TECHNICAL REPORT

ISO/TR 11636

First edition
2009-12-01

Health Informatics — Dynamic on-demand virtual private network for health information infrastructure

Informatique de santé — Réseau privé, virtuel, dymanique, sur demande pour infrastructure d'information de santé

Reference number
ISO/TR 11636:2009(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TR 11636 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

Introduction

Currently, healthcare information is normally transferred in the form of paper documents or electronic data through schemes such as dedicated fixed lines connecting the headquarters and branches within a company, through public networks such as an Integrated Services Digital Network (ISDN), or through a dedicated network between specific institutions, enabling a virtual network for the specified users in a dedicated service network managed by communication providers, such as an Internet Protocol virtual private network (IP-VPN). Therefore, healthcare information cannot be transferred easily while maintaining security in most cases, because network configurations adequate to these solutions are limited and the costs are very high.

The uses of various service networks in the healthcare field include online claims for medical fees, online maintenance of medical devices, and remote medical care, such as teleradiology, telepathology and healthcare information services for regional healthcare cooperation. To provide such services however, it is necessary for multiple medical institutions to pass healthcare information to each other. A network in which a single medical institution is dynamically connected to multiple medical institutions and switched to another institution is required.

To make such a network available to many medical institutions at low cost, an open network such as the Internet can be used for connecting with different medical institutions, medical device providers, and patients. We can use the following VPNs as secure channel systems in an open network:

Internet Protocol Security (IPsec) with Internet key exchange (IKE), described as IPsec + IKE which runs in the network layer with authentication and exchange of encryption keys, and

Secure Sockets Layer (SSL) protocol, which runs in the session layer with encrypted communication between a Web browser on a client and SSL servers.

Thus, this is adapted to web applications, but other applications, such as e-mail, File Transfer Protocol (FTP), and unique client/server systems, cannot be used. On the other hand, the combination of IPsec + IKE can be used with any application needed by medical institutions to provide secure channels without reconstructing any application software. In addition, SSL has an inherent risk because it provides no protection methods against well-known lower-layer attacks, session hijacking, false Address Resolution Protocol (ARP) statements, and so on.

The conventional VPN using IPsec + IKE however, requires complicated configuration of network devices, and setting up the system without expertise could result in failure to protect healthcare information. Also, it is a fixed-type VPN and can only be connected with fixed parties.

Lately, telecommunication carriers and online service providers (OSPs) have been developing systems to provide services with security on network lines, including setting up network devices to safeguard against these threats, even for a VPN connected in an open network. When a medical institution uses these types of service, most of the responsibilities related to managing the communication lines fall to these service providers (SPs). This reduces the responsibility of the medical institution in terms of its security-related liabilities, which is well suited for organizations without many IT engineers.

A dynamic on-demand VPN, which this Technical Report describes, is one type of VPN. It is not a fixed connection like 1-to-1, which is generally used in ordinary VPN services. It can easily change connection to N-to-N, and the connection parameters are provided automatically by the telecommunication carrier. This makes it suitable for healthcare network infrastructure, as medical institutes are not required to be responsible for or have expertise in setting up such networks. Also, utilizing the Internet makes the dynamic on-demand VPN an inexpensive network and thus readily acceptable to medical institutions in terms of cost.

This Technical Report describes the threats anticipated in a healthcare network, as well as how a dynamic on-demand VPN is actually applied in the healthcare field.

Health Informatics — Dynamic on-demand virtual private network for health information infrastructure

1 Scope

This Technical Report explains the network requirements in the healthcare field, the network security of an open network for the healthcare field, and the minimum guidelines for security management of health information exchange, including personal data, between external institutions.

These requirements will assist in understanding the operation of security and evaluation of security issues in the healthcare field, and the usefulness of a managed VPN, like a dynamic on-demand VPN.

This Technical Report introduces examples of security measures taken in a dynamic on-demand VPN for exchange of medical information; it is not intended to specify the dynamic on-demand VPN itself.

