



REMOTE SERVICE INTERFACE-- Solution (A): IPSec over the Internet Using Digital Certificates – Version 2

[Version 2 adds NAT]

This Paper was developed by the
Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC)

The Paper has been approved by:
NEMA (National Electrical Manufacturers Association-USA)
COCIR (European Coordination Committee of the Radiological and
Electromedical Industry)
JIRA (Japan Industries Association of Radiological Systems)

December 2003

© JOINT NEMA/COCIR/JIRA SECURITY AND PRIVACY COMMITTEE (SPC)

www.nema.org/medical/spc

Secretariat: NEMA (National Electrical Manufacturers Association) www.nema.org
1300 North 17th Street, Suite 1847, Rosslyn, VA 22209 USA

Secretary: Stephen Vastagh tel:703-841-3281 fax:703-841-3381 E-mailto:ste_vastagh@nema.org

May be quoted if reference and credit to SPC is properly indicated.

Table of Contents

1.	Purpose.....	1
2.	High Level View.....	2
2.1	Communications Network.....	2
2.2	Remote Service Center (RSC).....	3
2.3	Health Care Facility (HCF).....	3
3.	Communications Network.....	4
3.1	VPN using IPSec (v4).....	4
3.2	Mutual authentication of RSC and HCF while establishing the tunnel using out-of-band Certificate Delivery.....	6
3.3	Performance Requirements.....	7
3.4	Configuration of the Access Points.....	7
3.4.1	Firewalls, Filters, and routing rules.....	7
3.4.2	Network Address Translation.....	8
4.	Remote Service Center.....	10
4.1	Administration of the RSC.....	10
4.2	Technical Measures.....	10
4.2.1	RSC Network Architecture.....	10
4.2.2	Safeguarding Accountability.....	11
4.2.3	Treatment of Identifiable Patient Data.....	11
4.2.4	No Remote Connections Bypassing the RSC.....	11
5.	Health Care Facility.....	12
6.	Audit Trail.....	13
6.1	Medical Device.....	13
6.2	Access Points.....	13
6.3	RSC.....	13
7.	Conclusions.....	14
8.	Glossary.....	15
9.	Appendix.....	17
9.1	Domain Name Lookup.....	17
9.2	Dynamic Host Configuration Protocol.....	17
9.3	Network Address Translation.....	17
9.4	Risk Mitigation.....	17

1. Purpose

Remote Servicing is an innovative way to conduct maintenance and service activities on medical equipment from vendor-specific Remote Service Centers. As a consequence of the potential transmission of data outside the healthcare facility possible security threats need to be addressed to ensure availability, confidentiality, and integrity of the transmitted data. The NEMA/COCIR/JIRA Security and Privacy Committee ([SPC](#)) gathered the appropriate legal requirements of USA, Europe, and Japan, derived a common set of requirements and published the white paper “[Security and Privacy Requirements for Remote Servicing](#)”. This white paper has already gained global approval by NEMA, COCIR, and JIRA. It proposed an architecture where authentication, audit trails, and encryption are used between a pair of access points: at the Remote Service Centers (RSC) and Health Care Facilities (HCF). A single standardized connection would replace the multiple customized solutions that are used today.

The purpose of this 2nd white paper is to define one possible, reasonable, and practical solution that follows the SPC recommendations. We refer to it as “Solution (A)”. This document describes in detail how to configure IPSec over the Internet using cryptographic certificates, and how to distribute the certificates out-of-band. We will further define the supporting conditions at the HCF and RSC. With this document vendors and health care facilities can configure a single access point using off-the-shelf-equipment.

We recognize that there are many other technical solutions that would meet the SPC recommendations. Solution (A) covers the majority of sites that need servicing. However there are other sites where solution (A) may not be as easy to implement or cost effective for various reasons. In Japan this solution is not expected to be common because the IP address space is limited, and NAT administration costs are excessive. If, however, a site can do NAT and the RSC and HCF can administratively manage it, this solution works for the small, medium and large HCFs. In some countries encryption is restricted by regulation. The SPC will develop additional Solutions that better address these special cases.

This white paper is directed at IT professionals, and assumes an understanding of IT infrastructure and security technologies. The reader should have working knowledge of concepts such as Firewalls, Intrusion Detection, Antivirus, Virtual Private Networking, IPSec, Network Address Translation, Routing, and Audit Controls.

2. High Level View

There are three domains that need to be considered, as illustrated in Figure 1.

