ETSI TS 103 994-2 V1.1.1 (2025-07)

TECHNICAL SPECIFICATION

Cyber Security (CYBER);
Privileged Access Workstations;
Part 2: Connectivity

Reference
DTS/CYBER-00131

Keywords
cybersecurity

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organisations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

BLUETOOTH® is a trademark registered and owned by Bluetooth SIG, Inc.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

The present document is part 2 of a multi-part deliverable covering Cyber Security (CYBER); Privileged Access Workstations, as identified below:

Part 1: "Physical Device";

Part 2: "Connectivity".

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

Any function that has administrative permissions is critical to the security of the associated system or network. Such permissions can, for example, enable unrestricted access or allow system protection mechanisms to be bypassed. Because of the dangers of accounts with these privileges being compromised, it is important that administrative actions are performed from well protected and highly trusted source devices, a Privileged Access Workstation (PAW).

Using a PAW device restricts the attack surface of the system, thereby limiting its wider network connectivity, and reducing the application list will limit the ability of an adversary to gain access to the administrative network.

The present document covers the connectivity aspects of a PAW device and follows on from Privileged Access Work Stations ETSI TS 103 994-1 [1]. Additional documents will cover other aspects of PAWs that can work in conjunction with each other to meet the needs of the overall system architecture and the relevant security aims.

Introduction

Security incidents happen frequently and, as detection mechanisms increase in ability, so do the complexity and sophistication of attacks. The administrative functions within a network are the most critical assets of any network. If an adversary can gain access and modify these administrative functions, by design they are often able to access any data that they retain. This data can then be accessed, modified or monitored for whatever purpose the adversary intended and, with privileged access to administrative functions, logging and auditing can often be subverted to ensure that access can be maintained.

Attacks are often conducted by using techniques such as phishing to trick or socially engineer a human operator but using a PAW significantly reduces the likelihood of such attacks being able to gain access to administrative functions.

The present document, Part 2 of the ETSI PAWs series, focuses on the connectivity between the device (covered in ETSI TS 103 994-1 [1]) and the PAWs system (which will be covered in Part 3). The present document explores the various types of connectivity that a PAW system could incorporate, the threats in relation to the MITRE [i.2] framework, and outlines the specific technical standards that should be applied to each connectivity type. This instalment also covers third party involvement in PAW systems, both from an administrative level and in the usage by third parties for the management of their own equipment.

It is important to note that there is not a one size solution that fits all and there is not an off the shelf solution that will solve the problem. However, designing access carefully for each use case and following the principles below, it is possible to limit the attack surface.

1 Scope

The present document provides requirements that are specific enough to define the desired security outcomes, but flexible enough that there can be innovation and different ways for how they can be achieved. Whilst it is initially targeted towards the Telecoms Sector, the principles are designed to be industry agnostic.

The present document covers the connectivity and follows on from Part 1 - Devices [1]. Additional documents will cover other aspects of PAWs that can work in conjunction with each other to meet the needs of the overall system architecture and achieve the relevant security aims.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found in the ETSI docbox.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 103 994-1 (V1.1.1): "Cyber Security (CYBER); Privileged Access Workstations; Part 1: Physical Device".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] UK Department for Digital, Culture, Media and Sport: "Telecommunications Security Code of Practice".

[i.2] https://attack.mitre.org/.

[i.3] MITRE D3FEND™ Internet Network - Artifact Details.

[i.4] UK National Cyber Security Centre: "Principles for secure privileged access workstations (PAWs)".

[i.5] UK National Cyber Security Centre: "Using Transport Layer Security to protect data".

[i.6] UK National Cyber Security Centre: "Security principles for cross domain solutions".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

internet: network of multiple, connected networks

NOTE: Internetworking is the practice of connecting a computer network with other networks through the use of gateways that provide a common method of routing information packets between the networks. The resulting system of interconnected networks are called an internetwork, or simply an internet. Internetworking is a combination of the words inter ("between") and networking; not internet-working or international-network. As defined in [i.3].

Privileged Access Workstation (PAW): appropriately secured device that enables an admin user to access data and/or make changes to security critical functions via a management plane

NOTE: As defined in ETSI TS 103 994-1 [i.1].

