ETSI TS 103 994-3 V1.1.1 (2026-01)

TECHNICAL SPECIFICATION

Cyber Security (CYBER);
Privileged Access Workstations;
Part 3: System Integration

Reference
DTS/CYBER-00166

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 organizations 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.

Foreword

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

The present document is part 3 of a multi-part deliverable covering Cyber Security (CYBER); Privileged Access Workstations, as identified below:

Part 1: "Physical Device";

Part 2: "Connectivity";

Part 3: "System Integration".

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 system integration and follows on from Privileged Access Work Stations ETSI TS 103 994-1 [1] and ETSI TS 103 994-2 [2]. This series of documents will cover different 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 3 of the ETSI PAWs series, focuses on system integration and pulls Parts 1 and 2 (ETSI TS 103 994-1 [1] and ETSI TS 103 994-2 [2]) together.

Standardization of these concepts will provide greater consistency, ensure that costs can be reduced for all parties and will help to create a common understanding for implementation.

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 system integration and follows on from ETSI TS 103 994-1 - Devices [1] and ETSI TS 103 994-2 - Connectivity [2]. This series of documents will cover different 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.

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] ETSI TS 103 994-2 (V1.1.1): "Cyber Security (CYBER); Privileged Access Workstations; Part 2: Connectivity".

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

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

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: This is defined in [i.1].

3.2 Symbols

Void.

3.3 Abbreviations

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

IAM	Identity and Access Management
OS	Operating System
OT	Operational Technology
PAM	Privileged Access Management
PAW	Privileged Access Workstation
PDF	Portable Document Format
SOC	Security Operations Centre
VPN	Virtual Private Network

4 PAW design considerations and integration

4.1 PAW design considerations

4.1.1 Introduction

The deployment of a Privileged Access Workstation (PAW) solution shall account for the impact on user workflows. The design process shall incorporate input from end users as well as risk owners, ensuring that operational realities are reflected in the solution. Assumptions regarding role execution shall not replace direct engagement with users.

To minimize adoption challenges, the organization should:

- conduct user research and usability testing throughout the design and implementation phases, with emphasis on early-stage design;
- perform regular reviews of the solution design to accommodate evolving requirements.

4.1.2 Factors to consider during Commissioning and Procurement

Failure to define accurate requirements at this stage may result in procuring or developing an unsuitable solution. The organization should consider:

- current processes: what functions effectively and what does not;
- role-specific tasks and operational conditions;
- actual work practices versus prescribed processes;

- use of diverse information sources to improve understanding;
- scope and resourcing of usability activities to ensure adequate support;
- engagement of suitably qualified and experienced personnel for usability work;
- avoiding reliance solely on user-stated preferences (to prevent designing a "faster horse");
- avoiding reliance solely on technical excellence (which may result in an unused "perfect" control);
- identification of key stakeholders, including system owners, administrators, installers and end users.

A solution that fails to meet user needs is likely to result in workarounds or shadow IT, thereby increasing organizational risk. The organization shall establish a continuous learning and feedback mechanism to identify process deficiencies and drive iterative improvements.

4.2 Identify high-risk accesses

PAWs may be deployed for all privileged access scenarios; however, their use is most critical for high-risk accesses. An access shall be considered high risk if:

- the potential impact of compromise is severe; or
- the systems protected by such access are likely to be targeted by a capable threat actor.

High-risk accesses represent a subset of privileged access. A system or device shall be classified as high risk where existing security controls cannot adequately mitigate the consequences of misuse. This includes, but is not limited to:

- accesses that can directly modify or bypass critical security controls;
- accesses that can expose sensitive data;
- accesses where compromise may result in significant organizational impact.

EXAMPLE: An attack on a trusted component such as a certificate authority server may compromise system integrity and be difficult to detect or remediate.

To identify privileged and high-risk accesses, the organization should assess the potential actions of a threat actor following compromise, including:

- the use of any discovered credentials;
- the presence of connectivity to other systems, whether physical or network-based;
- the possibility of escalation to internal systems with weak security controls, which may serve as stepping stones for further attacks.

The organization should refer to threat modelling guidance to support this assessment.

Entities operating in high-threat environments, such as those within Critical National Infrastructure (CNI), shall assume that highly skilled adversaries may conduct multi-stage attacks following an initial compromise. In such cases, PAWs should be applied to a broader range of privileged accesses as part of a layered defence strategy. Defence-in-depth increases the cost and complexity of an attack, thereby reducing its likelihood of success.

It is important to note that PAWs operate under the assumption that an authenticated user is trusted; therefore, they do not inherently mitigate insider threats. However, PAWs support broader access management, monitoring, and auditing controls, which contribute to insider risk mitigation.