1. Communications Network (Internet)
2. Remote Service Center (RSC)
3. Health Care Facility (HCF)

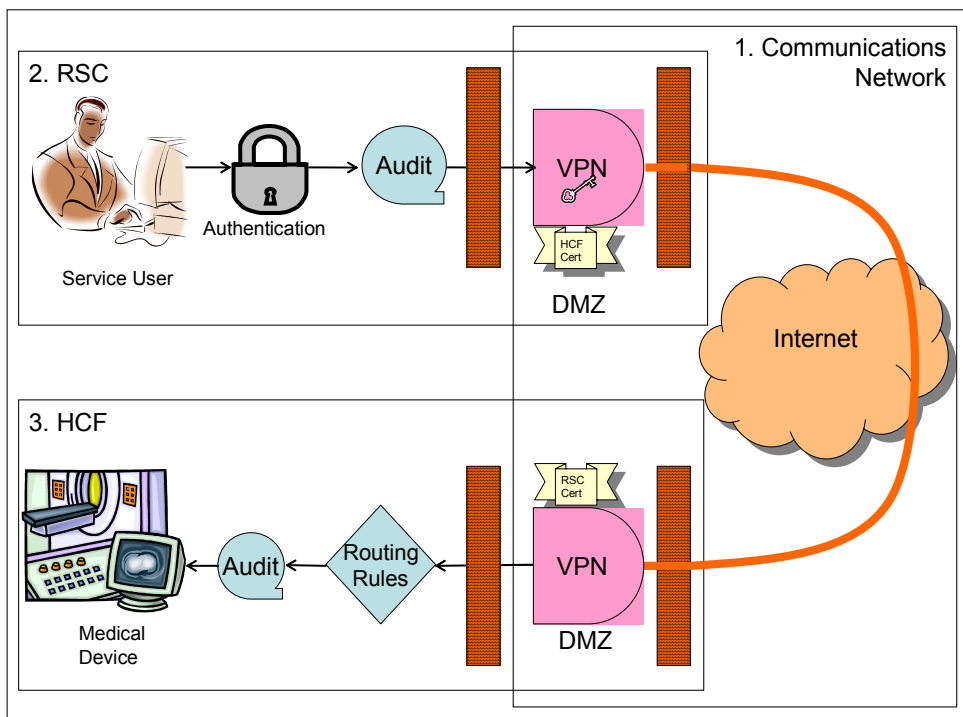


Figure 1: Scheme for secure connection between a vendor's RSC and a HCF.

2.1 Communications Network

In Solution (A) the network to be used between the RSC and the HCF is the Internet. Since this is a public network, there are risks that data can be intercepted, or changed while traveling across this network.

Solution (A) is targeted at facilities that already have an existing Internet connection. This solution will be relatively low cost with minimal additional infrastructure necessary beyond the existing Internet connection. Many HCFs already have existing Internet infrastructure. For those that don't have Internet connectivity and would like to use Solution (A), there are low cost Internet connectivity solutions that may be available to them via DSL or Cable type access.

Since the Internet Protocol (IP) does not inherently provide any protection of data being transferred over the Internet (or unsecured network), one of the components to secure the communications between the RSC to the HCF is to use the IPSec (IP Security) protocol. The IPSec protocol allows for secure private communications using cryptographic security services.

2.2 Remote Service Center (RSC)

The RSC is a particularly sensitive place as it becomes a logical extension of each Health Care Facility that it connects to. Therefore, the RSC must be highly protected with items like firewalls, intrusion detection, and anti-virus detection. In addition each vendor technician must be authenticated to the RSC and all actions have to be tracked there. Solution (A) places the burden of accountability on the RSC and the network access points, thus not requiring changes to existing medical equipment.

In the following sections we will outline how individual accountability is maintained through authentication of the service individual, access controls on the access points, and audit trails.

2.3 Health Care Facility (HCF)

The HCF is also a very sensitive place as it processes and stores quantities of identifiable patient data. Solution (A) expects that the Health Care Facility will take the necessary precautions to protect their facility and network. This would include items like firewalls, intrusion detection, departmental isolation, switched networks, and anti-virus technology. Internet access must be restricted to approved users, systems, and protocols. It is the HCF's ultimate responsibility to weigh the legal requirements, the risks, and the benefits of allowing access to identifiable patient data. This fundamental responsibility is being emphasized by governmental regulations around the world. Examples of local rules are: USA – HIPAA, European Countries – EC 95/46 and its country specific implementations, and Japan – HPB 517.

In the following sections we will outline the necessary security and privacy components for Solution (A) to be successful. This is not an exhaustive examination of security within a HCF, but rather the components that are critical to secure remote servicing. The HCF is free to implement more security than listed.

3. Communications Network

This section will discuss the connection components required to securely establish and maintain the VPN connection between the Internet connection point of the RSC and the Internet connection point of the HCF.

