Specification of requirements

ICT services and information security for Medical Devices

Table of contents

IMPORTANT INFORMATION **2**

OBJECTIVE 2
EXPLANATION OF FORM FOR SPECIFICATION OF REQUIREMENTS FOR ICT-SERVICES AND INFORMATION SECURITY FOR MEDICAL DEVICES 2
THE CLIENT'S PROVISIONS CONCERNING THE VENDOR'S ANSWER 2
ASSESSMENT OF THE QUALITY OF DOCUMENTATION 3

1 GENERAL SYSTEM DESCRIPTION **4**

2 LICENSE MANAGEMENT **8**

3 NETWORK **9**

4 HARDWARE **13**

5 OPERATING SYSTEM AND SOFTWARE **14**

6 INFORMATION SECURITY AND ACCESS CONTROL **18**

7 BACKUP **21**

8 INTEGRATIONS **22**

9 ICT RELATED OPERATIONS AND ADMINISTRATION **24**

ABBREVIATIONS AND TERMS 27

IMPORTANT INFORMATION

Objective

This document will be used for the evaluation/assessment of the Vendor's offered solution in the Information and communications technology (ICT) and information security areas. Additionally, it shall to the greatest possible extent map the solution's basic functionality and suitability of the Client's ICT infrastructure prior to a final customer design. This minimizes the risk of **unintended implementation costs, increased implementation time or that desired and offered functionality must be reduced** in order to meet the Client's mandatory requirements to information security and privacy. This document also serves to help the Client comply with the statutory requirements of the General Data Protection Regulation (GDPR).

Explanation of form for Specification of requirements for ICT-services and Information security for medical devices

Requirements: (A/B/C/D)		
A	Mandatory	Mandatory requirement that must be met. Inability to meet the requirement will entail that the offered solution will be rejected.
B	"Should" requirement	The Vendor's fulfilment of the requirement is either given a suitability assessment at evaluation or a score in the event of an actual tender evaluation.
C	Documentation	May be combined with A/B/D designation of requirement type. Emphasizes thus that the Client expects a more comprehensive answer (>100 words) that is elaborated/documented in appendices. If used alone, C is merely an information item that does not require a response or evaluation.
D	High	Combined with B to indicate that the requirement is very important, but not mandatory. The Vendor's ability to meet the requirement is awarded a score with an associated **high weighting** upon assessment of the offer.

The Client's provisions concerning the Vendor's answer

Answer:
All specified[1] requirements, regardless of requirement type, have to be answered by the Vendor. The answer establishes to which extent the vendor meets the requirement's wording and content.

Requirements must be answered with Yes (**Y**), No (**N**) or Elaboration (**E**). Answer category "**E**" covers all options that cannot be answered by an unambiguous Yes/No. For requirements answered with "**E**", that which the Vendor is unable to cover, a detailed elaboration is expected. This to ensure the Client's understanding of the answer to the requirements have the correct basis for an assessment and/or evaluation.

*As this specification of requirements is generic and will be used for a broad range of Medical Device procurements, there will be requirements that don't naturally apply to all procurements. The combination No as answer (**N**) and Not applicable (**N/A**) as elaboration may be used by the Client **to pre-indicate** that requirements are not considered as relevant for a procurement.*

***NOTE:** The combination No (**N**) and Not applicable (**N/A**) **may also be used where the Vendor** considers the requirement to be inapplicable based on the offered solution.*

There **must be no** references to or use of manuals, brochures, marketing material, etc. as ***answers*** to requirement items. To ensure a correct basis for comparison when different vendors are to be evaluated/assessed, an answer to a requirement must therefore include necessary copies of the relevant text. This clarification is particularly important for mandatory requirements (A-requirements), as these requirements shall commit the Vendor and ensure the Client that it is possible to establish the offered solution in the Client's infrastructure.

This ensures that a subsequent design process does not entail unintended implementation costs and a lengthy implementation period, and that requested and offered functionality may be brought

into use in accordance with The South-Eastern Norway Regional Health Authority's requirements to information security and privacy.

Nevertheless, the Vendor is responsible that its design proposal and solution elements are documented in a complete and comprehensive manner to cover all answers and specifications that are included in this specification of requirements. This entails that the Vendor is also responsible for describing all necessary solution elements in order to achieve a complete and working solution, even though such elements are not explicitly described by the Client in the specification of requirements. The Client therefore assumes that the Vendor draws attention to any relevant aspects of the solution that are not covered by the Client's specification of requirements.

Elaboration of answers:
Here the Vendor **may** elaborate responses of types "**Y**" or "**N**" if deemed necessary to ensure comprehension. However, it is not permitted to reword a "**Y**" to "**N**" or vice versa in such elaboration. Unambiguous answers of the type "**Y/N"** without mentionable elaboration are assumed only for simple requirements. With the "**Y/N"** response to simple requirements, the Client assumes that the Vendor has **accepted/denied** all terms of the requirement 100%, and will assess this accordingly. In the event of "**E**" responses, the Vendor **must** elaborate what is not met in the Client's requirement. The Vendor must describe to which extent a non-conformance is permanent, or whether this may be resolved through a design change or an alternative solution proposal. If alternative solution proposals impact the price, we have an elaboration with price consequence that is processed in accordance with the description in the section below for **"Price"**. Here the Vendor must document the actual price consequence for the Client.

Price:
Answered with a "**Y**" or "**N**". Here the Vendor states whether there is a separate, dedicated price element in order for the Vendor is to meet its obligations in accordance with the answer to the requirement. It is then assumed that the associated price element is indicated in the Price Appendix – with reference to the corresponding requirement item. If the answer is "**N**", the Client assumes that the requirement is met upon entry into contract, or within an agreed time during the term of the contract, without triggering additional cost for the Client.

Assessment of the quality of documentation

The Client require all answers of more than 100 words, or that include figures, to be described in the Vendor's appendices with references to improve readability and ensure a comprehensive understanding and correct assessment/evaluation. Such answers must reference the requirement number(s) and be specifically drawn up for the requirement in question.

The Client will assess the overall quality of the submitted documentation and answers in the specification of requirements. This may be assigned an overall score upon evaluation.

[1] By "specified" it is meant requirement items that the Client initially has not marked as inapplicable on his part with the combination: "N" and "N/A"

1 GENERAL SYSTEM DESCRIPTION

This section concerns requirements to the Vendor's general description of the overall delivery.

