

Opis przedmiotu zamówienia

Rozbudowa oraz odnowienie wsparcia dla posiadanych licencji ActiveIdentity

I. Odnowienie posiadanych licencji.

W ramach realizacji Umowy, Wykonawca dostarczy odnowienie wsparcia technicznego producenta dla posiadanych przez jednostki organizacyjne Lasów Państwowych licencji oprogramowania ActiveIdentity:

ActiveClient User License,	14 385 szt.
ActiveID CMS,	14 440 szt
4Trees AAA Server,	14 439 szt.

na okres 36-ciu miesięcy od dnia 1.01.2025r.

Wsparcie techniczne producenta musi zapewnić:

- prawo do korzystania z najnowszych dostępnych na rynku wersji oprogramowania, uaktualnień i poprawek,
- dostęp do pomocy technicznej producenta, w tym prawo do zgłaszania problemów związanych z działaniem oprogramowania.

II. Dostarczenie nowych licencji.

W ramach realizacji Umowy, Wykonawca dostarczy dodatkowe licencje, posiadanego przez jednostki organizacyjne Lasów Państwowych oprogramowania ActiveIdentity, zgodnie z wykazem zamieszczonym w załączniku nr 7 do Umowy:

ActiveClient User License,	1219 szt.
ActiveID CMS,	1165 szt.
4Trees AAA Server,	1165 szt.

Zamawiający zastrzega sobie prawo zamówienia w ramach prawa opcji dodatkowych licencji w/w oprogramowania. Wartość zamawianych w ramach prawa opcji licencji nie przekroczy 18% wartości licencji wymienionych w p. II.

Dostarczone licencje powinny być objęte wsparciem technicznym producenta na okres od daty dostawy do 31.12.2027 r.

III. Wsparcie Wykonawcy

Wsparcie wykonawcy będzie świadczone przez cały okres obowiązywania Umowy (od dnia jej zawarcia do dnia 31 grudnia 2027 r.), w formie telefonicznej, e-mail oraz przy pomocy usługi zdalnego dostępu – VPN lub w siedzibie Dyrekcji Generalnej Lasów Państwowych.

Wsparcie wykonawcy obejmuje infrastrukturę AAA, Microsoft Certification Authority – CA z infrastrukturą klucza publicznego (PKI) oraz rozwiązania autoryzacji serwisów WEB, a w szczególności:

1. Analiza zgłoszonych przez administratorów Płatnika lub Zamawiającego błędów w działaniu systemu,
2. Usuwanie na życzenie DGLP zatwierdzonych i zaakceptowanych do usunięcia błędów,
3. Wprowadzanie, na żądanie DGLP, drobnych korekt, poprawek i napraw systemu przy pomocy usługi zdalnego dostępu (VPN) lub w siedzibie DGLP.
4. W ramach realizacji Umowy, Wykonawca będzie zobligowany do aktualizacji oprogramowania/urządzeń:
 - ActiveID CMS 5.12,
 - 4Trees AAA Server,
 - Microsoft CA z infrastrukturą klucza publicznego,
 - Luna HSM Client,do najnowszych dostępnych wersji oprogramowania.
 - I. Aktualizacje krytyczne – Wykonawca zgłasza do Zamawiającego konieczność wykonania krytycznej aktualizacji, po zatwierdzeniu Wykonawca instaluje aktualizację w czasie do 24h.
 - II. Pozostałe aktualizacje Wykonawca realizuje na żądanie Zamawiającego, w terminie do 5 dni roboczych od zgłoszenia.
5. W czasie obowiązywania umowy Wykonawca zobowiązany jest do aktualizowania systemów ActivIdentity AAA, CMS oraz Microsoft Certification Authority – CA z infrastrukturą klucza publicznego (PKI) do najnowszej, zalecanej przez producenta, stabilnej wersji oprogramowania (minimum 2 razy w roku);
6. W ramach umowy Wykonawca zobowiązany jest dostosowywać konfigurację Infrastruktury AAA, Microsoft CA do przepisów prawa krajowego i europejskiego. Poziom bezpieczeństwa zastosowanych rozwiązań w odniesieniu do infrastruktury Zamawiającego ma spełniać wymogi kryptograficzne dla rozwiązań przejętych w kraju oraz standardów EU. W pierwszym kwartale obowiązywania umowy, Wykonawca przeprowadzi przegląd całości systemu objętego umową, w jego następstwie w terminie uzgodnionym z Zamawiającym, jednak nie dłuższym niż 6 miesięcy od