The communications network proposed in Solution (A) provides:

- Strong Authentication by means of certificates
- Access control in the form of routing and filtering rules on the basis of each RSC-HCF pairing
- Audit trails at the access points that can be utilized to provide individual accountability

3.1 VPN using IPSec (v4)

The IPSec protocol sets up a virtual private network (VPN) over the Internet offering the capability to establish an encrypted tunnel between both the access points to the RSC and the HCF, as illustrated in Figure 2. The VPN will ensure authentication of one end to the other, data integrity, data confidentiality, and protect against replay attacks for the traffic it carries. If configured as described below, IPSec will protect the traffic at the network layer and be transparent to service applications.

The following are the hardware, software, and configuration requirements to establish the VPN using IPSec. Because of the history of interoperability problems between IPSec vendors we recommend the following list of options and capabilities:

- 1) All devices (hardware and software) must support IPSec [RFC 2401] enabled communication.
- 2) The IPSec implementation must be certified as compliant by ICSA Labs to increase the likelihood of interoperability.
- 3) IPSec must be used in Tunnel Mode for transparency and maximum protection.
- 4) AH, Authentication Header [RFC 2402] provides authentication, integrity and replay protection
- 5) ESP, Encapsulated Security Payload [RFC 2406] provides authentication, confidentiality, integrity and replay protection at the payload or data level.
- 6) The system must be configured to use at minimum the Triple Data Encryption Standard (3DES) [RFC 2405] for the encryption algorithm and key length.
- 7) The system must be configured to use at a minimum Secure Hashing Algorithm 1 (SHA-1) [RFC 2404] for data authentication and integrity.
- 8) IPSec Security Association (SA) keys must be renegotiated every 24 hours or 1 Gig of data.
- 9) Perfect Forward Secrecy (PFS) is mandatory.
- 10) IKE, Internet Key Exchange [RFC 2407, 2409] IKE will set up the communication of the authentication keys that are needed for AH and ESP.
- 11) Main Mode is mandatory, Aggressive Mode is not allowed.
- 12) Edge-to-Edge authentication is accomplished using 1024 bit RSA Public / Private keys.
- 13) The Public key is distributed through out-of-band methods using BER encoded x.509 Certificates (See below).