Specification of requirements			The Vendor's answer		
No:	**Requirement text:**	**Requirements:** (A/B/C/D)	**Answer:** (Y/N/E)	**Elaboration:** (100 words maximum, or reference to the requirement in the Vendor's answer appendices)	**Price:** (Y/N)
	General documentation requirements				
1.1	The Vendor must present a general solution design and system documentation that in a clear and concise manner shows the relevant key components, general data flow and communication interfaces internally and externally for the solution. This requirement applies regardless of whether the solution consists of only software, only individual medical devices, or combined system solutions with server(s), medical device(s) and client PCs for medical device management/monitoring and data capture from medical device. **Note**: It is of utmost importance that the documentation reflects the solution, regardless of size and scope, for example with an accompanying illustration, as it is intended to be established at the Client. The documentation may include all individual components in the system (instruments, client PCs, servers, storage, network, converters, etc.).	**AC**			
1.2	The Vendor must present a detailed overview based on the documentation from requirement 1.1, of all relevant network-related data flows as they are to be established at the Client. This includes detailed data flows between the solution’s individual components, with existing service elements in the Client’s network and any requirements for external data access. **Note:** By “relevant” it is meant data flows that use or traverse the Client's data network and thus can require that firewall rules must be adjusted for the offered solution to function in the Client’s ICT infrastructure.	**AC**			

Specification of requirements			The Vendor's answer		
No:	**Requirement text:**	**Requirements:** (A/B/C/D)	**Answer:** (Y/N/E)	**Elaboration:** (100 words maximum, or reference to the requirement in the Vendor's answer appendices)	**Price:** (Y/N)
1.3	If the offered solution is based on the use of external services at the Vendor and/or manufacturer (cloud-services, web portal or similar), the offer should also include a relevant solution design and risk assessment for the Vendor's employed infrastructure for production of the necessary services that the offered solution depends on. **Note**: If external services are not used, the requirement should be answered with "N" and "N/A"	**BD**			
1.4	The ICT related scope of assistance in the Vendor's offer must include all vendor assistance that is offered for completion of the final solution design in the Client's infrastructure, installation, configuration, testing and deployment, and preparation of the required system and operational documentation.	**A**			
	Monitoring and change regime				
1.5	The offered solution or components in the solution should provide mechanisms and/or interfaces for monitoring in order to minimize occurrences of errors and downtime. **Note:** Any restrictions and limitations related to the possibility of integration with the existing monitoring system at the Client, and how eventual notification to the system administrator may be conducted, must be clarified in the Vendor's response.	**BC**			
1.6	The Vendor must relate to and comply with the Client's and the Client's operations provider's change regime[2] for deployed solutions. **Note:** The Vendor may not plan and/or implement changes that conflict with planned changes in the Client's infrastructure. This require mutual notification of planned changes between the parties' service personnel. In the event of conflict, it is the Client's and the Client's operations provider's change regime that takes precedence.	**A**			

[2] By change regime it is meant the rules that apply for planning, notification and execution of changes to infrastructure at the Client, including central data centres at the South-Eastern Norway Regional Health Authority. This includes all physical infrastructure such as power/cooling, physical cabling, network, network services and server platforms (physical and virtual) that the offered solution depends on to provide the agreed services. All changes that the Vendor wishes to perform must be agreed and aligned with the Client's service provider, as work by the Client's service provider always takes precedence in the event of time slot conflicts. This to prevent planned maintenance from failing during implementation with associated operational disruptions and risk of patient safety.

Specification of requirements			The Vendor's answer		
No:	**Requirement text:**	**Requirements:** (A/B/C/D)	**Answer:** (Y/N/E)	**Elaboration:** (100 words maximum, or reference to the requirement in the Vendor's answer appendices)	**Price:** (Y/N)
1.7	The offered solution should only use components that have valid, manufacturer-specific maintenance agreements for the entire term of the contract. **Note:** Any components that already are beyond the manufacturer-specific maintenance agreement (End Of Life/End Of Support) or that will become so during the term of the contract must be specified.	**B**			
1.8	The Vendor should provide a documented and binding roadmap for upgrades and further development of the offered solution.	**BC**			
1.9	The Vendor should ensure that the manufacturer's recommendations are followed for updates of software, configuration, coding, nomenclature or other registers to safeguard the associated change process for the offered solution. **Note:** It is important that it is clarified how the solution should be maintained (through integration, user interface, updates of database, or similar), as well as overall technical communication requirements to carry out such updates of the offered solution.	**BCD**			
	Redundancy requirements				
	By redundancy requirements it is meant requirements related to redundancy on e.g. server and network solutions that the offered solution includes or depends on to provide the agreed service quality and/or uptime. **Note**: Inapplicable requirement items are answered with “N” in the “Answer” column and “N/A” in the “Elaboration” column.	**C**			
1.10	The offered solution should cache data locally on client PCs used or instruments in order to maintain medical functionality in the event of loss of data communication with other systems. **Note:** For the Client it is important to have clarified the size of any local storage/buffer capacity (such as maximum time, number of sessions, etc.) and which transfer and deleting procedures that may occur when data communication is restored.	**B**			
1.11	The offered system solution should support internal load balancing	**B**			

Specification of requirements			The Vendor's answer		
No:	**Requirement text:**	**Requirements:** (A/B/C/D)	**Answer:** (Y/N/E)	**Elaboration:** (100 words maximum, or reference to the requirement in the Vendor's answer appendices)	**Price:** (Y/N)
1.12	The offered system solution should support an external load balanced network connection	**B**			
1.13	The offered system solution should support internal redundancy (failover)	**B**			
1.14	The offered solution should support a redundant external network connection (failover).	**B**			

2 LICENSE MANAGEMENT

This section shall describe the licensing mechanisms of the offered solution. The offered solution should have clear and well-documented licensing mechanisms. For the Client it is important to know whether a temporary local license file/certificate/dongle is used, or a dedicated license server (internal/external).