These examples provide network solutions to potential risks in such a user environment.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
demilitarized zone
DMZ
area of a network in which any data exchange with areas outside is allowed

2.2
high security zone
HSZ
area of a network in which no data is exchanged directly with areas outside, except for the purpose of certain remote maintenance

2.3
IPsec
standard for cipher communication, a protocol that prevents data tampering and provides confidentiality functions for each IP packet by using an encryption technique

2.4
internet VPN
VPN created via the Internet

NOTE By using the Internet, connections between remote networks can be managed as connections in a LAN, while maintaining confidentiality.

2.5
IP-VPN
VPN created via a wide-area IP network owned by a communication carrier

NOTE By using an IP-VPN, connections between remote networks can be managed in the same manner as connections in a local area network (LAN).

2.6
local area network
LAN
network in which computers, printers and other equipment are connected and data are transferred within one building

2.7
OSI reference model
model that divides the functions of communication equipment, such as computers, into a layer structure based on the design policy of Open Systems Interconnection (OSI) established by ISO for network structuring, in order to facilitate heterogeneous network data transfer

NOTE Communication functions are divided into seven layers, and the standard function module for each layer is defined.

2.8
provider service
service that exchanges data between a telecommunication carrier and an OSP

2.9
relay service
service that establishes a connection for the sole purpose of exchanging data between a network-connected device within a medical institute and an outside device

2.10
remote access
connection to a network or computer from outside by using lines such as telephone lines

NOTE Remotely accessing a distant computer enables direct operation of the computer as though it is right in front of the user.

2.11
social insurance medical fee payment fund
organization that reviews medical fees invoiced by medical institutions and makes appropriate payments

NOTE The reviews are performed by a three-party committee consisting of representatives of medical institute workers, medical insurers (e.g., health insurance companies), and academic experts. The medical institute submits a medical bill statement (receipt) and claims a payment for the treatment from the health insurance organization. An organization such as a social insurance medical fee payment fund reviews the receipt and makes a payment to the medical institution submitting the invoice.

2.12
SSL
protocol that encrypts and transfers data on the internet being able to encrypt current widely used data, such as World Wide Web (www) and File Transfer Protocol (FTP) data and securely transmit and receive privacy-related information and credit card numbers

2.13
security zone
SZ
area of a network in which limited data exchange with areas outside is allowed

2.14
virtual private network
VPN
service in which a public line can be used as if it is a dedicated line

NOTE It is used for connecting different bases of a company's internal network, instead of installing dedicated lines, in order to reduce cost.

2.15
wide area network
WAN
network in which computers in geographically different locations (e.g., at a headquarters building and multiple branches) are connected through telephone lines or dedicated lines to transfer data

3 Abbreviated terms

For the purposes of this document, the following abbreviations apply.

AES	Advanced Encryption Standard
AH	authentication header
ASP	application service provider
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
HEASNET	HEAlthcare information Secure NETwork consortium
HMAC	Hash Message Authentication Code
IC	integrated circuit
IKE	Internet key exchange
IPsec	Internet Protocol Security
IP-VPN	Internet-Protocol-based virtual private network
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
IT	information technology
LAN	local area network
L2TP	Layer 2 Tunneling Protocol
NAT	network address translation
OSI	Open Systems Interconnection
OSP	online service provider
OSPF	Open Shortest Path First
PKI	public key infrastructure
QOS	quality of service
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comments
SHA	Secure Hash Algorithm
SI	System Integrator
TLS	Transport Layer Security

TOS Type of Service

TTL time to live

WAN wide area network

4 Network features in the healthcare field

4.1 Pattern of current or expected information services in the healthcare field

In the healthcare field, the information services listed below are provided. In a healthcare network, both data security and security by way of access control must be considered so that these services will not influence each other. In order to clarify the form of network use for currently available or future information services, the form of service provision for these services will be defined according to the characteristics of data access.

a) Information provision service

This is a service to provide a particular medical institution with access to patient healthcare information from another medical institution. It includes the following.

— Local collaboration service (for medical institutions and healthcare-related services, such as welfare and nursing care).

Patient medical treatment or nursing care records, including medical records, examination data, medical record summaries, physical check-up data, and care records are provided in a variety of forms, such as letters of referral and local collaboration databases.

— Medical treatment/nursing care information provision service (for patient enquiry).

A patient's medical treatment and nursing care records are disclosed to the patient according to certain criteria.