4.3 PAM Integration

Prior to the deployment of a PAW, the organization shall establish a clear understanding of the operational need and associated risk scenarios. The implementation of a PAW shall form part of a risk-based approach that identifies potential threats and defines the required defensive measures.

Privileged Access Management (PAM) is a core component of cybersecurity that addresses the protection of privileged accounts and associated assets. The use and deployment of PAWs shall be considered within the context of the organization's overall PAM strategy.

When defining the PAM strategy, the organization should evaluate the security benefits of PAW solutions, which include:

- Reduction of attack surface: PAWs are effective in mitigating the risk of device compromise by external threat actors.
- Prevention of common attack vectors: PAWs provide strong protection against phishing and similar attacks.
- Mitigation of accidental misuse: PAWs reduce the likelihood of users unintentionally installing malicious software.
- Containment of lateral movement: PAWs limit the ability of attackers to pivot from compromised devices, reinforcing the need to minimize interaction between PAW activities and general business operations.

PAW devices may also support and enhance other Identity and Access Management (IAM) controls.

The adoption of architectural models such as Zero Trust does not eliminate the requirement for PAWs. Certain risks can only be mitigated through the use of highly trusted devices. A PAW shall serve as a foundational element to maintain trust in technical controls and overall security posture.

4.4 Cross Domain Dataflow

4.4.1 Introduction

When implementing an import/export mechanism for a PAW environment, the organization shall begin by identifying the types of data that require transfer between enterprise and PAW environments.

Complex data formats (e.g. Microsoft Word, PDF) present higher security risks and are more difficult to sanitise than structured formats (e.g. XML, JSON). The organization should minimize data transfers to essential content only and, where feasible, convert data into simpler, lower-risk formats.

4.4.2 Data Transfer Solution Requirements

The data transfer solution shall:

- generate a complete audit trail for all data entering or leaving the PAW environment;
- require user authentication prior to any transfer;
- ensure that only approved and authorized content is exported;
- automate transfers to predefined, pre-configured endpoints, prohibiting export to arbitrary destinations;
- inspect and scan all data for malicious content, particularly for imports into the PAW environment;
- validate data structure where appropriate to maintain integrity.

4.4.3 Threat Context Considerations

For high-threat environments, data control solutions should, where feasible, be implemented in hardware.

For lower-threat contexts, software-based controls combined with network boundary restrictions may be acceptable.

The organization should refer to their National Technical Authority on secure data import/export patterns for additional implementation details.

4.5 Legacy Technology

4.5.1 Introduction

The organization shall avoid running obsolete software or Operating Systems (OS) on PAWs. Where this is not feasible for operational continuity - primarily in Operational Technology (OT) environments - obsolete applications shall be isolated and segregated from the PAW environment.

4.5.2 Preferred Approach

The organization shall engage with the vendor of the obsolete application or OS to identify alternative solutions, such as:

- upgrading to a supported version;
- porting the application to a modern OS;
- implementing containerization or virtualization strategies.

4.5.3 Virtualization and Isolation Controls

If obsolete products remain necessary and no viable alternatives exist, the organization shall:

- use virtualization to segregate obsolete software from the PAW;
- restrict access to obsolete applications to only those users who require it;
- document obsolete products and associated users as technical debt, and maintain a roadmap for migration to modern solutions.

The organization shall treat any obsolete OS as insecure by default. Security functionality provided by the obsolete OS shall not be relied upon. Additional external security controls shall be implemented.

4.5.4 Virtualization Security Requirements

Each obsolete OS instance shall have:

- no direct network connectivity to the host machine;
- no connectivity to other virtualized hosts (each instance shall operate on an isolated virtual network).

A virtualized managed firewall appliance shall be pre-configured centrally:

- PAW users shall not have the ability to modify firewall configurations or log into the appliance.
- Any VPN configuration for the PAW running an obsolete OS shall be implemented at the firewall appliance, not on the obsolete OS.

Where legacy virtual environments require connectivity to external services, an additional virtualized security boundary shall be implemented and centrally managed. PAW users shall not have the ability to modify this boundary.

4.5.5 Security Tooling Considerations

The organization shall assess the risk of deploying security tools (e.g. antivirus) on obsolete virtual machines, as these tools operate on vulnerable OS platforms and their results cannot be fully trusted.

Additional external monitoring should be implemented to compensate for the limited effectiveness of on-host security tools.

5 Initial Device

5.1 Build in isolation

5.1.1 Introduction

The initial configuration of a Privileged Access Workstation (PAW) solution shall prioritize security to prevent cross-contamination and maintain system integrity. The organization shall not build PAW systems from existing devices. Instead, PAWs shall be provisioned using new, clean devices sourced through a trusted and well-understood supply chain.

