1. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa do Państwowej Inspekcji Pracy licencji pakietów oprogramowania standardowego wraz z prawem do aktualizacji do najnowszych wersji (Software Assurance/SA) w okresie 36 miesięcy od dnia dostawy oraz pakietów subskrypcji usług standardowych w okresie 36 miesięcy, od dnia dostawy zwanych dalej Oprogramowaniem.

Zakres przedmiotowy i ilościowy zamówienia

Specyfikacja ilościowa przedmiotu zamówienia

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Lp. | Numer katalogowy | Nazwa licencji | Liczba licencji | Typ licencji |
| 1 | 9EP-00037 | System Center DC Core ALng LSA 2L - licencja na 768 rdzeni | 1 | Licencja wieczysta + 36 mies. Software Assurance/SA |
| 2 | 9EN-00494 | System Center Standard Core ALng LSA 2L - licencja na 1326 rdzeni | 1 | Licencja wieczysta + 36 mies. Software Assurance/SA |
| 3 | AAA-10732 | EMS E3 ALng Sub Per User – licencja na użytkownika | 2760 | Licencja w formie subskrypcji na okres 36 miesięcy |

Minimalne wymagania w zakresie dostaw

1. Zamawiający wymaga, aby Oprogramowanie było przeznaczone dla jednostek administracji publicznej
2. Zamawiający wymaga, aby Oprogramowanie zostało dostarczone w ramach umowy Enterprise Agreement, która zostanie zawarta przed dostawą Oprogramowania
3. Zamawiający wymaga zagwarantowania niezmienności cen na Oprogramowanie w całym okresie trwania umowy.
4. Oferowane Oprogramowanie ma być produktami standardowymi – powszechnie dostępnymi na rynku (typu Commercial off-the-shelf - COTS)
5. Oprogramowanie musi pozwalać na swobodne przenoszenie pomiędzy stacjami roboczymi lub serwerami (np. w przypadku wymiany lub uszkodzenia sprzętu etc.).
6. Licencje pakietu systemu zarządzania muszą uprawniać do uruchomienia wymaganych serwerów zarządzających wraz z dedykowaną bazą danych
7. Oferowane subskrypcje usług hostowanych muszą zapewniać:
   1. Zagwarantowanie poziomu dostępności na poziomie min. 99,9%.
   2. Dostępność mechanizmów pełnej rozliczalności działań użytkowników w usługach platformy subskrypcyjnej.
   3. Dostępność na żądanie wyników aktualnych audytów, w tym audytów bezpieczeństwa, dla usług i centrów przetwarzania danych oferujących te usługi.
   4. Możliwość automatycznej, niewpływającej na ciągłość pracy systemu instalacji poprawek dla wybranych składników usługi.
   5. Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego.
   6. Możliwość niezaprzeczalnego uwierzytelnienia na bazie usługi katalogowej będącej składową hostowanej usługi platformowej.
   7. Możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory.
   8. Dostępność mechanizmu uwierzytelnienia wieloskładnikowego.
   9. Dostępność logów informujących o wszystkich zdarzeniach uwierzytelnienia do usług i danych Zamawiającego, zakończonych powodzeniem lub niepowodzeniem oraz prób uwierzytelnienia przy pomocy tożsamości będących na listach „wykradzione”.
   10. Dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych.
   11. Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN)
   12. Wbudowane w platformę mechanizmy zabezpieczające przez atakami DDoS,
   13. Przynajmniej dwa równorzędne ośrodki przetwarzania danych, odległe od siebie o co najmniej 100 km.
   14. Zapisy umowne zawierające tzw. Klauzule Umowne opublikowane przez Komisję Europejską w zakresie ochrony danych osobowych,
   15. Możliwość zastrzeżenia miejsca przetwarzania/składowania danych w usłudze do terytorium krajów Europejskiego Obszaru Gospodarczego.
   16. Zobowiązania umowne potwierdzające zgodność z rozp. RODO i potwierdzające rolę operatora usługi jako współprzetwarzającego dane,
   17. Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego,
   18. Mechanizmy pozwalające na realizację wymagań rozliczalności i monitorowania użytkowników i usług.
   19. Gwarancję usunięcia danych Zamawiającego z platformy subskrypcyjnej po zakończeniu umowy.
   20. Gwarancję braku dostępu do danych Zamawiającego na platformie subskrypcyjnej, z wyłączeniem działań serwisowych wymagających każdorazowo zgody zamawiającego i wykonywanych wyłącznie przez uprawnione osoby z organizacji dostawcy platformy subskrypcyjnej.
8. Oprogramowanie musi gwarantować prawo instalacji najnowszej wersji Oprogramowania dostępnej w trakcie trwania umowy.
9. Zamawiający dopuszcza oferowanie Oprogramowania o szerszej niż opisana funkcjonalności.
10. Z uwagi na szeroki zakres funkcjonalny i terytorialny wdrożenia planowanego na bazie zamawianego Oprogramowania oraz konieczności minimalizacji kosztów związanych z wdrożeniem, szkoleniami i eksploatacją systemów, Zamawiający wymaga oferty zawierającej Oprogramowanie, umożliwiające wykorzystanie wspólnych i jednolitych procedur masowej instalacji, uaktualniania, zarządzania, monitorowania i wsparcia technicznego oraz jednolitych mechanizmów wykorzystania tożsamości cyfrowej.
11. W związku z możliwością zwiększenia liczby użytkowników systemów w trakcie trwania umowy, Zamawiający wymaga zaoferowania mechanizmu licencjonowania gwarantowanego przez Producenta Oprogramowania, umożliwiającego w okresie trwania umowy instalację dodatkowych licencji z zamawianego zakresu Oprogramowania z rozliczaniem się za nie post factum - raz do roku.
12. Wykonawca zapewni dostęp do spersonalizowanej strony pozwalającej upoważnionym osobom ze strony Zamawiającego na:
    1. pobieranie zakupionego Oprogramowania,
    2. aktywację zakupionego Oprogramowania,
    3. sprawdzanie liczby zakupionego Oprogramowania w wykazie zakupionego Oprogramowania.
13. Zamawiający wymaga udzielenia uprawnień na stronie Producenta w terminie do 7 dni kalendarzowych od podpisania umowy.
14. Po stu dwudziestu (120) dniach od zakończenia okresu trwania umowy Wykonawca zapewni możliwość wyłączenia konta Zamawiającego na spersonalizowanej stronie Producenta i usunięcie jego danych.
15. Wykonawca zapewni obronę Zamawiającego z tytułu roszczeń strony trzeciej o naruszenie przez oferowany produkt prawa autorskiego w przypadku niezwłocznego powiadomienia Wykonawcy o roszczeniu odszkodowawczym.
16. Jeżeli nowa wersja Oprogramowania zawierać będzie bardziej restrykcyjne prawa do używania niż wersja, która była aktualna na dzień złożenia oferty, te bardziej restrykcyjne prawa do używania nie będą miały zastosowania do korzystania z tego Oprogramowania przez Zamawiającego.
17. Warunki równoważności Oprogramowania
    1. Warunki ogólne:

