Vendor-Neutral Tendering of Thin Clients

Guideline for Public Procurement
Version 2.0

www.bitkom.org

Published by

Bitkom
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.
(German Federal Association for Information Technology,
Telecommunication and New Media)
Albrechtstraße 10 | 10117 Berlin
T +49 (0) 30 27576-0
bitkom@bitkom.org
www.bitkom.org

Point of Contact

Marc Danneberg | Bitkom e.V.
T +49 (0) 30 27576-526 | m.danneberg@bitkom.org

Responsible Bitkom committee:

Expert Committee Vendor-Neutral Tendering

Project lead

Antonia Schmidt | Bitkom e.V. (until August 2020)

Title image

© Andres Rodriguez – fotolia.com

Copyright

This publication provides general and non-binding information. Its contents reflect the opinion of Bitkom at the moment of publication. The information has been compiled with the greatest possible care; nevertheless, there is no claim to correctness, completeness, and/or actuality. In particular, this publication cannot take into account the special conditions of individual cases. The user is therefore responsible for its use. All liability is excluded. All rights are reserved by Bitkom, including the reproduction of extracts.

Content

List of figures

List of tables

Acknowledgement

The present guideline is the result of collaboration between experts in public administration and representatives of partner companies of Bitkom. It owes its existence to the comprehensive groundwork of the Project Group »Product-Neutral Performance Description Thin Clients«. We would like to express our particular gratitude to:

- Jürgen Graf (Fujitsu)
- Uwe Harasko (Cherry GmbH)
- Thorsten Katzmann (IBM Deutschland GmbH)
- Niels Keunecke (Unicon Software Entwicklungs- und Vertriebs GmbH)
- Thomas Möllerbernd (Dell GmbH)
- Marco Raffel (IGEL Technology GmbH)
- Wolfgang Schestak (FCCL GmbH)
- Frank Schiewe (Dell GmbH)
- Martin Schnatmeyer (IGEL Technology GmbH)
- Eric Schreyer (Unicon Software Entwicklungs- und Vertriebs GmbH)
- Bernd Siegmund (HP Deutschland GmbH)
- Klaus-Peter Wegge (Siemens AG)
- Christian Werner (IGEL Technology GmbH)

1 Introduction

1.1 Using this guideline

This guideline provides an overview of the foundations and criteria for the procurement of thin clients by contracting entities. It is the product of a working group on the ↗ ICT Procurement working group. This document aims to provide contracting entities of Germany's federal, state and local governments with a dependable tool – one that is easy to understand – in order to help them formulate their tenders for the procurement of thin clients in a vendor-neutral manner, i.e. without the use of trademarked names and without mentioning individual manufacturers, while taking into consideration current technological standards.

At the heart of this guideline stands the list of technical criteria, which can be used to describe and compare the devices themselves as well as requirements placed on both their operational environment and other properties. Besides the technical criteria, compliance with which guarantees proper device functioning for the reason they were procured, the guideline also contains references to environmental protection, energy efficiency, IT security, and freedom from barriers. Even if statutory requirements only partly obligate procurers to observe these interests, they are growing increasingly relevant in public administration.

With thin client solutions, particular attention must be paid to the components required for use. Specifically, these include:

- The active network infrastructure must be sufficiently dimensioned for the expected increase in communication between the thin client(s) and server(s) (data throughput and failure safety)

- The servers must provide the thin clients that are to be used with sufficient computing power and storage space.

- The use of virtualisation technology incurs costs for licence procurement. These costs relate to both server operation and to the applications that are going to run on them.

- Not all applications can be operated using a terminal server solution. Particular care must be exercised when it comes to individual programming.

1.2 Vendor-neutrality as a legal requirement

Procurement law stipulates an obligation to equal treatment of providers and products. In accordance with the legal foundations, the subject of the procurement is to be described using professional criteria free of discrimination, i.e. in a product-neutral manner (cf. § 97 Act against Restraints of Competition (GWB) and § 31 para. 6 Ordinance on the Award of Public Contracts (VgV) for tender procedures across the EU as well as § 55 para. 1 of the Federal Budget Code (BHO) and § 2 para. 2 Regulation on Sub-threshold Procurement (UVgO) for sub-threshold procurement). Certain product descriptions or brand names may only be used in tenders in duly justified exceptions, if a sufficiently exact description using common descriptions or general criteria is not possible.

In public tendering, when drafting criteria for the product to be procured, the awarding party should ensure that different offers can be compared to one another, allowing for sufficient differentiation. Contracting entities can freely choose the criteria on which to select the procured goods or service; the award criteria, however, must be needs-based, vendor-neutral, and transparent.

Vendor-neutral tendering is difficult, particularly when it comes to the procurement of IT products, and public authorities frequently face considerable uncertainties. Technical complexity of the subject matter, rapid succession of product cycles, and, in particular, difficulties involved with assessing and precisely describing the desired performance of a system while taking all technical requirements into consideration: These all pose major challenges to public authorities.

This guideline specifically addresses this problem by providing a compact tool to support compliance with the legal requirements, thus ensuring fair competition. The guideline specifies and explains current technical standards to describe thin clients using general and pertinent characteristics. The product properties and technical requirements are concisely presented in tables. The guideline will be updated regularly, taking into consideration new developments in technology while aligning the proposed criteria and requirements with the current state-of-the-art.

2 Thin clients as an object of procurement

2.1 Definition of a thin client

General definition of a thin client

At its core, a thin client (also know as an ultra-thin client, zero client, smart zero client, cloud client, lean client, or slim client) is a computer that performs its main tasks with the assistance of remote resources (computer centre, web or cloud-based resources). The main objective is to shift local hardware resources (generally a large number of homogenous workspaces) to a computer centre, resulting in synergy effects and administrative benefits.

One thing in common with all thin clients is that local performance does not meet, or no longer meets, the performance of classic PCs. Specialised protocols are responsible for communication between the thin client and the server: Popular solutions are Citrix, VMware and Microsoft products. This is referred to as application streaming or the virtualisation of entire desktop environments (Virtual Desktop Infrastructure, VDI). Another alternative that has been increasing in popularity over the past few years is so-called »cloud computing«, whereby web applications are accessed via a browser.

Another key characteristic of thin clients: they have (virtually) no data available on local storage media, besides OS components/firmware. The fact that no personal or sensitive business data can be stored on thin clients makes them secure access devices for a diverse range of applications.

The counterpart to a thin client is a fat client. This PC has plenty of computing power and primarily, but not exclusively, processes and stores data locally.

A thin client should have production availability of at least 12 months (from the award date). The follow-up product must be of at least equal quality and price-neutral, with production availability of at least 18 months (from product introduction). To ensure the best-possible utilisation of the expected 5–7 year (approx.) usage period, not only should an additional 4–5 years of support be provided for the thin client hardware, but the manufacturer of the operating system should also ensure that a supported OS can run on the thin client hardware. This at least covers the provision of patches relevant to security and/or fixes for any malfunctions.

Thin client version

- **Hardware-defined thin clients**
  Hardware-defined thin clients are small computers with low power consumption. They do not use any rotating components (fans, rotating hard disks) and run on an »embedded« OS (see below). Hardware-defined thin clients are available with a wide range of interfaces, e.g. for peripherals.

- Hardware-defined thin clients comes in various form factors, starting with small housings below 0.5 L up to all-in-one models, units which consist of a thin client and monitor.

- The useful operating life of hardware-defined thin clients is generally 5–7 years.