5.1.2 Single-Device and Initial Deployment Scenarios

In small-scale or single-device deployments, the initial device may serve as the sole PAW. To ensure compliance, this device shall adhere to all applicable lockdown policies. Typically, this device is used to provision the PAW management environment, establishing a clean and physically segregated network segment. This segment shall subsequently be expanded to include additional PAW devices and supporting services.

5.1.3 Multi-Device Deployments

Where multiple PAW devices are required, the initial device shall be integrated into the PAW Mobile Device Management (MDM) solution and enrolled as a PAW device once the MDM is operational.

The initial device shall not be used for administrative tasks until all technical controls and lockdown policies are fully implemented. Following MDM configuration, the device shall be enrolled to ensure consistent policy enforcement across all PAW devices.

5.2 Secure your PAW Infrastructure

Once the Privileged Access Workstation (PAW) infrastructure has been deployed within an isolated environment, it shall be subject to a series of security and operational controls to ensure its integrity and compliance with organizational requirements. All systems shall be kept up to date through the application of relevant security patches, thereby reducing exposure to known vulnerabilities.

Appropriate policy enforcement shall be applied across the PAW environment, ensuring consistent configuration and adherence to the principle of least privilege. The environment should be integrated with a centralized identity provider, and Multi-Factor Authentication (MFA) shall be enabled for all user accounts. The only exception to this requirement shall be the designated break-glass account, which shall be strictly controlled and used solely for emergency access.

Comprehensive logging and monitoring shall be configured to capture authentication events, system changes, and access activity. These logs shall be forwarded to a secure, centralized logging solution and monitored continuously to detect and respond to any anomalous or unauthorized behaviour, thereby maintaining the security posture of the PAW infrastructure.

5.3 Scale with MDM / Zero touch deployments

Where a PAW solution comprises multiple devices, the organization shall ensure that security controls can be scaled effectively. This requires the use of a well-secured management platform, which shall be administered from a trusted system.

The organization should ensure that all modifications and configuration changes to the PAW environment are consistent, reliable, and auditable. To achieve this, the use of Infrastructure as Code (IaC) is recommended. IaC enables:

- automated provisioning and configuration of infrastructure, reducing the likelihood of human error;
- simplified duplication of environments;

- streamlined updates and patching processes;
- consistent compliance enforcement across the PAW estate.

The organization shall maintain a unified view of device compliance across the entire PAW deployment and shall closely monitor configuration changes to verify that all modifications are authorized.

6 PAW backup plan

6.1 PAW Resilience

6.1.1 Introduction

Once implemented, a PAW solution shall be the exclusive method for performing high-risk privileged access within the organization. The PAW solution shall be designed with sufficient resilience to support both normal operations and failure scenarios. During the design phase, the organization shall assess:

- the required level of resilience;
- the operational impact of partial or complete PAW failure.

The PAW solution shall remain accessible and available to authorized personnel when required. Its role in incident response and recovery shall be considered, including its function as a trusted device for emergency access using break-glass accounts. High availability reduces the likelihood of users resorting to non-PAW devices for emergency access.

6.1.2 Break-Glass Access Requirements

Break-glass accounts shall be exempt from technical enforcement controls to ensure availability during emergencies.

Break-glass accounts shall, where possible, be accessed from a trusted PAW device due to the high-risk nature of these credentials.

In exceptional circumstances where PAWs are unavailable and business-critical access is required, organizational policy may permit the use of alternative devices.

6.1.3 Security and Operational Controls

Activation of a break-glass account shall automatically trigger an alert for immediate investigation and be treated as a maximum criticality incident.

Break-glass access shall only be used as a last resort and never for routine operations or remote access by third parties.

Post-incident, the organization shall conduct a full investigation, including:

- assessing whether trust in the PAW solution has been compromised;
- determining if any systems require rebuilding to restore a known good state;
- reviewing and updating security measures for break-glass accounts, including password changes;
- evaluating opportunities to reduce reliance on break-glass accounts in future scenarios.

6.1.4 Credential Management and Testing

Break-glass credentials shall be stored securely, including maintaining a physical copy where appropriate.

Access to credentials shall be restricted to authorized personnel and subject to monitoring and auditing.

Break-glass access shall be routinely tested to confirm functionality, including validation of alerting and incident escalation processes.

7 Protective Monitoring

7.1 Monitoring Requirements

The monitoring solution shall provide visibility over:

- the PAW device itself;
- supporting systems, including configuration and change management platforms.