Specification of requirements			**The vendor's answer**		
No:	**Description:**	**Requirements:** (A/B/C/D)	**Answer:** (Y/N/E)	**Elaboration:** (100 words maximum, or reference to the requirement in the Vendor's answer appendices)	**Price:** (Y/N)
	The following requirement items are only answered if the offered solution includes licensing mechanisms. **Note**: Inapplicable requirement items are answered with “N” in the “Answer” column and “N/A” in the “Elaboration” column.	**C**			
2.1	The offered solution should have clear and well-documented licensing mechanisms where any vendor-specific technical requirements and consequences of these are unambiguously documented. **Note**: The Vendor is asked to elaborate whether a temporary local license file, certificate or dongle (USB, RS232, RJ45, etc.) is used, or a dedicated license server (internal/external).	**BCD**			
2.2	The offered solution should have clear, well-documented procedures for the management and maintenance of the license/certificate. Examples of important areas to elaborate are: • How is the temporary license/certificate activated/deactivated • How is versioning of the license/certificate carried out	**BCD**			
2.3	The Vendor should elaborate any limitations in the use of the solution that are a consequence of the licensing mechanism. Examples of important areas to elaborate are technical or functional limitations: • in the number of users • in the number of concurrent users • in the number of connected devices • storage volumes • when exceeding license limits	**BCD**			

3 NETWORK

Sykehuspartner is currently the Client's provider of network infrastructure, with associated network components such as switches, firewalls, physical cabling, etc. Medical device services will normally be established logically separate from other services and the Client's administrative network in general. When necessary, access is opened towards other medical devices and integration with other services in the Clients network, for example specialist systems.

If using conversion between Ethernet and other interface technologies, this must be documented in detail to ensure that the offered solutions are technology-compatible and may be used in a Client-specific design. The Client's network is ready for IPv6, but this is not yet implemented. The current protocol is IPv4. The Client's network may use NAC (802.1x), which shuts down LAN access for unknown or inactive devices. The Client also has standardized firewall control between network zones where inactive TCP sessions are terminated after 60 minutes due to security reasons. This places demands on equipment to be connected to the Client's network, and the Vendor must take this into account when preparing the offered solution.

The Client does not permit client PCs or servers included in the offered solution to be configured as possible gateway machines (i.e. must not have two or more network interfaces) between ***an internal medical device network and the Client's computer network.*** In such cases the delivery must include an approved router/firewall that **separates** the offered solution from the Client's computer network.

Specification of requirements			The vendor's answer		
No:	**Description:**	**Requirements:** (A/B/C/D)	**Answer:** (Y/N/E)	**Elaboration:** (100 words maximum, or reference to the requirement in the Vendor's answer appendices)	**Price:** (Y/N)
3.1	The offered solution should use standard technologies/protocols for wired external data traffic (RJ45/Ethernet, RS232, USB, Firewire, etc). **Note:** Elaborate any technologies/protocols which may be used, as well as non-conformances in the form of vendor-specific limitations or technical requirements.	**BC**			
3.2	The offered solution should use IPv4 if the offered solution has external data exchange over Ethernet within the Client's systems.	**BD**			
3.3	The offered solution should use IPv6 if the offered solution has external data exchange over Ethernet within the Client's systems.	**B**			
3.4	The offered solution should be configured with the Client's own IP address series if the offered solution has external data exchange over Ethernet/IP with the Client's systems. **Note:** If the offered solution does not support use of the Client's IP address series, the delivery may include a documented and vendor-operated router/gateway/firewall that performs “NAT/PAT” address translation between the Client's address series and the Vendor's address series. The documentation have to contain the necessary IP addresses and TCP/UDP port numbers for services that are made available. This router/gateway/firewall solution must always be risk-assessed and approved prior to connecting to the Clients network.	**BC**			

Specification of requirements			The vendor's answer		
No:	**Description:**	**Requirements:** (A/B/C/D)	**Answer:** (Y/N/E)	**Elaboration:** (100 words maximum, or reference to the requirement in the Vendor's answer appendices)	**Price:** (Y/N)
3.5	The offered solution should use the Client's network without imposing vendor-specific limitations or technical requirements. **Note:** Elaborate any limitations/requirements in relation to MDD or other certifications, for example restrictions on: • must the combined, offered solution be in one and the same VLAN, or can it be segmented in multiple VLANs? • may a solution segmented across multiple VLANs have consequences for existing certifications, e.g.: MDD and/or CE? • available network capacity (bandwidth), latency, packet size or packet loss in network, use of firewall, etc.	**BCD**			
3.6	The offered solution should handle network communication failures between the different parts of the solution in such a way that medical functionality is maintained while the system re-establishes its network communication without requiring manual user operations. **Note:** See section 2 in guide text for chapter 3. Security mechanisms in the Client's network close inactive network connections on layer2 & layer3 (MAC & IP). Any requirements and consequences on the part of the Vendor following from these mechanisms must be documented with regard to design and associated security approval.	**BC**			
3.7	If the offered solution implements data transmission based on wireless communication, standard technologies/protocols should be used (WLAN, Bluetooth, GSM/LTE, other RF). **Note:** Elaborate any non-conformances resulting from vendor-specific limitations or technical requirements, such as lack of support for security mechanisms, precautions related to frequencies, signal strength, possibility of interference, etc.	**BC**			

Specification of requirements			The vendor's answer		
No:	**Description:**	**Requirements:** (A/B/C/D)	**Answer:** (Y/N/E)	**Elaboration:** (100 words maximum, or reference to the requirement in the Vendor's answer appendices)	**Price:** (Y/N)
3.8	The Vendor's offered solution design should avoid the use of components with two or more network adapters that are connected to the Client's computer network. **Note:** If multiple network adapters are used, established security features in the Client's computer network *may* be breached or circumvented. This is an undesirable situation for Client. Exemptions may be made for required and documented functional requirements, for example for instruments connected directly to client PCs with an ethernet crossover cable.	**BD**			
3.9	Any local Vendor-specific instrument network and the Client's computer network should be connected with a Client/Service Provider-approved router/firewall that separates the offered solution from the Client's computer network, ref. requirement 3.8.	**BD**			
3.10	Data traffic from the offered solution should use IP-Unicast when traversing the Client's firewalls. **Note**: The Client's network does *not* currently support the use of IP-Multicast through router/VRF.	**BD**			
3.11	The Vendor's offered solution should be compatible with use of IEEE 802.1x (Network Access Control). **Note**: For all equipment to be connected and permitted access to the Client's network, as a main rule the equipment is registered with an approved MAC address for access control.	**BD**			
3.12	The Vendor's offered solution should not be dependent on WINS or Windows' hosts file.	**B**			
3.13	The Vendor's offered solution should use DNS name resolution rather than IP addresses.	**B**			
3.14	The Vendor's offered solution should function without a requirement for grounding via network (STP).	**B**			

4 HARDWARE

Sykehuspartner is currently the Client's preferred supplier of hardware such as client PCs, servers (physical and virtual), storage solutions, printers, scanners and barcode readers.