Zamawiający dopuszcza możliwość zaoferowania oprogramowania równoważnego do Oprogramowania, zwanego dalej Oprogramowaniem Równoważnym. Poniższej przedstawione są wymagania i kryteria równoważności w przypadku zaoferowania Oprogramowania Równoważnego:

Zamawiający wymaga, aby oferowane Oprogramowania Równoważne spełniały wymagania określone w pkt 2.2- 2.3, odpowiednio dla każdego Oprogramowania Równoważnego oraz niżej wymienione wymagania:

1. Oprogramowanie Równoważne musi bez zakłóceń współpracować z posiadaną przez Zamawiającego infrastrukturą sprzętową oraz wykorzystywanym oprogramowaniem i systemami, do których należą: serwery, laptopy, komputery stacjonarne, urządzenia drukujące i skanujące, urządzenia sieciowe, oprogramowanie systemowe Microsoft Windows, Windows Server, środowisko wirtualizacyjne Hyper-V.
2. Na Wykonawcy oferującym Oprogramowanie Równoważne spoczywa odpowiedzialność w zakresie prawidłowego działania zaoferowanego Oprogramowania Równoważnego w środowisku pracy użytkowników Oprogramowania Równoważnego u Zamawiającego
3. Wykonawca musi zapewnić warunki i zakres usługi świadczone w ramach pakietu wsparcia dla Oprogramowanie Równoważnego nie gorsze niż usługa określona dla odpowiedniego Oprogramowania Producenta Microsoft;
4. Wykonawca musi wykazać, że funkcjonalność każdego Oprogramowanie Równoważnego nie jest gorsza od funkcjonalności odpowiedniego Oprogramowania Producenta Microsoft;
5. Wykonawca musi zapewnić, że składniki Oprogramowania Równoważnego są kompatybilne i będą w sposób niezakłócony współdziałać ze sprzętem i oprogramowaniem systemowym, aplikacyjnym i użytkowym, eksploatowanym i obsługiwanym przez Zamawiającego;
6. Wykonawca zobowiązany jest pokryć koszty zmiany w zakresie Oprogramowania Microsoft na Oprogramowanie Równoważne, konieczne do właściwego działania środowiska sprzętowo-programowego Zamawiającego, o ile wystąpi taka konieczność;
7. Wykonawca zobowiązany jest przywrócić sprawne działanie infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokonać niezbędnych modyfikacji przywracających właściwe działanie tego środowiska sprzętowo-programowego, również po odinstalowaniu Oprogramowania Równoważnego w przypadku, gdy zaoferowane Oprogramowanie Równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu pracy tego środowiska sprzętowo-programowego;
   1. Warunki wspólne dla System Center Core:
8. Licencje na Oprogramowanie muszą uprawniać do uruchomienia wymaganych serwerów zarządzających wraz z dedykowaną bazą danych.
9. System zarządzania musi uprawniać do zarządzania środowiskiem fizycznym i maszynami wirtualnymi w ilości określonej w warunkach szczegółowych na nim posadowionymi w zakresie wszystkich wymienionych poniżej funkcji:
   1. Moduł monitorowania stanu, wydajności i wykorzystania infrastruktury, aplikacji I procesów.
   2. Moduł automatyzacji wykonywania zadań w centrum przetwarzania, pozwalający w prosty sposób wykorzystać, łączyć i automatyzować wykonanie natywnych skryptów PowerShell.
   3. Moduł powoływania maszyn wirtualnych na platformie Windows Server I zarządzania nimi w ramach centrum przetwarzania, umożliwiający zarządzanie wykorzystania sieci, przestrzeni dyskowych, przetwarzania i uprawnionego dostępu.
   4. Moduł ochrony danych poprzez ich bezpieczne składowanie (backup), zarządzanie składowanymi danymi, odtwarzanie danych produkcyjnych. Ma umożliwiać wykorzystanie dla chmury prywatnej, maszyn fizycznych, urządzeń klienckich i aplikacji serwerowych.