- **Software-defined thin clients**
  Software-defined thin clients allow for the use of personal computers or notebooks as thin clients. The available device OS is either replaced by an »embedded« OS or booted from the »embedded« OS using a bootable USB stick. This approach is expedient for scenarios in which either PCs that are no longer powerful enough for classic PC applications, but are still fully functional, or in which the requirements of hardware-defined thin clients cannot be met, e.g. because a large number of monitors have to be connected to a device. This approach comes with the additional benefit that PCs can be equipped with two operating systems, meaning they can be used alternatingly between a PC or thin client environment.

- **Further definitions**
  The Partner Commitments of the ENERGY STAR® Programme, Sections 1, A), 8), specify further characteristics of thin clients:
  ↗ https://www.energystar.gov/sites/default/files/ENERGY%20STAR%20Computers%20Final%20Version%207.1%20Specification.pdf

2.2 Services

The provider's range of services does not have to be restricted to the provision of hardware and/or software, but can also include additional services related to the supplied item. This might include, for example, an offer to service the delivered hardware and possibly software and keep them in line with the state of the art, either through a separate service agreement or an extension of warranty. Furthermore, additional services such as troubleshooting and hotline services can be commissioned besides mere hardware and software procurement.

If necessary, relevant support should be agreed, including details on response/recovery times. The chapter on Services (see Chapter 5.3) gives a detailed overview of additional services.

2.3 Commercial procurement models

Thin clients can be purchased, leased, rented, procured with as-a-service concepts, or as a combination hereof. One of the key factors informing the decision of the procurer is whether they can use a one-time or multi-year budget. A decision for one of these models should usually already be made as part of a cost-efficiency analysis while preparing for procurement.

Overall thin client costs comprise the costs for associated support services and software (licence fees/maintenance) as well as energy consumption costs.

There are various licensing options:

1. **Bound to hardware:**
   The licence costs are included in the device costs and are not listed separately:
   - Benefits: No proprietary licences have to be ordered.
   - Drawbacks:
     - Tendering independent of the software/management solution is not possible;
     - Hidden costs are incurred when a management solution that is not related to the devices is used;
     - It is not possible to transfer licences to newly procured hardware.

2. **Independent of the hardware:**
   - Benefits:
     - Software and hardware can be procured separately, allowing for separate budgeting;
     - Transparent overall costs, with the device calculation only being based on the hardware, allowing for independent calculation of the software;
     - Licences can be transferred, e.g. onto exchanged devices, if the operating system developers offer this option
   - Drawback:
     - Slightly higher effort/expenditure in procurement, with procurement of two positions instead of one position

3. **As »as-a-service«-model:**
   - Benefits:
     - »Flat-rate« for the entire lifetime of the device;
     - Costs transparency with pre-agreed lifetime costs
     - Lower complexity, and with that an easier procurement model;
     - Transfer of capital expenditures (CAPEX) and operative expenditures (OPEX);
   - Drawbacks:
     - Higher lifetime costs;
     - More complicated extension of the service agreement in some circumstances;

2.4 Performance classes as a representation of usage scenarios

In this section, the most important solutions used in thin client computing are summarised from the wide variety of server-software solutions currently in use. The following illustration provides an initial overview of the key solutions, together with the relevant solutions providers/server environments.

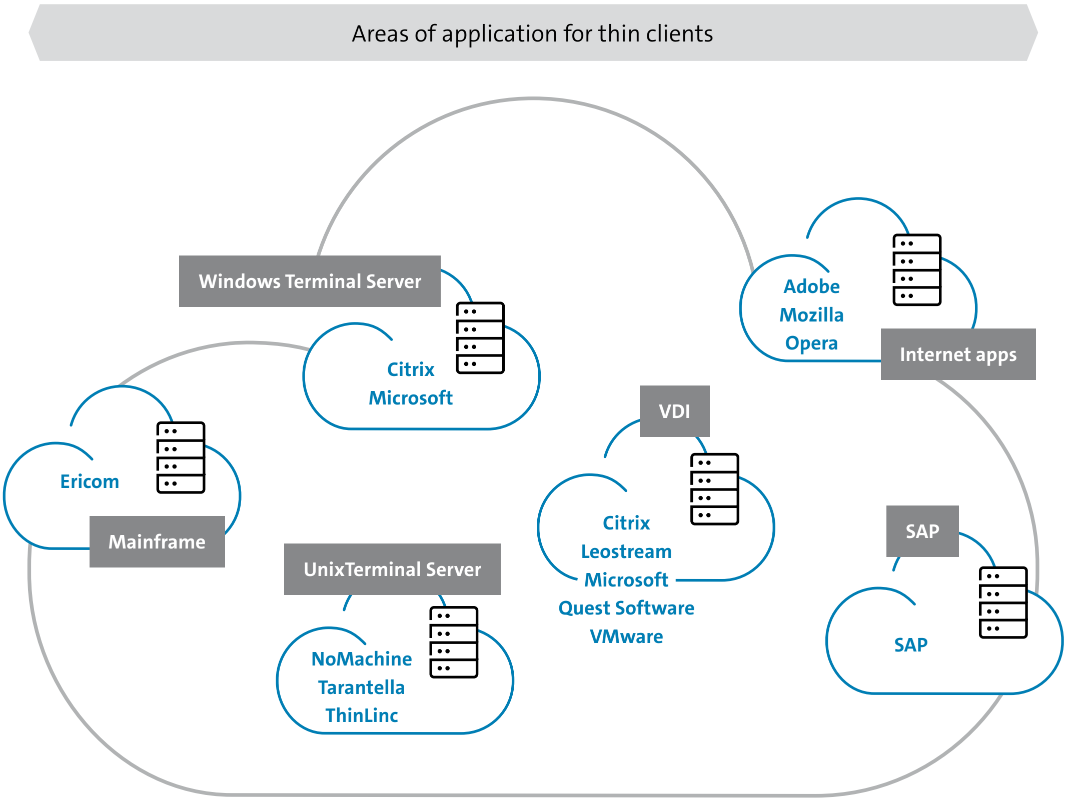

Figure 1: Areas of application for thin clients

Providers of VDI/virtual desktop infrastructure & virtual app solutions

Microsoft, Citrix, VMware, Nutanix, Teradici PCoIP, Parallels, Leostream, Quest

Internet apps/browser-based apps

HTML5 logo, Google Chrome, IE Explorer (Edge logo)

Cloud Services

Microsoft, AWS, Google and many more.

Windows Terminal Server

Linux/Unix Terminal Server
NoMachine, Tarantella, Cendio/ThinLine, Ericom PowerTerm, IBM iAccess, TTerm, TTWin, and other software terminal emulators

SAP

Mainframe

2.4.1 Server-based computing

Server-based computing (SBC) is the term used to describe the central provision of client/server applications on powerful servers. The terms »application virtualisation« and »terminal services« are commonly used synonymously. When executing application, server resources (e.g. processor and storage capacities) are generally used, rather than client-system resources. SBC allows users to access applications such as an Internet browser, typical office applications, or other terminal server-capable applications, through specialised client systems (e.g. thin clients) and a special presentation protocol (see illustration on the application areas above).

Thin clients serve as access terminals that are merely used to enter data (via keyboard and mouse or audio/video) and then transmit these data to a terminal server. This terminal server will take care of actual processing, in order to then return the resulting display output (and possibly also sound) back to the client PC. In this way, applications, among other things, can be used from remote locations without elaborate on-site installation. From an administrative point of view, SBC brings the benefit of central application provision and management/maintenance. Multiple users access and share the same resources (in sessions that are separate from one another). This contributes to cost-effective operation of IT infrastructure, particularly as concerns actual application provision.