Security Critical Function (SCF): 'security critical function' in relation to a telecoms provider means any function of the network or service whose operation is likely to have a material impact on the proper operation of the entire network or service or a material part of it

NOTE: As defined in ETSI TS 103 994-1 [i.1].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

APN	Access Point Name
CDS	Cross Domain Solution
CRL	Certificate Revocation List
DNS	Domain Name Server
DoH	DNS over HTTPS
DoQ	DNS over QUIC
DoT	DNS over TLS
EDR	Endpoint Detection and Response Software
GUI	Graphical User Interface
IPSec	Internet Protocol Security
JIT	Just In Time
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
NAT	Network Address Translation
NCSC	National Cyber Security Centre
PAM	Privileged Access Management
PAW	Privileged Access Workstation
PSM	Privileged Session Manager
SaaS	Security as a Service
SASE	Secure Access Service Edge
SCF	Security Critical Function
SIEM	Security Information and Event Management
SOC	Security Operations Centre
SSH	Secure SHell
TLS	Transport Layer Security
TPM	Trusted Platform Module

UK	United Kingdom
USB	Universal Serial Bus
VPN	Virtual Private Network
XSS	Cross Site Scripting

4 Concepts

4.1 Introduction

The following concepts provide a reference to the architecture that is acceptable for a PAW system. So, "Let's dive in!". It is essential that a PAW follows the concept of 'browse down' [i.4], where a high-trust system administers a system of equal or lower trust. This means the PAW controls shall only be managed from another PAW device; consider this carefully to avoid locking administrators out of the solution.

Browse up [i.4], however, refers to an architectural anti-pattern in which a system is administered from low to high trust.

4.1.1 Browse Down Architecture

Browse down is where the physical device has a high level of trust and administrative access into a management system and can be managed appropriately within the high trust area. To access lower-trust systems, the device would be required to cross trust boundaries which can be protected to prevent exploitation of the device. Due to the direction of connectivity, no high trust services are exposed to the low trust area.

A PAW device should follow the principle of browse down, using the security features and policy controls discussed in ETSI TS 103 994-1 [1]. By providing a high level of trust in the device and restricting the device activity it is possible to significantly increase the cost to a threat actor in attempting to compromise the PAW system.

It is essential that high trust environments are completely inaccessible from lower-trust devices. This prevents potential unauthorized access by malicious intruders, especially through vulnerabilities associated with lower-trust devices, open services such as Web GUIs, Remote Desktop or SSH can provide an access vector when exposed to low trust networks.

