INTERNATIONAL INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE

TENDER REFERENCES NO: 2026-06-092

Terms of Reference (ToR) for Procurement and Delivery of Software Licenses and Deployment Services of a Privileged Access Manager (PAM) for the Central Election Commission of Ukraine

1. Background

As Ukraine prepares for future electoral processes, the Central Election Commission (CEC) is strengthening the resilience, security, and operational readiness of its information and communication technology (ICT) infrastructure. The evolving cyber threat landscape, combined with the critical nature of election systems, requires enhanced controls to protect privileged access to information assets and administrative systems. Effective mechanisms for controlling, monitoring, and auditing the activities of privileged users are widely recognized as key components of modern cybersecurity and IT governance frameworks.

Privileged users are individuals who have elevated access rights to information systems, applications, databases, networks, or other ICT infrastructure components. Privileged accounts are among the most common targets in cyberattacks due to the extensive access and control they provide over critical systems and data. Traditional security controls such as antivirus software and network firewalls may have limited ability to detect or prevent the misuse of legitimate privileged credentials, which may result in significant operational, security, financial, or reputational impacts. In addition to internal administrators, organizations often grant privileged access to third-party service providers, contractors, and support personnel who require temporary or periodic access to ICT systems.

Privileged Access Management (PAM) is a category of cybersecurity solutions that provides organizations with capabilities to manage, monitor, and secure privileged accounts. PAM helps minimize risks associated with unauthorized, inappropriate, or malicious use of privileged credentials, reduces the organization's attack surface, and supports the mitigation of risks arising from both external cyber threats and insider misuse.

PAM solutions support the protection of ICT infrastructure against risks arising from both external cyber threats and insider misuse by enabling the monitoring, control, and recording of privileged user activities. These solutions help enforce access control policies, strengthen accountability, and provide auditing and reporting capabilities through the analysis of privileged access activities. Session recording and audit logs facilitate the investigation of administrative actions, support the identification of configuration changes that may affect system security, and assist in the investigation of unauthorized activities or suspected security incidents.

PAM solutions typically include secure credential management capabilities for operating systems and applications, such as password vaulting and rotation, as well as authentication and verification mechanisms (e.g., user identity and connection metadata such as source IP address). These capabilities help strengthen access control and reduce the risk of unauthorized access to privileged systems.

Privileged Access Manager allows to build monitoring, control and security processes that act to prevent threats and, in general, are now **a mandatory element of building a modern Security Operations Center (SOC)**.

2. Objectives of the Assignment

The objective of this assignment is to procure Software Licenses and Deployment Services for a Privileged Access Management (PAM) solution for the Central Election Commission (CEC) of Ukraine, ensuring secure, compliant, and effective implementation of the solution in preparation for post-war electoral processes.

3. Scope of Work

3.1 The selected Bidder will be expected to deliver Software Licenses and Deployment Services for a Privileged Access Manager. Any other software or / and hardware products or related services that may be required by the CEC in the future and are relevant to this procurement may be procured under Framework Contract to be concluded as an outcome of this tender based on a separate quotation provided that such goods and services are directly related to the scope of the PAM solution.

3.2 General architecture and software composition of a Privileged Access Manager:

- Provide ability to install all components on-premises in the Microsoft Hyper-V.
- Delivery as a 2 virtual appliances with built-in mechanisms for creating a fault-tolerant cluster in active/passive mode.
- Provide deployment in isolated IT infrastructure without the need to use additional external modules, third-party system or application software (operating systems, applications, database management systems, etc. This requirement applies to the PAM appliance itself and its core operation).
- Provide built-in mechanism for protecting information stored in the appliances from unauthorized access (possibility of using a special protection key (password) each time the appliance is launched (after shutdown or reboot)).

3.3 Functional requirements of a Privileged Access Manager:

- Configuration and administration of the software via a separate web administration portal using any modern browser (MS Edge, Chrome, Mozilla etc.) without the need to install additional components (plugins, applications, etc.). Use of a web console based on Flash or Java (JRE) technologies is not permitted.
- Providing users with a special web portal for access to controlled target systems. The possibility of optional use of this portal, i.e. providing access to controlled target systems, including without such a portal (by specialized applications: Microsoft Remote Desktop Client, Putty client, Microsoft SQL Management Studio, etc.).
- The ability to create fault-tolerant configurations based on built-in technologies; the use of third-party (external) tools for building fault-tolerant configurations is not permitted.
- The ability to store and process all events related to the operation of the software, as well as automatically transfer such events to external event processing systems.
- Includes built-in functionality for creating backup copies, including all software parameters and settings, as well as recorded sessions of privileged users, with mechanisms for protecting created copies from unauthorized access.