Server-based computing (SBC) concept

- Applications run on servers in the computer centre
- Users »share« the applications

Benefits

- Simple server-side administration
- High availability
- Data security and compliance
- Very flexible and fast
- Access from anywhere, from any access device
- Low power consumption
- Longer lifecycle
- … resulting in lower overall costs

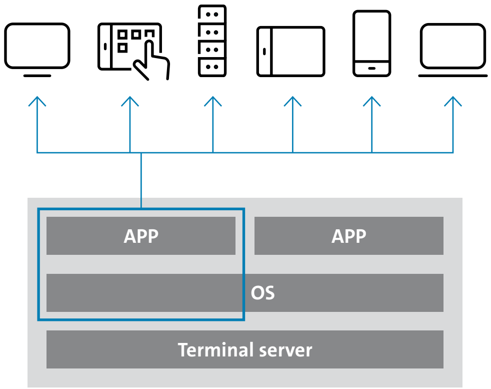

Figure 2: Server-based computing (SBC) concept

Depending on the server version and the desired scope of functionality, the performance of the used protocol must be taken into consideration, together with compatibility of the transmission protocol with the thin client used. Other products offering Windows-based SBC using MS TS include Ericom, Nomachine and ThinLinc.

2.4.2 Desktop virtualisation

Introduction to virtualisation

Virtual desktop infrastructure (VDI) is the term used to describe the hosting of client or server operating systems for the purposes of providing applications or virtual desktops within virtual machines (VMs) that are located on a central server. Several virtual machines with different operating systems and applications running on them can be executed – in an isolated manner on the one hand, but still on the same physical machine on the other.

Virtual desktop infrastructure (VDI) concept

- The desktop is operated as a virtual machine on servers in computing centres
- Decoupling of thin clients, operating systems (OSes), applications and users

Benefits

- Quick roll-out and updating
- Quick restoration after errors
- Secure data storage

Combined benefits of three paradigms

- Traditional desktop computing
- Server-based computing
- Server virtualisation

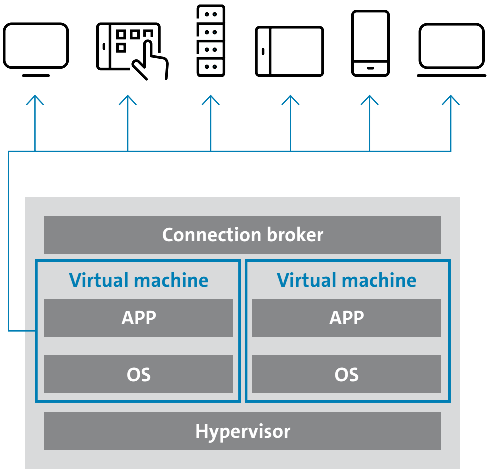

Figure 3: Virtual desktop infrastructure (VDI) concept

This enables better IT resource utilisation and greater flexibility. Every virtual machine has its own virtual hardware resources, such as RAM storage, processor, network card, etc., onto which the OS and applications are loaded. The operating system detects consistent and normalised hardware resources, independent of the actual physical hardware components.

The virtual machines are components encapsulated in files, which makes them quick to store, copy, and provide. A resulting benefit is that complete systems (fully configured applications, operating systems, the BIOS and the virtual hardware) can, for example, be moved from one physical server to another or relaunched in a matter of seconds (e.g. in the event of a physical server system outage), thanks to their encapsulated, modular structure. Virtualisation comes with a series of additional benefits over physical infrastructure. Explaining them all here would go beyond the scope of this document.

2.4.3 Other forms of application provision

Besides classic, computer centre-based virtualisation solutions, another variant has emerged over the past few years:

Cloud-service providers offer new opportunities to access applications that are hosted on the cloud operator's servers without having to operate one's own computer centre.

This concept is advantageous in that the client does not require their own separate data centre, as there is no need for local provision of data or applications. Only an Internet browser that supports current protocols (e.g. HTML5) is required to access these applications. Care must be taken to ensure that the thin client is powerful enough for the desired usage scenario.

Drawbacks of this concept relate closely to data storage: Depending on the requirements, it might be necessary to refrain from storing sensitive data in the cloud, or to at least store them in a local cloud. In addition, cloud-based concepts create a certain level of dependency on the chosen cloud provider.

A number of widespread products that can be used to provide an SBC environment are presented in the following section:

- Microsoft Windows Terminal Services: To use the product, a software component (RDP/RDC) is required on the thin client

- Citrix Virtual Apps: To use the product, a software component (Citrix Workspace app) is required on the thin client

- VMware Horizon: To use the product, a software component (VMware Horizon Client) is required on the thin client

A number of widespread products that can be used to provide a virtualised desktop environment are presented in more detail in the following section:

- Citrix Virtual Desktop Service: To use the product, a software component (Citrix Workspace app) is required on the thin client

- VMware Horizon: To use the product, a software component (VMware Horizon Client with RDP, PCoIP and/or a later-version Blast protocol) is required on the thin client

Depending on the server version and the desired scope of functionality, the performance of the used protocol must be taken into consideration, together with compatibility of the transmission protocol with the thin client used (see Annex A: Compatibility of transmission protocols).

3 Criteria and requirements for all performance classes

3.1 User profiles

Even with the objective being to create a system landscape that is as homogenous as possible, it might be expedient or necessary to define different models and/or configurations for different user groups. The following list contains an exemplary overview of typical user roles and associated hardware requirements.

Classification	Performance class	Typical applications
A system	Office thin client	1. MS Office or equivalent 2. Web-based applications with video 3. Video-playback applications 4. User-specific applications with multimedia content 5. Unified Communication such as Teams, Skype for Business, etc.
B system	Specialised workstations (e.g. CAD)	1. MS Office or equivalent 2. Web-based applications with video 3. Video-playback applications 4. User-specific applications with multimedia content 5. Unified Communication such as Teams, Skype for Business, etc. 6. 3D graphic applications

Table 1: User profiles

3.2 Technical minimum requirements for a vendor-neutral description of performance

Specifications for x86-based systems

System components	A System (Office thin client)	B System (special workstations (e.g. CAD))
Processor	x86 architecture	x86 architecture
Working memory (RAM)	**Windows:** Minimum: 4 GB Recommended: 8 GB **Linux:** 4 GB **Other operating systems:** Minimum: 2 GB Recommended: 4 GB	**Windows:** Minimum: 8 GB Recommended: 16 GB **Linux:** 8 GB **Other operating systems:** Minimum: 4 GB Recommended: 8 GB
Flash storage	Windows: 32 GB SSD Linux: 8/16 GB Other operating systems: 8/16 GB	Windows: 64 GB SSD Linux: 32 GB Other operating systems: 32 GB
Graphics (possibly dedicated)	from 512 MB shared	from 512 MB shared
Network connection	100/1000 RJ45 (WLAN optional, fibre optics optional)	100/1000 RJ45 (WLAN optional, fibre optics optional)
Interfaces	USB 2.0/3.0/3.1 RS-232 (optional) USB-C Line in-out/headset connection DisplayPort	USB 2.0/3.0/3.1 RS-232 (optional) USB-C Line in-out/headset connection DisplayPort Supports at least 4 monitors PCI/PCIe interface
Input and output devices	Mouse Keyboard SmartCard reader Biometric authentication	Mouse Keyboard SmartCard reader Biometric authentication
Energy consumption	Power consumption according to Energy Star	Power consumption according to Energy Star
Noise emissions	None	None