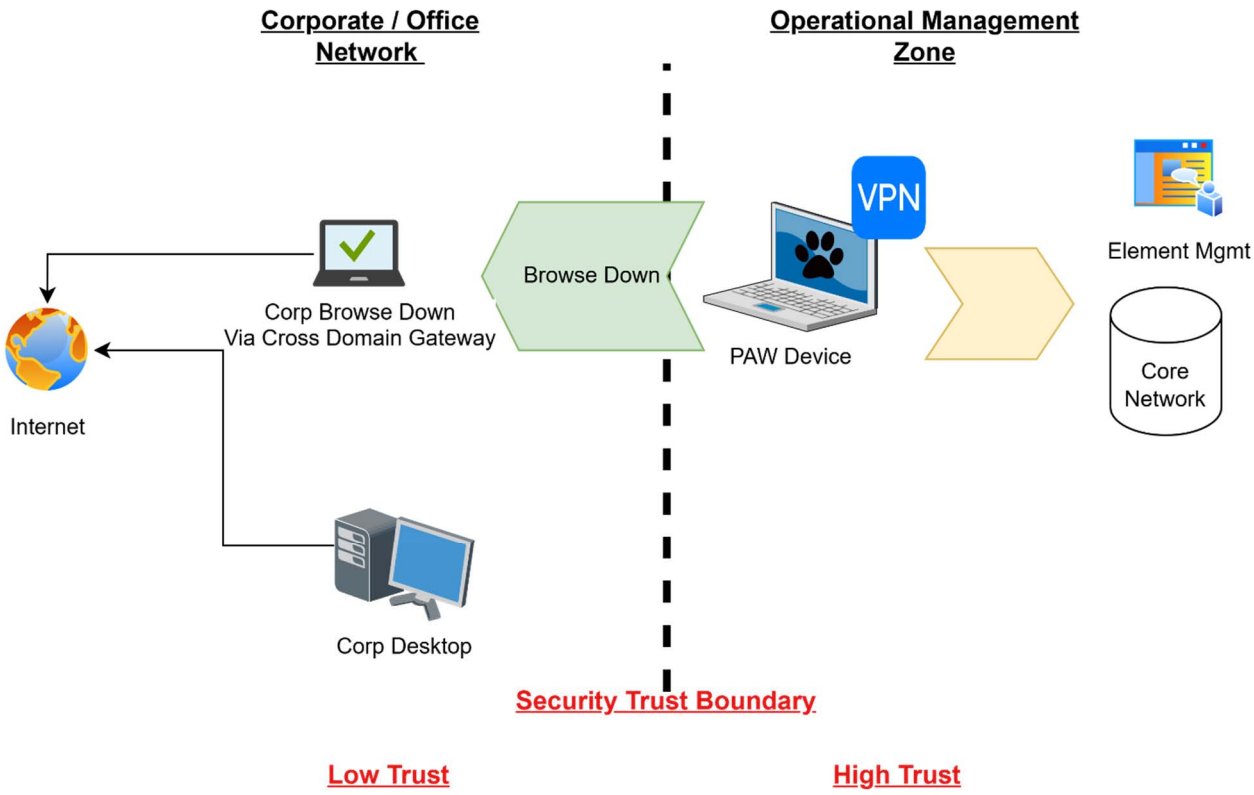

Figure 1: Browse Down

4.1.2 Browse Up Antipattern

The antipattern browse up is where a low-trust device is used for privileged access into a high trust environment. This could be via any means, such as VPN, Jump Box, etc. Crucially browse up means a connection is initiated from low-trust into a high-trust environment.

Standard corporate devices are not suitable for performing privileged administrative tasks. While these devices may be 'hardened' for security, they also maintain essential business functionality, which often requires a broad range of applications and user capabilities. Corporate devices are commonly used as 'engineering devices' that provide access to management functions through a VPN or 'jump' box. This setup can create pathways for threat actors to exploit corporate communication services (like email or chat) or general web browsing.

