UIC CODE 917-5

2nd edition, December 2003

Original

O

Description of the HERMES System

This leaflet will be published only in English

UNION INTERNATIONALE DES CHEMINS DE FER
INTERNATIONALER EISENBAHNVERBAND
INTERNATIONAL UNION OF RAILWAYS

Leaflet to be classified in Volume :

IX - Information Technology, Miscellaneous

Application :

With effect from 01.01.2003
All members of the International Union of Railways

Record of updates

1st edition, July 1985	First issue
2nd edition, December 2003	Overhaul of Leaflet - Retyped in FrameMaker Adaptation to the editor's guide M1 - New lay-out

The person responsible for this leaflet is named in the UIC Code

Contents

Summary

The purpose of this leaflet is to describe the data transmission system used as carrier for international IT applications of railway organisations (RO)[1] and to define the appropriate standards and components.

This data transmission system is subsequently referred to as the "HERMES system".

In order to make it possible for the ROs to use the HERMES system and to communicate with one another, it is necessary to make obligatory specifications of the connection characteristics for network access and security, of protocols and functions, of regulations at user level, of message structure etc. These regulations must strictly be observed by all users of the HERMES system, as otherwise any data communication between ROs will be impossible or lead to system breakdowns.

1. UIC & OSJD members and other railway-oriented organisations

1 - Introduction

1.1 - Brief description of the system

The HERMES system is a pan-European data communication service mainly built to ensure the communication between international IT applications of ROs operating on different IT platforms.

The IT applications are not part of the system as defined in this context.

The description refers to the OSI Reference model (see Appendix A - page 24).

1.1.1 - Standards and components up to network level

The chosen standard on network level is IPv4, later to be migrated to v6.

It is implemented via an international IP service provider.

Connection of ROs is according to the document "HERMES VPN Rules of Connection".

Security definitions are described in the document "HERMES VPN Security Policy" (see also point 2.2.4 - page 10.

For details on components see point 2.2 - page 6.

1.1.2 - Standards and components above network level

This leaflet defines the standards for transport and session level for the IT applications using the HERMES system.

The so called "HOSA Protocols" (HERMES Open Systems Architecture) are used.

On transport level: basically TCP.

On session level: FTP, BQM, HTTP and Internet Messaging.

Each RO is responsible for the implementation of the required HOSA Protocols within its own IT environment according to the document "HOSA Implementation Guidelines".

Security definitions are described in the document "HERMES VPN Security Policy" (see also point 2.2.4 - page 10).

For details on components, see point 2.3 - page 10.

1.2 - IT applications using the HERMES system

The most important international IT applications are: seat reservation, train pre-advice and wagon search.

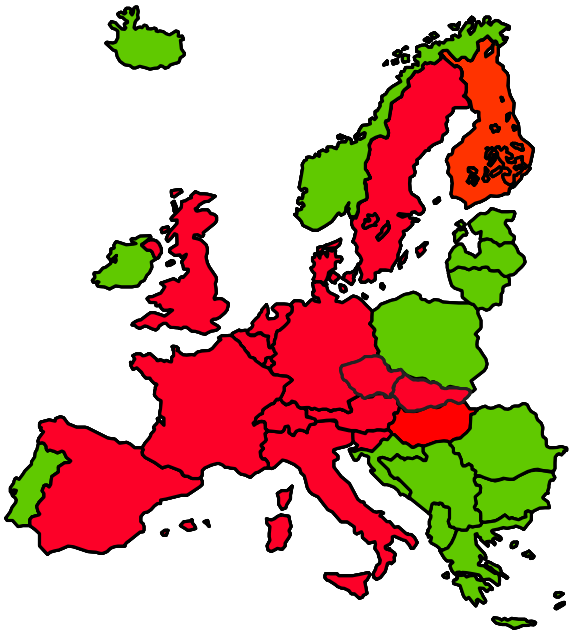
It is up to each RO to decide which application it uses.

A list of the UIC applications is published in *UIC Leaflet 912, Appendix 5*. More detailed descriptions are available in the GPH manual.

1.3 - Users of the HERMES system

On January 1st 2003 following RO's are connected to the HERMES System: ATOC, CD, CFL, DB-AG, DSB, FS, NS, MAV, ÖBB, RENFE, SBB, SJ, SNCB, SNCF, SZ, VR, ZSR, Interfrigo.

For an up-to-date list, refer to HIT Rail.



1.4 - History of the HERMES system

The European railways have always been in the vanguard of international data communications. HERMES took shape in 1978 when six railways - BR, DB, FS, SBB, SNCB and SNCF - agreed, under the patronage of the UIC, that there was a need to provide a high quality data communications network across railway boundaries. They decided to develop and operate a network supporting a wide range of structured exchanges of information between otherwise incompatible IT platforms serving passenger and freight business.

They commissioned the installation of the "HERMES" network. From the beginning the decision was made to use international standards where possible. This lead to the adoption of CCITT X.25 as the network protocol. In the absence of standards for the higher-level protocols, a common set of

messages was defined and each national data network had to interpret this message and create a suitable response.

It was envisaged that within the next two years, several other railway companies would be in a position to exchange data with existing HERMES members. HERMES was then extended to include DSB, NS, ÖBB, RENFE and SJ as well as organisations hosted by member railways, such as Interfrigo and Intercontainer.

The expenditure on HERMES and its applications was kept at a modest level. The limiting factor was not the provision of telecommunications support but the effort involved in implementing the data structures and messages required.

By 1990 the network connecting 11 railways had been in use for over ten years and needed renewing. HIT Rail was formed and given this task. The new "HERMES Plus" network used more up-to-date X.25 nodes and managed the migration of the railways' systems to the new extensively meshed network. Continuous management was provided from the Network Management Centre in Nottingham. The inter-application standards developed to communicate over the initial network were still in effect.

Railways cannot in practice define their own information standards and expect their customers and suppliers to accept them. The European railways require that the network should work cost-effectively and to a defined standard of quality. It is obvious that the only way to achieve this goal is to implement published computing standards, like the Open Systems Interconnection (OSI) or market standards (TCP/IP). As a first move to respond to an increasing need of railway partners to communicate using newer network protocols, IP routers for particular applications were connected to the existing X.25 backbone. By doing so contemporary protocols were transmitted over the legacy network.