przeprowadzenia przeglądu, dokona modyfikacji zgodnie z dobrymi praktykami zalecanymi przez HiD i Microsoft.

7. W ramach umowy Wykonawca zapewni, przez cały czas trwania umowy, możliwość użytkowania co najmniej dwóch wspieranych przez HiD modeli kart, dostępnych na rynku, wskazanych przez Zamawiającego (w tym zrealizuje ewentualną potrzebę stworzenia nowych profili kart w CMS) z funkcjonalnością określoną przez Zamawiającego;
8. Zamawiający wymaga, żeby Wykonawca znajdował się na liście autoryzowanych partnerów HiD.

IV. Zadania fakultatywne

W ramach zadań fakultatywnych Zamawiający może zlecić wykonawcy wykonanie następujących prac:

1. Modyfikacje istniejących raportów Active Identity CMS i 4Trees server,
2. Wykonanie nowych raportów Active Identity CMS i 4Trees server,
3. Inne zadania administracyjne dotyczące systemu objętego umową.

Zadania fakultatywne będą realizowane na żądanie Zamawiającego. Na realizację zadań dodatkowych Zamawiający przewiduje maksymalnie 200 roboczogodzin.

V. Wsparcie producenta

Wsparcie producenta dla dostarczonych licencji oraz odnowienie wsparcia dla oprogramowania ActivIdentity w tym: 4Trees AAA Server, ActivIdentity CMS, portal użytkownika (My Digital ID Card) na okres do dnia 31 grudnia 2027 roku.

VI. Obsługa zgłoszeń

Przez cały czas obowiązywania umowy, Wykonawca zapewni obsługę przyjmowanych zgłoszeń za pomocą dedykowanego numeru telefonu, dedykowanego adresu poczty elektronicznej, ewentualnie dedykowanego portalu internetowego, z odpowiadającymi poziomami SLA:

Realizacja zgłoszeń w trybie: 24 x 7 x 365

1. Dla zgłoszeń krytycznych¹ – 4 godziny czas rozwiązania zgłoszonego problemu.

¹ Błąd krytyczny – błąd uniemożliwiający korzystanie z całego systemu lub jego istotnych elementów (tj. podstawowych funkcjonalności) zgodnie z przeznaczeniem, w szczególności: brak możliwości logowania użytkowników, wystawiania certyfikatów.

2. Dla zgłoszeń z priorytetem wysokim² – 24 godziny czas rozwiązania zgłoszonego problemu.
3. Dla zgłoszeń z priorytetem średnim i niskim³ – czas realizacji do 5 dni roboczych.
4. Dla zgłoszeń w ramach „Zadań fakultatywnych” – czas realizacji do 20-stu dni roboczych.

VII. Kryterium równoważności

Zamawiający dopuszcza zaoferowanie rozwiązania równoważnego. Poniżej wymagania dla równoważnego przedmiotu zamówienia.