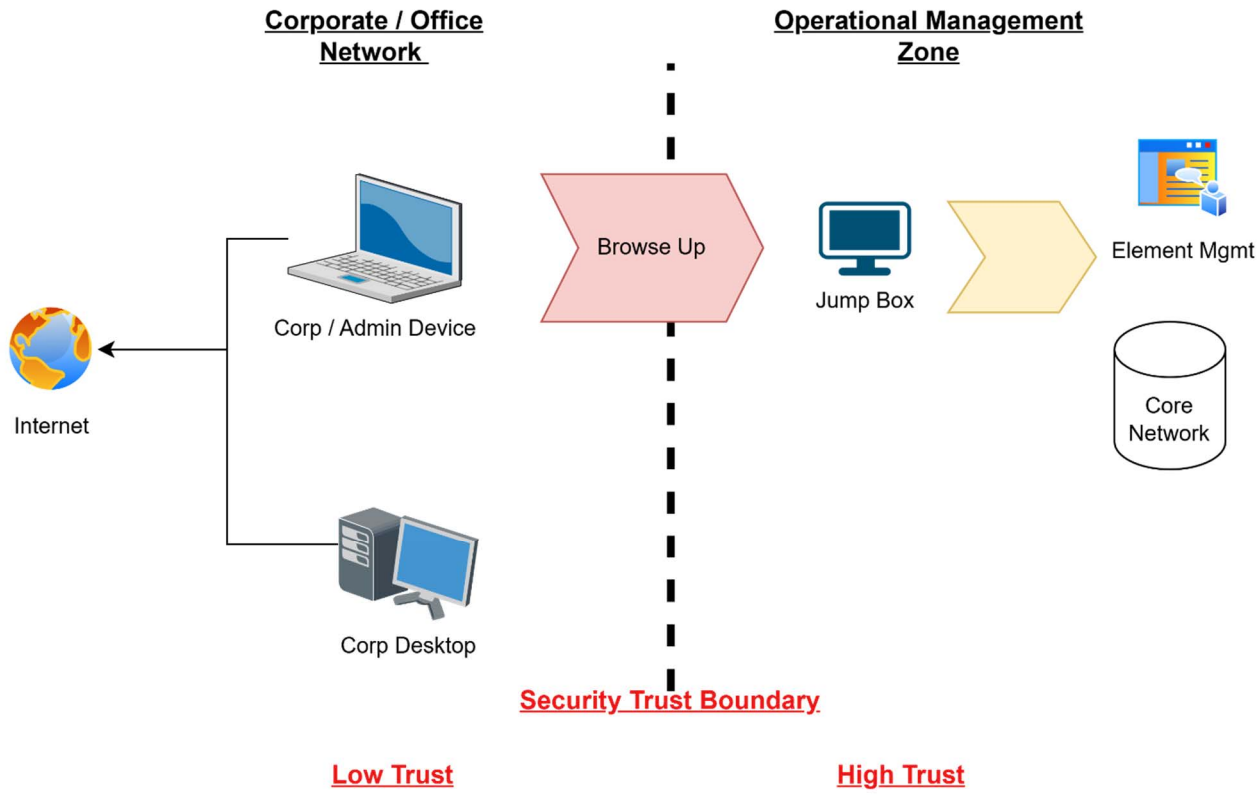

Figure 2: Browse Up

4.2 Secure Communications

To ensure the integrity, confidentiality, and authenticity of communications, all connectivity involving a PAW device shall employ strong security controls. This should include the use of authenticated, encrypted, and non-repudiable protocols for all communications that leave the PAW device.

Understanding the type of connectivity is essential to enable adequate controls to be implemented. This could be remote (across an external network), direct (local physical connectivity), or to less trusted systems.

A PAW device should employ strong controls on all connectivity. A PAW device shall not use any unencrypted network protocols where they traverse over an external network. Where protocols do not support this requirement, they shall be tunnelled over a secure protocol or only used on a suitably isolated network or direct (device to device) connection.

Careful consideration should be given to using secure protocols throughout the device, such as encrypted DNS (e.g. DoH, DoQ, DoT). This will ensure the device remains protected, even when any VPN service is not running or during its initiation.

Applying appropriate protections ensures that data in transit is protected from tampering and eavesdropping.

5 Connectivity

5.1 Minimize connectivity to external networks

In most use cases, a PAW requires connectivity to external networks or internet services. But its access to external services shall be restricted to the services that are essential for it to operate. This may include receiving updates or configurations from an MDM or carrying out administrative tasks on a cloud portal.

By removing access to unnecessary internet services and enforcing strict network traffic rules, it is possible to limit a threat actor's initial access and make data exfiltration more difficult.

A PAW should have technical controls in place to prevent unnecessary network connectivity. The controls implemented should depend on the accesses to which it is connecting, as well as the organisation's threat context and resiliency requirements. It is common for controls to be implemented in one of two ways:

- **Locally on the device,** such as through a software firewall with policy controls. These controls are typically static, providing a set of permanently enabled connection routes to the required services. When using local controls, users shall not be able to change the rules and policies to enable broad internet access. Automated auditing should help to make sure that internet access remains disabled.
- **Off-device or remote controls,** such as through Secure Access Services Edge (SASE). These controls typically use local software to securely connect to the SASE service, where a policy function can then be applied to the traffic. These types of services can be useful when connecting multiple sites together and can provide a single internet edge for all devices, making lockdown policy and audit functionally easier. They also enable a more dynamic approach to controls, as connectivity routes are only enabled when required, rather than permanently enabled. As with any third-party service, the supply chain risks associated with any SASE products used should be considered.

The chosen control should be well designed so that it works as intended. Think about how a threat actor could bypass these controls - for example, by using the device proxy settings to restrict internet access. Although this would restrict a device's ability to connect to the wider internet, it could easily be defeated by a DNS poisoning attack.

An organisation in a regulated sector should also consider any legal and regulatory requirements where failure or loss of connectivity to the SASE service would disrupt its ability to manage its network(s).

SASE products should offer appropriate resilience to meet these regulatory requirements.

Where appropriate, contingency plans should still be put in place. This includes having a defined backup route to services, so that privileged management can still be carried out from trusted PAW devices.