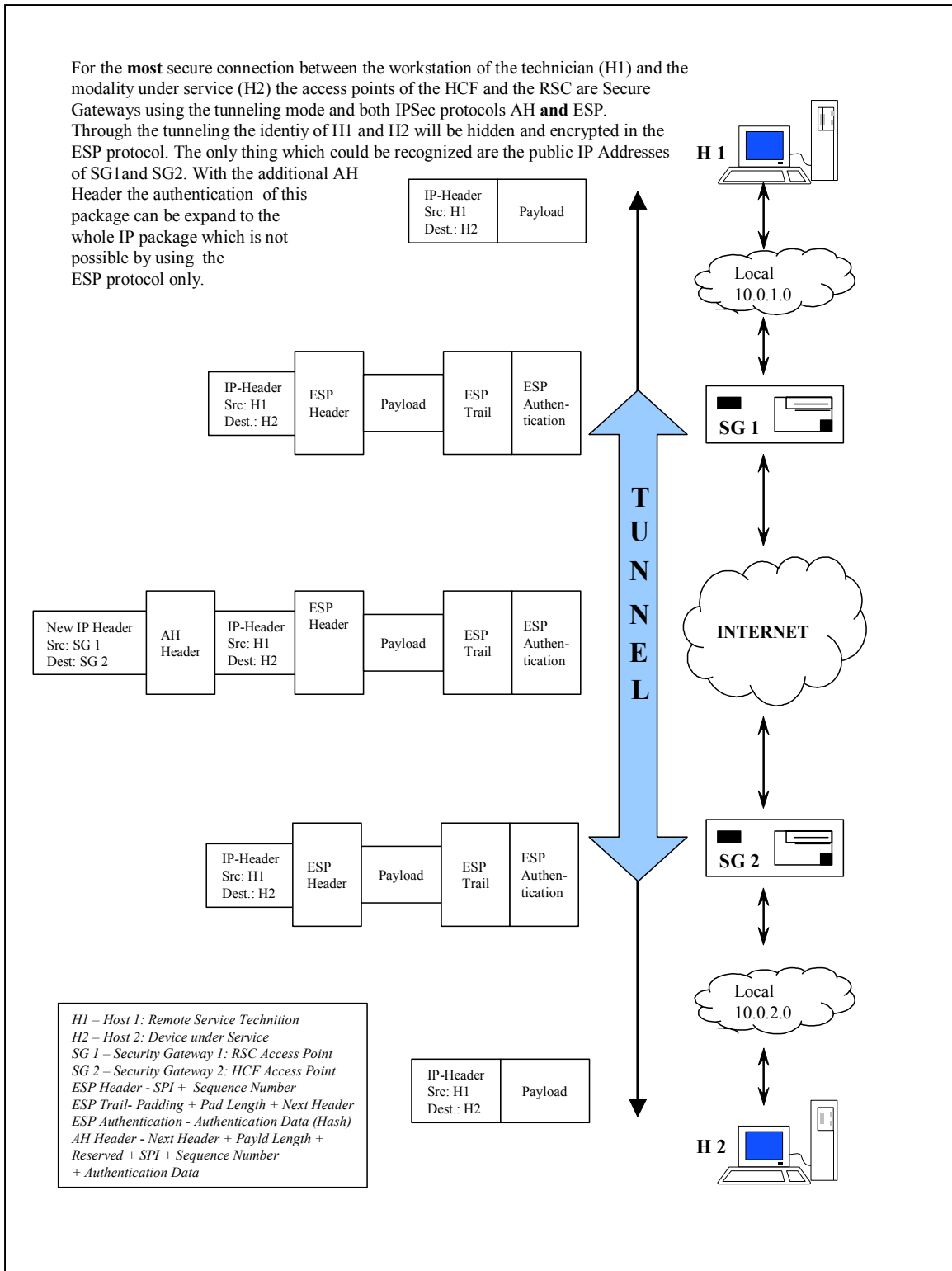


Figure 2: IPSec configuration

3.2 Mutual authentication of RSC and HCF while establishing the tunnel using out-of-band Certificate Delivery

It is imperative that the RSC know with a high assurance that they have connected with the proper HCF access point. Likewise it is imperative that the HCF knows that the proper vendor has been authenticated. It is this mutual authentication that gives strength to this remote service architecture. However, this strong IPSec edge-to-edge authentication is limited to that part of the connection between both access points to the Internet. The needed extension of accountability on the whole communication path from the RSC through to the medical device being serviced is described in both the specific sections about the configuration of the RSC and the HCF.

In this proposal we choose to use public key / private key technology for strong authentication. A digital certificate signed by a Certificate Authority (CA) can be used to authenticate the holder of the private key. Thus the private key must be a secret to the owner of the key pair. The private key must be protected and must never leave the owner's control.

There are many proposed methods of distributing Certificates but in the end, many of them have interoperability problems. We expect that some facilities will have certificate capabilities and will want to use their own Certificate generation method, while others will choose to use a public Certificate Authority (CA).

To avoid interoperability problems we suggest distributing the certificates with non-automated means (out-of-band). This method seems feasible because the HCF need only have a small population of Certificates associated with each vendor they are communicating with but they do not need Certificates of other HCFs. Each RSC also needs only have Certificates of each HCF they will be servicing. The number of keys at the various Sites thus is in the hundreds, not millions and we feel the small number of Certificates and keys necessary will not cause logistic and scalability problems. Thus, our solution avoids using and implementing a PKI.

In this way the HCF and RSC will create a certificate by whatever method they choose. The signing authority may be a hospital managed CA, vendor managed CA, or a trusted third party. The certificate must have an expiration of not more than 2 years.

The Certificate will be delivered and inserted as the authentic certificate for that specific Edge-to-Edge VPN connection only. The IPSec implementation does not need to check the certificate chain, nor any revocation lists. Both of these actions are done by the manual "out-of-band" distribution and communications between the HCF and the RSC. If any key pair is suspected of being compromised it will be manually revoked (de-installed), a new key pair created, a new certificate issued, and installed. The SPC recommends that a certificate be created for each VPN tunnel configuration.

A strength of using Certificates is that they themselves don't need to be protected from disclosure, and their authenticity can be proven through a chain-of-trust that links back to the certificate of the Certificate Authority. This characteristic of certificates allows for the distribution of authentication information without excessive protection methods.

However, as the public key infrastructure (PKI) standards mature the authentication should graduate to the more secure method of using PKI.

3.3 Performance Requirements

The communications network should provide a nominal throughput of 128Kbps. The process of encrypting packets takes time and thus might cause gaps of unused transmission time while waiting for encryption. Furthermore, encrypted data is less compressible and thus link level compression will be of little advantage. This requirement does not demand a guarantee of bandwidth. It is meant to recommend a level of performance that would support the many simultaneous sessions that are expected.

The HCF should be aware that the RSC might want to monitor and test the IPSec connectivity to ensure that the link can be established. The two parties should coordinate these events to prevent false alarms. This is an added measure to ensure that patient safety will not be affected when an event that requires servicing occurs.