- Includes functionality for managing various objects such as users, target systems, connection methods both locally (using a web portal) and remotely (using open API interfaces).
- Possibility to choose to use the software interface in English language.
- Support the recording of privileged user actions. This must be achieved natively at the PAM gateway level or via integrated software on the privileged user's endpoint (such as a dedicated endpoint client or web browser extension), without requiring any agents, drivers, or software modifications to be installed on the target systems
- Support for advanced network settings such as static routing settings for individual networks.
- Contains a built-in and changeable panel informing the system administrator about the status of operability and loads on software components, with information on the number of active user sessions, the number of suspicious sessions, the load on the disk system, processor, RAM and network components. The information panel should be available only to software administrators on the corresponding administration web portal.
- The ability to work with at least 4 virtual network adapters, with each network adapter assigned a unique IP address by the software (including from different network segments) in both static and dynamic mode (using the DHCP service).
- Ability to provide privileged users with the following capabilities through each privileged user web portal:
    - a list of target systems available for connection with the ability to open sessions using standard clients (for RDP, VNC and SSH protocols);
    - list of IP addresses and ports of target systems;
    - the type of protocol used to connect to the target system;
    - viewing the password to the target system (if such rights are granted to the privileged user by the corresponding password policy);
    - changing the password on the web portal for the account (if the password is stored in the software's own secure storage);
- Contains built-in secure storage for storing recorded privileged user sessions, access details (login, password, keys, domain names, etc.) to software and target systems, and event logs. Provides standard cryptographic algorithms to protect storage.
- Provides a role-based model for using software with the ability to differentiate between different accounts:
    - full administration rights, including the ability to configure software
    - partially limited rights to administer any action except configuring software
    - limited administration rights for configuring and further monitoring of specifically defined target systems and privileged users user rights - the ability to only connect to specified target systems without the ability to log in to the administration web portal.
- Supports multiple authentication methods simultaneously for each administrator account must be at least:
    - using a static password that is stored in a secure software storage;
    - one-time password generated by external services (for example, a RADIUS server);
    - using an external user directory (AD/LDAP);
    - using MFA functionality with the possibility of OTP authentication methods;
    - RADIUS support for integration with other MFA solutions.
- Ability to add privileged users in the following ways:
    - in manual mode;
    - synchronization with an existing user directory (AD / LDAP);
    - via API interface.
- Support for at least three simultaneous external authentication systems for privileged users and administrators of AD and LDAP user directory server software.

- Functionality for creating secure (encrypted) communication channels based on SSL certificates between privileged users and software and between software and target systems. Creation of such secure (encrypted) communication channels based on both self-signed certificates (using a pair of "public" - "private" keys) and on certificates of a certification authority (CA).
- Provides support for authenticating privileged users to target systems using:
    - entering a local account;
    - introducing a domain account;
    - SSH key.
- Ability to work with access credentials (logins, passwords, domain name, SSH keys, etc.) used by privileged users to connect to target systems:
    - manual creation and storage of access details in a secure software storage;
    - use of external authentication systems (including external specialized password storage).
- The ability to force password changes on individual target systems for specific privileged user accounts based on password policies, with the definition of parameters such as:
    - password length;
    - password complexity (including requirements for capital letters, numeric characters, special characters);
    - frequency of password changes.
- Support for forced password changes in accordance with the specified password policy on at least the following target systems:
    - Unix / Linux- based operating systems via SSH;
    - Windows operating systems via LDAP;
    - Cisco equipment via SSH.
- Provides the ability to create and add your own plugins to force password changes.
- Contains a built-in system for storing and processing events in the form of logs stored in a secure storage facility. Possibility of protection against deletion, including by software administrators with the highest levels of access (rights).
- Possibility of integration with external event processing systems using standard protocols such as SNMP, syslog, etc.
- Control of privileged users who connect to target systems via RDP, including in Enhanced RDP Security (TLS) and NLA modes. Contains functionality for forced disabling of clipboard, restriction of access to target system of the device. Receiving recorded graphic video material (video clip) as a result of control of privileged users who connect to target systems via RDP. Ability to export saved graphic video materials (video clips).
- Control of privileged users who connect to target systems via the SSH protocol, with the ability to work with the X11 standard via the SSH protocol, including the ability to play graphics via X11. Provides for the restriction of file operations (prohibition of the SFTP and SCP file exchange protocols). Provides for obtaining recorded graphic video material (video clip) as a result of control of privileged users who connect to target systems via the SSH (or X11) protocol.
- Control of privileged users who connect to target systems via the VNC protocol. The VNC protocol must support connection to target systems using a Web client. Receiving recorded graphic video material (video clip) as a result of control of privileged users who connect to target systems via the VNC protocol. The ability to export saved graphic video materials (video clips) to external video formats.
- Monitoring privileged users who connect to target systems via HTTP and HTTPS protocols (with support for TLS 1.2 and TLS 1.3 standards). Obtaining recorded graphic video material (video clip) as a result of monitoring privileged users who connect to target systems via HTTP and HTTPS protocols (HTML-based resources).

