Załącznik nr 1

SPECYFIKACJA OPROGRAMOWANIA SYSTEMOWEGO DO SZYFROWANIA DANYCH NA KOMPUTERACH MOBILNYCH

WYMAGANIA FUNKCJONALNE DOTYCZĄCE KONSOLI CENTRALNEGO ZARZĄDZANIA

1. Konsola centralnego zarządzania musi wspierać systemy operacyjne Microsoft Windows Server 2003 32-bit i 63-bit, 2008 32-bit i 64-bit, 2012 64-bit oraz Microsoft Windows XP SP3/Vista/7 32-bit i 64-bit.
2. Konsola centralnego zarządzania musi umożliwiać centralne administrowanie klientami systemu szyfrowania danych dla systemów Microsoft Windows.
3. Konsola centralnego zarządzania dzięki wykorzystaniu bazy danych SQL ma stanowić centralną bazę informacji o klientach systemu szyfrowania danych, kluczach szyfrujących oraz użytkownikach.
4. Konsola centralnego zarządzania musi współpracować z bazą danych Microsoft SQL Server 2005, Microsoft SQL Server 2008, Microsoft SQL Server 2008 R2, Microsoft SQL Server 2012 zarówno w wersji 32-bit i 64-bit oraz z Microsoft SQL Server 2005 Express Edition, Microsoft SQL 2008 Express Edition, Microsoft SQL Server 2012 Express Edition zarówno w wersji 32-bit i 64-bit.
5. Środowisko wymaga instalacji następujących składników:
    a. MS SQL w wersjach pełnych i Express,
    b. Apache od wersji 2 lub IIS od wersji 6,
    c. PHP od wersji 5.3.
6. Pakiet instalacyjny konsoli administracyjnej musi być wyposażony we wbudowane instalatory składników SQL Express, Apache oraz PHP.
7. Konsola centralnego zarządzania musi pozwalać na generowanie paczek instalacyjnych dla stacji końcowych na dwa różne sposoby:
    a. Instalacja ręczna na kliencie,
    b. Instalacja wypychana.
8. Konsola do zarządzania musi wymagać dostępu do Internetu na porcie 443 (do komunikacji z serwerem proxy w chmurze obliczeniowej).
9. Administrator powinien w konsoli do zarządzania mieć możliwość tworzyć wiele kluczy szyfrujących opartych o kilka algorytmów szyfrujących, co najmniej AES, DES, Blowfish.
10. Administrator powinien mieć możliwość tworzenia różnych użytkowników mających dostęp do konsoli centralnego zarządzania wraz z możliwością przypisywania im różnych ról.
11. Administrator powinien mieć możliwość tworzenia dodatkowych ról na podstawie opcji dostępnych w konsoli centralnego zarządzania.
12. Logowanie do konsoli centralnego zarządzania powinno być objęte warunkami złożoności hasła.
13. Hasło do konsoli centralnego zarządzania powinno zawierać co najmniej poniższe założenia:
    a. Ilość znaków,
    b. Ilość wielkich liter,
    c. Ilość małych liter,
    d. Ilość znaków numerycznych,
    e. Ilość znaków specjalnych,
    f. Ważność hasła,
    g. Ilość nieudanych logowań.
14. Administrator powinien mieć możliwość konfiguracji złożoności haseł dla użytkowników na stacjach roboczych.
15. Hasło dla użytkowników na stacjach roboczych powinno zawierać co najmniej poniższe założenia:
    a. Ilość nieudanych logowań,
    b. Możliwość zmiany hasła,
    c. Ważność hasła,
    d. Ilość znaków,
    e. Ilość wielkich liter,
    f. Ilość małych liter,

g. Ilość znaków numerycznych,
h. Ilość znaków specjalnych.