Table 2: Specifications for x86-based systems

Technical criteria on input/output devices

No.	Input/output device	Requirements	Standards
1	**Keyboard**	▪ Keyboard with adjustable inclination ▪ Lifetime of the individual keys at least 10 million strokes ▪ Non-slip keyboard, including when folded, thanks to non-slip coating	▪ Connection USB ▪ German keyboard layout following DIN 2137-1:2018-12 ▪ Ergonomics following DIN EN ISO 9241-400 ▪ TÜV GS (Tested Safety) or DGUV test ▪ CE marking
2	**Chipcard reader**	▪ Construction: Stand-alone, integrated in the housing or keyboard ▪ Lifetime of contacting unit at least 50,000 plug cycles	▪ Supports ISO 7816 cards
3	**Contactless reader**	▪ Construction: Stand-alone or integrated in the keyboard	▪ Supports ISO 14443 A/B cards and, if used, ISO 15693 cards, as well as NFC following ISO/IEC 18092 if required

Table 3: Technical criteria on input/output devices

Optional for all systems, depending on demands:

- Speaker, microphone
- Card reader (signature card, storage card [SD, etc.])
- Biometric sensor
- Scanner
- Braille keyboard
- Digital dictation device

Specifications for ARM-based systems

System components	A system	B system
Processor	ARM	ARM

Working memory (RAM)	from 1 GB RAM
	from 1 GB firmware
		from 4 GB

Firmware storage (ROM/flash	from 1 GB	from 1 GB RAM
		from 1 GB firmware

Graphics	from 64 MB shared	from 128 MB shared or dedicated video -RAM
Netzwerkanbindung	from 100 RJ-45	100/1000 RJ-45
Wireless	2.4 GHz and 5 GHz 802.11b/g/n/ac Wi-Fi	2.4 GHz and 5GHz 802.11b/g/n/ac Wi-Fi
Interfaces	4 × USB 2.0/3.0 1 × RS-232 (optional)	4 × USB 2.0/3.0 1 × RS-232 (optional)
Input and output devices	USB (keyboard/mouse) VGA or DVI, or HDMI Line out	USB (keyboard/mouse) monitors (DVI, HDMI, Display Port) Line out
Energy consumption	Leistungsaufnahme gemäß Energy Star	No Energy Star in this performance class
Noise emissions	None	No specification in this performance class (see ↗ **Section 7.1**)
Local browser support	No	Yes (Chromium or Firefox)

Table 4: Specifications for ARM-based systems

3.3 Local operating system

The procurement of thin clients differs from the procurement of PCs in that the relevant thin client operating system has a major impact on the functionality of the thin client. The operating systems used on thin client devices are almost always adapted to the thin clients they run on, and they differ from familiar PC operating systems.

A different range of local functions is integrated into the thin client software. Provision of OS software can follow a monolithic or modular approach. Due to the long device lifetime, long-term software support is important as well.

There are basically two categories of thin client operating systems, which are generally called firmware:

3.3.1 Hardware-independent operating systems

1. Linux-based operating systems
   - Based on the current Linux distributions with long-term support kernels
   - Adapted to thin client needs regarding installation size and functionality, without restricting performance
   - The community provides security updates to fix component errors
   - Executable on all x86 hardware platforms – vendor-independence

2. Microsoft Windows
   - In the currently up-to-date Windows 10 IoT version, it is executable on all x86 hardware platforms – vendor-independence

3.3.2 Hardware-dependent operating systems

3. Proprietary
   - The independent development of a manufacturer with its own development and release cycles
   - Based on unpublished vendor standards

4. Linux-based
   - Operating system with manufacturer-specific adaptation of a Linux distribution
   - Only executable on devices of the specific vendor

3.3.3 BIOS/UEFI and hardware driver

BIOS/UEFI and hardware driver

With the BIOS (Basic Input Output System), the functionality of all system components is tested during the so-called POST (power-on self-test).

The Unified Extensible Firmware Interface (UEFI) is the successor of BIOS and takes care of the same tasks. UEFI has the following advantages over classic BIOS:

- Graphic user interface and mouse operation
- Native support of 64-bit processors (factory default)
- Drivers can be reloaded as a module
- Linux compatibility

Additional required BIOS/UEFI functions

- Sandard setup (time, drives) in CMOS RAM with battery buffering
- If the BIOS/UEFI is freely accessible, it should be possible to set password protection for the setup routine and boot process.
- BIOS/UEFI can be updated (including remotely) via a utility program
- BIOS/UEFI reset to the required delivery state
- Booting via network PXE
- Wake-on-LAN (WoL)
- Selectable boot sequence: HDD (= internal compact flash memory), USB, LAN, PXE
- ACPI, serial-number support
- The BIOS/UEFI must meet the vendor’s current state-of-the-art upon delivery.

3.3.4 3.3.4 Supported network protocols

Protocols that are generally in frequent use at companies are called standards.

The procurer must ensure that the protocols relevant to its special network infrastructure are supported.

Explicit reference to the IPv6 protocol (↗ **https://tools.ietf.org/html/rfc8200**) is made here.

3.3.5 Supported server software and server functionality

The communication protocols available locally in the thin client firmware establish a connection with the relevant server software. Procurers must ensure that the thin client firmware contains the software clients appropriate for their server-side infrastructure. (See Annex A: Compatibility of transmission protocols).

3.3.6 Supported web services and local multimedia

An increasing number of applications are also provided through the web, both internally as well as through cloud computing. A web browser is generally required to use these applications or services. Additional scripting languages – such as Java and .net – are often required to be able to use the applications.

If multimedia content, e.g. presentations and videos with animations and/or sound, are not decoded on the server and then streamed over the network (so-called offloading), a process which takes up a lot of bandwidth, local media players are required, such as:

- Windows Mediaplayer
- Mplayer
- Gstreamer
- incl. the associated codecs.

Additional local applications can include:

- WebRTC applications
- Video conferences
- Voice-over-IP
- Screensaver
- And many more

3.3.7 Software-supported security

Certain security requirements must be demanded for use in public administration, e.g. to prevent unauthorised data access or prevent data theft. There is currently a wide range of security solutions available. However, these must be supported by the firmware.

Technologies that can be specified by the public entity include (valid as of guideline creation, 2020):

- TPM 2.0 support
- SmartCard solution
- eToken (USB stick security)
- (Biometric) user authentication
- VPN clients
- Multi-factor authentication

3.4 System management

The central management system should assume the largest possible number of tasks for centrally controlled administration of thin client environments.

This includes both simple tasks (such as remote switch-on/turn-off/reset) as well as updating of the local BIOS and software versions to guarantee continuous operation of the thin client infrastructure. It must be possible to execute all commands with a time-controlled scheduler function, and they must have a logging function.

Various aspects must be considered when it comes to comprehensive system management. These aspects can be grouped into the umbrella terms **Security, Device Management, Device Configuration, and Remote Administration**.

3.4.1 Security

The following functions are shown under the item **Security**. The management software must be able to implement a multi-layer rights concept (multi-administration concept) with various administrative levels. In the same vein, it must also be possible to use this concept in the management of multiple organisational units that are separate from one another. For optional logging of administration activities, auditability must be ensured, in order to guarantee that changes and adjustments can be traced transparently if needed.

Communication between the management system and the terminal device must be encrypted to prevent any attacks when transferring information. Another feature is the support of device-specific certificates. The management system should enable simple configuration and distribution.

The central management of peripherals is also a relevant security issue. Exact assignment of configurations for e.g. USB mass storage media and other USB devices should be possible. Redundant operation is required to safeguard fail-safety and continuous operation of the management environment. This should be guaranteed by the software developer's products.

3.4.2 Device management

The following functions must be considered for general **device management**.

For terminal device administration without on-site deployment (zero-touch), processes such as automatic onboarding with filter-based assignment to organisational units or device classes are recommended.

With various updates to the terminal devices, it is expedient to follow multi-stage distribution processes that take up a minimum of bandwidth. These come with the advantage that updates can be prepared at a different time than the actual update, which in turn improves the reliability and stability of the update process. Adequate reporting, which not only covers for the update processes, but rather all sent commands, helps in consistent and transparent monitoring of all processes.