To reduce the costs inherent to ownership of network nodes and leasing lines while keeping a flexible pan-European network responding faster to future changes in partnerships and the marketplace, in 1998 the railways, represented by HIT Rail decided to build a HERMES Extranet. This robust, stable, low-risk and cost-competitive collaborative framework of services, supports the existing and emerging HERMES community at a required level of quality and reliability for existing and emerging e-commerce opportunities. This HERMES Extranet intents to guarantee the initial fundamental objective: interoperability between the HERMES partners. Within the same strategy the partners have also adopted the HERMES Open Systems Architecture (HOSA) using standards drawn from the Internet protocol suite.

1.5 - Competence

Responsabilities within the HERMES system are as follows:

1. **Up to network level**

- administration:	HIT Rail
- establishment and operation:	VPN provider
- Point of contact towards VPN provider:	HIT Rail
- security:	GPH, locally: RO

2. **Transport and session level incl. API (Application Program Interface)**

- definition: GPH
- local implementation: RO
- operation: RO
- security: GPH,
  locally: RO

1.6 - Contact

HIT Rail B.V. Web: http://www.hitrail.com

2 - The HERMES system

2.1 - Basic Principles

- Meet railways' functionality

- Meet requirement of interoperability - openness

  Transport is one of the most important sectors of economic activities. The HERMES railways believe that the availability of transport applications which support seamless data exchange is decisive for the future of the rail industry. A fundamental requirement is interoperability between the different information and communications technology systems of the HERMES Railways but also openness to third parties, e.g. customers or partners in multimodal traffic, to support the railways' business processes.

- Be consistent with technological and market developments

  The key technological trends focus on Internet technology for universal networking and application connectivity while the Web provides an universal interface for access to applications. In addition, Internet and Web-based protocols are increasingly being implemented for intra-organisational communications ("Intranet"). Many industry communities also apply Internet and Web-based protocols for communications with selected business partners ("Extranet").

- Minimise costs

  The use of widely accepted standards dramatically reduces software costs and supplier dependency and also enables outsourcing to service providers benefiting from the competition on the market.

2.2 - The Network

2.2.1 - Principles

For reasons mentionned in point 2.1 the Internet standard IP v4 was selected.

- Paid SLA-based Services (why not just use the Internet?)

  The HERMES Railways need Reliability, Security and Quality assurance which only can be guaranteed via an SLA-defined service and clear responsibilities. Because the HERMES Railways cannot afford to risk running time- and business-critical applications on an "unreliable" and "anonymous" communication infrastructure, the Internet cannot be used. This is not a situation singular to the railways. Well known examples of other industry sectors using international VPN's are the motor industry (ANX), the banks (Bolero) and the airlines (Open Travel Alliance).

- Services Outsourced

  The decision to outsource the network services was principally a matter of cost reduction. Given the competition on the telecom market, it turned out that a reduction of 30% compared to the costs

of the former HERMES Plus Network could be attained. So after an RFP procedure, the services were outsourced to an international IP service provider.

- Meet Service Level and Performance Needs

  Service level agreement and performance criteria of the former HERMES Plus network must be met.

- Organisational and technical flexibility

  The network architecture and the supplier organisation have to be flexible in order to be able to adapt to structural changes, such as amalgamations, demergers and acquisitions. It also has to support access by new HERMES Railways and third parties. Network performance and other services should be easily and flexibly adaptable to the versatile requirements of the users (scalability).

2.2.2 - Specification

A VPN is a private network deployed over a service provider's backbone network providing levels of privacy, security, quality of service, and manageability similar to networks built on dedicated, privately owned or leased facilities.

The pan-European IP-based HERMES VPN provides a flexible, managed and cost efficient communications environment: it aims to bring tangible business value to the HERMES community. The end-to-end data communication services allow flexible railway business process interactions.

Main characteristics of the interfaces between the partners' corporate network and the VPN are:

- IEEE 802.3 10/100 is used as interface to the partners' corporate network

- depending on the end user's requirements, the transmission rate of the access circuits from the Customer Premises Equipment (CPE) to the VPN's Point of Presence (PoP) can be scaled up or down;

- in case of an outage of the access circuit the connection will be established using BRI ISDN back up;

- some partners dispose of 2 interconnected sites. Both CPEs are connected to the VPN and configured to support Cisco's proprietary Hot Standby Router Protocol (HSRP). If one CPE or access fails the other CPE will be used to provide VPN access. In this case the ISDN back up capability is not installed. HSRP is described by RFC2281 (March 1998). A "Request for Comment" describes an Internet standard handled by the Internet Activities Board (IAB).

The following features allow a VPN to deliver the required data communication services.

Basic network features

- The current network protocol is IP v4. If, in the future, IP v6 becomes mature enough the VPN can migrate to this new version. Should one of the HERMES partners use IP v6 before the network has migrated to the new protocol its data will be transparently transported over the existing infrastructure.

- As an optional feature a Domain Name System (DNS) can be added to provide mapping from hostnames to IP addresses.

- Network Address Translation (NAT) and Port Address Translation (PAT), a subset of NAT, as well as Access Lists are used to allow the HERMES partner networks to maintain their addressing plan while communicating over the VPN. These functions can be performed either by the CPE or by the railway firewall, but preferably by the railway firewall.

Security

Security features include all capabilities contributing to guarantee end-to-end traffic privacy. Among the major features provided by the VPN, we can enumerate:

- tunnelling including end-to-end IPSec multilevel encryption using standards such as AES, DES or 3DES secret key encryption system and MD5 or SHA1 hashing techniques,

- Authentication, Authorisation and Accounting (AAA) services,

- anti-spoofing protection preventing attacks based on the ability to falsify the source IP address,

- protection of the network against most of the known Denial-of-Service attacks and Flooding,

- protection against Network Sniffing revealing confidential data.

Traffic prioritisation

If traffic prioritisation is needed, an appropriate feature can be established by the VPN provider. It offers differentiated performance levels and prioritisation of delay and non-delay sensitive traffic.

Incoming packets from the Local Area Network (LAN) are tagged in the CPE to identify the priority and time sensitivity of its payload.

Traffic is then sorted and routed based on the delivery priority.

When congestion is detected, a queuing mechanism uses the packet classification to perform selective packet discard at the serial interface to the Wide Area Network (WAN).

HERMES traffic will be classified as follows: MQ traffic has high priority, FTP and HTTP are considered normal and SMTP is assigned low priority.

When there is no congestion, every application will be able to consume the full bandwidth.

Service levels

The VPN provider is able to offer solid and comprehensive service-level agreements based on CPE availability, Mean Time to Restore/Repair, Round Trip Delay and throughput. Every service level indicator has its own performance target, which will enable assessment of how effectively the services have been carried out. If a service fails to meet the service levels performance, penalties will be paid.

