer. As such, it performs similar functions as the Subject Alternative Name. Consequently, the MIP restrictions defined for the Subject Alternative Name apply identically to this field too.

8.2.2.3 Constraints on CRL Distribution Points

This extension field defines methods and locations for accessing CRLs associated with the certificate. From all the possible methods defined by [PKIX], clients implementing the MIP shall be capable of decoding and processing:

- The CRL repository locations identified by their non-relative “http” URI”

8.2.2.4 Constraints on the Authority Information Access

This extension field defines a method to locate additional information pertaining to Certificate Authorities. From the two objects defined by [PKIX], ITV clients supporting the MIP should be capable of decoding only id-ac-ocsp. This object signals the existence of an OCSP service to check the status of the certificate. From the several access methods that could be employed for this object, ITV clients implementing the MIP shall be capable of processing and decoding:

- The OCSP service locations identified by their “http” URIs.

8.3 Minimal Implementation Profile for CRLs

Table 8.4 lists all the CRL fields and extensions defined by [PKIX] and it specifies their inclusion and support in the context of the Minimal Implementation Profile.

Table 8.4 MIP support of PKIX CRL Fields and Extensions

PKIX element	MIP support	Comments
CRL Fields		
Version	Yes with constraints	Only Version 2 included in the MIP
Signature	Yes with constraints	Only some selected algorithms included in the MIP
Issuer	Yes with constraints	Only some selected name encoding formats included in the MIP
thisUpdate	Yes	
nextUpdate	Yes	
Revoked Certificates	Yes	
Signature Algorithm	Yes with constraints	Only some selected algorithms included in the MIP
Signature Value	Yes	
CRL Entry Extension Fields		
Reason Code	No	
Hold Instruction Code	No	
Invalidity Date	No	
Certificate Issuer	No	
CRL Extension Fields		
Authority Key Identifier	Yes	
Issuer Alternative Name	Yes with constraints	Only some selected name encoding formats included in the MIP
CRL Number	Yes	
Delta CRL indicator	No	
Issuing Distribution Point	No	
Freshest CRL	No	

8.3.1 Constraints on CRL fields

8.3.1.1 Constraints on Version

This field describes the protocol version for CRLs. An ITV client that supports the MIP shall be capable of processing version 2.

8.3.1.2 Constraints on Signature and Signature Algorithm

The selected algorithms exposed by these fields shall be the same ones allowed for certificates.

8.3.1.3 Constraints on Issuer

This field performs an identical function as the certificate Issuer field. The MIP restrictions for the certificate Issuer field shall apply in this case too.

8.3.2 Constraints on CRL Entry Extension Fields

An ITV client that does not provide functionality beyond the MIP is not required to process any of the CRL Entry Extension Fields.

8.3.3 Constraints on CRL Extension Fields

8.3.3.1 Constraints on Issuer Alternative Name

This extension field provides similar information as the field with identical name defined for certificates. It is used to provide alternative name representations for the CRL issuer. The MIP restrictions defined for the certificate's Issuer Alternative Name extension apply identically in this case too.

8.4 Certificate Processing and Operations

8.4.1 Certificate Status Validation

Upon verification of a certificate's cryptographic signature, and after verifying that the certificate has not expired, an ITV client implementation shall determine the status of the target certificate (that is, determine if the certificate is still valid or not). Status validation requires access to an up-to-date Certificate Revocation List or an on-line status-checking service.

If the status information for a certain certificate cannot be determined, the certificate shall be considered invalid.

Certificate Authorities that publish Certificate Revocation Lists shall ensure that the http URI locator required to access the list be clearly defined in the certificate's CRL Distribution Point extension field. ITV clients should attempt to obtain periodically the most recent CRL based on the information found in the nextUpdate field that exists in CRLs.

Certificate Authorities that rely on on-line validation services shall ensure that the http URI locator required to access the service be clearly defined in the certificate's Authority Information Access extension field. ITV clients should implement the Online Certificate Status Protocol (OCSP) [RFC 2560] as the means to enable on-line status validation.

8.4.2 Certificate Path Build-Up and Validation

8.4.2.1 Trust Association

Given a digitally signed entity *X*, and a collection of certificates

$$C = \{C_0, C_1, ..., C_N\}$$

where C_0 represents the trusted root certificate and C_N represents the certificate that carries the public key for signing *X*. The entity *X* shall be considered a trusted entity if a valid certificate path exists between C_0 and C_N. In addition, the principal that signs entity *X* (whose distinguished name also appears as the Subject in C_N) shall be considered a trusted principal.

8.4.2.2 Path Validation

Given a prospective certificate chain between C_0 and C_N, the chain shall be considered valid if it satisfies the conditions of the path validation algorithm defined in [PKIX].

8.4.2.3 Name Matching

Name matching describes the process of comparing and matching the Subject name in C_i and the Issuer name in certificate C_{i+1} during the build up of a certificate chain. Although [PKIX]

recommends field-based comparisons of distinguished name fields, for the purpose of this specification, ITV clients shall perform byte-level matching.

> Note: [PKIX] accepts the notion of byte-level matching instead of the field-based comparisons.