Reporting also covers all inventory data of managed devices and their peripherals (keyboard, mouse, monitors, USB devices, etc.).

3.4.3 Device configuration

The umbrella term **device configuration** cover all setting options that can be made across a range of devices within the overall infrastructure and/or subordinate organisational units on the one hand, and on an individual device on the other hand. This includes language, mouse, keyboard and printer (local/network) settings, as well as multi-monitor configuration and the detailed use of peripherals such as a smartcard reader or the connection of USB mass storage media.

3.4.4 Remote administration

Remote administration (mirroring/remote control)

Another important feature of central remote administration is user support through a configurable thin client mirroring functioning with assigned rights. When using the mirroring function, auditable rights distribution and the possibility to evaluate should be ensured. One of the most important functions of remote administration is the updating of terminal devices to a later software version of the OS developer and the importing of new software components relevant to tasks within the company.

The processing of this task should be, in line with the wide variety of requirements in place within a company, multi-stage with controllable scheduling, in order to minimise workspace downtime during updates. For security reasons, the vendor-specific firmware must be updated with imports of company-specific configurations. To make sure devices do not have to be serviced on-site, which takes up a lot of time, administration over a central management console is required.

For more extensive analysis of faults that occur with thin clients, it is essential for both support as well as the administrator to be able to diagnose the problem. Diagnosis data that document the system state when the fault occurred are helpful tools. Remote access of these data from the administrator console should be possible.

3.5 Services

3.5.1 Pre-installation and design

In the awarding of additional services, a distinction can be made between the following types:

- Installation of software on the hardware before hardware delivery
- Unpacking and installing the hardware, connecting it to the power supply of the client, and carrying out a device test

Pre-installations carried out at the vendor/provider are classed as service elements of the purchase contract. The EVB-IT (Supplementary Terms of Contract for the Procurement of IT) purchase contract explicitly includes pre-installation works, and even installation works.

A purchase contract is also in place if additional services besides actual small-scale delivery and installation are to be performed at the client's location (e.g. on-site installation or configuration). In this case, however, one should not use an EVB-IT purchase contract, but rather the EVB-IT system delivery contract (refer to the guideline on including BVB and/or EVB-IT contract types into IT procurement contracts, available at ↗ **http://www.cio.bund.de/cae/servlet/contentblob/83250/publicationFile/19754/entscheidungshilfe_pdf_download.pdf**).

The EVB-IT, along with information regarding its application, can be found on the website of the Federal Commissioner for Information Technology at ↗ **https://www.cio.bund.de/Web/DE/IT-Beschaffung/EVB-IT-und-BVB/Aktuelle_EVB-IT/aktuelle_evb_it_node.html**

3.5.2 Support

If necessary, relevant support should be agreed, including details on response/maintenance times. Common offers vary according to (list not exhaustive):

- Contract duration
- Response times (period between reporting a disruption and receiving a first response from support)
- Spare-parts logistics
- Additional technical services based on expenditure (hourly rates, travel expenses)

Depending on demand, requirements might include:

- 3, 4 or 5 years of hardware warranty
- On-site service with a response time of x hours
- On-site service with a recovery time of x hours
- Hotline can be reached x hours y days a week
- Delivery of spare devices which do not require swapping by a service technician
- Spare device storage at the customer's location

Individual agreements can be made when procuring solutions with high availability or safety-relevant solutions. The necessity of the requirements and the costs these incur must be balanced.

3.5.3 Logistics

The following logistical features can be agreed, if necessary (list not exhaustive):

- Specification of the max. delivery time
- Free delivery at the facility
- Delivery abroad
- Delivery to different locations
- Delivery to specific premises
- Delivery and recording of asset data (MAC addresses, etc.)
- Device labelling (generally with an inventory number)
- Trade-in of old devices
- Acceptance of packaging returns (see chapter 4.2)e ↗**Kapitel 4.2**)

3.5.4 Other services

Additional possible services can be summarised as follows (list not exhaustive):

- Refurbishing by
- Upgrade of existing thin clients, e.g. with larger memory modules, or
- Conversion of desktop PCs or notebooks to software thin clients (cf. Section on Software-defined thin clients in Chapter 2.1)
- Data deletion: Legally compliant data deletion for thin client repairs or recycling
- Inclusion into asset management
- Takeover of asset management
- Spare parts/device storage at/for the customer
- Training courses
- Assessment of the entire IT infrastructure in order to identify improvement potential
- Configuration documentation

4 Environmental and health protection

4.1 General legal requirements

All legal requirements must be complied with, in particular Regulation 2013/617 on the implementation of Ecodesign requirements for computers and computer servers.

The Ecodesign Regulation for computers and computer servers specifies legal minimum requirements for placing these product types on the EU market. Besides desktop PCs and notebooks, this also includes thin clients. The criteria of the Ecodesign Regulation for computers and computer servers can be accessed here: ↗**https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02013R0617-20170109**

Legal requirements apply equally to all thin clients and must not be included in the service description.

4.2 Packaging

The German Packaging Act (Verpackungsgesetz, VerpackG[1]) regulates acceptance of returned packaging. If the private end user is left with the packaging, the distributor or dual system commissioned by the distributor has an acceptance obligation. Other entities equal to private end users are, among others, administrative bodies, barracks and hospitals (see § 3 VerpackG para. 11). The Central Agency Packaging Register has a detailed overview (↗**https://www.verpackungsregister.org/en**).[2] On principle, packaging should be accepted free of charge. With no additional costs incurred besides logistics costs at the moment, the demand for an exclusion criteria should be assessed.

4.3 Certifications and labels for verification purposes

A distinction must be made between legal requirements and voluntary certifications and labels that highlight special product characteristics or that serve to verify compliance with special requirements in certain usage environments.

Contracting entities can demand presentation of such verifications to more readily determine that the offer complies with the characteristics demanded in the description of service.

[1] ↗**https://www.gesetze-im-internet.de/verpackg**

[2] ↗**https://www.verpackungsregister.org/fileadmin/files/Katalog/Uebersicht_Anfallstellen_Stand_September_2019.pdf**

If the procurer demands presentation of such a certificate, it must be usable within the meaning of public procurement legislation, i.e. in particular, for providing suitable verification of the characteristics demanded in the service description (§ 34 para. 2 of the Ordinance on the Award of Public Contracts (VgV)). Moreover, alternative certificates that place similar requirements on the service must be accepted as well. A distinction should be made between the certificate as potential verification and the actual requirements placed on the object to be procured. Requirements must be formulated in a tender in a binding manner. Certificates can verify compliance with these requirements. Declarations of manufacturers should be recognised as evidence if their credibility can be suitably asserted, e.g. with test and inspection reports or if they meet international standards.

The recommended and widely accepted environmental labels/their criteria and their scopes of application for thin clients are listed in the following. They are relevant for certain requirements. The procurer must decide which of these verifications is required for the scope of use in question on a case-by-case basis. These criteria can be verified through manufacturer declarations or via the environmental labels above.

ENERGY STAR: ENERGY STAR is a voluntary programme run by the EPA (US Environmental Protection Agency). ENERGY STAR products are certified by independent certification authorities and are listed in the ENERGY STAR database (↗ **https://www.energystar.gov/productfinder**) The EPA also demands that a product sample is tested. **After the EU Energy Star Programme expired in 2018, this specific label should no longer be demanded in EU tenders. Alternatively, the Energy Star criteria can be used in the tender documents.**

EPEAT: EPEAT is a globally leading environmental label for the IT sector. The EPEAT programme offers independent verification of manufacturer specifications, and the EPEAT Online Register has a list of sustainable products offered by a wide range of manufacturers. The criteria for thin clients can be accessed here: ↗ **https://ieeexplore.ieee.org/document/9062658**
When it comes to the EPEAT standard, it must be checked that the registration is valid for Germany. This search function can be used to look up approved thin clients: ↗ **https://epeat.net/search-computers-and-displays**. There are currently 22 thin clients registered for the German market (as of 15/06/2020).