Specification of requirements			**The Vendor's answer**		
No:	**Description:**	**Requirements:** (A/B/C/D)	**Answer:** (Y/N/E)	**Elaboration:** (100 words maximum, or reference to the requirement in the Vendor's answer appendices)	**Price:** (Y/N)
4.1	The Vendor's offered server solution should be implemented on a virtual server platform supplied by the Client's Service Provider. **Note**: Elaborate any vendor-specific requirements to virtual servers, for example: RAM, CPU, OS (HOST/GUEST), disk, RAID, expansion cards, etc.	**BC**			
4.2	The Vendor's offered solution should be implemented on client PCs supplied by the Client's Service Provider. **Note**: Elaborate any vendor-specific requirements to client PCs, for example: RAM, CPU, OS, disk, RAID, expansion cards, etc.	**BC**			
4.3	If required as a part of the solution, the Vendor's offered solution should be implemented on portable devices (e.g. laptop, smartphone, tablet, pager or similar) that can be supplied by the Client's Service Provider, assuming the equipment meets any Vendor requirements to medical approval of such equipment. **Note**: Also elaborate any other vendor-specific requirements to such portable devices (laptop, smartphone, tablet, pager or similar), for example: RAM, CPU, OS, disk, etc.	**BC**			
4.4	The Vendor's offered solution should use storage solutions that can be supplied by the Client's Service Provider. **Note**: Elaborate any Vendor-specific requirements to the used storage solution, for example: storage principles, file system, disk volume, read/write speed, etc.	**BC**			

Specification of requirements			The Vendor's answer		
No:	**Description:**	**Requirements:** (A/B/C/D)	**Answer:** (Y/N/E)	**Elaboration:** (100 words maximum, or reference to the requirement in the Vendor's answer appendices)	**Price:** (Y/N)
4.5	The Client's preferred solution for printing is based on centralized network printers with “Pull Print” (secure print). The Vendor's offered solution should use centralized network printers that can be supplied by the Client's Service Provider for printing solutions. **Note**: Elaborate any Vendor-specific requirements to local printers (local printer or own network printers), for example: RAM, CPU, disk, print speed, network card, etc. The use of “Pull Print” **presumes** that the Vendor’s offered solution can be integrated to a sufficient degree with, or enrolled in, the Client’s AD for necessary user management.	**BC**			
4.6	The Vendor's offered solution should use peripherals such as scanners, barcode readers, etc., which can be supplied by the Client's Service Provider, assuming the equipment meets any Vendor requirements to medical approval of such equipment. **Note**: Elaborate any other vendor-specific requirements to such peripherals (supported brands, models, barcode formats, printing formats, etc.).	**BC**			

5 OPERATING SYSTEM AND SOFTWARE

This chapter concerns the operating system and associated software and components of the offered solution. Currently the standard operating system is Windows 7 64/32-bit on client PCs and Windows Server 2012 R2 on servers. However, this will be changed to Windows 10 and Windows Server 2016. In addition the Service Provider supports newer versions of RedHat Linux. Through the Service Provider's contracts, the goal is that all solutions support a so-called “N/(N-1)” life cycle for all system components included in a solution. This means that the latest or latest previous version of all HW/SW components are used.

Applicable standard software at the Client for anti-malware is currently Trend on Windows servers and Microsoft System Center Endpoint Protection (SCEP) on Windows clients. For databases the current standard is Microsoft SQL Server 2014 and Oracle Enterprise R12.

Some of the health trusts in The South-Eastern Norway Regional Health Authority use RES One Suite from RES (res.com) for managing and securing client workspaces, including making client applications available with all associated plugins/third party components. The distribution of applications is mainly done via APP-V, alternatively via SCCM.

The requirements in this chapter also deal with required system components that the Client must make accessible for the offered solution to work as agreed. Such system components should be obtained from the current product and service catalogue from the Service Provider. For example, upon further agreement the Service Provider may issue the necessary certificates for use with HTTPS/SSL in connection with servers.

Specification of requirements			**The Vendor's answer**		
No:	**Description:**	**Requirements:** (A/B/C/D)	**Answer:** (Y/N/E)	**Elaboration:** (100 words maximum, or reference to the requirement in the Vendor's answer appendices)	**Price:** (Y/N)
5.1	Vendor-specific *client PCs* included in the offered solution should use the OS in accordance with the Service Provider's regime for life cycle management. **Note:** By *client PC* it is meant PCs that are either used for controlling/monitoring of a directly connected medical devices or PC with software installed for the processing of medical device-generated data.	**B**			
5.2	Vendor-specific *servers* with Windows or Linux OS included in the offered solution should use the OS in accordance with Service Provider's regime for life cycle management.	**B**			
5.3	The Vendor should elaborate all relevant requirements for required components (OS, client applications, server software, etc.) that are not supplied as a part of the offered solution, or that deviate from the Service Provider's standards. For example: Browser, web server, databases, Java, Flash, Silverlight, MS Office, .NET Framework, C++ Redistributable, MDAC etc. and any specific versions of these.	**BCD**			
5.4	If the offered solution used a local web server, mechanisms that protect the server and content from unauthorized access should be implemented. **Note**: Elaborate which security mechanisms that are activated, and which mechanisms that additionally may be activated.	**BC**			

