Universitair Ziekenhuis Brussel

UZ Brussel Installation Conditions

Objective

This document contains the installation conditions prepared by the IT service of UZ Brussel (UZB).
Its purpose is to allow a smooth start of the project after the procurement procedure and planning (resources etc ...). For additional questions or info please contact the system team (security@uzbrussel.be).

1. Licenses

- ☐ Easy to transfer to a replacement system.
  (Not enforced by hardware-based solutions such as keys & dongles)
- ☐ If specific properties such as MAC address or VM Hardware ID are required,
  indicate in advance.
- ☐ Requested for production only.
  (and thus no additional licenses required for test/training or acceptance environment)
- ☐ Licenses of any OS, DB & other supporting products clearly indicated,
  not an enforceable part of the solution.
  (UZB may rely on its own contracts to provide these licenses)
- ☐ Indicate how data from solution can be accessed & exported after replacement.
- ☐ If licenses such as Oracle DB, MS SQL Server etc. are to be purchased, this must be clearly indicated.
  If this license is through the solution provider, this must be handed in document (usually from the manufacturer) to UZB. This in case of checks by respective software manufacturer.

2. Infrastructure Integration

- ☐ Updates can be done as much as possible without downtime (if impossible, aligned with UZB scheduling).
- ☐ Each update should be rollback able (if DB integration,
  a script should be provided to roll back these updates at the DB level as well).
- ☐ Total concept must be sold for another 5 years & supported for 10 years after purchase.
  (For customization, a mechanism of knowledge transfer
  is in place
  with contractor)

☐ If the solution is hosted outside UZB environment,
it must meet the same conditions as on premise &
an internal or external audit can also be performed on this.

☐ Access management and role assignment at least linked to the UZB Microsoft AD via MS Azure AD.

☐ Application of multifactor authentication may be imposed. Whether or not on the advice of the UZB DPO.

☐ Each **client** (desktop, laptop, tablet, ...) in UZB has following standards:

- Client & accompanying license purchased by ICT
(unless they are part of solution offered or explicitly agreed otherwise, license documents of underlying products should be made available if they are part of the solution).

- All connected equipment (printers, reading pens, scanners, etc.) are provided from ICT
(unless they are part of solution offered or explicitly agreed otherwise).

- Standard OS is MS Windows 10, preference given to the LTSB version.
Windows 7 is no longer accepted.

- VDI is used for some users (on vmware Horizon). Any restrictions on running software on these platforms should be explicitly passed in the design document.

- Clients arejoined in the AD domain of uzbrussel.be & managed via GPOs. These settings apply to all devices and cannot be changed without consulting the contractor.

- Deliver software installed on clients in the domain in a Microsoft SCCM compatible format (preferably MSI). Distribution of software is done by ICT with SCCM. The software installation manual is part of the as-built documentation.

- SCCM is used to provide all domain clients with the regular Windows updates.
Exceptions to this do not occur unless thoroughly justified.

- All clients are equipped with Microsoft Edge (Windows 10). Google Chrome is also allowed as an alternative. If another browser is required or appropriate this should be discussed with ICT.

- All clients are equipped with the latest version of Adobe Acrobat Reader to open any PDFs created. This is kept up-to-date via SCCM.

- All clients are equipped with a centrally controlled anti-virus client. This is installed, managed and kept up-to-date by ICT. If specific exclusions are required, this should be explicitly mentioned in the design documents. Periodically, a full scan of the client is done that can affect the performance of the client (is especially important for any socket-based communication. If this form of communication is used, it should be explicitly mentioned in the design documents). Other antivirus systems are not allowed. Disabling antivirus systems is not allowed.

- No client on the domain can or may, without prior consultation with authorized UZ Brussel personnel, be taken over remotely by the contractor.

- The use of TeamViewer, WebEX, VNC, etc. is not permitted without consultation with UZ Brussel ICT.

- Software installed by contractors on clients must be able to run without local administrator rights. Applications must be able to handle UAC on the client.

- All clients are equipped with Office 2016 32bit or Office 365. Any other required versions of Microsoft Office or analogs must be explicitly indicated in the design document.

- If the solution uses Java, the solution should install the Java version used in addition to the Java already present. There should be no interference between different Java versions on a client.