The VPN is supervised by a Network Operations Centre (NOC). Proactive operations support and troubleshooting of network and service infrastructure components guarantee high network availability and performance and support Service Level Agreements (SLAs). Seamless management tools provide combined reports including all Key Performance Indicators (KPI) and traffic accounting data. These quality services are vital to supply onward services to all partners connected through the VPN.

2.2.3 - Problem Management and User Support

The VPN provider operates a Customer Support Centre (CSC) offering a set of services, such as:

- 7x24 h monitoring and maintenance, 365 days a year,
- proactive operations support and troubleshooting of network and service infrastructure components,
- planned maintenance mutually agreed between provider and customers such as to minimise impact on customer operations,
- for all incidents detected (by the VPN provider) a trouble ticket will be opened and the "Single Point of Contact" (SPoC) provided by each customer will be contacted by its chosen communication means (email notification, pager, fax, SMS, telephone). In case of hardware problems, a technician is called to fix the problem; in case of software failures, NOC engineers will ensure the rectification of the problem. The customer will be informed about the progress on a regular basis and about the closing of the ticket after the successful fix. The open tickets can be reviewed by a web-based tool. After successful fault clearance the following information is made available:

  - ticket reference number,
  - time of the fault,
  - cause of the fault,
  - action taken.

The CSC renders assistance to the ROs and provides proactive information. The NOC is in charge of tackling the faults as they arise. The VPN provider runs an internal escalation process which can also be requested by HIT Rail.

1st level	CSC (co-ordinator) / NOC (shift supervisor)
2nd level	CSC manager / NOC manager
3rd level	CSC / NOC directors
4th level	Vice-president, operations

The VPN provider documents the HERMES VPN information in an appropriate manner and publishes it via a web-based tool among the HERMES ROs.

Reports are generated and made available to HIT Rail by the web tool. These reports include:

- provisioning,
- network and site availability,
- CPE monitoring,
- throughput,
- fault reporting,
- CPE equipment database.

2.2.4 - Security Issues

Security issues have to be respected for both the HERMES VPN and the RO networks.

HERMES VPN:

The border between the VPN and the RO networks is represented by the HERMES VPN routers, controlled by the NOC.

The security related rules and measures to be applied to the HERMES VPN have been defined in the document "HERMES VPN Security Policy". It specifies the security policy requirements and the rules to be respected when other systems wish to connect to the HERMES VPN and vice versa.

The document "HERMES VPN Security Policy" is available on request from HIT Rail.

Local sites:

The security policy within the RO networks is the responsibility of the individual ROs.

2.3 - The HOSA Protocols

2.3.1 - Principles

For communication between UIC applications, the HOSA protocol suite is used on session level which is:

- **FTP** for file transfers between UIC file transfer applications,
- **BQM** for the communication between UIC dialogue applications,
- **HTTP** used to transfer hypertext documents,
- **Internet Messaging** for a secure electronic mail handling in the HERMES environment.

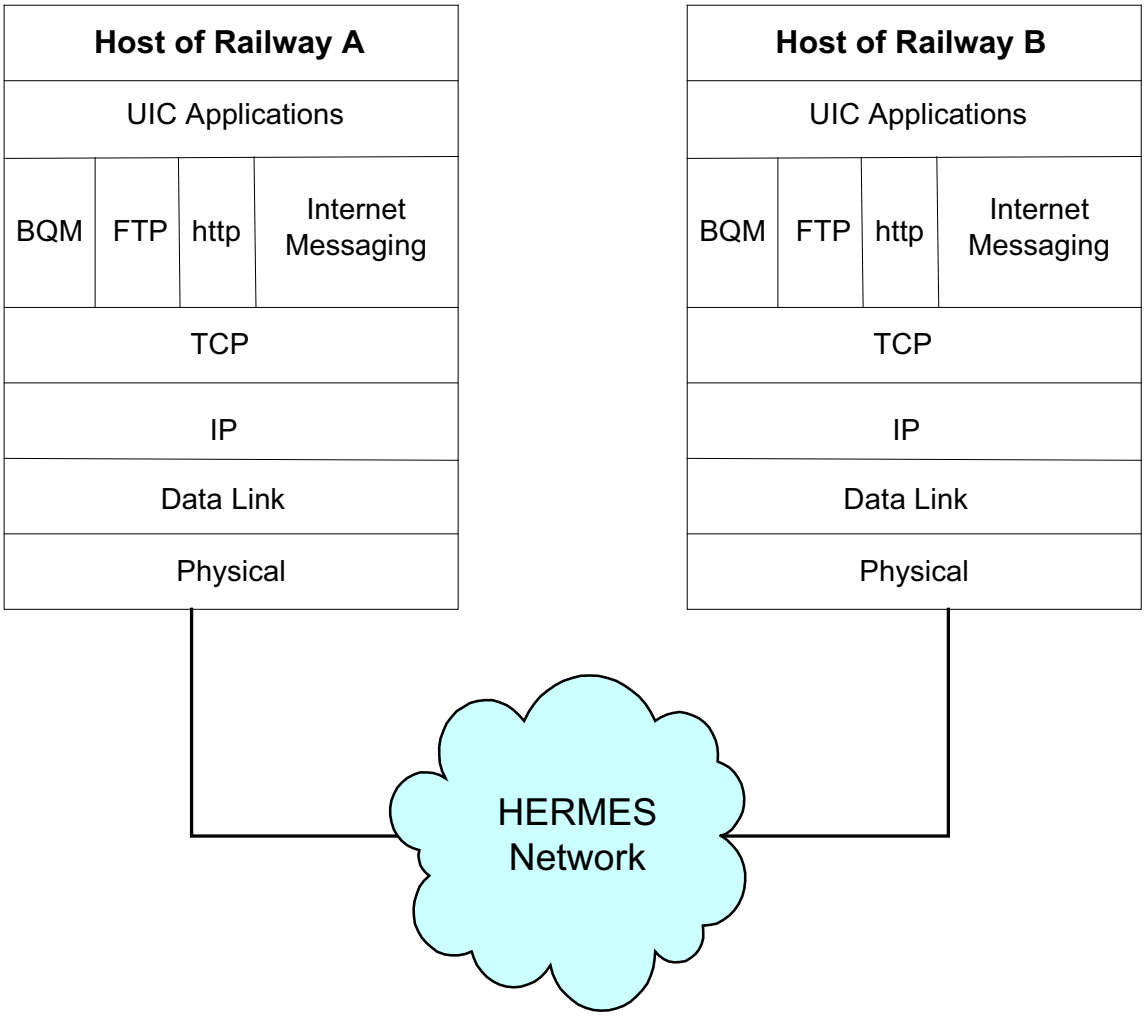
All of these HOSA protocols are standard protocols.