Specification of requirements			The Vendor's answer		
No:	**Description:**	**Requirements:** (A/B/C/D)	**Answer:** (Y/N/E)	**Elaboration:** (100 words maximum, or reference to the requirement in the Vendor's answer appendices)	**Price:** (Y/N)
5.5	The functionality of the offered solution should not at all times depend on communication with web services beyond the Client's network, for example at Vendor/Manufacturer or directly to the Internet. **Note:** The Client requires control and traceability for all external communication. Documentation of why such access is required, and to which extent the solution safeguards the Client's security requirements towards external communication must be presented at the time of the offer. Use of such communication requires a completed risk assessment, resulting in an approval.	**BD**			
5.6	The Vendor should implement relevant "hardening" of the OS and used applications on vendor-specific equipment included in the offered solution.	**B**			
5.7	The offered solution should apply encryption at the application level when exchanging data with other systems.	**B**			
5.8	Vendor-specific *client PCs* should use the Client's standard software for anti-malware. **Note:** The Vendor must elaborate any requirements for deviations from the Client's standard due to certifications such as MDD, CE, etc.	**B**			
5.9	Updating of definition files for known malware on *client PCs* should take place automatically. **Note**: Elaborate any requirements to manual updating of definition files.	**BC**			
5.10	Malware scanning on vendor-specific c*lient PCs* should take place without requiring folders to be excluded.	**B**			
5.11	Malware scanning on *client PCs* should take place automatically. **Note**: Elaborate any requirements to manual malware scanning.	**BC**			
5.12	Vendor-specific *servers* should use the Client's standard software for anti-malware. **Note:** The Vendor must elaborate any needs for deviations from the Client's standard due to certifications such as MDD, CE, etc.	**B**			

Specification of requirements			The Vendor's answer		
No:	**Description:**	**Requirements:** (A/B/C/D)	**Answer:** (Y/N/E)	**Elaboration:** (100 words maximum, or reference to the requirement in the Vendor's answer appendices)	**Price:** (Y/N)
5.13	Updating of malware signatures on *servers* should take place automatically. **Note**: Elaborate any requirements to manual updating of malware signatures.	**BC**			
5.14	Malware scanning on vendor-specific *servers* should not require that folders are excluded.	**B**			
5.15	Malware scanning on *servers* should take place automatically. **Note**: Elaborate any requirements to manual malware scanning.	**BC**			
5.16	Deployment of security patches and service packs from OS vendors should be carried out without manufacturer-specific requirements or restrictions. **Note:** Restrictions due to certifications or the manufacturer's self-imposed restrictions must be documented. It is also important to the Client that it is elaborated whether necessary security patches and service packs may be installed automatically, or whether it is required that automatic updating must be delayed or configured to install only at the next reboot of client PCs or servers.	**BCD**			
5.17	Vendor-specific *client PCs* included in the offered solution should be possible to enrol in the Client's AD.	**B**			
5.18	AD-enrolled *client PCs* that will be used in the offered solution should use disk encryption (e.g. MS Bitlocker). **Note**: Elaborate any limitations related to the use of disk encryption.	**B**			
5.19	Vendor-specific *servers* included in the offered solution should be possible to enrol in the Client's AD.	**B**			
5.20	The offered solution's associated client application(s) should be compatible with the Client's use of RES One and App-V as well as SCCM. **Note**: Elaborate any preconditions and limitations in the offered solution.	**BD**			

Specification of requirements			The Vendor's answer		
No:	**Description:**	**Requirements:** (A/B/C/D)	**Answer:** (Y/N/E)	**Elaboration:** (100 words maximum, or reference to the requirement in the Vendor's answer appendices)	**Price:** (Y/N)
5.21	Use and/or maintenance of installed software on the offered solution (beyond the actual OS installation) on *client PCs* should take place without the use of local administrator privileges on the operating system.	**B**			
5.22	Use and/or maintenance of installed software on the offered solution (beyond the actual OS installation) on *servers* should take place without the use of local administrator privileges on the operating system.	**B**			

6 INFORMATION SECURITY AND ACCESS CONTROL

The Client has strict requirements to security in connection with establishing and operating medical devices. Medical devices have to be protected from external threats, the hospital network and other medical devices. The hospital network in turn have to be protected against medical devices.

The Client is obligated to comply with the statutory requirements of the General Data Protection Regulation (GDPR). It is therefore required that the offered solution meets the requirements of “GDPR Article 25 – Data Protection by Design and by Default”, see:

- The Data Protection Authority’s guide to Software Development with Data Protection by Design and by Default (in English) - https://www.datatilsynet.no/en/regulations-and-tools/guidelines/data-protection-by-design-and-by-default/
- The Data Protection Authority’s information about GDPR and requirements for Data Protection by Design and by Default to vendors and developers in the healthcare industry (in Norwegian) - https://www.datatilsynet.no/personvern-pa-ulike-omrader/forskning-helse-og-velferd/leverandorer-og-utviklere-i-helse--og-omsorgssektoren/
- GDPR – Article 25, Data protection by design and by default (in English) - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL

The Client is obliged to comply with the Norwegian Directorate of eHealth's “Code of Conduct for information security” (“Normen”, or “The Code of Conduct”), see:

- “Normen” (in Norwegian) - https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet
- “Guide for privacy and information security - medical equipment” (in Norwegian) - https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet/normen/veileder-i-personvern-og-informasjonssikkerhet-medisinsk-utstyr
- “The Code of Conduct” (in English) - https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet/documents-in-english

Examples of guidelines provided by GDPR Data Protection by Design and by Default and the “Code of Conduct” are:

- The Client prefers medical device solutions where individual user identities are used with secured role-based access control
- Medical device solutions are prohibited to store personal data such as names, personal identity numbers, requisition numbers, diagnoses, test results and similar permanently without safeguarding requirements to information security
- The Client aims to standardize using the Client's Integration Service based on The South-Eastern Norway Regional Health Authority’s Regional Integration Platform for all forms of integration between network and security zones. This applies to both socket based socket communication and file transfer.
- For solutions that require the use of external storage media for manual transfer of data files, the Client complies with the guidelines of the regional management system for information security, currently encrypted storage devices with Bitlocker are used at the Client.