- If the solution uses .Net, the solution should align itself to the version common within UZ Brussel, or ensure that the .Net version used does not interfere with the standard common version.

- Internet access within UZ Brussel is linked to the personal user account. Service accounts do not have this privilege by default. If the application on the client or connected peripherals needs access to the Internet, this must be explicitly mentioned in the design documentation, with a clear statement of the necessary firewall rules.

- Application can run without local administrator rights & can handle UAC.

- Installation paths, file structure and disk layout is negotiable.

- If the solution requires a device that cannot be included in the domain, this must be explicitly stated. This must be an exception.

- UZ Brussel has its own Certificate Authority (CA) that is automatically trusted by every device in the domain. Mobile devices managed via Mobile Iron also trust this CA. Certificates from the UZ Brussel CA should be used unless a public certificate is needed which we will then provide from an external CA (Commodo).

- For email within UZ Brussel, MS Exchange is used.
(hybrid 2016/Exchange Online installation).
By default, no client or server can mail unauthenticated. Outgoing mail to the Internet is limited to mail addresses with suffix @uzbrussel.be. Other domain names are filtered by the mail gateway. If the application needs to be able to mail, there are 2 possibilities:

a. Authenticated

   i. Via AD credentials
   ii. Mail addresses must be provided

b. Non-authenticated

   i. The IP address is added in an ACL on the load balancer
   ii. No check for mail address

☐ The above standards may limit the applicability of some solutions without the intention of ICT. If the contractor anticipates that the components it needs to offer its solution will encounter problems with higher standards, it is extremely important to point this out when responding to this tender. In consultation with ICT, an alternative can then be sought for certain standards.

Depending on the contractor's problems with these standards, the following alternatives can be provided by mutual agreement:

- Client does not receive automatic updates: -
Consequence: After a period of time, this poses a security risk
- Expected Action: ICT will work with the contractor and relevant department(s) to determine a strategy to address these risks and looks forward to the contractor's proposals in its response

- Client is taken out of the domain and put in a separate network (VLAN) behind a Palo Alto firewall:

- Consequence: The main consequence is that the end user on this PC can no longer perform his normal
administrative tasks and/or patient administration can no longer be performed. This therefore implies that
he/she will need multiple clients in order to perform his/her other
tasks. This is strongly discouraged by ICT.
- Expected action: In addition to the actions mentioned in the previous bullet, ICT expects the contractor to
also a complete overview of the communication of the clients and the other IT components of
the solution, by port and (possibly to be filled in later) IP address.

- Client will be removed from the domain, placed in a separate network (VLAN) behind a Palo Alto firewall and managed by the contractor: - In addition to the consequences and actions mentioned in the previous bullet, ICT expects the contractor to propose SLAs when responding to this tender, and to provide ICT with the points of contact for service and escalation. It is also expected that the necessary security measures are taken such as e.g. antivirus. Use of strong passwords and use of Windows firewall.

☐ **Servers** in the UZ Brussel are preferably virtual and only physical if there is a very profound reason to do so and has been properly declared in advance. Each Server in the UZ Brussel domain, regardless of its function, strives for the following standards:

- Each server maintained by ICT has a Microsoft Server Operating System, with Windows 2019 - 1809 or Windows 2022 as the OS.

- For Linux, CentOS 8.x (Alma) or RHEL8 is offered.

- If an OVA/OVF is offered, we expect items 1 and/or 2 above to be met unless there is a thorough reason.

- Each server is always addressed within the provided application or peripheral via its Fully Qualified Domain Name (FQDN). The domain name is uzbrussel.be. Split DNS is used for FQDNs that must be available on the Internet.

- ICT understands that the validation of medical devices in particular takes time, and therefore Microsoft's roadmap cannot always be followed closely. Despite that understanding, ICT does not support any OS that is no longer supported by Microsoft itself. For new applications, UZ Brussel applies the rule that solutions offered by the contractor run on an OS that is still supported for at least 3 years.

- Basically, every server is virtualized via VMware vSphere. All associated software licenses support the HA & VMotion principle, and there are no requirements that could compromise VMotion.
a. If VMware Fault Tolerance is required, this should be indicated.
b. If VMotion is not supported, this should be indicated and we expect a detailed explanation for this
. VMotion is very important to UZ Brussel as it is used every 3 months for redundancy testing between computer rooms.