1. Zaproponowane kompletne rozwiązanie musi pochodzić od jednego producenta; nie dopuszcza się aby składowe moduły/funkcjonalności pochodziły od różnych producentów.
2. Rozwiązanie musi być produktem będącym w sprzedaży, nie dopuszcza się rozwiązania „stworzonego” na potrzeby Zamawiającego.
3. Rozwiązanie musi znajdować się w sprzedaży co najmniej 3 lata.
4. Rozwiązanie musi być „skalowalne” do 30 000 użytkowników.
5. Rozwiązanie musi wspierać/obsługiwać wszystkie typy i modele kart kryptograficznych, używanych obecnie w PGL LP.
6. Rozwiązanie musi być zgodne z rygorystycznymi standardami weryfikacji tożsamości (PIV) rządu federalnego USA, w tym pochodnymi poświadczeniami PIV co najmniej:

U.S. Government: FIPS 201-2 (PIV cards – NIST SP 800-73-4, derived PIV credentials – NIST SP 800-157), Smart Card Interoperability Specifications GSC-IS v2.0, GSA Basic Services Interface (BSI), GSC-IS v2.1, Section 508-compliant, U.S. Department of Defense Pre-Issuance Requirements v4.2.1, FIPS 140-2 certified cards and applications support, FIPS 140-2 certified HSM support.
7. Rozwiązanie musi posiadać funkcjonalność aktualizacji bez konieczności ponownej instalacji i konfiguracji nowszej lub rozszerzonej wersji oprogramowania.
8. Rozwiązanie musi być zaprojektowane do wdrożenia w infrastrukturze o wysokiej dostępności i wysokiej przepustowości.
9. Rozwiązanie musi pozwalać na korzystanie z tożsamości cyfrowych do bezpiecznego uwierzytelniania wieloczynnikowego, podpisu cyfrowego i szyfrowania.

² Priorytet wysoki – problem, który nie ma charakteru błędu krytycznego, znacznie ograniczający możliwość korzystania z systemu lub jego funkcjonalności;

³ Priorytet średni i niski – zgłoszenia pozostałe nie wpływające negatywnie na pracę systemu.

10. Rozwiązanie musi pozwalać na wdrożenie różnorodnych metod uwierzytelniania wieloskładnikowego, w tym karty inteligentne, klucze bezpieczeństwa i urządzenia mobilne:
 - uwierzytelnianie mobilne push,
 - biometrię (rozpoznawanie odcisków palców i twarzy),
 - tokeny jednorazowego hasła (OTP) oparte na sprzęcie i oprogramowaniu,
 - dane uwierzytelniające PKI, (SMS) lub e-mail,
 - kody oraz statyczne dane uwierzytelniające, takie jak hasła, kody PIN oraz typu challenge/response.
11. Rozwiązanie musi pozwalać na weryfikację wygenerowanych podpisów transakcji przy użyciu poświadczeń OATH OCRA, EMV CAP, PKI.
12. Rozwiązanie w połączeniu z kartami kryptograficznymi posiadanymi przez Zamawiającego, musi być kompletnym narzędziem pozwalającym na tworzenie, zarządzanie i używanie poświadczeń PKI. W szczególności musi pozwalać na:
 - wydawanie kart,
 - zarządzanie cyklem życia,
 - zarządzanie kodami PIN,
 - zarządzanie hasłami OTP.
13. Rozwiązanie musi pozwalać na uwierzytelnianie infrastruktury klucza publicznego (PKI) – opartej na kartach inteligentnych na potrzeby logowania do systemu Windows, VPN, logowania internetowego, sesji zdalnych, a także bezpieczeństwa danych, podpisu cyfrowego i bezpiecznej poczty e-mail.
14. Rozwiązanie musi posiadać możliwość tworzenia wielu procesów („workflow”) i polityk, które łatwo dostosowują się do różnych środowisk i scenariuszy wdrażania; obsługiwać różne polityki według metody uwierzytelniania, grup użytkowników i kanałów dostępu. Rozwiązanie integruje mechanizm reguł do adaptacyjnego uwierzytelniania i moduł autoryzacji w celu zwiększenia kontroli dostępu.
15. Rozwiązanie zapewnia interoperacyjność: natywna obsługa SCIM, SAMLv2, OpenID Connect / OAuth2, interfejsu API opartego na usługach internetowych i RADIUS.
16. Rozwiązanie musi posiadać funkcje audytu zabezpieczające przed manipulacją, które rejestrują wszystkie działania związane ze zdarzeniami w celu raportowania.
17. Rozwiązanie musi się cechować łatwą integracją z szeroką gamą systemów operacyjnych, usług katalogowych (Microsoft Active Directory, Microsoft Active Directory Lightweight Directory Services, Red Hat Directory Server, OpenLDAP), systemów zarządzania tożsamością front-end lub back-end, urzędów certyfikacji (IdentTrust®, HID PKI-as-a-Service, Entrust® Authority Security Manager™, Microsoft Windows Certificate Authority, Opentrust by IDnomic, Digicert / Symantec® Managed PKI, Verizon® UniCERT®), a także systemów kontroli dostępu fizycznego.