Specification of requirements			**The Vendor's answer**		
No:	**Description:**	**Requirements:** (A/B/C/D)	**Answer:** (Y/N/E)	**Elaboration:** (100 words maximum, or reference to the requirement in the Vendor's answer appendices)	**Price:** (Y/N)
	The requirements below **must** be completed if the offered solution will generate, process or store personal data across the Client’s network or if this is functionality that may be brought into use during the term of the contract. **Note**: Inapplicable requirement items are answered with “N” in the “Answer” column and “N/A” in the “Elaboration” column.	**C**			
6.1	The Vendor must elaborate relevant deviations from statutes and rules relating to information or patient security the offered solution may have. **Note**: The Client is obliged to comply with the Norwegian Directorate of eHealth's “The Code of Conduct for information security” (the “Code of Conduct”).	**BCD**			
6.2	The Vendor should perform necessary adjustments to manage and close any deviations from “The Code of Conduct” at no cost to the Client within a contractually stipulated time.	**B**			
6.3	The offered solution should use centralized file storage and/or database. **Note**: Elaborate which database platform is supported, as well as whether the solution is based on local services, and if so, may this be replaced with centralized server based services.	**BC**			
6.4	The offered solution should use individual user identities at both the OS and application levels.	**B**			

Specification of requirements			The Vendor's answer		
No:	**Description:**	**Requirements:** (A/B/C/D)	**Answer:** (Y/N/E)	**Elaboration:** (100 words maximum, or reference to the requirement in the Vendor's answer appendices)	**Price:** (Y/N)
6.5	Individual user authentication should be implemented towards groups defined in Active Directory via LDAP. **Note**: Elaborate whether a LDAP integration simply synchronizes users from AD to a local user database, or whether authentication takes place directly towards AD.	**BC**			
6.6	All forms of local user profiles (user names/passwords) stored in local user databases, configuration files, etc. that are used for client, database or application login should be secured with standardized mechanisms for access control and encryption. **Note**: Elaborate how requirements for access control and encryption are intended to be handled in the offered solution.	**BCD**			
6.7	The offered solution should support role-based and/or decision-based access control/access management. Key elements to elaborate are: • which role types that exist – for example admin user, superuser, Read&Write user, Read-only user, etc.? • are roles fixed or may roles be (re-)configured in the solution? • which security measures that have been established to prevent changes to role-based access management are built into the offered solution?	**BCD**			
6.8	The offered solution should have functionality for limiting access to personal information for single users and groups of users.	**BCD**			
6.9	If the offered solution includes standard or system users, only unique passwords should be used for connection to the Client's ICT infrastructure. **Note:** Passwords that may be retrieved directly from user manuals or other forms of available documentation must not be used.	**BD**			
6.10	In the event of a requirement for external storage or dissemination of sensitive personal or patient data, the offered solution should use encrypted USB storage devices from IronKey.	**B**			

Specification of requirements			The Vendor's answer		
No:	**Description:**	**Requirements:** (A/B/C/D)	**Answer:** (Y/N/E)	**Elaboration:** (100 words maximum, or reference to the requirement in the Vendor's answer appendices)	**Price:** (Y/N)
6.11	If the offered solution uses external web solutions/portals for analysis, reporting or operation and management, it should have an "Overall Rating" of at minimum "A"on the report generated at Qualys SSL[3] Labs. **Note**: If external web solutions/portals are not used, answer the question with "N" and "N/A"	**B**			
6.12	The solution should have functionality for automated deletion of personal data when these are processed or confirmed transferred to the enterprise application software.	**BCD**			

7 BACKUP

The Client wishes to comply with the principles of Data Lifecycle Management, where Backup/Restore is a key component to ensure data security and integrity. The goal is to use centralized Backup/Restore to the greatest possible extent.

Specification of requirements			The Vendor's answer		
No:	**Description:**	**Requirements:** (A/B/C/D)	**Answer:** (Y/N/E)	**Elaboration:** (100 words maximum, or reference to the requirement in the Vendor's answer appendices)	**Price:** (Y/N)
	The requirements below are completed if the offered solution will use self-produced or central backup services across the Client's network or if this is functionality that may be brought into use during the term of the contract. **Note**: Inapplicable requirement items are answered with "N" in the "Answer" column and "N/A" in the "Elaboration" column.				
7.1	Backup of disk, including software, configuration, calibration, etc., on server and client PC should use existing centralized and automated backup services at Client. **Note:** It is thus presumed that the backup client can be installed on the offered solution and that any vendor-specific firewalls are opened for access from the Client's backup solution..	**B**			

[3] Qualys SSL Server Test is an open verification of encryption - https://www.ssllabs.com/

Specification of requirements			The Vendor's answer		
No:	**Description:**	**Requirements:** (A/B/C/D)	**Answer:** (Y/N/E)	**Elaboration:** (100 words maximum, or reference to the requirement in the Vendor's answer appendices)	**Price:** (Y/N)
7.2	Backup of databases should use centralized and automated backup services at the Client. **Note:** It is presumed that the backup client can be installed on the offered solution and that any vendor-specific firewalls are opened for access from the Client's backup solution.	**B**			
7.3	Databases included in the offered solution should support both full and incremental backups (through e.g. log backup/log shipping) of databases.	**B**			
7.4	Vendor assistance in connection with restore from backup should either be included or specified in the price appendix for the service agreement.	**B**			

8 INTEGRATIONS

If the offered solution uses data exchange with the Client's key systems, this should take place using open/De Facto standards for such data exchange.

The South-Eastern Norway Regional Health Authority has a Regional Integration Platform for all integration and interaction internally at the health trust, between health trusts, and with external parties. This platform includes standardized integration services, based on international standards and national messaging standards. Examples of such standards are HL7, KITH and DICOM (DICOM is standard for medical device communication with RIS / PACS). Examples of known and applied communication protocols are HTTP(S), FTP, SFTP/FTPS, CIFS.

The purpose of the following requirements is to identify whether the product supports the Regional Integration Platform established at the South-Eastern Norway Regional Health Authority. This applies to key elements such as log functionality, security mechanisms, applied communication protocols, message formats and semantics. All of these factors will impact time and cost when establishing integration.

Specification of requirements			The Vendor's answer		
No:	**Description:**	**Requirements:** (A/B/C/D)	**Answer:** (Y/N/E)	**Elaboration:** (100 words maximum, or reference to the requirement in the Vendor's answer appendices)	**Price:** (Y/N)
	The requirements below are completed if the offered solution exchange data with other central server services in the Client's network or if this is functionality that may be brought into use during the term of the contract. **Note**: Inapplicable requirement items are answered with "N" in the "Answer" column and "N/A" in the "Elaboration" column.	**C**			
8.1	The offered solution should include APIs or technical solutions to adapt to an Integration solution, for example: Web service, file export/import, WCF, DICOM.	**B**			
8.2	The offered solution should use APIs in a secure manner for integration and information exchange. Elaborate which security mechanisms the offered solution can support using APIs.	**BC**			
8.3	The exchange of medical information (HL7, KITH, DICOM, ASTM or similar) should be done without being subject to vendor-specific requirements or restrictions in relation to which protocols that may be used. Examples of protocols that may be used at the Client are: TCP/UDP, FTP/FTPS/SFTP, CIFS, SMTP, SOAP (HTTP/HTTPS), MSMQ, DICOM.	**BC**			
8.4	The offered solution should use integration and information exchange without being subject to vendor-specific requirements or restrictions on which message formats may be used. Examples of such formats are: XML, CSV, DICOM.	**BC**			