3.4 Configuration of the Access Points

As mentioned earlier in section 3 the access points to the RSC and the HCF are the end points of the VPN. The VPN itself provides for replay protection, mutual authentication of the sites as well as integrity and confidentiality of the transmitted messages. The access points must be properly configured in order to avoid security breaches. Even though the same technical measures can be used at both access points, specific configuration can be defined only after an assessment of the risks introduced by the VPN has been conducted.

Among the risks we considered are masquerading (e.g. spoofing) attacks and malicious actors that utilize the VPN link to propagate to other facilities. This section describes minimum requirements for access points to assure the needed level of security. The risk assessment may identify additional technical or procedural requirements.

It should also be noted that either end of the VPN access points may initiate the tunnel. With the configuration and security measures recommended, this allows either the HCF or RSC to initiate the tunnel depending upon the agreement between both parties.

It is recommended that the RSC have a static global IP address. While there are many benefits that the HCF have a static global IP address assigned to its VPN device, this solution will work if the ISP dynamically assigns an IP address to the HCF VPN device. In this case the HCF could initiate the tunnel knowing the static IP address of the RSC peer VPN device and with the use of the digital certificates for authentication, the tunnel can be established securely.

3.4.1 Firewalls, Filters, and routing rules

At a minimum the access points should utilize filters and routing rules to restrict connection attempts. These rules may be different for different vendors. In this way the HCF can

control which vendor has access to which medical device and the RSC can control where to direct messages originating from that device.

Both the RSC and HCF access points must have a specific routing rule that allows only packets sourced from within their own network to go through the access point. This will restrict communications through the VPN, and prevent one HCF from accessing another HCF through a common RSC, or vice versa. This will prevent unauthorized Internet traffic from using the VPN.

It is highly recommended that the Access Points be configured behind a primary firewall, and before a secondary firewall. This position is commonly referred to as a DMZ (“de-militarized zone”). A properly configured DMZ has security advantages that give defense-in-depth via prescreening and post-screening. The actual implementation of the primary firewall and second firewall are a part of an optimal solution. The HCF is ultimately responsible for reducing Internet risk within their enterprise using whatever method they choose.

It should be noted that in some cases the HCF may have multiple networks that are logically separated (i.e. VLANs) or physically separated (i.e. campus network from clinics). In some cases the HCF may put the VPN access point to be closer to the network where the vendor equipment resides. This means the VPN device may actually be located at the perimeter of an internal network such as a Radiology department network. The RSC tunnel could be routed through the HCF DMZ to an internal network where the VPN tunnel could be terminated. From there the traffic could be routed to the specific device needing service. Again, it is recommended that wherever the HCF access point is located, that the access points be behind a primary firewall and before a secondary firewall.

3.4.2 Network Address Translation

The use of Network Address Translation (NAT, RFC 1631) is very typical in intranets today. The IPSec configuration proposed in this white paper ends outside any NAT influence because the edge-to-edge authentication is done on Internet Routable IP Addresses. The NAT must then provide for access paths to the medical device to be serviced. These NAT rules can be specific to the IPSec authentication as mentioned above.

By using NAT, this solution should work for any site. NAT rules properly implemented can uniquely identify each device at all sites as well as handle any default routing policies that may be imposed at the RSCs or HCFs. However, for NAT to work properly to service devices, it must be noted that a static IP must be assigned to the HCF device to be serviced. This IP address assignment may be a private or a global IP address but must not change every time the device is booted/reloaded.

Most sites will assign static IP addresses to server-type or network type devices and may use Dynamic Host Configuration Protocol (DHCP) for end-user personal computers, workstations or laptop computers. DHCP is a dynamic way of assigning an IP address to a device, but this essentially means the IP address could be different every time the device is booted. DHCP can also be used to reserve an IP address for a device which is similar to

assigning a static IP address. If a site uses DHCP to assign a static IP address, then this solution works. If DHCP assigns dynamic IP addresses then this complicates this solution. For this paper, the NATing information below assumes that static IP addresses have been assigned to the devices to be serviced remotely over the VPN tunnel.

3.4.2.1 NAT With Private Addressing

Many HCFs use private addressing [Address Allocation of Private Address Space, RFC-1918] and since private addressing can be used by multiple sites, different HCFs may use the same addressing schemes within their internal networks. This can result in duplication of addresses assigned to devices located at different HCFs. In order to route to the correct HCF and device to service it, the RSC needs to manage a block of addresses that can be used to uniquely identify each device at every HCF. These IP addresses can be another private address range not used at the HCF. As long as the RSC manages the NAT assignments, the RSC should be able to route correctly to the individual device at the HCF. The RSC may need to add a routing rule so that a specific range of IP addresses can route over the VPN network and do not go out another gateway that leads to the unsecured Internet network. If this private range of IP addresses were accidentally routed out the unsecured Internet, there is minimal risk because private addresses cannot route correctly through the open Internet network. The data would simply be dropped.