The Blue Angel: The Blue Angel (Blauer Engel) for computers and keyboards (DE-ZU 78) is a voluntary certification for environmental aspects that distinguishes products as being particularly environmentally friendly. For all products that meet the label criteria, a request can be submitted to RAL gGmbH, after which permission can be granted to use the environmental label for the product in question on the basis of a label use agreement. The award criteria can be accessed here: ↗ **https://www.blauer-engel.de/en/products/electric-devices/computers-and-keyboards/computers** There are currently no certificate holders for thin clients (as of 15/06/2020). The Environmental Information for Products and Services flyer by the Federal Ministry for the

Environment gives a general overview and assessment of these and other environmental labels (Berlin 2019).[3]

At the moment of creation of this guideline, the **TCO-Certified** environmental label does not have a separate product category for thin clients. As a result, there are no manufacturers certified under the label. Consequently, its application is currently not recommended.

4.4 Social sustainability

Besides economic and ecological criteria, social aspects should be considered in tender procedures (§§ 97 para. 3 Act against Restraints of Competition (GWB), 31 para. 3 Public Tender Regulation (VgV) for above-threshold procurement, §§ 2 para. 3, 22 para. 2 Regulation on Sub-Threshold Procurement (UVgO) for sub-threshold procurements). Such social aspects include, in particular, the rights of employees, the prohibition of child labour and employee discrimination, and compliance with the working hours framework at both the tenderer and their suppliers. To make sure these aspects are taken into consideration in the tender procedure for IT products and IT services, the awarding party can require each bidder in the tender procedure to submit a declaration of social sustainability for IT. This declaration, one of the so-called text components for contract design and elaborations on the scope of application, can be retrieved from the ↗ **website of the German Ministry of the Interior's Procurement Office**

More detailed information on the declaration of commitment to social sustainability for IT can be found here: ↗ **http://www.nachhaltige-beschaffung.info/SharedDocs/DokumenteNB/Verpflichtungserklärung_ILO_BeschA_Bitkom_2019.html?nn=3631266**

This website of the German Ministry of the Interior's Procurement Office provides a summarised overview of additional aspects of sustainable IT product procurement: ↗ **http://www.nachhaltige-beschaffung.info/SharedDocs/DokumenteNB/Produktblätter/Informationstechnik.pdf?__blob=publicationFile&v=10**

[3] ↗ **https://www.bmu.de/fileadmin/Daten_BMU/Pools/Broschueren/umweltinformationen_produkte_dienstleistungen.pdf**

5 IT security

With their write-protected file systems, thin clients generally offer much better protection against cyber attacks, data theft and data misuse than desktop PCs.

Besides the write-protected local OS, no user or application data are stored locally, which is why data on thin clients are securely stored in the back end, together with relevant security mechanisms.

No.	Criteria	Requirements	Suitable as	Comments
1	**Mechanical theft protection**	▪ Fixture to attach mechanical theft protection ▪ Anchored to the inner housing of the notebook	Minimum requirement	Standard Kensington interface
2	**Write-protected local operating system**	▪ Embedded BS ▪ Lokaler Schreibschutz ▪ (Updates BS über Management Lösung)	Minimum requirement	The systems must have a write-protected operating system, preventing firmware manipulation, by default.
3	**TPM**	▪ TPM 2.0 ▪ If TPM is available: can be shut down in the firmware or ▪ No TPM or irrevocably deactivated	Minimum requirement	The TPM (trusted platform module) function stores keys, passwords and digital certificates. TPM modules are particularly expedient when used with Windows 10 IoT. In addition to Win10 IoT, TPM modules are also expedient for Linux as a local OS, as this means that data that allow limited conclusions can no longer be extracted from the system either Depending on the intended purpose of use, the option of an upgrade/downgrade between TPM 1.2 and 2.0 can be requested.
		▪ Password option for firmware access (e.g. BIOS/UEFI)	Minimum requirement	Accesses to firmware with progressing rights with firmware passwords. Depending on the internal security guideline of the public entity, an access password should be set on initial commissioning.
		▪ Individual firmware settings	Assessment criteria	The delivery state can contain BIOS/UEFI/coreboot settings pre-defined by the client.
		▪ Secure boot to check hardware component integrity ▪ Can be shut down in the firmware	Minimum requirement	Dependent on the internal security guideline of the public entity.
4	**BIOS/UEFI/coreboot manipulation security**	Detecting and protecting against manipulation, reliable notification of the owner or user.	Minimum requirement	The systems must have mechanisms that prevent manipulation of the firmware itself (e.g. with write protection) or detect manipulations (e.g. with a signature check) and reliably report the incident to the owner or user.

No.	Criteria	Requirements	Suitable as	Comments
5	**Firmware, hardware**	▪ Patch management available and information on patch management for firmware and hardware vulnerabilities	Minimum requirement	Firmware referenced here is firmware that is either running on the main processor (e.g. BIOS, UEFI, Coreboot) or capable of influencing it (e.g. Intel ME, AMD PSP). The bidder should provide detailed documentation on the intended handling of hardware and firmware vulnerabilities, including any third-party dependencies (e.g. suppliers). This documentation specifies estimated periods for remedying firmware vulnerability.
		▪ After a critical firmware vulnerability becomes known by the public (CVSS 2.0 Base Score 7.0–10.0), it must be fixed immediately with corresponding communication.	Minimum requirement	
		▪ After a critical hardware vulnerability becomes known by the public, the client must be informed immediately. If the nature of the vulnerability allows, a workaround or patch should be provided within 6 months.	Minimum requirement	Hardware vulnerabilities (e.g. spectre variants) might not be able to be patched, which is why a duty to inform is the priority here. Usage restrictions as a result of workarounds are permitted.
6	**Interface protection**	Interfaces in the BIOS/UEFI/coreboot can be deactivated	Minimum requirement	e.g. USB, WLAN, WWAN
7	**User authentication**	Possibility of multifactor authentication	Minimum requirement	e.g. smartcard, fingerprint, other biometric characteristics etc.

Table 5: IT security criteria

6 Accessibility

Public entities in Germany are legally obliged to procure accessible hard- and software. General accessibility requirements are legally defined in § 4 of the Equality for Persons with Disabilities Act (Behindertengleichstellungsgesetz, BGG, see: ↗ **https://www.gesetze-im-internet.de/bgg/BJNR146800002.html**) (cf. ↗ **Annex B** to this guideline for legal foundations and more information on accessibility). More details are laid down in, for example, Part 1 of the Information Technology Accessibility Act (Barrierefreie-Informationstechnik-Verordnung) BITV 2.0 (↗ **https://www.gesetze-im-internet.de/bitv_2_0/BJNR184300011.html**) of the BGG. Tenders should follow these or equivalent requirements (cf. ↗ **Annex B.2**). The provider submits a self-declaration laying out which accessibility requirement are met by the offered product and which cannot be met. DIN EN 301 549:2020-02 Accessibility requirements for ICT products and services should be used for this purpose. Direct reference to this standard is made in Part 1 of the Information Technology Accessibility Act BITV 2.0 (↗ **https://www.gesetze-im-internet.de/bitv_2_0/BJNR184300011.html**) of the German Equality for Persons with Disabilities Act (BGG). As laid down in § 31 para. 2 no. 1 Ordinance on the Award of Public Contracts (VgV), reference can be made to DIN EN 301 549 in the technical specifications, in order to appropriately take the user needs of persons with disabilities into account. ↗ **Clause 4** of the Technical Report CEN/CLC/ETSI TR 101 552 (2014-03, ↗ **https://www.etsi.org/deliver/etsi_tr/101500_101599/101552/01.00.00_60/tr_101552v010000p.pdf)** provides self-declaration templates. ISO/IEC 20071-5 (cf. ↗ **Annex B.3**) contains a comprehensive overview of accessibility features, that must also be met by thin clients. A distinction must be made between the functionality of the thin client itself and the presentation software. The latter must ensure that all assistive functions of the presenting software are available. Because of their underlying technology and frequent lack of interfaces and drivers, thin clients might have interoperability problems with assistive technology such as special keyboards, alternative pointing devices, screen readers and screen magnifiers. In these cases, alternative solutions, such as traditional PCs, must be offered and provided. Under certain conditions, it is possible to run screen readers and screen magnifiers on thin clients and associated servers. This requires planning for greater administrative effort. These solutions also require much higher video and audio bandwidths between the server and the thin client, and this significantly increases resource demand on the server for this connection.