- Servers are always installed by UZ Brussel staff. Own installations are not allowed except in the form of an OVA/OVF for a hardened solution
(typical for Linux servers but not for Windows servers).

- Windows servers arejoined in the UZ Brussel AD-domain uzbrussel.be and are managed via GPOs. These settings apply to all devices and cannot be changed without consulting the client.
a. The baseline GPO enforces the following:
i. Disable SMBv1 (Windows filesharing) ii. Disable LM (LanManager) & NTLMv1
iii. UAC is enforced
iv. Windows Firewall is enforced. TCP/UDP ports to be set up should be specified. It will also be allowed to define an application in the Windows firewall if necessary. Only inbound traffic is currently filtered, in the future outbound traffic may also be filtered & also of this we expect detailed information.
v. User Rights Assignment (Windows privileges) are only managed via GPO and cannot be controlled via a local GPO (e.g. act as part of the OS, logon locally rights etc)
vi. SSL2.0, 3.0, TLS1.0 & 1.1 will be disabled by default.

- Any specific software installed shall be delivered by the contractor in an MSI format. The software installation manual is part of the as-built documentation. Installation of the software on the server itself should be agreed between ICT and the contractor. Any new versions/updates will follow the same path.

- All servers will receive Windows patches at regular intervals. If certain patches from the past may not be installed, it is up to the contractor to inform ICT via the design document. The contractor shall organize himself to communicate clearly and specifically to UZ Brussel about future patches that may

not be installed, and this within 2 weeks after Microsoft releases them. If the Contractor fails to communicate, any consequences of patching shall be borne by the Contractor.

- All servers are equipped with anti-virus software. This tool is installed, managed and kept up-to-date by ICT. If exceptions need to be set, this should be mentioned in the design documents. Periodically a full scan of the server is done that can affect performance (this is especially important for possible socket-based communication. If this form of communication is used, it must be explicitly mentioned in the design documents).

- No server on the domain can or may be taken over remotely by the contractor without prior consultation with authorized UZ Brussel personnel. During the project phase, a domain account will be provided for the solution with which the installations will take place. After the project phase, this account will be disabled. After the project the supplier can get access to the environment in the standard UZ Brussel way; If this is necessary, this should be discussed with ICT during the project. One can use an SSLVPN or a VPN Pulse Secure Client (either via One Time Password, eID or TOTP) in combination with our PAM solution.

- If one uses one's own remote control system such as e.g. Axeda, this must be described and approved by UZ Brussel. UZ Brussel must know at all times who has logged on to the systems.

- There is a clear difference between installation/support accounts and service accounts:
a. An account is provided for the installation and support of the application(s) but is disabled after installation. This account may not be used to run a service, make a database connection or mount a fileshare.
b. If a service requires domain credentials instead of the default system account, a service account will be created.
c. The password of a service account may not be visible in clear text in configuration files.
    i. It is clearly indicated where these service accounts are used (registry, configuration files etc).

- In operational phase (production), all applications run as services that do not require administrator rights to perform their function. GUI-based executables used on the servers (processes that cannot be started as services) are not accepted. If necessary, domain service accounts created by UZ Brussel are always used. The description of the rights of these service accounts are part of the as-built documentation.
a. Preferably, a Group Managed Service Account whose password is managed by AD is used.
b. If a (g)MSA account cannot be used, this must be justified.

- Internet access from on operational servers or communication with specific public addresses on the Internet, is not allowed by default. If the supplier considers this indispensable for its application, it can indicate this. In that case an exception to this rule will be made and we expect from the supplier:
  a. For traffic to the Internet: A proposal for detail configuration of our firewall (both Windows firewall and network firewall).
b. For applications that need to be available from outside: the details to enable this in a controlled way (URLs, IP addresses, ports, protocols, ...)

- All resources, services and all server operating systems are monitored via MonitorNow. In the design document, the contractor specifies which services, URLs are important to its application, the thresholds to be measured and the interrelationship between the various services and the user experience.

- All necessary certificates are signed internally by the UZ Brussel certificate authority.

- UZ Brussel has its own Certificate Authority (CA) that is automatically trusted by every device in the domain. Mobile devices managed via Mobile Iron also trust this CA. Certificates from the UZ Brussel CA should be used unless a public certificate is needed which we will then provide from an external CA (Commodo).