3.4.2.2 NAT and Global Addressing

Some HCF networks may use their own global IP addresses to assign to each server-type device. With the use of global addresses, each device is uniquely identified to the world. Since global addresses can traverse the Internet correctly to the HCF that owns them, the RSC can enter routing rules in their network to route traffic out the RSC VPN gateway to the HCF VPN gateway. The HCFs router can then route the RSC service technician directly to the end device using these global IP addresses. With global addresses, NAT is not needed but it may be simpler for some RSCs to use NAT any ways. In some cases, NAT may simplify the number of routing rules the RSC must enter in their default gateways for sites that use global addressing. Additionally, RSCs may wish to continue to use NAT for consistency on setting these VPN connections up as well. Again, while NAT may not be necessary if an HCF uses global addresses in their network, NATing will make the RSCs network administration tasks simpler.

3.4.2.3 Additional HCF Security Controls.

With the use of NAT and either global or private addressing schemes, the HCF may impose additional security controls. For example, by setting up one to one NAT statements this can limit connections from the RSC to the specific devices to be serviced. With one to one NAT statements this limits the RSC to the device and not the whole HCF network or subnet. The HCF could also implement additional security rules through an internal firewall to restrict access and additional port and protocol filtering.

Network Address Translation tables must be properly managed and maintained to allow multiple RSCs to use Solution A to service many HCF sites by uniquely identifying every

device they need to service at every HCF site. The HCF will have to be aware of the NAT rules as well so that one RSC does not use the same range of private IP address to identify its devices as another RSC.

4. Remote Service Center

The vendor has ultimate responsibility to securely administer and operate the RSC-LAN. In section 3.5 we discussed the configuration of the access points ending just outside the RSC-LAN. This section in turn suggests the actions and technology that are necessary for the RSC-LAN to ensure a secure implementation of Solution (A). The RSC is encouraged to augment these recommendations to their satisfaction depending on the local situation.

4.1 Administration of the RSC

It is the responsibility of the RSC to properly administer and ensure the integrity of their VPN access point and their LAN. This responsibility will be further emphasized through the Business Associate Agreements called for in the HIPAA legislation when connecting with HCFs in the USA, or other country-specific agreements needed or recommended between a HCF and a vendor. In these agreements the HCF typically will impart specific rules regarding the treatment of identifiable patient data. These factors will drive the RSC to their own risk assessment. Further issues to be considered are, for example, a risk mitigation plan, an internal security policy including regulations for audits and user access management, and workforce training.

When the access point configuration is changed, care must be taken to communicate, perhaps out-of-band, with the HCF. This communication is critical to ensure that no session is active across the VPN link when configuration changes are attempted, and to ensure that changes are authorized and synchronized. The RSC must create policy and follow procedures to ensure that only authorized individuals at the HCF can request changes.

At all times patient data should be de-identified to the fullest extent possible, but there are instances where all efforts to de-identify may still leave identifiers in the data. RSCs must have a policy on treatment of even de-identified data that covers how the data is stored, processed, tracked and ultimately destroyed.

4.2 Technical Measures

4.2.1 RSC Network Architecture

The RSC network must be isolated not only from the Internet as described above but also from the vendor's own intranet to minimize the risk of unauthorized disclosure of patient identifiable data.

The RSC must implement an internal security system isolating the RSC from the Internet and the vendor's intranet.

4.2.2 Safeguarding Accountability

Individual accountability of technicians needs to be maintained at the RSC through ID and authentication of each individual RSC user prior to accessing the VPN to the target HCF, via audit trails tracking any activity.

The following recommendations should be realized at the RSC:

- ❖ The RSC must identify each Service Personnel involved in a session
- ❖ The claimed identity of each RSC user must be authenticated prior to its use of any RSC resources, including gaining access to the VPN
- ❖ The RSC must maintain log files that tracks service access and actions. (discussed further in §6.3)
- ❖ Access to all resources of the RSC must be revoked promptly upon personnel changes, e.g., reassignment, termination
- ❖ Policy and Procedures must control hopping from one system under service to another without HCF approval.
- ❖ RSC written policy must specify the methods used to authenticate HCF requests (e.g. service requests, certificate management, password change)

4.2.3 Treatment of Identifiable Patient Data

All efforts must be taken to restrict RSCs from pulling identifiable patient data from the HCF. There are some times when it is necessary to pull some patient identifiable data in order to carry out the service operation. This must only be done in accordance with local regulations. When this data is pulled across the VPN, it must be carefully managed in accordance with contractual agreements between the HCF and the RSC.