— Medical treatment/nursing care information provision service (for general enquiry).

Information on hospitals, diseases and various medical and nursing care practices are provided for general enquiry.

b) Internet connection service

This is a service to provide medical institutions with access to information sites on the Internet. It includes the following.

— Internet connection service (for businesses).

Medical institutions access sites judged safe by institutions related to business clients, via the Internet according to the medical institutions' security policies, obtaining academic information sites and sites providing service information, such as that of Japan's Ministry of Health, Labour and Welfare.

c) Storage/relay service

Information is stored in a location within or outside a medical institution and then transferred to another medical institution in order to exchange the information with the distant institution. This service includes the following.

— Mail service.

E-mails are stored and relayed by mail servers.

— Online claim for medical fee service.

Online claims for medical fees are electronically received and transferred to other institutions. For example, a social insurance medical fee payment fund receives and examines a claim and then relays or transmits the claim to an insurer.

— Examination data delivery service.

Results of clinical examination or image diagnosis are delivered from an examination company. The examination results are later used for electronic medical charts and the ordering and information processing department systems in a hospital, so that the data are readily available in these systems, for reference.

d) Information processing service

An external institution that has been entrusted with information processing functions by a medical institution receives information from the medical institution and processes the information as a proxy. This service includes the following.

— ASP service.

Services for medical institutions, such as electronic medical charts and online claims for medical fees, are provided as shared-use services. The healthcare information is externally stored.

— External storage (backup) service.

In the event of faults or disasters, to perform system recovery of electronic medical charts and data from ordering and information processing department systems in a hospital, backup data are transmitted to and stored in an external institution.

e) Remote maintenance service

Various maintenance services, such as fault diagnosis of medical devices and fault recovery, are remotely provided by a subcontracted service company. Only connections with specific medical devices whose services are subcontracted should be available to the service company.

f) Authentication/audit service

Fundamental authentication and audit services, such as public key infrastructure, digital signatures and time delivery, are used by medical institutions to access particular information. These services include the following.

— Time stamp service.

  Time stamps affixed on digital signatures are issued, and a system clock is adjusted to collect audit logs.

— Validation authority (VA) service.

The validity of public key certificates issued by a certificate authority (CA) is verified.

The forms of provision of these systems are analysed, and the form of secure connection in the network is defined.

4.2 Category of healthcare information to be protected (information assets)

External attacks on networks are becoming more and more frequent. To protect healthcare information against such network threats requires maintaining its confidentiality, integrity and availability. Information to be protected in the healthcare field includes the following, in accordance with ISO/IEC 27799:2008, 5.4:

— personal healthcare information;

— pseudonymised data derived from personal healthcare information via some methodology for pseudonymous identification;

— statistical and research data, including anonymised data derived from personal healthcare information by removing personally identifying data;

— clinical/medical knowledge not related to a specific patient or patients, including clinical decision support data (e.g., data on adverse drug reactions);

— data on health professionals and staff;

— information related to public health surveillance;

— audit trail data produced by healthcare information systems and containing personal healthcare information or pseudonymous data derived from personal healthcare information, or data about the actions of users in regard to personal health information;

— system security data, including access control data and other system-related configuration data, for healthcare information systems.

Such healthcare information will be used in networks for a variety of healthcare/hygiene services, including online claims for medical fees for medical treatment, online maintenance of medical devices, remote medical care such as teleradiology and telepathology, and healthcare information services for regional healthcare cooperation. Ensuring the security of healthcare information with respect to the privacy of patients' personal information requires a more secure network.

4.3 Network requirements in the healthcare field

The following are the key features for a network used in the healthcare field:

— patients' sensitive personal information is handled;

— large-volume data such as image data are handled;

— medical institutions exchange information in a local area;

— medical devices, network devices, and users must be authenticated as the number of parties to communication increases;

— network construction expenses will increase.

In view of these features, the requirements for a network in the healthcare field are as follows:

— secure communication;

— high-speed communication of large-volume data;

— implementation and extension of the network to support N-to-N connection;

— authentication of members (users, organizations and devices);

— cost deduction related to secure network connection.