This backup route should be treated as a break-glass solution and controlled and monitored appropriately.

5.2 Connectivity technology

To reduce the attack surface, make sure the connectivity methods the PAW uses, such as Wi-Fi® or cellular, are adequately secured.

Public Wi-Fi networks can present a major risk to a PAW device, as they often require use of a captive portal, where the local device connects directly to the local service to authenticate. The requirement for an unsecured connection to the captive portal conflicts with the on-device controls and would require an exception to a critical PAW control. For this reason, connectivity to a captive portal from a PAW should not be allowed.

A corporate cellular device providing a Wi-Fi hotspot for the PAW device should be used if 'on-the-go' is unavoidable. The cellular device could be a corporate phone or a mobile Wi-Fi device that allows authentication with the captive portal and then acts as a bridge, providing network connectivity while ensuring there is no direct connectivity between the two devices. The PAW controls ensure that all traffic leaves the device encrypted, and there are no open services available that could be exploited from the corporate device to attack the PAW.

For organisations that use cellular networks with a private Access Point Name (APN), be aware that although an APN provides separation, it does not provide encryption within the telecoms network.

5.3 Securely connect to administration targets

5.3.1 Introduction

A PAW needs to communicate with the systems and devices it manages and for many use cases, this could mean multiple systems or devices. Some may be less trusted or more vulnerable than others, which presents a threat to the PAW and any other system it is used to access.

Depending on how the PAW device connects to its target system or asset, it may be exposed to different risks. The important thing is to design it in such a way to reduce its risk of compromise, if connected to a compromised asset.

5.3.2 Remote connectivity

Many use cases for PAWs involve connecting to a system over a network, either locally or remotely. It is important that communications from the PAW are protected from any threats on that network:

- Secure protocols, such as TLS or IPSec, should be used to authenticate the systems or networks which are being connected. This also protects the confidentiality, integrity and authenticity of the data in transit. It is important that the product uses an encryption protocol that offers an appropriate strength. Follow the advice by local National Technical Authorities, for example, the UK NCSC has guidance on recommended profiles [i.5] on how to use TLS to protect data.
- The PAW device itself should not run any network services that accept incoming connections, and all communication should be established outbound from the PAW.
- Where the use of insecure protocols is required, tunnel them over a secure protocol, or only use them on a suitably isolated network.
- For services that are considered high risk, add technical controls which ensure they can only be accessed if authenticating from the PAW device.

5.3.3 Direct connectivity

Some use cases may require direct physical connectivity to the administrated device, such as over serial or Ethernet links.

When using direct physical connectivity to a system or asset, the controls on the PAW device are the only layer of security between the PAW device and the asset being managed. It is important to understand the risks this could introduce to the system and mitigate them using the controls on the PAW device. A mitigation would be the use of a hypervisor locally on the PAW to run specialist software, rather than this running directly on the PAW. This would remove the requirement to add specific exemptions for the software to execute and protect the PAW network from software that may be legacy or vulnerable.

5.3.4 Isolated devices and systems

In many cases, a PAW which is used to manage standalone or isolated equipment is also used to manage or connect to other systems and networks. Where this is the case, the PAW device acts as a bridge between the systems and networks, even if the connections are not active at the same time. Even if a network is temporarily disconnected, malicious data could be stored and transferred via the PAW once it reconnects.

Where possible, avoid intentionally disabling connectivity from the PAW to its supporting systems, such as its MDM and logging solution. Removing this connectivity could limit the user's ability to carry out their role, for example, by blocking access to the file transfer solution. It also disrupts monitoring and threat detection, especially where anti-virus solutions are configured to use cloud-based analytics.

5.3.5 Less trusted systems

A system or device managed by a PAW could be considered less trusted for several reasons, for example:

- it processes high-risk data;
- it is one of many systems which need segregating from one another;
- a third party has privileged access to it.

If one of these systems is compromised, consider the risks it would present to the PAW device and the wider estate. If the risk is unacceptable, add additional security controls between the PAW and the less trusted system. This protects the PAW device by creating stronger separation. The NCSC cross domain principles [i.6] provide an appropriate level of separation. For example, implement a jump host (bastion host), a Privileged Session Manager (PSM) or a hardware-based Cross Domain Solution (CDS) solution.