A short description with pointers to the respective documentation is given in point 2.3.3 - page 12.

Data transport from host to host is secured by the Transmission Control Protocol (TCP), which is briefly described in point 2.3.2 - page 11.

All network functions are provided by the HERMES network described in point 2.2 - page 6.

For implementation schedules refer to GPH / HIT Rail



2.3.2 - Transport

The transport layer (or "host-host layer") is the middle layer in the OSI seven-layer model. The transport layer determines how to use the network layer to provide a virtual error-free point-to-point connection so that host A can send messages to host B and they will arrive uncorrupted and in the correct order. It establishes and dissolves connections between hosts. It is used by the session layer.

In the HERMES environment, the transport layer protocol is the TCP. The session protocols (BQM; FTP; Internet Messaging) make use of the services of the TCP.

TCP is the most common transport layer protocol used on Ethernet and the Internet. It was developed by DARPA, an agency of the US Department of Defense responsible for the development of new technology for use by the military.

TCP is built on top of Internet Protocol (IP) and is nearly always seen in the combination TCP/IP (TCP over IP). It adds reliable communication (delivery guaranteed), flow-control, multiplexing and connection-oriented communication. It provides full-duplex, process-to-process connections.

TCP is defined in STD 7, RFC 793. It is connection-oriented and stream-oriented, as opposed to the User Datagram Protocol (UDP).

TCP itself exploits the services provided by the Internet Protocol (IP) on network level.

2.3.3 - Session

2.3.3.1 - The File Transfer Protocol (FTP)

2.3.3.1.1 - Introduction

FTP is a well-known method for file transfers and for easy file handling between different systems in a TCP/IP environment. It is a client-server protocol which allows a user on one computer to transfer files to and from another computer over a TCP/IP network. The user executes a client program to transfer files.

It is based on the TCP transport protocol and provides the transfer of character-encoded information as well as binary data.

The objectives of FTP are:

- to promote sharing of files (computer programs and/or data),
- to encourage the use of remote computers,
- to shield a user from variations in file storage systems among hosts,
- to transfer data reliably and efficiently.

FTP is usable directly by a user at a terminal and by programs.

FTP has had a long evolution over the years. Many RFC documents relating to FTP have been produced since 1971.

2.3.3.1.2 - FTP via the HERMES network

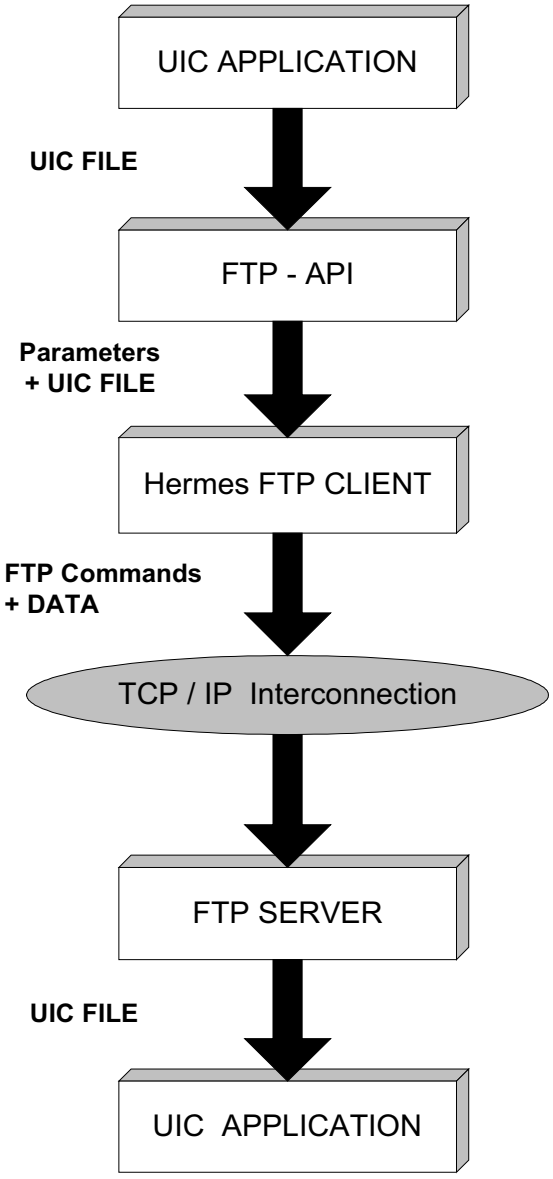
For file transfers via the HERMES network the UIC applications make use of the FTP File Transfer Protocol.

According to the OSI Reference Model for communication, the FTP protocol resides on session level and is based on TCP on transport level.

The sending party initialises the FTP session and controls the entire transaction. Most of the functions needed to perform the transmission have to be concentrated at this site. Therefore, besides the application, a HERMES FTP API and a special FTP Client are needed here.

The addressee receives and stores the file. This is a basic function of the standard FTP server. No special API is needed here.

System elements involved in an FTP transaction active in both outgoing and incoming directions:



Creates the UIC file and stores it in an outgoing area.

Triggers the outgoing area for files to be sent.
Deduces the parameters for the FTP commands.
Calls the FTP Client.

Arranges the connection and dispatches the file.

Receives the file and writes the data in an incoming area.

Triggers the incoming area for files to be taken over.

For comprehensive information on the Internet Standard FTP itself, such as architecture, FTP method of working, state diagrams, call details, parameter variations etc, please refer to RFC 959 and supplementary RFC documents.

For information about FTP implementation details, please refer to the FTP Implementation Guidelines maintained by GPH.

For information about the effects on UIC applications using FTP for file transfer, please refer to the papers and leaflets held at the railways and organisations operating these UIC file transfer applications.

2.3.3.1.3 - FTP Standards

Standards are necessary for interaction, portability, and reusability. They may be de facto standards for various communities, or officially recognised national or international standards.

Some bodies concerned in one way or another with computing standards are IAB (RFC and STD), ISO, ANSI, DoD, ECMA, IEEE, IETF, OSF, W3C.

FTP is defined in the standards STD 9 and RFC 959.