5 Concept of network construction in the healthcare field

5.1 Overview

A typical situation of healthcare information exchange with external institutions involves networks connecting a regional core hospital, clinics, pharmacies and examination centres as part of regional healthcare cooperation efforts, together with online maintenance companies for medical devices. Another situation involves online claims for medical fees to a medical fee payment fund by using ASP-type services.

If medical institutions use networks to exchange healthcare information with other institutions, the information must be sent to the intended organization in a secure way that never allows others to have access. This network security must be guaranteed on the communication path from the sender's device to the recipient's device. Transmitted data must be protected from threats like wiretapping, tampering, intrusion, spoofing and interference.

This clause assumes certain situations inherent to healthcare information exchange via networks, focusing on the network connection methods that are to be used.

5.2 Responsibility to manage security of healthcare information exchange including personal information between independent institutions

5.2.1 Clear demarcation of responsibility

By contract, the sender and the recipient must agree on demarcation of responsibility for data transmission on the communication path, such as handling of communications failure and other accidents. Then, they must decide how to share managerial responsibility among themselves, the OSP and the telecommunication carrier. They must also clarify the scope of managerial responsibility to be assigned to another organization and define which organization should take the initiative in dealing with possible service failures.

5.2.2 Precautionary measures taken within a medical institution

The medical institution sending healthcare information has managerial responsibility for the information during the whole process in which the information is transmitted via networks (provided by the telecommunication carrier) and then received by the intended recipient in an appropriate manner.

Note here that “managerial responsibility” means responsibility for the information in electronic form; in other words, it means responsibility for ensuring the authenticity of both the content and the persons referred to. For example, encryption here means encrypting healthcare information to prevent outsiders from determining what the information means, even if they have wiretapped the communication path. Digital signatures are helpful for detecting tampering.

From these viewpoints, medical institutions that are going to transmit information are responsible for suitably protecting the information and must therefore be aware of the following.

a) Protection against wiretapping

When information is exchanged over networks, it can be stolen by way of, for example, a virtual bypass built on the communication path or a physical device attached to a network device. Medical institutions should take proper measures to protect healthcare information even if it is stolen during transmission or an unexpected information leakage or incorrect transmission occurs. One possible measure is to encrypt the healthcare information itself. The timing and strength level of the encryption vary depending on the confidentiality level of the information and the usage of the information system in a medical institution. If healthcare information is transmitted through networks from medical institutions, it is preferable that the information be encrypted.

b) Protection against tampering

When information is transmitted over networks, the risk of tampering is reduced if it is encrypted. The information can still, however, be altered intentionally or unintentionally because of a failure on the communication path or other possible causes. Since information can be transmitted without encryption, the sender must take precautions against tampering. One tampering detection method is the use of digital signatures.

c) Protection against spoofing

Since networking is not a face-to-face communication method, medical institutions must ensure that the recipient medical institution is correct when sending information over networks. Also, medical institutions must verify the identities of both the medical institution sending the information and the transmitted information itself. For this purpose, some mutual authentication method should be used to identify the recipient/sender properly

at the start/end point of communication, particularly by using proven authentication systems such as public key and symmetric-key cryptography. In addition to its application for tampering prevention, the use of digital signatures for healthcare information is also helpful in identifying the medical institution sending the information.

5.3 Security concepts in network systems for medical institutions

5.3.1 General

Networks with appropriate costs and operation must be selected according to analysis of information security. Then, the parties responsible for network security must be defined by contract: the telecommunication carrier, the medical institution or both. This situation roughly divides into the following two cases:

— a protected network path provided by the telecommunication carrier and an OSP;

— a dubious network path provided by the telecommunication carrier and an OSP.

As stated above, medical institutions planning to exchange healthcare information via networks should select an appropriate type of network, considering how responsibilities should be shared according to the form of services that they use. They should also understand the characteristics of their security technologies, identify allowable risks and, if necessary, explain the risks to their patients in order to demonstrate their accountability.

Among a wide variety of network services, the following sections assume several cases and list some key points.

5.3.2 Communication via closed networks

A “closed network” here means a dedicated network for business use and is defined as a network not connected to the Internet. There are three connection forms that offer closed networks: a common carrier leased line, a public network and a closed IP communication network.