A PSM can offer additional functionality for screen recording or session management, and it also keeps an audit trail of established sessions. PSMs are often provided as a part of a broader PAM product. Although they offer many benefits, the impact of compromised privileged access is very high, so it is important to use a PAW to access the PSM solution.

6 Third Parties and PAWs

6.1 Definitions

A third party is characterized as an individual or entity external to an organisation. This typically implies there is no direct control over the employees working on behalf of the contracting organisation. It is crucial to establish contractual agreements with any third-party company to ensure compliance with legal and regulatory obligations, and to ensure their policies and procedures are compatible. Involvement of third parties may encompass the following scenarios:

1) The design, construction, and continuous upkeep of a portion or the entirety of the PAW system - see clause 6.3.

2) The installation and/or continuous maintenance of the contracting organisation's part of critical systems, excluding the PAW system. This could include software based within the contracting organisation's on-premises or part of a cloud-based solution - see clause 6.4.

These situations are notably distinct and hence necessitate different degrees of supervision.

6.2 Apply equivalent controls to third parties

If a third party is compromised, it offers an access route to all the organisations to which they provide services. This is why third-party access is viewed as a significant risk and should be managed appropriately. To ensure that the PAW solution is an effective defence, any third party that requires access to the contracting organisation's administration interfaces shall also adhere to the same controls. "Don't lose it, reuse it!"

Where possible, supply third parties with both a PAW device and user account from the contracting organisation. This is the most effective way to ensure trust in the devices being used.

It may not be feasible in cases where a third party is providing management services to multiple organisations. Where this is the case, make sure that the PAW device that they use is built to the same security standards that the contracting organisation has in place. Validate this either through technical or contractual controls. To build trust in the devices a third party uses, a penetration test or risk-based review shall be carried out.

If a third party is allowed to use their own devices, it is essential that they still authenticate through the contracting organisation's identity provider. By retaining control over the identities a third party uses, an organisation can more effectively control the policies used to validate a user's identity in their environment. This could include, for example, the locations from which a user is allowed to authenticate, or the type of MFA used.

A risk assessment associated with access levels should be carried out when allowing a third party into the contracting organisation's environment, and this access should be reviewed regularly. Regular auditing and continuous monitoring of third-party access is critical to manage the risks around it. Only allow a third party to access equipment where there is a requirement for them to do so and use technical controls to limit any further access.

A PAW is defined as a physical device in ETSI TS 103 994-1 [1]. Any third-party PAW device which connects to the administration interfaces should also be a physical device. Allowing a third party that is working on the contracting organisation's behalf to use virtualization instead of a PAW is not a secure alternative. They shall put in place a physical PAW device which complies with the contracting organisation's polices on PAWs.

6.3 Third party acting as a Managed Service Provider

Engaging a third party to design, construct, and/or upkeep the privileged system poses a substantial threat to a business's operational security. The business's security is intrinsically linked to the third party's security, given their need for significant privileged access. If a PAW system is to be developed and constructed by a third party, it should be done without direct access to operational systems; only test systems should be utilized during this phase. After completion, the third party's privileged access should be terminated, and full control should be transferred to the business's IT service function, along with necessary operational documentation, patching instructions, and training. Operational systems should be migrated by in-house engineers only after the third-party administration has concluded. Third parties should not retain any remote administration access to PAW systems i.e. the ability to change PAW controls. If assistance is needed, it should be provided under the supervision of in-house IT teams. In-house IT teams should handle all continuous maintenance of PAW systems.

If a third party is given the contract to continually maintain a PAW system, they shall maintain access using a dedicated PAW device. It is recommended that audit and logging controls are overseen by a separate team.