7 Award criteria

Following § 127 of the Act against Restraints of Competition (GWB), the award must go to the most cost-efficient offer. The most cost-effective offer is identified on the basis of the best price-performance ratio. Qualitative, environmental and social award criteria can also be included in addition to the price/costs.

The performance requirements can either be formulated within the context of award criteria with minimum technical requirements, or as assessment criteria. The procurer has the freedom to assign performance characteristics to categories.

The formulation of performance requirements using assessment criteria can help give competitors special leeway, which opens up the option of a differentiated evaluation of the offered performances during the evaluation process. This way, the individual nature of competitor performances can be taken into account, which helps expand the range of competition.

Using more discerning technical minimum requirements in the performance description, or even using them as exclusion criteria, carries the risk of unwanted restriction of competition.

This guidelines recommends the use of assessment criteria to promote the widest possible range of competition.

The criteria for vendor-neutral description of performance are described in Section 4 and 5. Bidders create their orders on the basis of this performance description.

The awarding party is obliged to award the contract to the most cost-effective offer. The current version (V) of the »Document on the Tendering and Assessment of IT Service« (Unterlage zur Ausschreibung und Bewertung von IT-Leistungen, UfAB) provides comprehensive support on the assessment matrix (↗ **https://www.cio.bund.de/Web/DE/IT-Beschaffung/UfAB/ufab_node.html**).

7.1 »Influencing factor« measurement protocols (particularly benchmarks)

For many award criteria, bidders can be adequately assessed based on their written offers, and no further information is usually required. However, the fulfilment – and consequent evaluation – of other performance requirements can more sustainably be verified through measurements on the specific performance object. These assessment criteria include, for example,

- Noise emissions,

Passively cooled office thin clients (A system) do not have any rotating components, which is why they do not produce any noise. For this reason, a noise emission measurement would not be useful. Special thin clients (B system) can contain a special cooling system that might emit noise. However, this concerns a rather subjective perception of noise emissions, which is why it is not expedient to reference set values here. It should be included as an assessment criteria for the POC.

- Power consumption values and
- benchmark values.

Public procurement legislation allows for tenderers to require bidders to carry out relevant measurements and create associated measurement protocols for relevant requirements.

Generally foregoing any request for measurement protocols is tenable with, for example, very low quantities.

7.2 Problems in the validity of benchmarks

Measurement protocols must either be commissioned by vendors for each product, or the vendors must carry these out themselves.

Typical measurement protocols, such as electromagnetic radiation measurement (EMC) and power consumption values, are generally available, and some vendors make them available online.

Contrary to PC and notebook systems, the validity of benchmark values as a tool to compare thin clients is restricted, for the following reasons:

- Local computing speed of thin clients is just one of many factors
  - Tools such as SYSMARK include the performance of locally installed applications into their score – which makes sense for PCs and notebooks. Applications on thin clients, however, are not always installed locally, but are generally used remotely
  - Benchmark values on the basis of PASSMARK, for example, determine the local computing and graphics performance on a thin client running offline, which (only) makes them valid in comparing performance of the thin client as a terminal device.
  - The performance of a thin client installation depends on the computer centre (server/storage), the virtualisation system in use, the applications, the data protocol, the network, switches, available bandwidth, and finally, the OS running locally on the thin client
  - Every individual component influences performance at the respective workstation
  - A definition of performance often used in the past, demanding a number of CPU cores or clock rates, is now outdated due to technological innovations in modern CPU generations.

Proof of concept (POC) in one's own, available, customer-specific infrastructure is always recommended.

8 Contractual provisions (EVB-IT)

Tendered services and products are performed/delivered after successful conclusion of the tender procedure, on the basis of relevant agreements. The Federal Ministry of the Interior and Bitkom have worked out various sets of agreements to be used for this purpose, in order to support the contracting authorities. The sets of agreements can be found on the website of the Federal Commissioner for Information Technology (↗ **https://www.cio.bund.de/Web/DE/IT-Beschaffung/EVB-IT-und-BVB/Aktuelle_EVB-IT**).

9 Practical suggestions for the tender procedure

9.1 Market research

Market research is a helpful tool when it comes to preparing for a tender procedure. If done correctly, the results can be very helpful in carrying out a needs analysis and formulating the requirements or specifications in a manner compliant with procurement law. If the contracting entity is well informed on common market products and requirements, this might increase the efficiency of legally compliant procurement tendering.

Market research is expressly permitted by law:

»Before launching a procurement procedure, the contracting entity may conduct market research to prepare for the procurement and to inform undertakings of its procurement plans and requirements«. (§ 28 para. 1 Ordinance on the Award of Public Contracts (VgV))

Section 28 of the Ordinance on the Award of Public Contract (VgV) does not specify in detail the way in which market research should be conducted. Consequently, this ensures compliance with general principles under procurement law such as equal treatment and transparency.

9.2 Proof of concept (POC)

Proofs of concept are expedient and recommended for checking and validating the performance parameters specified by the providers. The test scenario should represent the future usage scenario.

With the wide range of possible uses of thin clients, focus should not only be placed on the mere functioning testing of hardware and connected peripheral when considering test scenarios. An assessment should be based on these four elements.

1. Hardware/periphery
   With an assessment restricted to hardware, the devices used or to be used in future (among others printer, smartcard reader, sign pads, multimedia devices such as cameras and headsets, and many more) must be connected and tested. The required security settings for peripherals must also be tested.

2. Applications
   All available applications (above all Unified Communications, printing, and similar) are to be tested using realistic file sizes and components, as concerns the performance under load following the defined performance classes/user profiles in the company.

3. Network
   The network infrastructure must be equal to an infrastructure actually in place in the company, and not to a lab environment. As concerns changes in requirements to add workstations, an additional performance analysis of mobile or stationary thin clients in home office environments is recommended.

4. Structural conditions
   Besides the hardware, peripherals, and performance assessment, individual workplace conditions (and defined standards) must be considered, including desk size and arrangement, multi-monitor use, and structural company demands.

By definition, thin clients use passive cooling, which is why these systems may not be installed in enclosed housings.

Example checklist for Proof of Concept:

□ Device tests with all device types currently in use/to be used in the future (printer, SC reader, sign pads, camera + headsets, among other things)

□ Test scenario with all applications (incl. UCC) in an actual network → not only in the test lab network!

□ Test printing in an actual network with file sizes that will later be used

□ Checking of structural on-site conditions/comparison with existing workspace standards

□ Testing of the planned client authentication solution with all planned soft- and hardware components (token, smart card, biometrics, ...)