16. Konsola centralnego zarządzania powinna 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 instalacji klienta systemu szyfrowania danych,
    d. statusu szyfrowania zastosowanego na stacji robocze ,
    e. typie urządzenia na którym jest zainstalowany klient systemu szyfrowania danych,
    f. informacjach czy profil ustawień został zaktualizowany na stacjach roboczych,
    g. wersji klienta systemu szyfrowania danych,
    h. wersji systemu operacyjnego stacji roboczej,
    i. liczby użytkowników uprawnionych do logowania do klienta systemu szyfrowania danych na stacji roboczej.
17. Konsola centralnego zarządzania powinna pozwalać na generowanie dla każdej ze stacji płyty ratunkowej.
18. Konsola musi być dostępna z poziomu przeglądarki internetowej.
19. Administrator powinien mieć możliwość zarządzania stacjami klienckimi, które mają dostęp do sieci Internet, niezależnie od tego, gdzie komputery w danym momencie się znajdują.
20. 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. zablokowania stacji,
    e. zablokowania użytkownika,
    f. administrowania kluczami szyfrującymi,
    g. administrowania użytkownikami, którzy mają dostęp do stacji,
    h. administrowania profilem ustawień dla użytkowników,
    i. administrowania profilem ustawień dla stacji roboczych
    j. wymuszenia zmiany hasła,
    k. zarządzania wieloma organizacjami z poziomu jednej konsoli.

WYMAGANIA SYSTEMOWE

1. System szyfrowania danych musi wspierać instalacje aplikacji klienckiej w środowisku Microsoft Windows XP SP3/Vista/7/8 32-bit i 64-bit oraz w środowiskach Microsoft Windows Server 2003 32-bit i 64-bit, 2008 32-bit i 64-bit.
2. Użytkownik musi mieć 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 (zależnie od rodzaju licencji).
3. Hasło dla użytkowników na stacjach roboczych powinno zawierać co najmniej poniższe założenia (w przypadku wersji centralnie zarządzanej):
    a. Ilość nieudanych logowań,

b. Możliwość zmiany hasła,
c. Ważność hasła,
d. Ilość znaków,
e. Ilość wielkich liter,
f. Ilość małych liter,
g. Ilość znaków numerycznych,
h. Ilość znaków specjalnych.

4. System szyfrowania danych powinien umożliwiać wykonanie defragmentacji dysku również przy pomocy narzędzi wbudowanych w system operacyjny.
5. System szyfrowania danych musi umożliwiać transparentne szyfrowanie nośników CD/DVD oraz nośników wymiennych.
6. System szyfrowania danych musi umożliwiać szyfrowanie nośników wymiennych w następujący sposób:
   a. Sektor po sektorze,
   b. Kontener.
7. 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.
8. Dostęp do zaszyfrowanych nośników wymiennych lub zaszyfrowanych nośników CD/DVD może być zabezpieczony hasłem.
9. System szyfrowania danych musi pozwalać na szyfrowanie wiadomości e-mail w locie wraz z załącznikami.
10. System szyfrowania danych musi umożliwiać automatyczną deszyfrację otrzymywanych wiadomości e-mail.
11. System szyfrowania danych musi pozwalać na szyfrowanie całego tekstu aktywnego dokumentu, jego części a także zawartości schowka systemowego.
12. Zaszyfrowany tekst oraz zawartość schowka systemowego powinna być możliwa do odczytania we wbudowanej przeglądarce.
13. Zaszyfrowany tekst może być odczytany za pomocą darmowego narzędzia dostarczanego przez producenta na stacji bez zainstalowanego klienta systemu szyfrowania.
14. System szyfrowania danych powinien umożliwiać wybór klucza szyfrującego (w przypadku posiadania wielu kluczy w pęku), który ma być używany w procesie szyfrowania.
15. System szyfrowania danych powinien umożliwiać wybór domyślnego klucza szyfrowania.
16. System szyfrowania danych powinien umożliwiać zaszyfrowanie obiektu z poziomu menu kontekstowego.
17. System szyfrowania danych powinien umożliwiać zaszyfrowanie obiektu z poziomu menu kontekstowego a następnie wysłanie go przy pomocy dedykowanego klienta pocztowego, jako załącznik.
18. Możliwe jest utworzenie skrótów klawiszowych umożliwiających zaszyfrowanie/odszyfrowanie całego tekstu aktywnego dokumentu, jego części a także zawartości schowka systemowego.
19. System szyfrowania danych powinien umożliwiać tworzenie wirtualnych partycji. Dostęp do takich partycji ma być możliwy przy użyciu klucza szyfrującego lub hasła.
20. System szyfrowania danych powinien umożliwiać zdefiniowanie wielkości wirtualnej partycji, z dokładnością do 1MB.
21. System szyfrowania danych musi umożliwiać tworzenie zaszyfrowanego archiwum. Dostęp do takiego archiwum ma być możliwy przy użyciu klucza szyfrującego lub hasła.
22. System szyfrowania danych musi umożliwiać generowanie dodatkowych kluczy szyfrujących z możliwością wyboru algorytmów szyfrowania.
23. Użytkownik, przesyłając klucz szyfrujący, ma mieć możliwość zdefiniowania liczby dalszych udostępnień dla konkretnego klucza.
24. Wygenerowany klucz szyfrujący powinien być udostępniony co najmniej 255 razy.
25. System szyfrowania danych powinien 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. Cryptographic Random Number Data.
26. System szyfrowania danych powinien umożliwiać bezpieczną wymianę kluczy szyfrujących pomiędzy użytkownikami (użytkownicy mogą żądać kluczy szyfrujących/przesyłać je dalej) przy użyciu algorytmu RSA oraz klucza publicznego.

