

Opis przedmiotu zamówienia
Część 5 Licencje oprogramowania do szyfrowania danych

Opis i minimalne parametry

Zamawiający dopuszcza sprzęt o równoważnych, nie gorszych parametrach niż te przedstawione poniżej.

Rozwiązanie oferujące zestaw prostych i intuicyjnych, a jednocześnie niezwykle skutecznych narzędzi do ochrony danych – zarówno lokalnie, jak i podczas ich przesyłania lub przenoszenia. Zaawansowana autorska technologia sprawiająca, że oprogramowanie spełnia szereg rygorystycznych standardów oraz wytycznych, wymaganych w normach do zabezpieczeń danych.

Posiadający funkcję m.in:

- Konsola centralnego zarządzania musi wspierać systemy operacyjne Microsoft Windows Server 2008 32-bit i 64-bit, 2012 64-bit, 2016 64-bit oraz Microsoft Windows 7/8/10 32-bit i 64-bit.
- Serwer centralnego zarządzania musi współpracować co najmniej z silnikami baz danych takimi jak Microsoft SQL Server 2005, 2008, 2012.
- Konsola centralnego zarządzania musi pozwalać na generowanie pakietów instalacyjnych dla stacji końcowych w formacie MSI.
- Komunikacja pomiędzy serwerem centralnego zarządzania, a serwerem proxy musi odbywać się na bezpiecznym porcie 443.
- Administrator musi mieć możliwość tworzenia i zarządzania wieloma kluczami szyfrującymi, opartymi o kilka algorytmów szyfrujących, co najmniej AES, 3DES, Blowfish.
- Administrator musi mieć możliwość tworzenia różnych użytkowników, mających dostęp do konsoli centralnego zarządzania wraz z możliwością przypisywania im różnych ról.
- Administrator musi mieć możliwość tworzenia dodatkowych ról, na podstawie opcji dostępnych w konsoli centralnego zarządzania.
- Logowanie do konsoli centralnego zarządzania powinno być objęte warunkami złożoności hasła.
- Musi istnieć możliwość konfiguracji złożoności hasła do konsoli centralnego zarządzania, w oparciu o przynajmniej:
 - a) ilość znaków,
 - b) czy hasło ma zawierać wielkie litery,
 - c) czy hasło ma zawierać małe litery,
 - d) czy hasło ma zawierać cyfry,
 - e) czy hasło ma zawierać znaki specjalne,
 - f) okres ważności,
 - g) ilość nieudanych logowań.
- Administrator musi mieć możliwość konfiguracji złożoności haseł dla użytkowników na stacjach roboczych.

- Musi istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w oparciu o przynajmniej:
 - a) ilość znaków,
 - b) czy hasło ma zawierać wielkie litery,
 - c) czy hasło ma zawierać małe litery,
 - d) czy hasło ma zawierać cyfry,
 - e) czy hasło ma zawierać znaki specjalne,
 - f) okres ważności,
 - g) ilość nieudanych logowań,
 - h) możliwość zmiany hasła
- Konsola centralnego zarządzania musi gromadzić informacje o:
 - a) nazwach stacji roboczych, na których jest zainstalowany klient systemu szyfrowania danych,
 - b) dacie ostatniej modyfikacji ustawień klienta systemu szyfrowania danych,
 - c) dacie aktywacji klienta systemu szyfrowania danych,
 - d) statusu szyfrowania,
 - e) typie urządzenia na którym jest zainstalowany klient systemu szyfrowania danych,
 - f) stanie polityki,
 - g) wersji klienta systemu szyfrowania danych,
 - h) wersji systemu operacyjnego stacji roboczej,
 - i) użytkownikach uprawnionych do logowania do oprogramowania na stacji roboczej.
- Konsola centralnego zarządzania musi pozwalać na wygenerowanie dla każdej zaszyfrowanej stacji płyty ratunkowej.
- Konsola musi być dostępna z poziomu interfejsu WWW.
- Administrator musi mieć możliwość zarządzania stacjami klienckimi, które mają dostęp do sieci Internet.
- Administrator musi mieć możliwość konfiguracji automatycznego szyfrowania pełnej powierzchni dysku po wykonanej instalacji oprogramowania.
- Konsola centralnego zarządzania musi posiadać możliwość automatycznej aktywacji licencji w ramach kont domenowych.
- Administrator musi mieć możliwość wykonania poniższych czynności w sposób zdalny:
 - a) instalacji klienta na stacji,
 - b) zaszyfrowania/odszyfrowania stacji,
 - c) wygenerowania klucza aktywacyjnego dla użytkownika,
 - d) administrowania kluczami szyfrującymi,
 - e) administrowania użytkownikami, którzy mają dostęp do stacji,
 - f) administrowania profilem ustawień dla użytkowników,
 - g) administrowania profilem ustawień dla stacji roboczych,
 - h) wymuszenia zmiany hasła,