   5. Moduł wsparcia technicznego dla rozwiązywania problemów technicznych, zarządzania zmianą konfiguracji i zarządzania cyklem życia.
   6. Moduł zarządzania serwerami I komputerami klasy PC w środowisku własnej organizacji, pozwalający na wykonywanie aktualizacji oprogramowania i zarządzanie aktualizacjami, planowanie i wdrażanie polityk konfiguracyjnych i bezpieczeństwa oraz monitorujący status systemów.
   7. Moduł ochrony systemów Windows Server przed złośliwym oprogramowaniem.
   8. Integracja umożliwiająca przekazywanie alertów z monitoringu do kanału Microsoft Teams.
   9. Możliwość oparcia dostępu do narzędzi w oparciu o rolę administratora w organizacji.
10. Wsparcie dla zarządzania hostami Azure Stack HCI 21H2 i VMware 7.0.

Warunki szczegółowe:

System Center DC Core ALng LSA 2L

Licencja uprawnia do zarządzania nieograniczoną ilością maszyn wirtualnych

System Center Standard Core ALng LSA 2L

Licencja uprawnia do zarządzania dwiema maszynami wirtualnymi

* 1. Warunki dla EMS E3 ALng Sub Per User

Subskrypcja usługi zarządzania urządzeniami oraz tożsamością użytkowników musi spełniać następujące wymagania:

Wymagania ogólne:

1. Zastosowanie w usłudze powszechnie uznanych i rozpowszechnionych standardów przemysłowych i normatywów, pozwalających na potencjalne wykorzystanie różnych technologii i rozwiązań w ramach jednej platformy subskrypcyjnej,
2. Zagwarantowanie poziomu dostępności na poziomie min. 99,9%,
3. Stale modyfikowane i rozszerzane mechanizmy i procedury bezpieczeństwa, poddawane corocznie audytom niezależnych firm.
4. Dostępność na żądanie wyników aktualnych audytów, w tym audytów bezpieczeństwa, dla usług i centrów przetwarzania danych oferujących te usługi.
5. Możliwość skalowania usługi z ustalonymi kosztami takiego skalowania,
6. Możliwość automatycznej, niewpływającej na ciągłość pracy systemu instalacji poprawek dla wybranych składników usługi,
7. Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego,
8. Możliwość niezaprzeczalnego uwierzytelnienia na bazie usługi katalogowej będącej składową hostowanej usługi platformowej.
9. Możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory.
10. Dostępność logów informujących o wszystkich zdarzeniach uwierzytelnienia do usług i danych Zamawiającego, zakończonych powodzeniem lub niepowodzeniem oraz prób uwierzytelnienia przy pomocy tożsamości będących na listach „wykradzione”.
11. Dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych,
12. Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN),
13. Wbudowane w platformę mechanizmy zabezpieczające przez atakami DDoS,
14. Zawarcie w umowie na wykorzystanie zamawianej usługi tzw. Klauzul Umownych opublikowanych przez Komisję Europejską w zakresie ochrony danych osobowych,
15. Możliwość zastrzeżenia miejsca przetwarzania/składowania danych w usłudze do terytorium krajów Unii Europejskiej.
16. Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego,
17. Mechanizmy pozwalające na monitorowania użytkowników i usług oraz realizację wymagań rozliczalności.
18. Gwarancja usunięcia na żądanie danych Zamawiającego z usługi po zakończeniu umowy.
19. Gwarancja braku dostępu do danych Zamawiającego na Platformie, z wyłączeniem działań serwisowych wymagających każdorazowo zgody zamawiającego i wykonywanych wyłącznie przez uprawnione osoby z organizacji dostawcy usługi.