A STD is a subseries of RFCs that specify Internet standards. The official list of Internet standards is STD 1.

STD 9 is the standard defining the File Transfer Protocol (FTP).

RFC 959 (issued in October 1985) is the Internet networking standard containing the official specification of File Transfer Protocol (FTP). It obsoletes RFC 765 and is updated by RFC 2228 and RFC 2640.

A series of supplementary RFCs extends the FTP protocol as described in RFC 959.

2.3.3.2 - The Dialogue Protocol

2.3.3.2.1 - Introduction

Business Quality Messaging (BQM) is a general term for software technologies that provide both:

- Message queuing functions that simplify application communication, and
- Highly reliable communications between unlike applications or application modules.

BQM is message queuing middleware that allows disparate applications or different modules of a distributed application to communicate via a solid and reliable message delivery mechanism.

BQM meets two key technical requirements that help enable integrated distributed computing:

- It ensures reliable (reliability required by business-critical applications) once and only once delivery of data between applications or application modules even over unreliable networks.
- It removes the requirement for simultaneous connections between components, so modules and applications can run at different times.

Applications (or modules) communicate through a series of messages, which the BQM provider stores in holding areas called queues. For example, an application can send a message and then continue processing without worrying about whether the recipient is running or reachable over the network. If the receiver is unreachable, whether because of a network problem or because the receiver is running on a mobile computer, the BQM provider holds the message and delivers it when the receiver is ready. The BQM provider also uses powerful mechanisms to ensure that messages are not lost in transit (the data will always reach its destination), delivered out of sequence or duplicated.

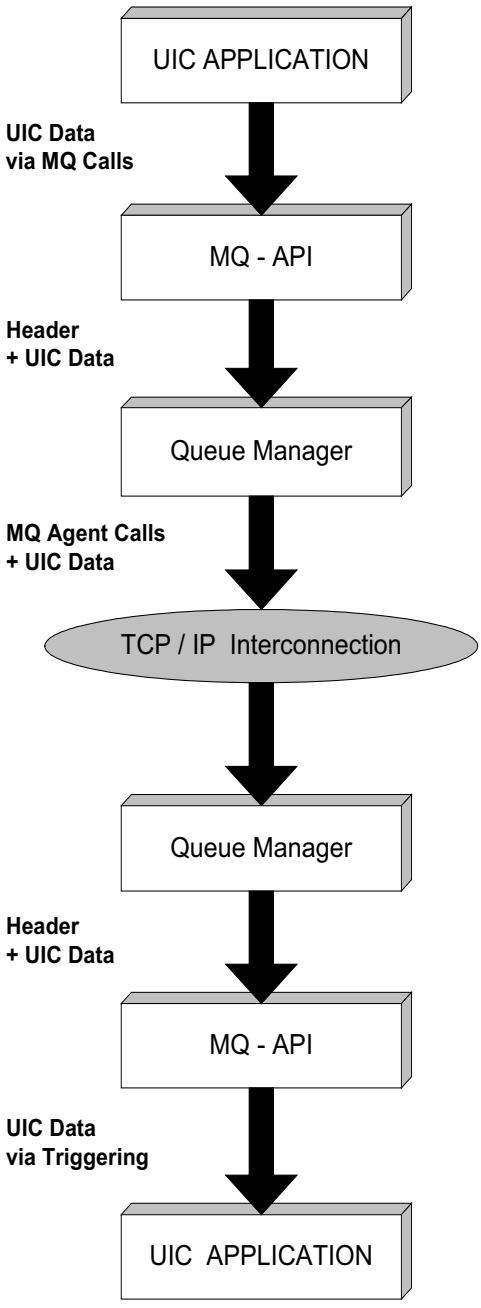
The basic idea for BQM is to keep the application separated from the communication and thus let the application do what it is best at, processing the data.

2.3.3.2.2 - BQM via the HERMES network

The implementation of BQM in the HERMES system and the implementation standard of the BQM products are described in detail in the "MQ implementation guidelines". This document is available from GPH.

BQM is used in the HERMES system for the transaction-oriented applications, the so-called dialogue applications.

BQM model



Creates the UIC file and stores it in an outgoing queue using MQ Interface Calls.

Triggers the outgoing queue for data to be sent.

Transfers the data using MQ Agent Calls to the remote Queue Manager.

Receives the data and stores it in the appropriate incoming queue.

Triggers the incoming queue, sends the data and starts the application process.

Processes the data.

2.3.3.2.3 - BQM Standards

BQM is considered to be a de facto standard. It is based on ISO/IEC 10026 : "OSI Distributed Transaction Processing - Part 7: Message Queuing".

2.3.3.3 - Hypertext Transfer Protocol

2.3.3.3.1 - Introduction

Similar to FTP, HTTP is based on the client-server technique. The client usually uses a browser to connect to a server, retrieve or store documents from or on the server. The HOSA implementation of HTTP uses TCP as transport layer. Like FTP, HTTP is a character-encoded (ASCII) protocol. Since the transfer uses the Multipurpose Internet Mail Extensions (MIME) standard, all kinds of data are transferable, i.e. character-encoded as well as binary data.

The HTTP protocol can be used to access

- hypertext documents (documents which are linked to each other by hypertext references - usually Uniform Resource Locators URL's), e.g. for documentation and information systems,
- forms for interactive use, e.g. order forms, schedule retrieval,
- mixed documents containing text, images, animations, movies and sound "multimedia documents".

HTTP is usable by a user at a web browser (or using a telnet connection) and by programs.

2.3.3.3.2 - HTTP via the HERMES network

For accessing hypertext documents via the HERMES network, UIC applications make use of the HTTP Hypertext Transfer Protocol.

According to the OSI Reference Model for communication, the HTTP protocol resides on session level and is based on TCP on transport level.

The client initialises the HTTP session. Most of the functionality is based on the client side.

An example:

1. The browser determines the URL.
2. The browser asks the DNS for the IP address given by the URL.
3. The DNS replies.
4. The browser establishes a TCP connection to port 80 of that IP address.
5. The browser sends a command (usually get).
6. The server sends an object (usually a file).
7. The connection is closed.
8. The browser displays the file.

9. If the file contains embedded images, the steps from 4 onwards are repeated, i.e. for each object a connection has to be established.

2.3.3.3.3 - HTTP Standards

The HTTP standards are described in

- Hypertext Transfer Protocol - HTTP/1.1 - Draft Standard RFC 2616,

- HTTP Authentication: Basic and Digest Access Authentication - Draft Standard RFC 2617

Additional information is provided by the HTTP working group of the Internet Engineering Task Force (IETF).