- i) zarządzania wieloma organizacjami z poziomu jednej konsoli.

WYMAGANIA SYSTEMOWE APLIKACJI KLIENCKIEJ

- System szyfrowania danych musi wspierać instalacje aplikacji klienckiej w środowisku Microsoft Windows Vista/7/8/10 32-bit i 64-bit oraz w środowiskach Microsoft Windows Server, 2008 32-bit i 64-bit, 2012 64-bit, 2016 64-bit.
- System musi posiadać certyfikat FIPS 140-2 Level 1

WYMAGANIA DOTYCZĄCE UWIERZYTELNIANIA

- Aplikacja musi posiadać autentykację typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny.
- Aplikacja musi umożliwiać określenie, co najmniej 127 unikalnych użytkowników, którzy będą mieć dostęp do chronionej stacji roboczej na poziomie Pre-Boot.
- Aplikacja musi umożliwiać przetrzymywanie, co najmniej 64 kluczy szyfrujących w jednym pęku kluczy (key file).
- Dostęp do pliku klucza musi być chroniony przy pomocy hasła. Domyślnie wykorzystywane hasło musi być hasłem systemu Windows.
- Administrator musi posiadać możliwość modyfikacji ekranu logowania (Pre-boot).ddd

WYMAGANIA DOTYCZĄCE USTAWIEŃ APLIKACJI KLIENCKIEJ

- Aplikacja musi być dostępna, przynajmniej w języku polskim i angielskim.
- Defragmentacja dysku nie może mieć negatywnego wpływu na system szyfrowania.
- Aplikacja musi umożliwiać szyfrowanie nośników wymiennych w następujący sposób:
 - a) sektor po sektorze,
 - b) kontener.
- Zaszyfrowany nośnik wymienny oraz nośnik CD/DVD może być odczytany na dowolnej stacji, na której nie ma zainstalowanego klienta systemu szyfrowania. Dostęp do takiego nośnika musi być możliwy po podaniu hasła.
- Aplikacja musi pozwalać na szyfrowanie wiadomości e-mail wraz z załącznikami.
- Aplikacja musi umożliwiać automatyczną deszyfrację otrzymywanych wiadomości e-mail.
- Aplikacja musi pozwalać na szyfrowanie całego tekstu dokumentu, jego części, a także zawartości schowka systemowego.
- Zaszyfrowany tekst może być odczytany, za pomocą narzędzia, dostarczanego przez producenta, na stacji bez zainstalowanego klienta systemu szyfrowania.
- Aplikacja musi umożliwiać wybór klucza szyfrującego (w przypadku posiadania wielu kluczy w pęku), który ma być używany w procesie szyfrowania.
- Aplikacja musi umożliwiać wybór domyślnego klucza szyfrowania.
- Aplikacja musi umożliwiać zaszyfrowanie pliku lub folderu z poziomu menu kontekstowego.
- Możliwe jest utworzenie skrótów klawiszowych umożliwiających zaszyfrowanie/odszyfrowanie całego tekstu dokumentu, jego części, a także zawartości schowka systemowego.
- Aplikacja musi umożliwiać tworzenie wirtualnych partycji. Dostęp do takich partycji ma być możliwy przy użyciu klucza szyfrującego lub hasła.