27. Możliwość żądania kluczy szyfrujących/przesyłania ich dalej powinna być możliwa także z poziomu wspieranego klienta pocztowego, za pomocą dedykowanej wtyczki.
28. Dedykowana wtyczka powinna wspierać co najmniej klientów pocztowych MS Outlook 2003 lub nowszych, również dostępnych z poziomu Office 365.
29. System szyfrowania danych powinien umożliwiać automatyczne zalogowanie użytkownika do konsoli klienta systemu szyfrowania danych po uruchomieniu systemu operacyjnego.
30. System szyfrowania danych powinien umożliwiać automatyczne wylogowanie z aplikacji w przypadku bezczynności systemu.
31. System szyfrowania danych powinien posiadać opcję automatycznego odpytywania serwerów producenta o dostępność nowszych wersji.
32. Użytkownik powinien posiadać możliwość ręcznego sprawdzania czy dostępna jest nowsza wersja programu, z poziomu GUI.
33. System szyfrowania danych powinien umożliwiać określenie akcji podjętej w przypadku rozszyfrowania obiektu w tym co najmniej:
    a. Usunięcia zaszyfrowanego obiektu,
    b. Pozostawienia pliku w formie zaszyfrowanej,
    c. Zapytania o akcję.

WYMAGANIA DOTYCZĄCE SZYFROWANIA

1. System szyfrowania danych powinien dawać możliwość szyfrowania powierzchni dysku sektor po sektorze.
2. System szyfrowania danych powinien umożliwiać wstrzymanie procesu szyfrowania powierzchni dysku i jego wznowienie. Proces szyfrowania danych powinien rozpocząć się od momentu w którym został przerwany.
3. System szyfrowania danych powinien umożliwiać wstrzymanie procesu szyfrowania w sytuacji gdy laptop nie jest podłączony do zasilania. Proces szyfrowania powinien zostać wznowiony automatycznie po podłączeniu zasilacza.
4. System szyfrowania danych, 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.
5. Wymagane jest wykorzystanie do szyfrowania poniższych algorytmów szyfrowania:
    a. AES (Rijndael),
    b. Blowfish,
    c. Triple DES (3DES).
6. System szyfrowania danych powinien umożliwiać współpracę z dyskami SSD.
7. System szyfrowania danych powinien umożliwiać szyfrowanie danych na komputerach z UEFI
8. Użytkownik ma mieć możliwość sprawdzenia przed zaszyfrowaniem całej powierzchni dysku, czy nie pojawią się problemy po ponownym uruchomieniu komputera.
9. Użytkownik ma mieć możliwość wybrania szyfrowania dodatkowych partycji dysku (niesystemowych).

WYMAGANIA DOTYCZĄCE SYTUACJI KRYTYCZNYCH

1. W przypadku utraty hasła, system szyfrowania danych powinien umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku poprzez użycie zdefiniowanego wcześniej hasła administratora. System ma wymagać zapisania hasła administratora na zewnętrznym nośniku lub zasobie sieciowym.
2. System szyfrowania danych powinien umożliwiać wygenerowanie płyty ratunkowej (dostępnej na nośniku wymiennym USB lub CD/DVD).
3. System szyfrowania danych powinien umożliwiać wygenerowanie płyty ratunkowej (dostępnej na nośniku wymiennym USB lub CD/DVD) także z poziomu konsoli centralnego zarządzania (w przypadku wersji centralnie zarządzanej).
4. W przypadku utraty hasła, system szyfrowania danych powinien umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku poprzez użycie otrzymanego od administratora unikalnego hasła OTP (One Time Password), wygenerowanego z poziomu konsoli centralnego zarządzania (w przypadku wersji centralnie zarządzanej).