2.3.3.4 - Internet Messaging

2.3.3.4.1 - Introduction

Electronic mail (Email or e-mail) is widely used on any computer network. In the late 1980s the IETF developed the Simple Mail Transfer Protocol (SMTP), which has become the de facto standard used for e-mail. For multimedia mail (e.g. carrying e-mail attachments), Multipurpose Internet Mail Extensions (MIME), which expands the capabilities and functionality of SMTP, is used.

2.3.3.4.2 - Internet Messaging via the HERMES network

The target HOSA protocols include SMTP/MIME for e-mail. SMTP/MIME should be used for person-to-person communications and occasional document exchange. In the HERMES environment it is also used for application or user information (alarms) in case of system errors etc. Also confirmations can be signalled in some cases. It is recommended to enable this communication through the HERMES Extranet for better performance and security.

In order to answer security concerns, various security features have been specified for e-mail. However, implementation of these security specifications is very patchy. Therefore it is not recommended to use e-mail for the communication of secure information. MIME attachments should be virus checked at the sender and at the recipient.

2.3.3.4.3 - Internet Messaging Standards

The IETF SMTP is specified in RFC 821/822. SMTP is the de facto standard used for e-mail.

The IETF MIME for multimedia mail is specified in the primary documents RFC 1521, 1522 and 1590. They have been re-grouped into MIME Part One... Five. In addition, a significant number of RFCs address various aspects of MIME.

2.3.4 - Applications

Within the framework of the HERMES system, an application is a computer program or a set of programs for the processing of data. The characteristics of an application depend on the functions to be performed and in some cases on the structure of the data. For practical reasons the functions of the OSI presentation layer, in other words the selection of the code to represent the characters, are included.

Two types of applications are to be distinguished: UIC applications and non-UIC applications.

2.3.4.1 - UIC Applications

UIC applications (also called HERMES applications or international applications) are applications, which are used on an international level between railway companies. Examples of UIC applications are the electronic seat reservation, train pre-advice, the advance consist and the wagon search application. Currently, all UIC applications are communicating via host-to-host data exchange.

The functions to be performed by the application and the data to be exchanged are defined by the relevant UIC bodies, notably by the three UIC Commissions for Passengers, Freight and Infrastructure. They should be strictly identical on both ends of a data communication chain. Each UIC application has a unique 2-digit application code. The catalogue of UIC applications, together with the associated application codes, is published in *UIC Leaflet 912, appendix 5*.

A UIC application can only be addressed in one way (see point 2.3.5), independently of whether it is to be found in one or several computers by virtue of the railway company itself. The interface between the UIC application and the associated session layer (see point 2.3.3 - page 12) should be in conformance with the functional need of the UIC application on one hand and the available services in the session layer on the other hand.

2.3.4.2 - Non-UIC applications

Since a couple of years, the HERMES network accommodates also data exchange between non-UIC applications. These are applications which are not defined nor maintained by UIC bodies. Examples of non-UIC applications are SNCB/NS-Sabin and Eurostar-connections.

The responsibility for the functionality of non-UIC applications is completely in the hands of the related partners. Conditions for connection (technical, security and commercial) are to be negotiated with HIT Rail.

2.3.5 - Addressing

2.3.5.1 - IP Addresses

- Ipv4 is supported as part of the standard IP VPN service.

- As soon as IPv6 has matured enough in terms of stability and QoS, the HERMES network will be migrated to this new version.
  In the meantime, should a party connected to the HERMES VPN already be using IPv6, this protocol version will be transparently transported through the IPv4-based infrastructure.

- Parties connected to the HERMES VPN can use either registered (public) or unregistered (private) IP addressing schemes on their LAN infrastructure.
  At the VPN border, Network Address Translation (NAT) or Port Address Translation (PAT) can be employed if necessary.

- The VPN provider manages, under the direction of HIT Rail, the HIT Rail public Class C IP address range. Additionally, the VPN provider is able to extend the HIT Rail range of Public Addresses in case this is needed.

For information about HERMES IP addresses, please contact HIT Rail, contact address at point 1.6 - page 5.

2.3.5.2 - Domain Name System (DNS)

DNS service is an optional part of the VPN. A secondary DNS Authority Service can be installed on a different location in the VPN in order to ensure accessibility in case the Primary Domain Name server fails.

2.3.6 - Administration

HERMES network administration is performed by HIT Rail in close collaboration with the network provider and its NOC. The objective of this administration is to maximise the network's efficiency and productivity. Network management and administration are divided into five categories: fault management, accounting management, configuration management, security management and performance management.

- Fault management: identifying and locating faults in the network. This includes discovering the existence of the problem, identifying the source, and possibly repairing (or at least isolating the rest of the network from) the problem.

- Accounting management: identifying user access to various network resources to ensure proper access capabilities (bandwidth and security) and to properly charge the various HERMES network users.

- Configuration management: identifying, tracking and modifying the set-up of devices on the network. This category includes addressing issues, such as IP address and DNS name assignment.

    - IP address assignment. Requests for assignment have to be directed to HIT Rail. HIT Rail will implement IP addresses via the NOC.
    - DNS name assignment. Requests for assignment have to be directed to HIT Rail. HIT Rail will implement DNS names via the NOC.

- Security management: controlling (granting, limiting, restricting or denying) access to the network and resources thereon. This includes setting up and managing access lists in routers, creating and maintaining password access to critical network resources, identifying the points of entry used by intruders and closing them.

- Performance Management: measuring the performance of various network components. This also includes taking measures to optimise the network for maximum system performance (periodical measuring of the use of network resources).

Commercial terms and the contractual relationship between HIT Rail and the individual ROs are laid down in bilateral contracts. These contracts also regulate monetary matters, such as accounting and billing.

3 - HERMES Management

The following are responsible for HERMES management:

- HIT Rail B.V.,
- the HERMES Project Group / Groupe de projet HERMES (GPH),
- the HIT Rail Supervisory Board,
- the HIT Rail Shareholders Meeting.

3.1 - HIT Rail B.V.

HIT Rail B.V. is a limited private company governed by Dutch law. It is owned by its members, which are railways and railway-oriented organisations. Its mission is to organise the provision of data communications services.

The HERMES members are the shareholders of HIT Rail, which acts as a managing agent for them.