18. Rozwiązanie wykorzystuje certyfikowane przez FIPS-140-2 (Common Criteria) sprzętowe moduły bezpieczeństwa (HSM) do szyfrowania danych w spoczynku i podczas podpisywania wszystkich dzienników audytu. Rozwiązanie musi wspierać Hardware Security Modules: Thales (uprzednio Gemalto SafeNet) Network HSM / PCIe HSM.
19. Rozwiązanie musi umożliwiać wydawanie i resetowanie tokenów za pomocą portalu użytkownika.
20. Rozwiązanie musi posiadać funkcjonalność polegającą na możliwości wysłania wiadomości SMS zawierającej jednorazowe hasło (OTP) w przypadku gdy nie ma tokena OTP użytkownika, na zarejestrowany wcześniej numer telefonu komórkowego użytkownika.
21. Rozwiązanie musi posiadać możliwość definiowania profili uwierzytelniania, autoryzacji, profili „accounting” oraz możliwość zarządzania urządzeniami.
22. Rozwiązanie musi posiadać możliwość konsolidacji, przeglądania i usuwania dzienników audytu, RADIUS accounting (RFC 2866).
23. Rozwiązanie musi obsługiwać:
 - a) Metody autentykacji użytkowników:
 - One-time password: Synchronous, OATH HOTP and TOTP,
 - One-time password: Synchronous + Server-based PIN,
 - One-time password: Challenge / response,
 - SMS One-Time Password,
 - X.509 certificate (EAP-TLS),
 - Static password,
 - LDAP password,
 - Routing to external RADIUS authentication server.
 - b) Urządzenia uwierzytelniające użytkowników:
 - Hardware Tokens: Token, Pocket Token, Keychain Token, Mini Token (AE, AT, OE and OT), Desktop Token,
 - Smart Cards and USB Keys: Smart Card, ActivKey SIM, ActivKey Display.
 - c) Wsparcie dla standardów protokołów:
 - RADIUS RFC 2865, 2866, and 2869,
 - TACACS+,
 - RADIUS support for EAP: RFC 3579 and 3748,
 - EAP-TLS RFC 2716,
 - IEEE 802.1X (EAP-TLS, PEAP-MSCHAP v2, PEAP-GTC).
 - d) Wsparcie dla standardów kryptograficznych:
 - DES, 3DES.



- ANSI X9.9 (challenge / response).
- ANSI X9.17 (key management).
- Retail Financial Services Symmetric Key Management ANSI X9.52.
- One-Time-Password: OATH HOTP and TOTP,

e) Wsparcie dla aplikacji VPN, Firewalls i Wireless LAN kompatybilnych z RADIUS lub TACACS+, w szczególności:

- Check Point, Cisco, Juniper, Microsoft, Nortel, Symantec,
- Web servers (Microsoft IIS, Sun One),
- Citrix XenApp Server,
- Microsoft Terminal Server,
- Microsoft Outlook Web Access / Web App,
- Inne wspierające RADIUS or TACACS+.