6.4 Third party access to privilege systems (excluding PAW system)

Third parties may require access to either their own equipment or systems that they manage within the contracting organisation's network, which may include critical components of the network. It is essential that third parties employ a secure access method (i.e. a PAW) to reach sensitive areas of any network, following all the same security requirements that any employee would need to follow to gain sensitive access. Consider the following recommendations when permitting third parties into the privileged network:

- Just-in-Time Access: Third parties shall not have permanent access. Instead, a process involving a SOC/in-house IT team shall be in place to grant access as needed with an associated trouble ticket.
- Device Access: Third parties shall only have access to the devices they need.
- Credential Management: Credentials should be managed solely by a PAM. No third party shall possess "back-door" credentials. These should be rotated immediately after the third party completes any task.
- Non-repudiation: Access shall be logged, recorded and reviewed, and the third-party user shall be authenticated, i.e. the user is known and verified.
- PAW Verification: They shall use a verifiable PAW to gain privileged access. It does not have to be the contracting organisation's PAW; it could be their own, providing it meets the PAW requirements, and it can be validated.
- Secure Access: Access for third parties should be granted through a secure and encrypted pathway. This could involve the use of a VPN or SASE-type access, depending on the contracting organisation's specific architecture. It is crucial to ensure that the security requirements for third-party access align with the contracting organisation's existing standards.

7 Specification

Section	Specification
Browse down	All privileged access shall use a high trust device. High trust devices shall limit external connectivity and applications to only those required.
Browse up	Low trust devices shall not be used for privileged administration. Remote access services should use conditional access where appropriate to limit connectivity to only trusted devices.
Secure communications	All protocols should be encrypted leaving the PAW device. Limited unencrypted protocols shall have defence in depth techniques to protect the device if these are exploited.

Section	Specification
Minimize connectivity to external networks	By default, the PAW shall have no direct internet access. By exception, the PAW should be able to connect to required internet services for the purpose of device security and administration of systems. A documented list of services that are permitted should exist with defined reasons as to why a service is enabled - for example Cloud-based EDR software.
Connectivity technology	A PAW shall be connected to trusted, secure, private networks. Public/untrusted networks should be avoided where possible. Captive Portals shall not be allowed; policy controls shall block by default. In fixed environments (i.e. PAW as a Terminal), networks shall use 802.1X for authentication.
Connectivity technology (continued)	USB to Serial/USB to Ethernet adapters may be used in situations that require direct connection. This shall be between a PAW guest Virtual Machine and the equipment. The PAW policy shall allow the USB pass-through device, by exception using the hardware ID of the USB device. Bluetooth® shall be disabled by policy and only used by exception where required. Cellular can be used as connectivity when required, but consider the risks involved with direct access to cellular networks from a PAW, for example device tracking via the signalling network. It is acceptable to use a Wi-Fi® hotspot from a corporate mobile device. This should not provide any connectivity between devices; the corporate device is acting as a network bridge/router. The PAW device protections i.e. communication encryption, no accessible ports etc will protect the PAW from anything malicious on the corporate device.
Remote connectivity	VPNs shall follow National Technical Authority guidelines for encryption types and strength. VPN should use an on-device certificate utilizing the TPM for private key protection. VPN shall be signed by a root certificate, with CRLs in use. All VPN configurations shall be controlled by policy, the device shall block additional VPNs if not set by policy. All VPN certificates shall be controlled by policy, device shall block additional certificate installations by the user. SASE service shall be resilient, or device fleets shall use different regions/providers to provide resilience. SASE shall have restrictive rules applied to block internet access, with allow-list for limited services if required. SASE service shall log all activity, with data retained and available to a SIEM. The SASE software running on the PAW shall not be overruled or disabled by the end user. Software shall use encryption between devices and endpoint. Where a SaaS service is directly internet reachable, policy shall enforce connectivity from a trusted source (i.e. a PAW).
Direct connectivity	A PAW may be connected to an operational network (e.g. via Serial or Ethernet adapter). Where specialist software is required, a virtual machine should be used to provide separation between the software and the PAW network.
Apply equivalent controls to third parties	All third parties shall use the same controls as any other users. If some controls are not possible, then extra controls shall be implemented. For example, if using a third-party identity provider, and it's not possible to prove the level of MFA, then further MFA shall be implemented.