4.2.4 No Remote Connections Bypassing the RSC

All support individuals must use the RSC established security architecture and infrastructure to remotely connect to the HCF. This is to insure that the audit trails, authentication, firewall protection and all components described in this paper can not be bypassed by allowing remote connections directly from a support individual's PC to the HCF.

5. Health Care Facility

The HCF is ultimately responsible for the security and privacy of their patient's identifiable data. It is this need that will drive each facility to do a risk assessment and create facility-specific security and privacy policies and procedures. The HCF must perform this assessment—this section does not replace that effort. We do, however, suggest where procedures need to be developed, and describe the technology necessary to assure a successful implementation of Solution (A). The HCF is encouraged to augment these recommendations to their satisfaction.

It is the responsibility of the HCF to administer and ensure the integrity of their VPN Access point. In section 3 we discuss the configuration of the Access point. At the discretion of the HCF this effort can be outsourced. As discussed above from the point-of-view of the RSC, when the access point configuration is changed care must be taken to communicate beforehand with the RSC. This communication is critical to ensure that no session is active across the VPN link at the time configuration changes are attempted, and to ensure that changes are authorized and synchronized following agreed procedures.

Solution (A) relies on a secure environment. The HCF intranet to which the VPN is to be connected must be appropriately protected against relevant security vulnerabilities using, for example, firewalls, intrusion detection, and antivirus controls. Further, the HCF network architecture needs to ensure the integrity of the data it carries, control access to its resources, and provide for the confidentiality of its traffic. Note that the architecture described in this white paper neither proposes nor requires any intranet encryption.

The Medical Device to be serviced must support remote access through the hospital network. It also needs to have access to and be enabled to communicate through the IPSec tunnel. If the device is not connected to the hospital network then the solution described in this white paper cannot provide remote servicing.

6. Audit Trail

Audit trails are key components of individual accountability. It is through the audit trails that actions performed at the device being serviced, in which patient identifiable data can be assumed to reside, can be traced to specific individuals at a specific RSC. A goal of the SPC Remote Service Interface architecture is to provide this accountability without imposing additional requirements on the devices being serviced. This is a key to the success of this architecture, as it protects the HCF investment in current equipment while providing required accountability.

All audit log entries must include a date and time stamp that has minimal precision and accuracy of one second. Accurate time stamps are important to ensure that log file corroboration can be accomplished even though the log files were created on different systems in different locations. Note that this white paper does not discuss format, storage, communication, or access to log files since other industry and standards groups, e.g., the SPC, IHE, HL7, and DICOM, are working such issues. For a discussion of auditing in medical imaging please see the SPC paper “[Security And Privacy Auditing In Health Care Information Technology](#)”.

6.1 Medical Device

There are no new requirements for existing medical equipment. Any audit log capabilities should be used as defined originally for that medical device.

6.2 Access Points

There are no specific requirements from this white paper that are allocated to the access points themselves. Any audit log capabilities that the access point has should be used as deemed necessary by the RSC or the HCF.

6.3 RSC

The RSC must maintain an audit log that tracks their service individual’s actions as it relates to access to the HCF and its patient identifiable data. This audit log must be as specific as reasonably possible and should contain the following:

- Individual Service user identification
- Medical Device IP Address and Port number (or NAT-translated address)
- Date and time of connection and disconnection
- Statement of work performed (e.g. access and actions) (may be manual)
- Success or failure of access attempts

7. Conclusions

This is one reasonable solution out of several possible solutions that conform to the SPC Remote Service Interface white paper. It is very important to understand that this is not a just a technology solution. The HCF and RSC will need to make policy and procedural changes, along with implementing the technology as suggested, in order to allow a truly secure remote service capability to be realized.

The focus of a single point of access vs. multiple modem connections enhances the HCFs control of their internal network.