- Aplikacja musi umożliwiać zdefiniowanie wielkości wirtualnej partycji, z dokładnością do 1MB.
- Aplikacja musi umożliwiać tworzenie zaszyfrowanego archiwum. Dostęp do takiego archiwum ma być możliwy, przy użyciu klucza szyfrującego lub hasła.
- Aplikacja musi umożliwiać trwałe usuwanie danych za pomocą poniższych algorytmów:
 - a) Guttman.
 - b) US Department of Defence 5220.22-M (8-306. /E).
 - c) US Department of Defence 5220.22-M (8-306. /E, CiE).
 - d) Kryptograficzne losowe dane liczbowe.
- Aplikacja musi posiadać dedykowaną wtyczkę co najmniej dla klientów pocztowych MS Outlook 2003 lub nowszych, również dostępnych z poziomu Office 365.
- Aplikacja musi umożliwiać automatyczne zalogowanie użytkownika do pęku klucza (key file) systemu szyfrowania danych po uruchomieniu systemu operacyjnego.
- Aplikacja musi umożliwiać automatyczne wylogowanie z aplikacji w przypadku bezczynności użytkownika w systemie.
- Aplikacja musi posiadać opcję automatycznego odpytywania serwerów producenta o dostępność nowszych wersji.
- Użytkownik musi posiadać możliwość ręcznego sprawdzania czy dostępna jest nowsza wersja programu, z poziomu GUI.

WYMAGANIA DOTYCZĄCE SZYFROWANIA

- Aplikacja musi dawać możliwość szyfrowania powierzchni dysku sektor po sektorze.
- Szyfrowanie pełnej powierzchni dysku musi umożliwiać wykorzystanie modułu TPM.
- Aplikacja musi umożliwiać wstrzymanie procesu szyfrowania powierzchni dysku i jego wznowienie. Proces szyfrowania danych powinien rozpocząć się od momentu, w którym został przerwany.
- Aplikacja musi umożliwiać wstrzymanie procesu szyfrowania, w sytuacji gdy laptop nie jest podłączony do zasilania. Proces szyfrowania musi zostać wznowiony automatycznie, po podłączeniu zasilacza.
- Wymagane jest wykorzystanie kluczy szyfrujących, utworzonych przy użyciu jednego z poniższych algorytmów szyfrowania:
 - a) AES (Rijndael).
 - b) Blowfish.
 - c) Triple DES (3DES).Ghjhj
- Aplikacja musi umożliwiać współpracę z dyskami SSD.
- Aplikacja musi umożliwiać współpracę z dyskami sprzętowo szyfrowanymi, działającymi w technologii TCG OPAL.
- Aplikacja musi umożliwiać szyfrowanie danych na komputerach z UEFI.
- Administrator musi mieć możliwość sprawdzenia, przed zaszyfrowaniem całej powierzchni dysku, czy nie pojawią się problemy po ponownym uruchomieniu komputera.
- Administrator musi mieć możliwość opcjonalnego szyfrowania niesystemowych partycji dysku.

WYMAGANIA DOTYCZĄCE SYTUACJI KRYTYCZNYCH

- W przypadku utraty hasła, aplikacja musi umożliwiać Administratorowi odzyskanie dostępu do zaszyfrowanego dysku poprzez użycie zdefiniowanego wcześniej hasła administratora.
- W przypadku utraty hasła, aplikacja musi umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku, poprzez użycie otrzymanego od administratora jednorazowego hasła, wygenerowanego z poziomu konsoli centralnego zarządzania.