Specification of requirements			The Vendor's answer		
No:	**Description:**	**Requirements:** (A/B/C/D)	**Answer:** (Y/N/E)	**Elaboration:** (100 words maximum, or reference to the requirement in the Vendor's answer appendices)	**Price:** (Y/N)
8.5	The offered solution should use the Client's standardized integration services without being subject to vendor-specific requirements or restrictions for semantics in applied standardised message formats, including which format versions that may be used. **Note**: Elaborate any such requirements/restrictions, including any implementation deviations in the applied standard. Examples of such semantics are: ASTM, HL7, ebXML, KITH.	**BC**			
8.6	The offered solution should have the option for logging of message flow and message receipts when using integration services. **Note**: Elaborate the logging functionality the offered solution may have, and how this can support the need for message documentation, any troubleshooting and analysis of deviations for sent and received data in the interface between medical devices and other parties.	**BCD**			

9 ICT RELATED OPERATIONS AND ADMINISTRATION

The South-Eastern Norway Regional Health Authority has standardized remote access through solutions from F5 BigIP and Citrix. The Client currently provides a remote access solution for all external equipment suppliers. It is referred to as "Vendor access" and must be used for all vendor-specific operation and management where personal attendance at the Client's premises is not presumed. To use this solution the Vendor must use a web plugin for SSL VPN and the Citrix Receiver web client on their PCs. The Vendor may then access an access server at the Client where the necessary software and/or remote control application for the medical device client/server is made available. All use of the remote access solution must be linked to personal, identified users at the Vendor.

Some health trusts have, in addition, a standardised "file lock" for controlled and secure transfer of data between the Client and the Vendor.

A regional VPN Gateway has been established for the termination of VPN connections between vendors and the Client. This is the preferred method for outgoing VPN access from the Clients network. All planned use of VPN must always undergo a risk assessment that approves any use before this may be established. The Vendor must provide binding assurance/documentation of employed data formats, that VPN use includes only technical data, and that there is no risk of the transfer of personal data, including encrypted data. All changes in the format setup and use of VPN must be approved by the Client in advance.

It is of key importance to the Client and the Client's Service Provider that equipment in the Client's network can provide logging functionality at several levels (hardware/OS/security/user activity, etc.). All logs that the offered solution generates where content must be classified as sensitive business or personal

information, must be secured in compliance with requirements to information security (ref. the “Code of Conduct”). This must be done to ensure that essential log information cannot be read, changed or deleted by unauthorized personnel.

If the Client agrees with the Vendor that operation and management requires the use of Vendor access, as a rule of thumb a Data Processor Agreement must be entered into with the Client’s service provider.

Specification of requirements			**The Vendor's answer**		
No:	**Description:**	**Requirements:** (A/B/C/D)	**Answer:** (Y/N/E)	**Elaboration:** (100 words maximum, or reference to the requirement in the Vendor's answer appendices)	**Price:** (Y/N)
	The requirement items below are related to the use of the Client’s remote access solution and are only necessary to complete if there are plans to use this upon commissioning or if this is functionality that may be brought into use during the term of the contract.	**C**			
9.1	The supplier should use the Client's offered remote access solution for operation and management of the offered solution. **Note**: Elaborate which needs the Vendor has for available software in the Client's standard remote access solution to support the offered solution via remote access. Currently Vendor access provides access to an access server with installed management/operation tools such as *UltraVNC, WinSCP, RDP* and *SSH*. Use of custom internal vendor access using solution such as 3G/4G or ADSL modem, as well as software such as TeamViewer, LogMeIn, etc. is *not* permitted by the Client.	**BCD**			
9.2	There should only be a requirement for vendor access to *technical production logs* for support. **Note**: Elaborate whether vendor access to production logs includes only technical data, and whether there is a risk of access to personal data, including encrypted data.	**BCD**			
9.3	The Vendor should perform technical support without required to obtain/transfer technical logs and example material via VPN.	**BCD**			
9.4	The solution's devices for storing of data that may contain personal data should use *“service access”* or *“service user mode”*, where data is concealed/anonymized in connection with Vendor assistance on the offered solution.	**BD**			

Specification of requirements			The Vendor's answer		
No:	**Description:**	**Requirements:** (A/B/C/D)	**Answer:** (Y/N/E)	**Elaboration:** (100 words maximum, or reference to the requirement in the Vendor's answer appendices)	**Price:** (Y/N)
9.5	The offered solution should include features for logging and storage of log data. **Note**: Elaborate whether logging to Windows EventLog, log files, databases, SNMP traps etc. are used.	**BC**			
9.6	The offered solution should log and store technical incidents or errors.	**BD**			
9.7	The offered solution should log and store user operations (user activity, including unauthorized or attempts at unauthorized use).	**BD**			
9.8	The offered solution should provide authorized users at the Client access to logs using a standardized user interface. **Note**: Elaborate how logs are made accessible.	**BC**			
9.9	For the various types of log data that are stored in the offered solution, including reading, changing and deletion of logs, the applicable public information security requirements should be safeguarded. **Note**: Elaborate how security requirements related to confidentiality, integrity and availability are ensured for the different types of log data stored in the offered solution.	**BCD**			