- Kerberos authentication rather than NTLMv2 is preferred.

- In addition to as-built documentation, the vendor will also provide a clear diagram where server components and information flows and dependancies are visible.

- A short operational procedure should be provided so that system availability can be quickly checked after patching/rebooting the server.

- CommVault is used as the backup solution. For virtual servers, by default 3 snapshots per day are provided where an application consistent backup is taken which means that the application must be able to process a quiesce during the snapshot action. If the application cannot handle this, this must be indicated.

- When using web servers, HTTPS must be used. UZ Brussel can provide a certificate from the internal CA or if necessary from an external CA.
a. For this, expect from the supplier a subject & SAN names and what the certificate will be used for (server authentication and/or client authentication or other).

- No insecure protocols should be used e.g. http, ftp, telnet ...

- Application data is preferably always stored outside the VM on a NAS location so that the VM does not become too large. UZ Brussel has a highly available storage platform (MetroCluster) where this data can be stored. This approach ensures that the VMDK disks do not become too large and that the storage can be expanded quickly and efficiently. A separate retention policy for backup can then be used for applicative data.

- No local shares should be created on windows servers without the knowledge of UZ Brussel. If they are needed, they will be created by UZ Brussel so that the necessary AD groups can be created and NTFS permissions can be set.

- LDAPS must be used if one wants to connect to Active Directory (not LDAP).

- For email within UZ Brussel, MS Exchange (hybrid 2016/Exchange Online installation) is used. By default, no client or server can mail unauthenticated. Outgoing mail to the Internet is limited to mail addresses with suffix @uzbrussel.be. Other domain names are filtered by the mail gateway. If the application needs to be able to mail, there are 2 possibilities:

a. Authenticated

i. Via AD credentials
ii. Mail addresses must be provided

b. Non-authenticated

i. The IP address is added in an ACL on the load balancer ii. No check for mail address

- If there is a need to use nVidia GPU cards, this should be specified. The license type for nVidia Grid should be passed in, as should the desired profile.

☐ A number of servers offer specific functions. UZ Brussel strongly encourages consolidation of these. In this case, these are:

- Communication server (HL7 based messages).
All communication of the contractor's solution with the central systems is over HL7 or in high exception another agreed protocol. Mirth is facilitating this communication within UZ Brussel. Either the contractor provides socket-based communication with Mirth (preferred), or a share is provided on the central storage platform or on (one of) the server component(s) of the application one or two shares defined for inbound and outbound file-based communication.

- Database server
From ICT, only Microsoft SQL Server & SAP ASE will be supported as standard. ICT provides the contractor with one or more databases on its central SQL 2016 database (AlwaysOn Availability Group) cluster and takes responsibility for licensing, installation of the database (SQL script to be provided by the contractor), for availability and for backup and restore of the environment. Any report services and other database activities (SSIS, SSAS, SSRS, ETL...) are run from another server. For installation and any troubleshooting activities, the contractor will be provided with appropriate contacts.
If DBA analyses show that a particular query threatens the performance of the system, we expect a timely and efficient response from the contractor. No sysadmin rights are granted to the vendor on the central MS SQL cluster.
If other databases are required the supplier will have to install and maintain them himself. The supplier will also have to update/patch the database software on a regular basis on its own responsibility (security patches).
The license for this database must be provided by the supplier. The supplier must take into account that this database server runs on a vmware virtual platform which may have licensing implications.
Backup (scripts) must be provided by the vendor and backups must be stored in a location outside the server on a NAS. This NAS location is provided by UZ Brussel.
Communication between application and database servers must be encrypted with at least TLS1.2 or higher.

- Load balancer
To make a solution full tolerant and high available, UZ Brussel offers its NGINX software load balancer, HA Proxy or Reverse Proxy for those applications that can handle it.

- File server
UZ Brussel owns central file server systems (metro cluster) and long-term file storage on archive. Data can be maintained for up to a year on a tier2 disk array and for longer term tape is provided. All file serving / NAS needs should be provided on these already existing systems.