- Support for user input of characters of both the Latin alphabet and other alphabets (for example, Cyrillic characters) in HTTP and HTTPS sessions, with the ability for users to independently switch alphabets.
- Ability to create policies for responding to keyboard input (including command input) performed by privileged users when working with target systems, with support for regular expression syntax. Ability to configure responses when such policies are triggered, such as: notifying the responsible person, disconnecting the session, blocking the user. It is necessary to be able to send the entered text (command) for approval.
- Ability to create customized policies that define the time intervals during which privileged users are allowed to access target systems, with the ability to define the following criteria: days of the week during which privileged users can connect to target systems, hours and minutes during which privileged users can connect to target systems, and the policy's validity interval (specifying the start and end date and time).
- Ability to search and view the results of privileged user actions, namely: viewing video of recorded sessions, entered commands and responses of the target system to such commands. Viewing video recordings of sessions through the administration web portal without the need to install any tools (software applications, plugins, etc.) .
- Ability to search for privileged user actions by various criteria: privileged user or username, entered text and/or commands, protocol type, target system name, and specified date range. Ability to create reports based on the obtained search results with specified filters in the form of CSV, PDF.
- Contains the ability to create custom policies that allow individual privileged users to view passwords for target systems they connect to.
- Ability to force a request for justification for connecting to the target system by a privileged user, with the corresponding field displayed for the user's response.
- The ability to configure confirmation (approval) of connection to the target system of privileged users by one or several responsible persons (PAM administrators) through the software administration web interface.
- The ability to configure notifications via email of the responsible person about the actions of privileged users (connection to the target system, disconnection from the target system, triggering a specified policy).
- Ability for responsible persons to view privileged user sessions in real time with provision of information about the session to the responsible person: name and IP address of the target system, name of the privileged user, protocol type, session start time. Ability to view a record of previously performed user actions for sessions occurring in real time (before its completion).
- Ability to temporarily or completely force privileged user sessions to be terminated by responsible persons in real time. Ability to block the privileged user account whose session is terminated when the privileged user session is terminated.
- The ability for privileged users to submit access requests to target systems via a personal account on the web portal, specifying the time frame for access and the justification for access, the ability to view historical data for approved access (who approved access to the target system and when), the ability to revoke permission for granted access.
- Functionality for scanning and searching for new accounts in the Microsoft Active Directory infrastructure, both once and on a specified schedule, with the ability to automatically quarantine new privileged accounts.
- The solution must ensure control of access to privileged services in accordance with Zero Trust principles using ZTNA tags. Access to the PAM portal, privileged sessions, and secrets should be granted only if the endpoint meets corporate security requirements, which are verified through FortiClient (presence of antivirus protection, up-to-date security patches, properly configured firewall, compliance with corporate security policies, etc.). The system

must support continuous posture verification and dynamically restrict access in case of non-compliance.

- The solution must provide integration with the centralized analytics and monitoring platform FortiAnalyzer to transmit logs in real time. It should support the collection and correlation of authentication events, privileged session initiation and termination, usage and rotation of privileged credentials, configuration changes, and administrative activities, ensuring centralized monitoring, audit capabilities, and enhanced visibility.
- The system must support automated incident response based on events received from other Fortinet Security Fabric components, including FortiMail, FortiWeb, FortiGate, and FortiClient. In case of detected threats, the solution should automatically block or restrict privileged access, terminate active sessions, initiate credential rotation, enforce step-up authentication, and enable additional monitoring to minimize the risk of compromise of critical resources.