HIT Rail concentrates on the following tasks:

- provision and management of the HERMES network (see point 2.3.6 - page 19),
- geographical extension of the HERMES network,
- provision of added value services for the HERMES railways (web services, GPH support, statistics etc.),
- negotiation and signing of contracts and SLAs with the VPN provider. HIT Rail is the single contact for the HERMES users. HIT Rail acts as the management interface between a single VPN provider and a multiple users organisation.

HIT Rail B.V. was founded by the HERMES community on November 20th, 1990.

The registered office of the company is:

HGB II K.485, postbus 2025, 3500 HA UTRECHT, Netherlands.

HIT Rail's administration consists of:

- Chairman,
- Supervisory Board,
- Shareholders meeting
- Administrative staff,
- Technical staff.

3.2 - The HERMES Project Group (GPH)

The GPH consists of two sub-groups with different orientation: GPH Strategy and GPH Technical.

3.2.1 - GPH Strategy

The intention of the GPH Strategy Group is to provide HIT Rail with strategic directions for the development and production of the HERMES system.

The GPH strategy group also acts as a supervisor for the GPH Technical Group.

Members of the GPH Strategy Group are:

- chairperson as appointed by the Supervisory Board,
- representatives of the railways and organisations holding the HIT Rail shares. These members have to have responsibility for the financial and strategic aspects of HERMES,
- the technical director of HIT Rail.

Based on recommendations and information provided by the GPH Technical Group, the GPH Strategy group:

- sets out a forward technical strategy and future directions for the HERMES network and services;
- determines a fair cost recovery mechanism for the services (HERMES tariffs);
- approves the Service Level Agreements and corresponding contracts between HIT Rail and users and signs them on behalf of the users;
- approves budgets for HERMES-related projects.

3.2.2 - GPH Technical

The GPH Technical Group accounts for technical issues of production and further development of the HERMES communication system and provides recommendations for the GPH Strategy Group.

The GPH Technical Group monitors the performance of HIT Rail's contracts with its clients and ensures adherence to SLA as well as resolving problems and agreeing changes as necessary.

It reports to the GPH Strategy Group and to the Supervisory Board of HIT Rail.

The GPH Technical Group may create specialised subgroups for specific issues.

Members of the GPH Technical Group are:

- chairperson as appointed by the Supervisory Board;
- members appointed by each HERMES Railway who has responsibility for the technical quality of HERMES services as a user;
- additional guests as required;

- Technical Director of HIT Rail.

Based on strategic directions, given by the GPH Strategy Group and by the HIT Rail Supervisory Board, the GPH Technical Group:

- advises HIT Rail on technical issues;

- proposes a fair cost recovery mechanism for the services (within the parameters set out by the HIT Rail Supervisory Board for budgetary constraints);

- concentrates on network matters, such as:

  - suitable services,
  - suitable service levels,
  - future demands,
  - suitable technologies,
  - selection of service providers per service;

- on behalf of the HERMES railways it monitors and reviews the performance of HIT Rail in meeting the service levels. The daily network supervision by HIT Rail and the NOC will be the basis of any monitoring or reviewing;

- reviews and defines the level of the HERMES services as appropriate;

- ensures that there are appropriate quality mechanisms in place to evaluate the performance of the network suppliers;

- looks on a continuous basis for opportunities to improve quality and to reduce costs;

- proposes the Service Level Agreements and corresponding contracts between HIT Rail and the HERMES users;

- monitors and reviews the Change Management procedures for efficiency and effectiveness;

- acts as UIC leaflet responsible body for the *UIC Leaflet 917-5*, referring also to relevant parts of the *UIC Leaflet 912* and *UIC Leaflet 918-0, 918-1, 918-2*.

3.3 - HIT Rail Supervisory Board

The HIT Rail Supervisory Board's main responsibilities are as follows:

- define HIT Rail's overall strategy,

- define HIT Rail's business cases and projects,

- monitor the overall development of the company's stategy,

- ensure the proper day-to-day management of the company,

- decide on budgets, investments and financial issues,
- review HIT Rail's annual accounts.

3.4 - HIT Rail Shareholders Meeting

The HIT Rail Shareholders Meeting decides by majority vote. It concentrates on the following tasks:

- approve HIT Rail's strategy,
- approve HIT Rail's annual account,
- decide on the appropriation of profits,
- elect the members of the HIT Rail Supervisory Board.

Appendix A - The OSI Reference Model / Open Systems Interconnect

The OSI model is described by ISO (International Organisation for Standardization) in the International Standard 7498. Additional ISO/IEC documents deal with service definitions, protocol specifications and implementation statements.

OSI-RM or OSI Reference Model or seven-layer model:

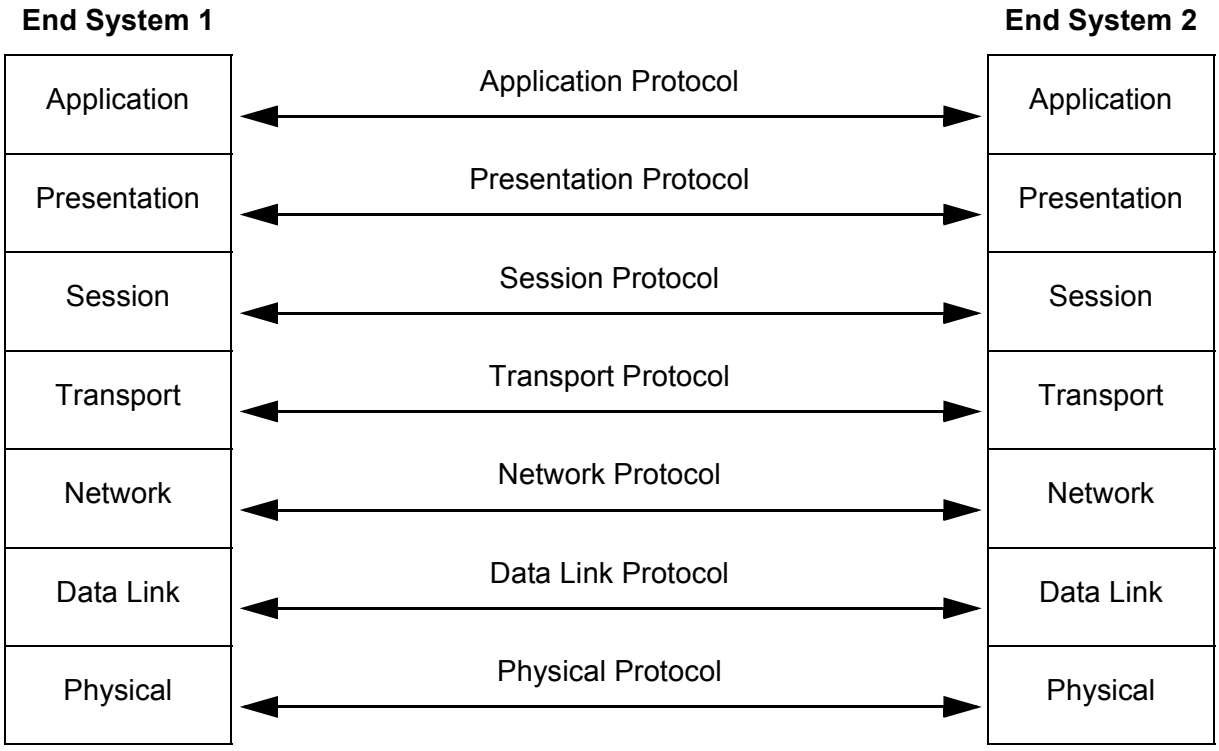
A model of network architecture and a suite of protocols (a protocol stack) to implement it, developed by ISO in 1978 as a framework for international standards in heterogeneous computer network architecture.