- Back up / restore
a. Of each virtual server managed by UZ Brussel, 3 snapshots are provided daily by default.
i. These are by default application consistent (application may not have problems with a quiesce) or possibly crash consistent. The choice must be indicated by the supplier. b. A CommVault agent is installed by UZ Brussel of physical servers. ICT expects a list of the folders to be included in the backup in the as-built documentation.
c. For databases, ICT provides the full backup and restore on condition that the database is supported (see above). For MSSQL, transaction backups are provided every half hour. If other DB

systems are used, the paragraph on databases in this document expires and the supplier must take care of installation, backup and support. In such cases, ICT will only provide a file-based backup of a database export provided by the supplier.

☐ The above standards may limit the applicability of some solutions without the intention of ICT. If the contractor anticipates that the components it needs to offer its solution will encounter problems with higher standards, it is extremely important to point this out when responding to this tender. In consultation with ICT, an alternative can then be sought for certain standards.
Depending on the contractor's problems with these standards, the following alternatives can be provided in consultation:

- If server hardware is nevertheless provided by a contractor for a sufficiently justified reason, installation and placement on the domain is always done by the ICT department, and the ICT guidelines below must be respected. - Server will be removed from the domain into a separate network (VLAN) and put behind a firewall.
Besides the above mentioned point, ICT also expects from the contractor a complete overview of the communication of the server(s) and the other IT components of the solution, on (possibly to be filled in later) IP address and port.

3. Security

☐ Traceability.
Mutations of data in the system and/or on the equipment are logged. At any time it is possible to trace what happened, when it happened and who made the change.

☐ Installations.
The equipment is protected against unauthorized installation of device-foreign software by UZ Brussel.

☐ Security leaks in hardware and software.
The Contractor undertakes to notify UZ Brussel of these leaks as soon as possible.

☐ Ethical Hacking platform:
UZB uses an Ethical Hacking platform where ethical hackers detect vulnerabilities on public websites under our domain.
If a vulnerability can be found within the software placed under the management of the contractor, the corresponding bounty
can be passed on to the contractor.

☐ Only encrypted connections are used. Thus, no http but https is used, ldap instead of ldaps etc. If this is not the case, this must be indicated by the supplier.

☐ All supplier-supplied software and runtime environments (java, .net, python, etc.) must be free of known security issues as described in CVE-entries, among others. Only supported versions of applications and runtime environments are accepted. For each software component we expect a description of the version and ongoing warranty/support. It is up to the supplier to keep all software components up to date. UZ Brussel has a vulnerability scanner tool that will check this.

☐ Errors and error detection.
The system contains means for detecting and correcting errors in data input, processing, output and dissemination. The system contains means for verification of the completeness, correctness and authenticity of the internal and external dissemination of data.The system complies with the applicable guidelines at the time of use from government for, among other things, securing the information data.Higher mentioned logging of activities are kept and UZ Brussel is able to consult this logging without interaction with the contractor.

☐ Authentication and authorization.
- Preferably, passwords are not stored within the application itself. If they are, they should be salted and hashed. - Kerberos authentication over NTLM authentication is preferably used. - Each user has their unique login/password combination; no generic accounts are allowed. Authentication within the application is preferably integrated into the Microsoft Active Directory environment of UZ Brussel. - Authorization options within the offered product should be clearly indicated.
Within a multi-user application, the functional administrator can systematically record the authorizations of the (type) users and provide insight to management through reporting. There is at least a distinction in rights for reading, adding, changing and deleting data Ideally, the (types of) users can be related to a Microsoft Active Directory group. User management should be maximally automated through Active Directory, without the need for manual intervention for creation, changes and termination of users. Naming is agreed upon in advance with the ICT service. - A secure connection to Active

Directory is made when logging into the application, asking AD whether the user in question is granted access, at what level, and whether their specified password is correct. If this is not possible, this should be explicitly stated in the design documentation. - Passwords for administration purposes used in the applications must be communicated to UZ Brussel (non AD based accounts). - Preferably, installations are performed onsite with a UZ Brussel system engineer supervising the installation. - Upon delivery, the installation is reviewed with a UZ Brussel system engineer to see if all guidelines have been followed. This can/will also serve as a basic knowledge transfer. - Within a multi-user application, authentication should always take place at application start-up. We offer Single-Sign-On for our users through Imprivata. Integration with SSO is preferred. Users authenticate via their staff badge.

Failure to meet one or more of the above requirements may result in a negative recommendation for purchase.