Abbreviations and terms

Terms	Description
3G/4G modem	USB modem used for 3G/4G GSM communication
AD	Active Directory – Microsoft's catalogue service for authentication and authorisation of users in a Windows domain
ADSL	Asymmetric Digital Subscriber Line - line for data transfer via copper wire/telephone network
API	Application Programming Interface, interface for integration
ASTM	Standardisation body for international standards within e.g. lab communication
Bluetooth	Wireless communication technology
Change regime	By change regime it is meant the rules that apply for planning, notification and execution of changes to the infrastructure at the Client, including central data centres at the South-Eastern Norway Regional Health Authority. This includes all physical infrastructure such as power/cooling, physical cabling, network, network services and server platforms (physical and virtual) that the offered solution depends on to provide the agreed services. All changes that the Vendor wishes to perform must be agreed and aligned with the Client's service provider, as work by the Client's service provider always takes precedence in the event of time slot conflicts. This to prevent planned maintenance from failing during implementation with associated operational disruptions and risk of patient safety.
CIFS	Common Internet File System - protocol for file sharing
CPU	Central Processing Unit - processor in e.g. client PC/server
CSV	CSV - Comma Separated Values - text file containing data separated by a comma or other character for separating data fields
DICOM	Digital Imaging and Communications in Medicine – standard for the exchange of image files
DNS	Domain Name System - System service for translating between machine name and IP address
Enterprise application software	Purposed-designed software that takes care of specific functions within one or more fields. For example, LIMS or EHR.
ebXML	Electronic Business using eXtensible Markup Language - XML standards used for electronic transfer of business information
EHR	Electronic Health Record
External data exchange	By external data exchange it is meant all data traffic that utilizes the Client's infrastructure. This can be, for example, communication with centralized services for authentication and authorization of users, file storage, databases or integrations with other services.
F5 BigIP VPN	Standard vendor access VPN is delivered using the BigIP product from F5
Firewire	IEEE1394, technology for wired high speed data transfer
FTP/FTPS	File Transfer Protocol/File Transfer Protocol w/SSL encryption, protocols for file transfer
GDPR	General Data Protection Regulation (EU) 2016/679
GSM	Global System for Mobile Communications - standard for telecommunication for cellular phones
Hardening	Hardening of PC client, server and other ICT components is a method used to increase component security by eliminating or limiting possible security vulnerabilities that can be exploited by an attacker. This can be done, for example, by ensuring that operating systems, software and third-party software components are security-patched or updated to the latest version, using anti-virus/anti-malware, local firewals, and disabling/blocking unused services.
HL7	Health Level 7 – standard for exchange of messages with clinical and administrative information between health-related information systems
HOST	Windows hosts file, static text file with machine name and corresponding IP address
HTTP/ HTTPS	HyperText Transfer Protocol/HyperText Transfer Protocol Secure - communication standards for World Wide Web
IEEE 802.1x	Standard for authentication of hardware connected to network. Must not be confused with standards for wireless networks (WLAN).
IP-multicast	IP communication where data is sent simultaneously to a specified group of listening recipients in the network
IPv4	Standard addressing protocol for connectionless communication in networks
IPv6	Latest version of the IP communications protocol that eventually will replace IPv4
Ironkey	Approved USB storage device with encryption technology (www.ironkey.com)
KITH	Standard for the exchange of messages with clinical and administrative information between health-related information systems
Storage solution	Collective term for various network connected solutions where data may be stored externally. Examples are file server (physical/virtual), NAS/SAN
LAN	Local Area Network, wired network

Terms	Description
LDAP	Lightweight Directory Access Protocol – Standard protocol for connection/integration with Active Directory
Vendor	In this document this is used as a term for those submitting tenders based on a request for tender from the Client
LIMS	Laboratory Information Management System, laboratory system
MAC address	Unique ID assigned the network interface at layer 2 in the OSI model
MDD	Medical Device Directive
MS SCEP	Microsoft System Center Endpoint Protection – standard antivirus solution for client PCs in The South-Eastern Norway Regional Health Authority
MSMQ	Microsoft Message Queuing – Microsoft's solution for message queues, supported in most versions of Windows
MD	Medical devices
NAC	Network Access Control – See IEEE 802.1x
NAS	Network Attached Storage
NAT/PAT	Network Address Translation/Port Address Translation – a method for mapping an IP address/Port range to another
Client	In this document this is used as the term for the applicable Health Trust in The South-Eastern Norway Regional Health Authority
OS	Operating system
PACS	Picture Archiving and Communication System
Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
RAM	Internal memory
RDP	Remote Desktop Protocol – Microsoft protocol for remote control of Windows PC/server
RF	Radio frequency
RJ45	Modular connection used for termination of network cable (Ethernet)
Risk assessment	A risk assessment is carried out when establishing new and changing existing medical device solutions at The South-Eastern Norway Regional Health Authority. The risk assessment must identify risks and vulnerabilities in the solution, as well as any risk-reducing measures with the responsible for implementation.
RS232	Serial port – interface for serial data transfer
SAN	Storage Area Network
Sensitive personal data	See special categories of personal data.
SFTP	FTP over SSH
SNMP trap	Simple Network Management Protocol, Trap – a method for a client to inform a monitoring system of events, such as errors, in the network or in software.
SOAP	Simple Object Access Protocol - Protocol for exchanging structured information over web services using XML
Special categories of personal data	In this contex, special categories of personal data means: • Datra regulated by GDPR Article 9. • Health data that includes names, personal identity numbers or other identifying characteristics so that the data may be traced back to an individual • Health data where names, personal identity numbers and other identifying characteristics are removed and replaced with a serial number, a code, fictional names or similar, that refers to a separate list with the direct personal data, for example a requisition number, sample ID or similar.
SSH	Secure Shell - Application protocol with encrypted communication for access to login and command line on remotely controlled client/server
SSL	Secure Sockets Layer – Certificate-based encryption protocol often used for web
STP	Shielded Twisted Pair, network cable with shielding and possibility of grounding
TCP	Transmission Control Protocol – Secure communication protocol for applications that communicate over an IP network
Service Provider	The company/organization that at any time is responsible for operation and administration of the Clients collective ICT infrastructure and ICT service catalogue
UDP	User Datagram Protocol – Non-secure communication protocol for applications that communicate over an IP network
UltraVNC	Application for remote control of client/server via a remote access solution
USB	Universal Serial Bus – interface for connecting peripheral devices

Terms	Description
VLAN	Virtual LAN - a method for logical separation of a network in broadcast domains
VRF	Virtual Routing and Forwarding. A virtualization technology that enables several different routing tables in one and the same router. This allows overlapping or identical address spaces in the routing tables without resulting in address conflicts. One avoids establishing separate networks with several physical routers, everything may be established and segmented on one and the same router.
WCF	Windows Communications Foundation – Microsoft API for integration services
WINS	Windows Internet Name Service. Service defined by Microsoft to map machine names to the IP address and the service type the machine has to offer
WLAN	Wireless Local Area Network, wireless network
XML	eXtensible Markup Language - Standard for structured data in text format