9. SECURE CHANNEL PROTOCOLS

In a typical scenario, the communication channel established between the ITV client and the ICSP server includes several network segments belonging to multiple parties such as in the Internet. For this reason, the communication channel could suffer attacks ranging from interceptions to impersonations. .It is therefore necessary to secure the communication channel by using encryption technologies.

Protocols that have been extensively deployed over the Internet include SSL/TLS and IPSec. SSL/TLS protects a channel at the transport layer, whereas IPSec acts at the network layer. In this specification TLS is used as the security layer for HTTP to enable secure data exchange at the application layer using HTTPS.

9.1 TLS

The Transport Layer Security (TLS) protocols shall be used to provide secure data exchange between the ITV client and ICSPs at the application layer.

9.1.1 Protocol Version Support

An ITV client that communicates with an ICSP server using an interaction channel shall support TLS version 1.0 as described in [RFC 2246]. The ITV device should implement the client portions of these protocols, whereas the ICSP server should implement the server specifications.

In accordance to the TLS specifications, during the TLS handshake, the ITV client requests a secure connection with the highest possible protocol version available. An ITV client shall expose a version value of 3.1 which corresponds to TLS. The server reply exposes the server's own preference and it may indicate version 3.1 (for TLS), or 3.0 (for SSL v3), or 2.0 (for SSL v2). Accordingly, an ITV client shall accept the TLS proposal. An ITV client should reject proposals to use SSL v2 due to vulnerabilities in the protocol.

9.1.2 TLS Cipher Suites

From the list of TLS cipher suites defined in [RFC 2246], an ITV client shall be capable of processing the subset defined in Table 9.1.

Table 9.1 TLS Cipher Suites

Cipher suite token	Authent.	Key Exchange	Encryption	Digest
TLS_RSA_WITH_NULL_MD5	RSA	RSA	None	MD5
TLS_RSA_WITH_NULL_SHA	RSA	RSA	None	SHA-1
TLS_RSA_WITH_DES_CBC_SHA	RSA	RSA	DES, CBC mode	SHA-1
TLS_RSA_WITH_3DES_EDE_CBC_SHA	RSA	RSA	3DES, EDE & CBC	SHA-1

9.1.3 Other Cipher Suites

Clients and servers expose their supported cipher suites and then select one for operation as part of the TLS handshake protocol. Accordingly, an ITV client shall expose at least the cipher suites defined in Table 9.1. An ITV client may expose and select for operation other cipher suites defined in [RFC2249], however the client should refuse operations that involve the use of cipher suites with export grade algorithms. Export grade algorithms use short 512-bit public keys and 40-bit symmetric keys and are easily breakable. Export grade algorithms are recognized in TLS by the use of the word EXPORT as part of the token that defines a particular cipher suite.

Other countries may define a different set of algorithms consistent with their own policies and practices.

9.2 HTTPS

ITV clients and servers interested in establishing a secure channel for HTTP connections shall use the rules and recommendations defined in [RFC2818] to establish TLS channels that carry HTTP messages.

9.2.1 Protocol Identifier

As defined in [RFC 2818], ITV clients shall use ‘https’ as the URI protocol identifier for HTTP transactions over TLS.

9.2.2 Port Number

As defined in [RFC 2818], transactions that use ‘https’ connect normally using port number 443 unless a different port number is explicitly specified in the URI.

Annex A:
Informative Notes on Access Technologies for Physical and Data-Link Layer Protocols

From the connection topology perspective, there are two major modes to connect physically an ITV client device to the network. The first option uses a dedicated remote access line such as a telephone modem (see Figure 4.1 for an example) to connect with an ISP or ICP. The second option implies connecting the device to a home LAN (see Figure 4.2 for an example) which includes a separate device (router or gateway) that connects with other networks or an ISP.

Remote access connections create usually a dedicated line between the ITV client and the Interaction Channel Provider. A typical setting for example would involve using a POTS line with a V.90 modem for digital-to-analog signal conversion and transmission at rates up to 56 Kbps. The typical data-link protocol in this case is PPP. Broadband access technologies that use DSL or a Cable Modem are also becoming popular.

If the ITV client device connects to a home LAN, then it may require a Network Interface Card (NIC) that provides support for particular physical and data-link layer protocols. Ethernet networks using UTC cabling constitute the most typical scenario in practice. Wireless networks with rates of 11 Mbps and above are also becoming popular. A router or gateway system will control access to the local home network. This router or gateway may bridge the local home network to a separate LAN, WAN, or the Internet using DSL, Cable Modem, ISDN, leased T1 lines, and other related protocol series.

The list of popular access technologies include but it is not limited to:

- Remote access via POTS and PPP
- IEEE 802.3 series of Ethernet protocols
- IEEE 802.11 series of Wireless Networking protocols
- DOCSIS series of Cable Modems
- DSL Protocol series (high bit rate, symmetrical, asymmetrical, rate adaptive, lite, etc)

Implementers should notice that connectivity of ITV clients using a home LAN requires support for additional protocols above the physical layer, including configuration protocols such as DHCP, device and service discovery, network management, and others.