Since these networks are not connected to the Internet, they are basically at lower risk of wiretapping, spoofing and tampering. The risk of wiretapping by a physical method cannot be eliminated however, and it might be necessary to encrypt the information to be transmitted.

The different features of the three forms of closed networks are described below.

a) Connection over a telecommunication carrier leased line

While network quality is good, extensibility as a form of network connection is low, and the cost is generally high. Still, it is worthwhile implementing this line if a large amount of significant information needs to be constantly transmitted.

b) Connection over a public network

Omitting a mechanism for phone number confirmation can result in connection and information transmission to a wrong number. As with a telecommunication carrier leased line, this public network system has low extensibility. The transmission speed is lower than that of currently popular broadband connections. This system is not suitable for sending large amounts of information and large files such as those containing image data.

c) Connection over a closed IP communication network

This form of connection can be implemented at lower cost than connection over a telecommunication carrier leased line. Appropriate selection of the contract type and the category of network service can ensure enough bandwidth to transmit large amounts of information and large files.

These three forms of communication via closed networks have no risk of intrusion from outsiders, and in that sense, they are safe. Connection services generally do not, however, offer encryption of the data to be transmitted. There can be cases where different networks supported by different telecommunication carriers are interconnected via connection points. When networks are interconnected in this way, the recipient's

address can sometimes be interpreted, or additional data can be added to the sender information to be transmitted. This might cause accidental information leaks.

For these reasons, even with a closed network, medical institutions should take security measures, such as encryption of healthcare information to make their data harder to discern and introduction of a tampering detection system, as described in 5.2.2.

5.3.3 Communication via open networks

Considering the wide spread of the broadband network environment, its applications are likely to expand, for example, by reducing implementation costs by using open networks or building extensive mechanisms for regional healthcare cooperation. Since there are various threats on the communication path, such as wiretapping, tampering, intrusion, spoofing and interference, sufficient security measures must be taken. Encryption of healthcare information is also necessary.

a) Connection over a protected network path by telecommunication carriers and OSP

   Even with an open network connection, the telecommunication carrier and OSP might provide their services via a protected network path with security measures against threats. Medical institutions that use such services can transfer most of their responsibility for communication path management to these businesses by defining demarcation points of responsibility by contract.

b) Connection over a medical institution's own open networks

If medical institutions use their own open networks to exchange personal information and other healthcare information with other institutions, most of the managerial responsibility falls on the medical institutions themselves. Hence, they must take full responsibility for implementing such networks, and be aware of their responsibility for guaranteeing technical safety.

With an open network connection, the necessary level of security on the network path depends on the layer at which the security is guaranteed, among the seven layers of the OSI hierarchical model. (Refer to Annex C).

For example, when communication is made using the SSL protocol, the communication path is encrypted at the fifth layer, the Session Layer. While the path may be encrypted appropriately, there is a possible risk of wiretapping in the course of encryption and an inappropriate path being established, since the negotiations before starting communications are not encrypted. When IPsec is used, a path is encrypted in a layer below the second or third layer, the Network Layer, and thus the risk of wiretapping is lower than for communication encrypted by the SSL protocol. Exchange of an encryption key for the path uses IKE to encrypt the details of the negotiations (SA parameter of IPsec). This eliminates the risk of wiretapping, and the combination of IPsec + IKE ensures safety.

Regarding SSL/TLS (a modified version of SSLv3), RFC3552 specifies that TLS depends on a reliable protocol, such as the Transmission Control Protocol (TCP) or Stream Control Transmission Protocol (SCTP). SSL using TCP in the Transport Layer does not support applications using the User Datagram Protocol (UDP). TLS is influenced by attacks on the IP Layer without IPsec. Research has pointed out the possible risk of a security hole in this approach, such as session hijacking or ARP spoofing at a LAN access point. Cases of financial damage have been reported, including data pilferage and data tampering in financial applications or the like.

6 Threat analysis and measures

To satisfy the requirements of networks in the healthcare field according to the concept of implementation, it is necessary to perform threat analysis and to take corresponding measures technically or by way of operation.

A network for healthcare information, including patients' personal information, is composed of multiple elements, such as the players, technology and operation of medical institutions and network devices. To assure the security of the entire network, the safety of each element should be established. It is necessary to