Wymagania funkcjonalne

1. Zarządzanie urządzeniami mobilnymi (iOS, Android, Windows Phone, Windows RT),
2. Możliwość wykorzystania Right Management Services (RMS) - ochronę treści na urządzeniach mobilnych,
3. Portal klasy self-service dla użytkowników mobilnych pozwalający na zdalny reset haseł i zarządzanie przynależnością do grup security w usłudze katalogowej,
4. Podniesienie poziomu bezpieczeństwa dostępu do aplikacji webowych – poprzez uwierzytelnianie wieloskładnikowe (np. poprzez jednorazowe hasła SMS),
5. Prawo do korzystania z rozwiązania klasy on-premise, który służy do zaawansowanego zarządzanie tożsamością w organizacji.

Wymagane scenariusze użycia:

1. Automatyczna klasyfikacja treści dokumentów (przechowywanych na zasobach plikowych, bibliotekach lub transportowanych poprzez system pocztowy) zgodnie z definiowanymi wzorcami,
2. Wykorzystanie klasyfikacji danych do dynamicznego aplikowanie restrykcji związanych z dostępem do informacji zapobiegające niekontrolowanemu wyciekowi informacji,
3. Bezpieczna wymiana plików wewnątrz organizacji oraz z zewnętrznymi odbiorcami niezależnie od typu pliku, posiadanego urządzenia (PC lub urządzenie mobilne Windows Phone, Android, iOS) lub przynależności do organizacji, umożliwiające granularną kontrolę dostępu do poufnych informacji i wymuszenie ustalonych polityk ochrony informacji,
4. Możliwość wykorzystania telefonów do uwierzytelniania wieloczynnikowego z wykorzystaniem jednorazowych haseł SMS lub specjalizowanych aplikacji, potwierdzających tożsamość użytkownika podczas dostępu do aplikacji webowych pozwalające na podniesienie poziomu zabezpieczeń np. podczas dostępu do danych firmowych z dowolnego urządzenia, lub z poza sieci lokalnej,
5. Możliwość pracy na prywatnych urządzeniach użytkowników zapewniający bezpieczny i kontrolowany dostęp do danych i aplikacji, w możliwością wydzielenia i usunięcia danych służbowych z urządzenia,
6. Jednokrotne logowanie (single sign-on) w oparciu o poświadczenia domenowe do aplikacji SaaS wykorzystujących różne źródła tożsamości użytkownika, przy zachowaniu niezaprzeczalności działań,
7. Samoobsługowy mechanizm resetu hasła użytkownika, zarządzania członkostwem w grupach i obsługi kart inteligentnych pozwalający na redukcję ilości zgłoszeń działów wsparcia,
8. Automatyczne przepływy pracy i reguł biznesowych pozwalające przyspieszenie procesów i wyeliminowanie błędów (np. przy zatrudnianiu nowych pracowników od pojawienia się osoby w systemie HR poprzez tworzenie kont dostępowych i nadawanie uprawnień do różnych systemów, zastrzeganie tożsamości na podstawie ustalonych polityk i procedur),
9. Ochrona danych poprzez wykrywanie i mapowanie ról biznesowych pozwalające na audyt i kontrolę zgodności realizacji uprawnień użytkowników z ustalonymi politykami oraz ciągłą weryfikację stanu bezpieczeństwa systemów.
10. Zarządzanie urządzeniami mobilnymi pozwalające na kontrolowany lub warunkowy dostęp do zasobów organizacji, a w sytuacjach awaryjnych umożliwiające zdalne kasowanie danych firmowych lub całego urządzenia.

Podsystem zarządzania tożsamością:

Podsystem zarządzania tożsamością elektroniczną ma zapewniać pobieranie, agregację oraz synchronizacje danych o użytkownikach z różnych systemów w ramach organizacji wraz z zarządzaniem certyfikatami wydawanymi w ramach własnego centrum certyfikacji (CA).

*Bezpieczeństwo*

1. System zarządzania tożsamością musi umożliwiać zastosowanie - przy połączeniu ze źródłami danych - mechanizmów zabezpieczeń odpowiednich dla danego źródła danych (mechanizmy uwierzytelnienia i zabezpieczenia transmisji).
2. System musi zapewniać prawidłową współpracę z zarządzanymi źródłami danych w sieci podzielonej zaporami firewall oraz w sieci z zaimplementowanymi mechanizmami ochrony danych na poziomie transmisji danych (IPSec, SSL).
3. System zarządzania tożsamością musi umożliwiać w ramach dostarczanych mechanizmów na delegację uprawnień związanych z zarządzaniem i obsługą systemu.
4. System musi umożliwiać odtwarzanie utraconych certyfikatów bezpośrednio na kartę.

*Skalowalność*

System zarządzania tożsamością musi umożliwiać skalowanie mechanizmów systemu, pozwalające na obsługę informację w zakresie do 10 000 obiektów tożsamości, posiadających reprezentację w zarządzanych źródłach danych połączonych z systemem oraz mieć możliwość skalowania stanowisk wydających certyfikaty.

*Interoperacyjność*

1. System zarządzania tożsamością musi zapewniać możliwość działania systemu w środowisku heterogenicznym. Współpraca ta powinna być realizowana z użyciem standardowych dla źródeł danych protokołów dostępu oraz przy minimalnej ingerencji w mechanizmy działania źródła danych połączonego z systemem.
2. System zarządzania tożsamością musi zapewniać możliwość realizacji dwukierunkowej, uprawnionej wymiany informacji z połączonymi źródłami danych oraz musi udostępniać standardowe interfejsy umożliwiające komunikację dwustronną (np. wymianę danych o użytkownikach) z innymi systemami informatycznymi.

*Skalowalność funkcjonalna*

1. System zarządzania tożsamością powinien umożliwiać rozszerzanie funkcjonalności o połączenia z nowymi typami źródeł danych jak i rozszerzenie mechanizmów logiki systemu.
2. System zarządzania tożsamością powinien umożliwiać rozszerzanie rozwiązania o mechanizmy raportowanie i audytu informacji o tożsamości.

*Wymagania w zakresie cech i funkcjonalności rozwiązania*

Agregacja i synchronizacja danych:

1. System musi zapewniać możliwość odczytu i zapisu danych pomiędzy źródłami danych działającymi w heterogenicznym środowisku systemów połączonych siecią lokalną lub rozległą.
2. System zarządzania tożsamością, w ramach początkowego wdrożenia musi zapewnić możliwość integracji rozwiązania zarządzania tożsamością z następującymi źródłami danych:

* Pliki tekstowe CSV, AVP, LDIF;
* Bazy danych MS SQL 2000 - 2016, Oracle;
* Usługi katalogowe Microsoft Active Directory, Novell eDirectory, OpenLDAP.

1. System musi zapewniać możliwość komunikacji z powyższymi informacjami z użyciem standardowych dla każdego ze źródeł danych mechanizmów i protokołów oraz dwustronną wymianę danych w zakresie informacji o obiektach zarządzanych w ramach każdego ze źródeł danych.
2. System musi zapewniać możliwość rozszerzenia zakresu połączonych źródeł danych o połączenie z systemami, do których nie są standardowo dołączane mechanizmy integrujące poprzez budowę odpowiedniego rozszerzenia systemu.
3. System musi zapewniać możliwość uprawnionego tworzenia, uaktualniania oraz usuwania obiektów z połączonych źródeł danych.
4. System musi dostarczać mechanizmy pozwalające na definiowanie zakresu informacji odczytywanych z każdego ze źródeł danych oraz możliwość filtrowania danych o obiektach pochodzących ze źródeł danych na podstawie zadanych kryteriów.
5. W oparciu o informacje dostarczane z poszczególnych źródeł danych, system musi umożliwiać agregację informacji o tożsamości elektronicznej we wspólnym repozytorium, umożliwiając synchronizację danych pomiędzy różnymi źródłami danych na podstawie zagregowanej informacji o tożsamości elektronicznej.
6. System musi oferować możliwość definiowania zasad przepływu danych pomiędzy systemami oraz rozszerzenia przepływu danych o możliwość zdefiniowania reguł transformacji danych w ramach realizowanego przepływu danych.
7. System musi umożliwiać zrealizowanie funkcjonalności zmiany i resetu hasła dla obiektu w ramach dowolnego ze źródeł danych. System powinien umożliwiać również zrealizowanie funkcjonalności synchronizacji hasła pomiędzy różnymi źródłami danych.

Repozytorium danych teleadresowych:

1. System musi umożliwiać agregację danych teleadresowych użytkowników przechowywanych w różnych źródłach danych w ramach wspólnego źródła danych.
2. System misi zapewnić interfejs użytkownika zapewniający możliwość wyszukiwania oraz przeglądania danych dla wszystkich uprawnionych użytkowników systemu.
3. W ramach interfejsu użytkownika system powinien umożliwiać zdefiniowanie uprawnień dla wybranych użytkowników lub grup użytkowników w zakresie dostępu, zarządzania oraz uaktualnienia danych teleadresowych.
4. W ramach interfejsu użytkownika system musi zapewniać możliwość udostępnienia edycji zakresu udostępnianych danych samodzielnie przez każdego z uprawnionych użytkowników. System powinien pozwalać na edycję danych użytkownika w oparciu o mechanizm uwierzytelnienia użytkowników zintegrowany z usługą katalogową Active Directory.

Zarządzanie kartą elektroniczną

1. Zarządzanie kartami elektronicznymi musi obejmować: personalizację graficzną kart (nadruk), zdalne zarządzania PIN’ami dostępowymi do karty, personalizację elektroniczną kart (kasowanie wystawianie certyfikatów),
2. Dostarczony system musi umożliwiać zarządzanie certyfikatami wydanymi dla minimum 10 000 użytkowników,
3. Dostarczony system musi umożliwiać zarządzanie wydawaniem certyfikatów i ich odtwarzaniem w przypadku uszkodzenia karty (w tym możliwość odtworzenia wybranych certyfikatów wraz z kluczem prywatnym przechowywanym i wygenerowanym na karcie)
4. System musi umożliwiać wydawanie i zarządzanie wieloma certyfikatami na jednej karcie (przewiduje się wykorzystanie 4 certyfikatów dla jednego użytkownika)e. Zastosowanie wydawanych certyfikatów może być ograniczane do konkretnych potrzeb, np. tylko do podpisywania, tylko do szyfrowania itp.,
5. Wydawane certyfikaty muszą umożliwiać ich wykorzystanie do autoryzacji użytkownika w systemach usług katalogowych typu Microsoft Active Directory, Novell e-Directory, Open LDAP,
6. System musi wspierać zarządzanie certyfikatami używanymi do logowania w systemie usług katalogowych zewnętrznym do systemu usług katalogowych zintegrowanego z infrastrukturą PKI,
7. System musi wspierać zarządzanie certyfikatami używanymi do uwierzytelnienia w sposób umożliwiający wykorzystanie tych certyfikatów do autoryzacji w systemach informatycznych, np. aplikacjach webowych, bazach danych, serwerach pocztowych.
8. System musi umożliwiać delegację zarządzania wybranymi grupami certyfikatów i kart dla lokalnych administratorów,
9. Po wystawieniu certyfikatu, system musi umożliwić włączenie automatycznej publikacji certyfikatu w katalogu LDAP,
10. Po wygaśnięciu certyfikatu, system musi udostępniać możliwość automatycznego usunięcia certyfikatu z katalogu LDAP,
11. Certyfikaty wystawione na jednej stacji muszą być automatycznie dostępne dla użytkownika na innej stacji o ile się tam zaloguje (dotyczy certyfikatów przechowywanych w profilu użytkownika jak i certyfikatów przechowywanych na karcie elektronicznej),
12. Systemu musi posiadać przyjazny interfejs oparty o WWW, przez który użytkownik końcowy może wykonywać operacje zarządzania swoimi certyfikatami i PIN’ami dostępowymi (zmiana PIN’u, odblokowanie karty),
13. System musi umożliwiać (po wykonaniu graficznej personalizacji karty) wprowadzenie/ wygenerowanie PIN’u inicjującego do karty elektronicznej następującymi drogami:
14. Użytkownik lub administrator wprowadza PIN inicjujący,
15. PIN inicjujący jest losowo generowany przez system i przekazywany użytkownikowi po autoryzacji na stronie WWW,
16. System generuje PIN inicjujący i drukuje go w sposób uniemożliwiający odczytanie go przez osoby postronne bez rozerwania koperty / wydruku,
17. PIN może być dostarczony do systemu z zewnętrznego źródła (musi być dostarczone odpowiednie API),
18. Personalizacją graficzna musi pobierać ze wskazanego przez Zamawiającego źródła danych, zdjęcia pracowników i umieszczać je wraz z innymi danymi identyfikacyjnymi na karcie.
19. System musi umożliwiać odblokowanie kart w oparciu o autoryzację użytkownika w katalogu LDAP z wykorzystaniem hasła jednokrotnego,
20. Bezpośrednie odblokowanie karty musi być wykonywane w oparciu mechanizm challenge/response (zabrania stosowania się SO PIN’u statycznego),
21. Na PIN’y wykorzystywane przez użytkownika musi być możliwość nakładania polityk bezpieczeństwa definiujących stopień skomplikowania PIN’u, w szczególności:

* nie mniej niż 6 znaków,
* wymagane cyfry litery małe i duże,
* PIN może się powtarzać przez N zmian,

1. System musi wspierać karty Cryptotech MultiliSign 2.0 lub równoważne,
2. Zarządzanie wystawianiem certyfikatów musi się odbywać w oparciu o definiowalny przepływ roboczy (workflow), który będzie mógł być modyfikowany bezpośrednio przez operatora systemu z poziomu interfejsu graficznego,
3. Workflow musi umożliwiać, implementacji następujących scenariuszy użycia:

* w pełni automatyczne wystawianie certyfikatów dla użytkowników,
* wystawianie certyfikatów wymagające każdorazowej aprobaty operatora systemu,
* automatyczne odświeżanie wybranych certyfikatów,
* automatyczne odtwarzanie wszystkich certyfikatów na kartę elektroniczną w przypadku jej zastąpienia,
* weryfikację czy użytkownik ma odpowiednie certyfikaty lub czy certyfikaty nie wygasają i w razie potrzeby system musi uruchamiać odpowiednią procedurą wystawiania lub wznawiania certyfikatu,
* powiadamianie administratorów systemu o wygasaniu certyfikatów dla serwerów / urządzeń wchodzących w skład infrastruktury teleinformatycznej,

1. Wbudowane workflow musi udostępnić możliwość definiowanie wielu wzorców certyfikatów (w zależności od ich zastosowania) w połączeniu z odpowiednią ścieżką wystawiania/dostarczania certyfikatów do użytkownika, w szczególności:

* certyfikat do szyfrowania poczty wystawiany jest automatycznie o ile użytkownik posiada certyfikat na karcie elektronicznej do podpisu, podpis ten musi być użyty do podpisania wystawianie certyfikatu do szyfrowania,
* certyfikat do logowania jest wystawiony, jeśli użytkownik posiada kartę elektroniczną przypisaną do siebie oraz poprawnie zautoryzuje się hasłem jednokrotnym na stronie WWW systemu,

1. Definiowanie takich reguł musi być dostępne bezpośrednio dla operatora systemu i nie może wymagać dodatkowych opłat licencyjnych,
2. System musi udostępniać mechanizmy raportujące o wykorzystaniu kart kryptograficzny oraz certyfikatów, liczby zmian PIN’ow, czy liczby odblokowanych kart,
3. Dane służące do deszyfracji kluczy prywatnych użytkowników przechowywanych w systemie, muszą być bezpiecznie składowane na urządzeniu HSM typu nCipher netHSM 500 lub w pełni równoważnych,
4. Bezpośrednie zarządzania kartami musi odbywać się przez dostarczany wraz z systemem Microsoft Windows interfejs „Microsoft Smart Card Base CSP” lub standard PKCS#11,
5. System musi udostępniać interfejs programistyczny pozwalający rozbudowywać system (koszt licencji musi być wliczony w cenę rozwiązania).

Podsystem zarządzania urządzeniami mobilnymi

Dostępna poprzez Internet na zasadzie subskrypcji usługa pozwalająca na budowę bezpiecznego i skalowalnego środowiska, a w szczególności:

1. Integrację z systemem Microsoft Configuration Manager w oparciu o natywne interfejsy komunikacyjne,
2. Wykorzystanie bazy użytkowników znajdujących się w Active Directory,
3. Inwentaryzację sprzętu i zarządzanie zasobami możliwą do przeprowadzenia w ustalonych interwałach czasowych,
4. Inwentaryzacja sprzętu musi pozwalać na zbieranie następujących informacji:

* Nazwa urządzenia
* Identyfikator urządzenia
* Nazwa platformy systemu operacyjnego
* Wersja oprogramowania układowego
* Typ procesora
* Model urządzenia
* Producent urządzenia
* Architektura procesora
* Język urządzenia
* Lista aplikacji zainstalowanych w ramach przedsiębiorstwa

1. W celu zapewnienia bezpieczeństwa danych usługa musi umożliwiać funkcjonalność zdalnej blokady, wymazania urządzenia (przywrócenia urządzenia do ustawień fabrycznych) oraz selektywnego wymazania danych i aplikacji. Usługi te mają być możliwe do zrealizowania z poziomu SCCM (dla operatorów systemu) lub poprzez dedykowany interfejs webowy lub aplikację (dla użytkownika urządzenia mobilnego).

Wymagania w zakresie dystrybucji oprogramowania:

1. Usługa musi umożliwiać przechowywanie pakietów instalacyjnych dla aplikacji mobilnych na specjalnie wydzielonych zasobach sieciowych – punktach dystrybucyjnych (tak jak ma to miejsce dla dystrybucji aplikacji). Punkty te mogą być zasobami sieciowymi lub wydzielonymi witrynami WWW lub punktami dystrybucyjnymi w usłudze.
2. Usługa ma umożliwiać dystrybucję oprogramowania na żądanie użytkownika, realizowane poprzez wybór oprogramowania w ramach dostępnego dla danej grupy użytkowników katalogu aplikacji
3. Katalog aplikacji ma być zrealizowany w oparciu o dedykowaną witrynę webową lub dedykowaną aplikację (dostępną dla poszczególnych platform w dedykowanych sklepach mobilnych).
4. Katalog aplikacji ma wspierać następujące formaty aplikacji mobilnych:

* \*. appx (Windows RT)
* \*.xap (Windows Phone 8)
* \*.ipa (iOS)
* \*.apk (Android)

1. Katalog aplikacji musi mieć możliwość publikowania aplikacji znajdujących się w następujących sklepach mobilnych aplikacji:

* Windows Store
* Windows Phone Store
* Android Google Play Store
* iOS App Store

1. W obszarze polityki haseł usługa zapewni:

* Zdefiniowanie wymuszenia hasła,
* Określenie minimalnej długości hasła,
* Określenie czasu wygasania hasła,
* Określenie liczby pamiętanych haseł,
* Określenie liczby prób nieudanego wprowadzenia hasła przed wyczyszczeniem urządzenia,
* Określenie czasu bezczynności urządzenia, po jakim będzie wymagane podanie hasła.

1. Usługa ma umożliwiać skorzystanie z szeregu predefiniowane raportów dedykowanych dla klas urządzeń mobilnych. W szczególności w obszarze raportowania zainstalowanego oprogramowania jest możliwość zebrania informacji o zainstalowanym oprogramowaniu na urządzeniu firmowym lub urządzeniu użytkownika.

Podsystem ochrony informacji

Usługa bezpieczeństwa informacji musi pozwalać na stworzenie mechanizmów ochrony wybranych zasobów informacji w systemach jej obiegu i udostępniania w ramach systemów Zamawiającego i poza nimi, chroniąc ją przed nieuprawnionym dostępem. Usługa musi spełniać następujące wymagania:

1. Chroniona ma być informacja (pliki, wiadomości poczty elektronicznej), niezależnie od miejsca jej przechowywania,
2. Usługa musi współdziałać przynajmniej z narzędziami Microsoft Office, Microsoft Office 365, Microsoft SharePoint i Microsoft Exchange w wersjach 2010 lub nowszych poprzez wbudowany w te produkty interfejs,
3. Możliwość kontroli, kto i w jaki sposób ma dostęp do informacji,
4. Możliwość wykorzystania zdefiniowanych polityk w zakresie szyfrowania, zarządzania tożsamością i zasadami autoryzacji,
5. Możliwość określenia uprawnień dostępu do informacji dla użytkowników i ich grup zdefiniowanych w usłudze katalogowej, w tym:

* Brak uprawnień dostępu do informacji,
* Informacja tylko do odczytu,
* Prawo do edycji informacji,
* Brak możliwości wykonania systemowego zrzutu ekranu,
* Brak możliwości drukowania informacji czy wiadomości poczty elektronicznej,
* Brak możliwości przesyłania dalej wiadomości poczty elektronicznej,
* Brak możliwości użycia opcji „Odpowiedz wszystkim” w poczcie elektronicznej.

1. Możliwość wymiany informacji objętej restrykcjami dla użytkowników pocztowych domen biznesowych spoza usługi katalogowej,
2. Możliwość wyboru restrykcji dostępu w postaci standardowych, gotowych szablonów, powstałych na bazie polityk ochrony informacji,
3. Możliwość automatyzacji pobierania aplikacji zarządzania uprawnieniami do informacji lub „cichej” instalacji w całej organizacji,
4. Możliwość wykorzystania na platformach systemu Windows 7 lub wyższych oraz na platformach mobilnych iPad i iPhone, Android, Windows Phone i Windows RT,
5. Możliwość wykorzystania mechanizmów połączenia z infrastrukturą poczty (Exchange), plików lub bibliotek SharePoint.

Podsystem usługi katalogowej

Usługa katalogowa musi zapewnić:

1. Możliwość zintegrowania jednokrotnego logowania (SSO) dla popularnych aplikacji typu SaaS,
2. Gotowe mechanizmy uwierzytelniania do aplikacji webowych dla użytkowników zewnętrznych,
3. Możliwość połączenia lub synchronizacji z usługą Active Directory wewnątrz organizacji,
4. Scentralizowane zarządzanie przydzielania dostępu do aplikacji,
5. Wbudowane możliwości uwierzytelniania wieloskładnikowego (np. jednorazowe hasła SMS przy dostępie do aplikacji webowych),
6. Zaawansowane raporty maszynowe (np. wykrywanie logowania użytkownika z różnych geolokalizacji w podobnym czasie, z podejrzanych adresów IP),
7. Samoobsługowe resetowania hasła,
8. Dostarczanie mechanizmów usługi katalogowej uwierzytelniania użytkowników,
9. Konsolę zarządzania tożsamością i dostępem.