8. Glossary

- 3DES – Triple Data Encryption Method [RFC 2405] provides the encryption
- Access Point – the logical combination of hardware and software that is used to implement the IPSec VPN.
- Aggressive Mode – an IKE method of key exchange that combines two main mode exchanges. Aggressive Mode is optional in IPSec implementations.
- AH -- Authentication Header [RFC 2402]
- BER – Basic Encoding Rules (ASN.1)
- CA – Certificate Authority – Mutually agreed upon authority of certificate validity
- Certificate – Digital Certificate
- COCIR -- European Coordination Committee of the Radiological and Electro-Medical Industry, representing European imaging vendors,
- Device – Generic term used to define the product at the HCF that is being remotely serviced
- DHCP – Dynamic Host Configuration Protocol – This is a protocol used to assign IP addresses to devices.
- Digital Certificate – A cryptographic public key that is signed by a CA
- DMZ – DeMilitarized Zone - Derived from the military term for an area between opponents – A network located between internal and external firewalls where software and hardware are deployed to enable controlled access to resources.
- ESP – Encapsulated Security Payload [RFC 2406]
- Firewall – Routing and filtering network device for connection screening and may do packet inspection.
- Global Address – Internet Routable Address – An IP address that uniquely identifies a node on the Internet.
- HCF – Health Care Facility
- HIPAA – An Act of Congress in the United States of America – Health Insurance Portability and Accountability Act
- IKE – formerly ISAKMP – Internet Key Exchange [RFC 2407, 2409] Authentication and Negotiation protocol used to initiate an IPSec session.
- IPSec – Internet Protocol Security [RFC 2401]
- ISP – Internet Service Provider – A company that provides access to the Internet.
- JIRA – Japan Industries Association of Radiological Systems (Japan’s Medical Imaging Vendor group)
- Main Mode – an IKE method of key exchange that is mandatory to IPSec implementations.
- NAT – Network Address Translation [RFC 1631]
 - ❖ One-to-one NAT – The method of mapping one IP address to translate to another specific IP address.
- NEMA – National Electrical Manufactures Association
- NEMA MII – Medical Imaging Informatics Section of NEMA
- PFS - Perfect Forward Secrecy: PFS ensures that a given IPSec SA's key was not derived from any other secret key.

- PHI – Protected Health Information – This term is used generically in this paper to reference any form of protected health information
- PKI – Public/Private Key Infrastructure
- Preshared Key – A symmetric encryption key that is manually shared and used by IPSec to initiate a session.
- Private Address [RFC 1918] – This is a reserved block of addresses for use by private internets (i.e local area networks).
- RSC – Remote Service Center
- SA – Security Association, is a set of protocols and keys automatically negotiated on a regular basis between IPSec devices
- SHA-1 – Secure Hashing Algorithm 1 [RFC 2404] provides data authentication and integrity
- SPC – Joint NEMA/COCIR/JIRA Security and Privacy Committee
- Vendor – Manufacturer of medical equipment that is providing remote servicing capability
- VPN – Virtual Private Network

9. Appendix

This section points out some common problem areas. Remote Servicing of Medical Equipment through an IPSec VPN with firewalls, NAT, and DHCP is a very complex configuration. If all of these items are properly configured then the solution will work. We itemize the following issues as they are some common areas where something may be miss-configured.

9.1 Domain Name Lookup

Remote servicing happens from the RSC center to a medical device within the HCF. The RSC individual needs to be able to correctly address the medical device and have the network infrastructure resolve any hostnames.

9.2 Dynamic Host Configuration Protocol

A common practice is to use Dynamic IP Address assignment using protocols like DHCP. With this type of dynamic assignment it is important to ensure that the RSC can access the equipment. The DHCP server needs to properly inform and update any NAT system. DHCP can be used if properly configured.

9.3 Network Address Translation

If the HCF implements Network Address Translations (NAT) within their network, then any medical devices that will need to be remotely serviced will need to have NAT translations that are exposed to the IPSec VPN. The network infrastructure (typically DMZ) can ensure that that exposed NAT translation is restricted to the IPSec VPN, and thus is not accessible through the outer firewall. All IP addresses used through the IPSec VPN from both sides must be Internet Routable addresses. The NAT translation must take place outside of the IPSec VPN.

9.4 Risk Mitigation

We feel that Solution (A) has sufficiently reduced the risks, but want to fully disclose how these risks are mitigated. :

- PKI is still not mature and may present interoperability issues.
 - ❖ By using out-of-band certificate distribution we are trying to mitigate this problem.
- Authentication of the specific service individual is done at the RSC.
 - ❖ The hospital has access to the audit trails for post processing.
- This solution requires an Internet Connection
 - ❖ There are some reasonable Internet solutions that utilize frame relay, ISDN, or cable modem. The firewall protection mentioned may be implemented with router rules and filtering if the HCF is willing to accept this risk.
- The SPC white paper “Security and Privacy Requirements for Remote Servicing” outlined the need for Manual Disconnection. This concept provides for hospital staff to have the ability to monitor the remote service session in real-time and further have the ability to terminate a suspicious session.

- ❖ This solution doesn't help or hinder that requirement. It is possible to monitor the network traffic, but there is not a reasonable user interface for privacy decisions to be made.