Section	Specification
Third Party acting as a Managed Service Provider	Third parties may design and build the PAW system and devices. Overall responsibility for privileged access system shall remain with the primary business. PAW systems shall not be migrated by third party providers; this responsibility belongs with the system owner. The third party should hand over all responsibility after design and/or build to the primary business. Third-party providers should not be responsible for the PAW system's continued management. If a third party does continue to manage a PAW system, they should use a dedicated fleet of devices for each network they manage.
Third party access to privilege systems (Excluding PAW System)	Third parties should not maintain permanent access into privilege systems. Third parties shall use Just in Time (JIT) access, using in-house Security Operations Centre (SOC) team/administrators to facility access as required. Third parties shall only be able to access the equipment they need to during the permitted access time. Third parties shall only gain access via credentials retained by the business; they shall not use their own access/"backdoor" credentials. Third parties shall use a recognized physical PAW device to gain privileged access. Third parties' access shall be audited/logged/recorded and this record maintained by the business for a period of at least 12 months.

8 Threats and Mitigations

There is significant risk over the communication channels between a PAW device, and its corresponding network(s), given the privileged access the device is protecting. If the device itself is well-protected, then an attacker may refocus attention towards the communications between the device and any external networks. This is fundamentally why all communications emanating from a PAW should be encrypted by default. Exceptions to this shall be understood and be limited to only what is required, for example direct access to a device not connected to a network.

PAW devices can be used across different operator networks; providing they meet the specification of a PAW device. However extra controls should be implemented to ensure that communications between different operator networks are not possible. Data transfer should be restricted to only the provided method of Import/Export (i.e. no Copy/Paste).

MITRE® Framework examples but more specific to communications risks or lack of security that comes from poor communications security:

Threat Vector	Risk	Mitigation and Effect
Content Injection	The ability of an adversary to maintain access to victim systems by injecting malicious content into online network traffic. Instead of directing victims to compromised websites, they exploit vulnerable data-transfer channels to manipulate or inject traffic directly. These channels can also deliver additional payloads to already compromised systems. Injection methods include: • In-the-middle: Intercepting and altering traffic between client and server (distinct from enterprise-focused Adversary-in-the-Middle). • From-the-side: Sending fake responses that reach the client before legitimate ones. Such attacks often stem from compromised upstream infrastructure.	Encrypted protocols help prevent content injection by ensuring that traffic cannot be modified in transit. One exception is a Captive Portal which poses a unique risk, even with encrypted traffic, since an adversary controlling the portal can still inject malicious content. Blocking the use of Captive Portals mitigates this threat.
A drive-by Compromise	Access can be gained from visiting a website with malicious content e.g. JavaScript, iFrames or Cross Site-Scripting (XSS). This could be down to the user clicking a link - often a referrer or shorten link without knowing the true destination. Alternatively, it could be that a known website has been hijacked, and malicious content has been embedded which would execute without the user knowing.	The limiting of internet-based services will significantly curtail the ability of any adversary in using this method. The removal of corporate tools such as email and instant messaging services removes the ability to receive spear phishing links or malicious payloads directly on the PAW device.
Supply Chain compromise	Attacking a third-party supplier to gain access to a key service/function is becoming increasingly common. Third parties often require deep, specialist access to the systems which they have supplied for on-going maintenance and support.	Third party suppliers following the same stringent privilege access process, including the use of PAWs, MFA, and credential management will ensure that these suppliers are not an easy "backdoor" into sensitive systems.
Exploit Public Facing Application	A running service which exposes a TCP/IP port on a device can be used to gain access to the device, whilst end user devices are typically behind a Network Address Translation (NAT), (which means they are not directly reachable from the internet) this does not stop a local attacker gaining access to the device (e.g. where the device is on an untrusted network - Open Wi-Fi®) or where an attacker has already gained network access and can now move laterally within a network.	Designing a browse down architecture removes the requirement of leaving open services available to lower trust systems.

Annex A (informative): Bibliography

- MITRE ATT&CK®: "Content Injection".
- MITRE ATT&CK®: "Drive-by Compromise".
- MITRE ATT&CK®: "Supply Chain Compromise".
- MITRE ATT&CK®: "Exploit Public-Facing Application".

Annex B (informative): Change history

Date	Version	Information about changes
May 2025	V0.0.1	First draft.
May 2025	V0.0.2	Filled out many of the headings with text. Updated with the new template wording for normative and informative references.
May 2025	V0.0.3	Included specification table.
June 2025	V0.0.4	Reordered specification and threats and mitigations headings and populated clause 8.
June 2025	V0.0.5	Minor amendments.

History

Document history		
V1.1.1	July 2025	Publication