3.4 The Privileged Access Manager license should provide the following capabilities:

- Up to 30 privileged users.
- Unlimited q-ty of target system (servers, network devices, virtual machines etc.).
- Vendor's support for 3 years.

3.5 General list of Software Licenses and Deployment Services that needed to be procured and delivered is provided below in Table 1.

Table 1 Privileged Access Manager licenses and deployment services

#	Item	Q-ty
1.	Privileged Access Manager Software License for 30 users, Unlimited Targets, High Availability with Vendor's Support for 3 Years	1
2.	Privileged Access Manager Deployment Services	1

3.6 The detailed technical specification of the Software Licenses that needed to be procured and delivered is provided in Annex 2.2 (Specification in Annex 2.2 takes precedence over the general list in Table 1 above).

3.7 Additional licenses may be procured from the successful Bidder if needed, and this (should the need arise) will be the subject of a separate quotation. As an outcome of this tender, the framework contract will be concluded with the bidder.

3.8 The detailed technical requirements for Deployment Services that needed to be procured is provided in Annex 2.3 (Specification in Annex 2.3 takes precedence over the general list in Table 1 above).

4. **Timing and Work Plan**

Project implementation schedule should not exceed 120 calendar days starting from the contract signature. A detailed timeline of deliverables will be developed and agreed with the selected bidder.

5. **Deliverables and Reporting Requirements**

5.1 The deliverables for this assignment shall include:

- Software Licenses according to Annex 2.2
- CEC Acceptance Letter which proves the delivery of Software Licenses
- Deployment Services for the Privileged Access Manager according to Annex 2.3

- CEC Acceptance Letter which proves the acceptance of Deployment Services.

5.2 As the part of reporting the Bidder must submit:

- An initial delivery plan within 3 working days of contract signature
- Biweekly progress reports highlighting technical tasks completed, blockers, and next steps
- Final delivery report including:
    - List of delivered software licenses and deployment services
    - Documentation packages (see below in 7.2, 7.3 and Annex 2.3).

The technical documentation of acceptance tests is provided for approval in electronic (PDF) and paper form in Ukrainian language.

6. **Management and Organization**

From International IDEA, a relevant Project Manager will be designated to provide relevant guidance for the achievement of the overall objective of the assignment and deliverables. All bidder communications shall be directed to the designated IDEA Project Manager. Final deliverables must be jointly confirmed by IDEA and the designated CEC technical contact.

7. **Monitoring and Evaluation**

This Monitoring and Evaluation section defines how International IDEA will track the progress, quality, and outcomes of the purchase and delivery of Software Licenses for the CEC of Ukraine. The aim is to ensure timely purchase and secure delivery, compliance with technical specifications.

7.1 Key Performance Indicators (KPIs):

- Delivery of all Software licenses within 30 calendar days of contract signature
- Compliance with the technical specifications outlined in Annex 2.2
- Provide deployment services for the cyber-resilient architecture within 90 calendar days of contract signature
- Compliance with the technical requirements for deployment services outlined in Annex 2.3
- Delivery of a valid Acceptance Letter from the CEC.

7.2 Monitoring Activities:

- Biweekly check-ins with the bidder to track progress against the delivery timeline
- Document verification: review of delivery reports, license documentation and invoices
- Confirmation with the CEC of receipt, functionality, and usability of the Privileged Access Manager.

7.3 Evaluation Framework

Evaluation Criteria:

- Adherence to timeline milestones
- Full compliance with architecture and integration requirements in Annex 2.2 and Annex 2.3.
- Absence of critical errors in new Privileged Access Manager
- Quality and completeness of documentation (High-Level Design, Information System Data Sheet / System Specification, Test Protocols)

Evaluation Process:

- Baseline technical assessment at project launch
- Mid-term evaluation at completion of deployment
- Final evaluation after testing and integration
- Feedback survey from CEC technical staff

Annexes (to be provided)

Annex 2.2. Technical specification of Privileged Access Manager (PAM) software licenses for the Central Election Commission of Ukraine

Annex 2.3. Technical requirements for Privileged Access Manager (PAM) deployment services for the Central Election Commission of Ukraine