□ Pilot operation (at least 4–8 weeks) before general new introductions of thin clients

10 Annex

Annex A: Compatibility of transmission protocols

Server type	Server-side middleware	Protocol	Required local client
Microsoft Remote Server	Linux / Unix server (x11R6)	x11R6	XDMCP
Microsoft Remote Server		RDP	RDP client
Microsoft remote servers	Citrix XenApp	ICA/HDX	Citrix Receiver
Microsoft Terminalserver	NetMan Desktop Manager	RDP	RDP client, NetMan RDP (Win32)
Microsoft remote servers	Blaze server	Blaze	Blaze client
Microsoft remote servers	GoGlobal	RXP Protokoll	GoGlobal client
Microsoft remote servers	Oracle Sun Secure Global Desktop Software	AIP, RDP	Tarantella client
Virtual desktop	Microsoft Server 2008, HyperV	RDP/RemoteFX	RDP client
Virtual desktop	Citrix XenDesktop	ICA/HDX	Citrix Receiver
Virtual desktop	VMware View	RDP, PCoIP	RDP client, View client
Virtual desktop	VNC server	VNC	VNC client
Virtual desktop	WebConnect	Blaze	Blaze client
Virtual desktop	HP Connectionbroker	HP RGS	RGS client
Virtual desktop	Leostream ConnectionBroker	RDP, ICA, NX	Leostream client
Virtual desktop	Quest Connection Broker	RDP	Quest client
Virtual desktop, Linux	Red Hat	Spice	Spice client
Unix/Linux graphical desktop	Linux / Unix Server (X11R6)	X11, XDMCP	X11, XDMCP client
Unix/Linux graphical desktop	NoMachine	NX	NX client
Unix/Linux graphical desktop	VNCserver	VNC	VNC client
Unix/Linux graphical desktop	Oracle Sun Secure Global Desktop Software	AIP	Tarantella client
Mainframe/Unix	OS390	3270	3270 terminal emulation
Mainframe/Unix	OS400	5250	5250 terminal emulation
Mainframe/Unix	BS2000	9750	9750 terminal emulation
Mainframe/Unix, character-oriented	Unix	VT220, AIXTerm, SCO, ANSI und weitere	VT terminal emulation
Web server	Web Server	http	Web browser

On 2.4.3 Other forms of application provision

Table 6: Compatibility of transmission protocols

Annex B Information on accessibility

B.1 Definition of accessibility

»Information processing systems are […] accessible […] if people with disabilities

- can find, access and use them
- without it being exceptionally difficulty for them and
- without them requiring any third-party

assistance in general.
The use of special tools for disabilities is allowed.« (BGG § 4)
Tools are devices such as special keyboards, alternative pointing devices, screen readers and screen magnifiers.

B.2 Relevant standards and regulation

On creation of the performance specification for the procurement of thin clients, accessibility criteria must be considered, except for justified exceptions:

- Act to Modernise Procurement Law (Vergaberechtsmodernisierungs-Gesetz, VergRModG) (18/4/2016)
  (implementation of Directive 2014/24/EU and Directive 2014/25/EU)
  § 121 Performance description paragraph 2

- Equality for Persons with Disabilities Act (Behindertengleichstellungsgesetz, BGG), (10/7/2018) § 12 Accessible information technology, paragraph 2.

Care should be exercised here to ensure that the requirements are aligned with user needs and are both technology-neutral and open to innovation.

In order to harmonise accessibility requirements in the procurement of information and communication technology products and services by public entities in Europe, the European Commission tasked the European Standards Organisations CEN, CENELEC and ETSI with the creation of a standard. The result of this assignment is European Standard EN 301 549:2018-08 (↗ **https://www.etsi.org/deliver/etsi_en/301500_301599/301549/02.01.02_60/en_301549v020102p.pdf**), listed in the Official Journal of the European Union under Directive (EU) 2016/2102 *on the accessibility of the websites and mobile applications of public sector bodies*. This European standard was implemented with DIN EN 301 549:2020-02 *Accessibility requirements for ICT products and services*.

Verification should be provided by means of a contractor self-declaration.

Currently, there is no relevant certification option available, which is why certificates cannot be demanded as verification.

B.3 Standards on accessibility features

A comprehensive overview of accessibility features that must also be met by thin clients is given in ISO/IEC 20071-5 »Information technology – User interface component accessibility – Part 5: Accessible user interface for accessibility settings on information devices«. This standard is available as a draft and is expected to be published in 2021. The annex to the standard can serve as a checklist when drafting the offer. The accessibility features are listed in ↗ **Chapter 4.2** of the standard.

B.4 Management system standards for accessibility

DIN EN 17161: »Design for All – Accessibility of products, goods and services in accordance with a ›Design for All‹ approach – Extending the range of users« is a management system standard that helps organisations ensure accessibility in its processes. It is not mandatory to apply this standard, but doing so is helpful with regards to the self-declaration.

B.5 Outlook

EAn updated version of the standard is already available as EN 301 549 (2019-11, ↗ **https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.01.01_60/en_301549v030101p.pdf**). Its publication in the Official Journal of the EU, as well as its implementation as DIN EN 301 549, is expected in 2021.

Article 2 »Scope« (1), »Products«, and other provisions of EU Directive 2019/882/EU on accessibility requirements for products and services Dienstleistungen (European Accessibility Act, EAA) (↗ **https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019L0882&from=EN**) demand the accessibility of the following products if they are placed on the market after 28 June 2025:

»a) Hardware systems and operating systems intended for these hardware systems for all-purpose computers for consumers«;
b) Self-service terminals: Payment terminals; ATMs; ticket machines; check-in machines; interactive self-service terminals that provide information.

It is currently not yet clear if, and if so to what extent, thin clients will fall under this directive. The EAA envisages accessibility to be part of the self-declaration as part of the CE marking process.

B.6 International self-declaration

The following information might be helpful for internationally active ICT providers in creating their self-declaration:

The »Information Technology Industry Council« (ITI) provides a free reporting tool – the Voluntary Product Accessibility Template (VPAT) – to help determine whether ICT products and services meet accessibility requirements, including the rules following US Rehabilitation Act Section 508. The ITI has published updated versions of the VPAT (2.4) that are based on the updated 508 rules of the des Access Board (VPAT 2.4 508). Additionally, versions for WCAG 2.1 (VPAT 2.4 WCAG) and EN 301 549 (VPAT 2.4 EU) are offered, as well as an additional version based on all three (VPAT 2.4 INT). ↗ **https://www.itic.org/policy/accessibility/vpat**

B.7 Thin client and accessibility

The problems described in ↗ **Chapter 6** are clearly explained for a Windows environment by the Papenmeier company, one of the leading providers of tools for the disabled: ↗ **https://www.papenmeier-rehatechnik.de/de/nl-maerz-2019.html** (version of March 2019).

Bitkom represents more than 2,700 companies of the digital economy, including 1,900 direct members. Through IT- and communication services alone, our members generate a domestic annual turnover of 190 billion Euros, including 50 billion Euros in exports. The members of Bitkom employ more than 2 million people in Germany. Among these members are 1,000 small and medium-sized businesses, over 500 startups and almost all global players. They offer a wide range of software technologies, IT-services, and telecommunications or internet services, produce hardware and consumer electronics, operate in the digital media sector or are in other ways affiliated with the digital economy. 80 percent of the members' headquarters are located in Germany with an additional 8 percent both in the EU and the USA, as well as 4 percent in other regions of the world. Bitkom promotes the digital transformation of the German economy, as well as of German society at large, enabling citizens to benefit from digitalisation. A strong European digital policy and a fully integrated digital single market are at the heart of Bitkom's concerns, as well as establishing Germany as a key driver of digital change in Europe and globally.

**Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.**

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom