**OPIS PRZEDMIOTU ZAMÓWIENIA**

**dostawa programu szyfrującego**

**Specyfikacja programu szyfrującego - 600 szt.**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Cecha/Parametr** | **Minimalne wymagania przez Zamawiającego** |
|  | Wymagania funkcjonalne konsoli centralnego zarządzania | 1. Konsola Centralnego Zarządzania:  * musi wspierać systemy operacyjne Microsoft Windows 2008 32-bit i 64-bit, 2012 64-bit, 2016 64-bit oraz Microsoft Windows 7/8/10 32-bit i 64-bit * musi umożliwiać centralne administrowanie klientami systemu szyfrowania danych dla systemów Microsoft Windows * musi wykorzystywać bazy danych SQL, które mają stanowić centralną bazę informacji o klientach systemu szyfrowania danych, kluczach szyfrujących oraz użytkownikach * musi współpracować z dostarczonymi przez Wykonawcę * relacyjnymi bazami danych zarówno w wersji 32-bit, jak i 64-bit, * powinna gromadzić informacje o:   1. nazwach stacji roboczych, na których jest zainstalowany klient systemu szyfrowania danych   2. dacie ostatniej modyfikacji ustawień klienta systemu szyfrowania danych   3. dacie instalacji klienta systemu szyfrowania danych   4. statusu szyfrowania zastosowanego na stacji roboczej   5. typie urządzenia na którym jest zainstalowany klient systemu szyfrowania danych   6. informacjach czy profil ustawień został zaktualizowany na stacjach roboczych   7. wersji klienta systemu szyfrowania danych   8. wersji systemu operacyjnego stacji roboczej   9. liczby użytkowników uprawnionych do logowania do klienta systemu szyfrowania danych na stacji roboczej * powinna pozwalać na generowanie dla każdej ze stacji płyty ratunkowej * musi być dostępna z poziomu przeglądarki internetowej * musi pozwalać na generowanie paczek instalacyjnych dla stacji końcowych na dwa różne sposoby:   1. instalacja ręczna na kliencie   2. instalacja „wypychana”.  1. Pakiet instalacyjny konsoli administracyjnej musi być wyposażony we wbudowane instalatory składników SQL Express, Apache oraz PHP. 2. Komunikacja pomiędzy konsolą centralną zarządzania, a serwerem proxy musi być na bezpiecznym porcie 443. 3. Administrator może w konsoli do zarządzania tworzyć wiele kluczy szyfrujących opartych o kilka algorytmów szyfrujących, co najmniej AES, DES, Blowfish. 4. Administrator powinien mieć możliwość tworzenia różnych użytkowników mających dostęp do konsoli centralnego zarządzania wraz z możliwością przypisywania im różnych ról. 5. Administrator powinien mieć możliwość tworzenia dodatkowych ról na podstawie opcji dostępnych w konsoli centralnego zarządzania. 6. Logowanie do konsoli centralnego zarządzania powinno być objęte warunkami złożoności hasła. 7. Powinna istnieć możliwość konfiguracji złożoności hasła do konsoli centralnego zarządzania, w tym:    1. ilości znaków    2. czy hasło ma zawierać wielkie, małe litery    3. czy hasło ma zawierać cyfry, znaki specjalne    4. okres ważności    5. ilość nieudanych logowań. 8. Administrator powinien mieć możliwość konfiguracji złożoności haseł dla użytkowników na stacjach roboczych. 9. Powinna istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w tym: 10. ilości znaków 11. czy hasło ma zawierać wielkie, małe litery 12. czy hasło ma zawierać cyfry, znaki specjalne 13. okres ważności 14. ilość nieudanych logowań 15. możliwość zmiany hasła 16. Administrator powinien mieć możliwość zarządzania stacjami klienckimi, które mają dostęp do sieci Internet, niezależnie od tego, gdzie komputery w danym momencie się znajdują. 17. Administrator musi mieć możliwość wykonania poniższych czynności w sposób zdalny: 18. instalacji klienta na stacji 19. zaszyfrowania/odszyfrowania stacji 20. wygenerowania klucza aktywacyjnego dla użytkownika 21. zablokowania stacji, 22. zablokowania użytkownika, 23. administrowania kluczami szyfrującymi, 24. administrowania użytkownikami, którzy mają dostęp do stacji, 25. administrowania profilem ustawień dla użytkowników, 26. administrowania profilem ustawień dla stacji roboczych 27. wymuszenia zmiany hasła 28. zarządzania wieloma organizacjami z poziomu jednej konsoli |
|  | Wymagania systemowe aplikacji klienckiej | 1. System szyfrowania danych musi wspierać instalacje aplikacji klienckiej w środowisku Microsoft Windows XP SP3/Vista/7/8/10 32-bit i 64-bit oraz w środowiskach Microsoft Windows Server 2003 32-bit i 64-bit, 2008 32-bit i 64-bit, 2012 64-bit. 2. Możliwość zainstalowania systemu szyfrowania danych w środowisku wirtualnym VMware. 3. System musi posiadać certyfikat FIPS 140-2 Level 1 |
|  | Wymagania dotyczące uwierzytelniania | 1. Konieczna jest autentykacja typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. 2. System powinien umożliwiać określenie co najmniej 127 unikalnych użytkowników, którzy będą mieć dostęp do chronionej stacji roboczej na poziomie Pre-Boot. 3. System powinien umożliwiać przetrzymywanie co najmniej 64 kluczy szyfrujących w jednym pęku kluczy (key file) 4. Dostęp do klucza powinien być chroniony przy pomocy hasła. |
|  | Wymagania dotyczące ustawień aplikacji klienckiej | 1. System szyfrowania danych powinien być dostępny przynajmniej w języku polskim i angielskim. 2. System szyfrowania danych powinien umożliwiać zarządzanie z poziomu konsoli centralnego zarządzania. 3. Hasło dla użytkowników na stacjach roboczych powinno zawierać co najmniej poniższe założenia (w przypadku wersji centralnie zarządzanej): 4. ilości znaków 5. czy hasło ma zawierać wielkie, małe litery 6. czy hasło ma zawierać cyfry, znaki specjalne 7. okres ważności 8. ilość nieudanych logowań 9. możliwość zmiany hasła 10. Defragmentacja dysku nie może mieć negatywnego wpływu na system szyfrowania. 11. System szyfrowania danych musi umożliwiać szyfrowanie nośników wymiennych w następujący sposób: 12. Sektor po sektorze, 13. Kontener. 14. Zaszyfrowany nośnik wymienny oraz nośnik CD/DVD może być odczytany także na dowolnej stacji na której nie ma zainstalowanego klienta systemu szyfrowania. Dostęp do takiego nośnika musi być udzielony po podaniu hasła. 15. Dostęp do zaszyfrowanych nośników wymiennych lub zaszyfrowanych nośników CD/DVD może być zabezpieczony hasłem. 16. System szyfrowania danych musi pozwalać na szyfrowanie wiadomości e-mail wraz z załącznikami. 17. System szyfrowania danych musi umożliwiać automatyczną deszyfrację otrzymywanych wiadomości e-mail. 18. System szyfrowania danych musi pozwalać na szyfrowanie całego tekstu aktywnego dokumentu, jego części a także zawartości schowka systemowego. 19. Zaszyfrowany tekst oraz zawartość schowka systemowego może być odczytana w wbudowanej przeglądarce. 20. Zaszyfrowany tekst może być odczytany za pomocą darmowego narzędzia dostarczanego przez producenta na stacji bez zainstalowanego klienta systemu szyfrowania. 21. System szyfrowania danych powinien umożliwiać wybór klucza szyfrującego (w przypadku posiadania wielu kluczy w pęku), który ma być używany w procesie szyfrowania. 22. System szyfrowania danych powinien umożliwiać wybór domyślnego klucza szyfrowania. 23. System szyfrowania danych powinien umożliwiać zaszyfrowanie obiektu z poziomu menu kontekstowego. 24. System szyfrowania danych powinien umożliwiać zaszyfrowanie obiektu z poziomu menu kontekstowego a następnie wysłanie go przy pomocy dedykowanego klienta pocztowego jako załącznik. 25. Możliwe jest utworzenie skrótów klawiszowych umożliwiających zaszyfrowanie/odszyfrowanie całego tekstu aktywnego dokumentu, jego części a także zawartości schowka systemowego. 26. System szyfrowania danych powinien umożliwiać tworzenie wirtualnych partycji. Dostęp do takich partycji ma być możliwy przy użyciu klucza szyfrującego lub hasła. 27. System szyfrowania danych powinien umożliwiać zdefiniowanie wielkości wirtualnej partycji, z dokładnością do 1MB. 28. System szyfrowania danych musi umożliwiać tworzenie zaszyfrowanego archiwum. Dostęp do takiego archiwum ma być możliwy przy użyciu klucza szyfrującego lub hasła. 29. System szyfrowania danych powinien umożliwiać trwałe usuwanie danych za pomocą poniższych algorytmów: 30. Guttman 31. US Department of Defence 5220.22-M (8-306. /E) 32. US Department of Defence 5220.22-M (8-306. /E, CiE) 33. Cryptographic Random Number Data 34. Dedykowana wtyczka powinna wspierać co najmniej klientów pocztowych MS Outlook 2003 lub nowszych, również dostępnych z poziomu Office 365. 35. System szyfrowania danych powinien umożliwiać automatyczne zalogowanie użytkownika do konsoli klienta systemu szyfrowania danych po uruchomieniu systemu operacyjnego. 36. System szyfrowania danych powinien umożliwiać automatyczne wylogowanie z aplikacji w przypadku bezczynności użytkownika w systemie. 37. System szyfrowania danych powinien posiadać opcję automatycznego odpytywania serwerów producenta o dostępność nowszych wersji. 38. Użytkownik powinien posiadać możliwość ręcznego sprawdzania czy dostępna jest nowsza wersja programu, z poziomu GUI. |
|  | Wymagania dotyczące szyfrowania | 1. Wymagane jest wykorzystanie do szyfrowania poniższych algorytmów szyfrowania: 2. AES (Rijndael) 3. Blowfish 4. Triple DES (3DES) 5. Administrator ma mieć możliwość sprawdzenia przed zaszyfrowaniem całej powierzchni dysku, czy nie pojawią się problemy po ponownym uruchomieniu komputera. 6. Administrator ma mieć możliwość wybrania szyfrowania dodatkowych partycji dysku (niesystemowych). 7. System szyfrowania danych powinien:  * dawać możliwość szyfrowania powierzchni dysku sektor po sektorze, * umożliwiać wstrzymanie procesu szyfrowania powierzchni dysku i jego wznowienie. Proces szyfrowania danych powinien rozpocząć się od momentu w którym został przerwany, * umożliwiać wstrzymanie procesu szyfrowania w sytuacji gdy laptop nie jest podłączony do zasilania. Proces szyfrowania powinien zostać wznowiony automatycznie po podłączeniu zasilacza, * oprócz szyfrowania całej powierzchni dysku, powinien posiadać możliwość szyfrowania pojedynczych plików, zawartości katalogów, pamięci przenośnych, wiadomości e-mail wraz z załącznikami, tekstu oraz schowka systemowego, * umożliwiać współpracę z dyskami SSD, * umożliwiać szyfrowanie danych na komputerach z UEFI. |
|  | Wymagania dotyczące sytuacji krytycznych | 1. W przypadku utraty hasła, system szyfrowania danych powinien umożliwiać Administratorowi odzyskanie dostępu do zaszyfrowanego dysku poprzez użycie zdefiniowanego wcześniej hasła administratora. 2. System szyfrowania danych powinien umożliwiać wygenerowanie płyty ratunkowej (dostępnej na nośniku wymiennym USB lub CD/DVD) z poziomu konsoli centralnego zarządzania. 3. W przypadku utraty hasła, system szyfrowania danych powinien umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku poprzez użycie otrzymanego od administratora unikalnego hasła, wygenerowanego z poziomu konsoli centralnego zarządzania. |