Logging events shall be streamed to a secure log-processing system in near real-time. Protections shall be implemented to prevent tampering with logs on the device and within the log-processing system. Logs shall be immutable to ensure integrity.

Where administrative users require privileged access to log collection or storage systems, such access shall be highly restricted and routinely audited. Where feasible, logs from PAW devices shall be transmitted directly to a central monitoring solution, such as a SOC.

7.2 Monitoring Configuration and Change Management Systems

The organization shall monitor configuration and change management systems to maintain trust in the PAW solution. Alerts shall be generated for any configuration changes, enabling security teams to verify whether changes are authorized and expected. This is critical as unauthorized changes may re-enable functionality or introduce additional tooling, undermining PAW security.

7.3 Anomaly Detection

The organization shall implement anomaly detection for all uses of privileged identities. Additional logging should be enabled to capture actions performed on PAW devices, enhancing accountability and mitigating insider threats.

Given the constrained nature of PAWs, anomaly detection shall identify any activity outside the expected operational scope as an indicator of misconfiguration or compromise. Where feasible, logs from PAW devices should be correlated with logs from target systems to detect anomalies.

8 Threats and Mitigations

The present document addresses four primary threat vectors; however, these are not exhaustive, and additional risks may be covered within the points outlined here. It also considers the risk of lock-out and its mitigation through a Break-Glass procedure. While lock-out may not be a direct threat vector, being unable to access systems, whether due to accidental misconfiguration, service outage or malicious activity, can have a significant impact on recovery efforts. It is essential that any Break-Glass procedure is carefully designed to ensure access is always possible and that it is closely monitored for signs of malicious activity. The four main threats identified by MITRE are summarized in Table 1.

Table 1

Threat Vector	Risk	Mitigation and Effect
Credential Access	Credential Access consists of techniques for stealing credentials such as account names and passwords. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.	By designing and integrating PAWs alongside the PAM solution, credentials are safeguarded, only exposed when required, and regularly rotated by the PAM system. Additional mitigations previously outlined in ETSI TS 103 994-1 [1] and ETSI TS 103 994-2 [2], such as device lockdown and the principle of browse-down, further strengthen defence-in-depth measures. The combined effect is that stealing and successfully exploiting credentials becomes significantly more difficult when PAW and PAM are properly designed, integrated and implemented.
Exfiltration	Exfiltration consists of techniques that adversaries may use to steal data from your network. Once they have collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption. Techniques for getting data out of a target network typically include transferring it over their command-and-control channel or an alternate channel and may also include putting size limits on the transmission.	Implementing a well-defined cross-domain solution with structured data flows makes systems significantly harder to compromise by reducing attack surfaces and enforcing controlled, secure interactions between domains. This approach also strengthens defence-in-depth by adding an additional layer of protection against lateral movement and data exfiltration.
Lateral Movement	Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target, then pivoting through multiple systems and accounts to gain access to it. Adversaries might install their own remote access tools to accomplish Lateral Movement or use legitimate credentials with native network and operating system tools, which may be stealthier.	Building the PAW separately from other systems, applying security policies, and only connecting it once fully secured significantly reduces the risk of a threat actor laterally moving to the PAW or its network during the initial build. Furthermore, when all management interfaces are isolated within a dedicated management network that can only be accessed from a PAW, the ability to launch attacks is greatly diminished.
Discovery / Reconnaissance	Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. These techniques help adversaries observe the environment and orient themselves before deciding how to act. They also allow adversaries to explore what they can control and what's around their entry point in order to discover how it could benefit their current objective. Native operating system tools are often used toward this post-compromise information-gathering objective.	Building an isolated PAW and network, supported by well-defined security policies and controlled data transfer processes, significantly reduces the ability of a threat actor to discover vulnerabilities or perform reconnaissance on systems and services. Isolation limits exposure to untrusted networks, while structured data flows ensure that only authorized and validated interactions occur. This approach not only minimizes the attack surface but also disrupts common tactics such as lateral movement and privilege escalation, making reconnaissance and exploitation substantially more difficult.

Annex A (informative): Bibliography

- MITRE ATT&CK®: "Credential Access".
- MITRE ATT&CK®: "Exfiltration".
- MITRE ATT&CK®: "Lateral Movement".
- MITRE ATT&CK®: "Discovery".
- MITRE ATT&CK®: "Reconnaissance".
- NCSP: "Principles for secure privileged access workstations (PAWs)".

Annex B (informative): Change history

Date	Version	Information about changes
November 2025	V0.0.1	First draft
November 2025	V0.0.2	Minor editorials & Section 8 Completed
November 2025	V0.0.3	Minor editorials - hanging text and references

History

Version	Date	Status
V1.1.1	January 2026	Publication