The OSI architecture is split into seven layers, from lowest to highest: 1 physical layer, 2 data link layer, 3 network layer, 4 transport layer, 5 session layer, 6 presentation layer, 7 application layer.

Each layer uses the services of the layer immediately below it and provides a service to the layer above. In some implementations a layer may itself be composed of sub-layers.

OSI is the umbrella name for a series of non-proprietary protocols and specifications comprising, among others, the OSI Reference Model, ASN.1 (Abstract Syntax Notation 1), BER (Basic Encoding Rules), CMIP and CMIS (Common Management Information Protocol and Services), X.400 (Message Handling System, or MHS), X.500 (Directory Service), Z39.50 (search and retrieval protocol used by WAIS), and many others.

The OSI Reference Model



The OSI model is also described by ITU: refer to the ITU web-based documentation system.

List of abbreviations

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Program(ming) Interface
ASN	Abstract Syntax Notation
ASCII	American Standard Code for Information Interchange
BER	Basic Encoding Rules
BRI	Basic Rate Interface
BQM	Business Quality Messaging An industry initiative called BQM, brought about by IBM Corp., Intel Corp., Microsoft and others to promote message-oriented middleware.
CMIP	Common Management Information Protocol
CMIS	Common Management Information Service
CPE	Customer Premises Equipment
CSC	Customer Support Centre
DES	Data Encryption Standard (3DES = DES with triple key length)
DNS	Domain Name System
DoD	Department of Defense (US Government)
ECMA	European Computer Manufacturers Association
FTP	File Transfer Protocol
GPH	HERMES Project Group
HERMES	Handling through European Railways Messaging Electronic System
HIT	HERMES Information Technology
HOSA	HERMES Open System Architecture
HSRP	Hot Stand-by Router Protocol
HTTP	Hyper Text Transfer Protocol
IAB	Internet Activities Board

IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4 / IPv6	Internet Protocol version 4 / Internet Protocol version 6
ISDN	Integrated Services Digital Networks
ISO	International Organisation for Standardization
ITU	International Telecommunication Union
KPI	Key Performance Indicator
LAN	Local Area Network
Mbps	Megabit per second
MD5	Message Digest 5 (a checksum algorithm)
MHS	Message Handling System
MIME	Multipurpose Internet Mail Extensions
MQ	Message Queuing
NAT	Network Address Translation
NOC	Network Operations Centre
OSF	Open Software Foundation
OSI	Open Systems Interconnection
PAT	Port Address Translation
PoP	Point of Presence
QoS	Quality of Service
RFC	Request For Comments
RFP	Request For Proposals
RM	Reference Model
RO	Railway Organisation
SHA 1	Secure Hash Algorithm One

SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SPoC	Single Point of Contact
STD	Internet Standard
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network
W3C	World Wide Web body (the main standards body for the World Wide Web)
WAIS	Wide Area Information Server
WAN	Wide Area Network

Bibliography

1. UIC leaflets

International Union of Railways (UIC)
UIC Leaflet 912: Principles governing standard messages for data exchange at international level, 2nd edition, including 2 amendments, July 1994

UIC Leaflet 918-0: Electronic seat/berth reservation and electronic production of travel documents - General regulations, July 2003

UIC Leaflet 918-1: Electronic seat/berth reservation and electronic production of travel documents - Exchange of messages, in course of preparation

UIC Leaflet 918-2: Electronic seat/berth reservation and electronic production of travel documents - Transport documents (RCT2 Standard), in course of preparation

2. International standards

International Organization for Standardization (ISO)
ISO/IEC 7498-1:1994 : Information technology, Open Systems Interconnection, Basic Reference Model: the Basic Model, 1994

ISO 7498-2:1989 : Information processing systems, Open Systems Interconnection, Basic Reference Model, Part 2: Security Architecture, 1989

ISO/IEC 7498-3:1997 : Information technology, Open Systems Interconnection, Basic Reference Model, Part 3: Naming and addressing, 1997

ISO/IEC 7498-4:1989 : Information processing systems, Open Systems Interconnection, Basic Reference Model, Part 4: Management framework, 1989

ISO/IEC 10026 : OSI Distributed Transaction Processing, Part 7: Message queuing,

Internet Engineering Task Force (IETF)
IETF-RCF 821/822 - SMTP,

IETF-RCF 2281 - March 1998 - HSRP,

IETF-RCF 1521, 1522, 1590 - MIME,

IETF-RFC 2616 and 2617 - HTTP,

IETF-RFC 959, (2640, 2228, 765) and STD9 - FTP,

IETF-RFC 793 - STD 7 - TCP,

Institute of Electrical and Electronics Engineers (IEEE)
IEEE 802.3 Ethernet LAN technology,

3. Miscellaneous

HERMES Documentation available at HIT Rail
HERMES VPN Security Policy,

HOSA Migration Guidelines,

FTP Implementation Guidelines,

MQ Implementation Guidelines,

HTTP Guidelines,

Welcome to the HERMES VPN Service, Welcome Pack

Warning

Printed by the International Union of Railways (UIC)
16, rue Jean Rey 75015 Paris - France, December 2003
Dépôt Légal December 2003

ISBN 2-7461-xxx (French version)
ISBN 2-7461-xxx (German version)
ISBN 2-7461-0662-0 (English version)