Wstęp

Cel

Celem niniejszego dokumentu jest przedstawienie wymagań nakładanych na system przeznaczonego do dzielenia się plikami zabezpieczonymi kluczem symetrycznym. W opracowaniu oparto się na normach,zaleceniach lub ich szkicach w momencie tworzenia tego dokumentu.

Wprowadzenie

Przedstawiony poniżej profil zabzpieczeń definiuje wymagania bezpieczeństwa dla systemu dzielenia się zabezpieczonymi plikami pomiędzy użytkownikami systemu. Przez "system do dzielenia się zabezpieczonymi plikami" rozumie się system realizujący szyfrowanie/deszyfrowanie pliku z wykorzystaniem do tego celu klucza symetrycznego wygenerowanego przez nadawcę, natomiast proces przekazania klucza jednemu bądź wielu odbiorcom odbywa się z wykorzystaniem protokołu Diffiego-Hellmana. Właściciel współdzielonego pliku w niniejszym systemie może predefiniować jego czas życia — po jego upływie zostaje on usunięty.

Identyfikacja

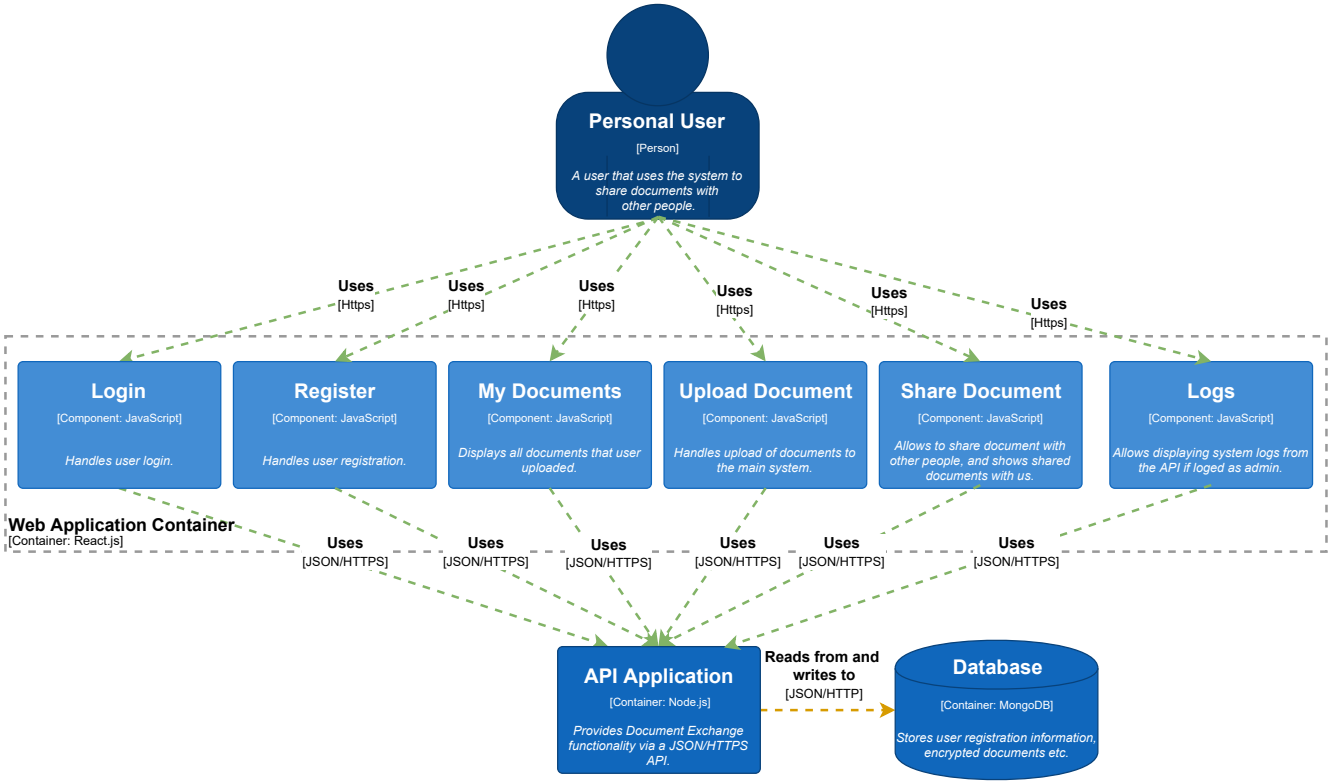
Tytuł: Profil zabezpieczeń - system do dzielenia się zabezpieczonymi plikami
Autorzy: Krzysztof Kołodziejczak, Patryk Piotrowski, Patryk Prokurat, Jakub Dyba, Artur Ziemba, Bartosz Gawdzis, Albert Liberski, Mateusz Gnyp
Status głosowania: CC Version: 1.0 (Grudzień 2018)
Ogólny status: Draft
Numer wersji: 1.0
Słowa kluczowe: szyfrowanie/deszyfrowanie danych, współdzielenie danych, klucz symetryczny, klucz asymetryczny, protokół Diffiego-Hellmana.

Opis przedmiotu oceny

Ta część profilu zabezpieczeń zawiera opis przedmiotu oceny (TOE), rodzaj produktu, który prezentuje, jak również opis ogólnej funkcjonalności TOE. Przedstawiona funkcjonalność, podlegająca ocenie, dotyczy szyfrowania/deszyfrowania danych z wykorzystaniem klucza symetrycznego, przekazania klucza za pomocą protokołu Diffiego-Hellmana i ustanawiania bezpiecznego połączenia klienta z serwerem z wykorzystaniem połączenia HTTPS.

Opis TOE

Przedmiotem oceny, rozważanym w niniejszym dokumencie, jest pięć komponentów: "Login, Register, My Documents, Upload Document, Exchange Keys", wchodzące w skład Document Exchange System — system dzielenia się zaszyfrowanymi plikami pomiędzy użytkownikami.



Component diagram for the Web Application Container

Login - komponent odpowiada za:

- logowanie użytkownika do systemu po poprawnym jego uwierzytelnieniu;
- logowanie z wykorzystaniem protokołu HTTPS.

Register - komponent odpowiada za:

- rejestrację użytkownika do systemu (użytkownik podaje login, hasło, powtórzone hasło i adres e-mail);
- weryfikację poprawności wprowadzonych danych;
- tworzenie nowego konta użytkownika po uprzednim spełnieniu wymagań dotyczących rejestracji;
- rejestrację z wykorzystaniem protokołu HTTPS.

My Documents - komponent odpowiada za:

- zarządzanie dokumentami, których właścicielem jest zalogowany użytkownik;
- nadawanie uprawnień dostępu do poszczególnych, zaszyfrowanych dokumentów konkretnym użytkownikom;
- komunikację z użytkownikiem z wykorzystaniem protokołu HTTPS.

Upload Document - komponent odpowiada za:

- wysyłanie pliku uprzednio zaszyfrowanego kluczem symetrycznym;
- pobranie od użytkownika daty i godziny wygaśnięcia pliku;
- zarządzanie przez użytkownika listą osób uprawnionych do korzystania z pliku;
- komunikację z użytkownikiem z wykorzystaniem protokołu HTTPS.

Share Document - komponent odpowiada za:

- wymianę klucza pomiędzy użytkownikami za pomocą protokołu Diffiego-Hellmana;

- pobranie od użytkownika klucza szyfrującego plik;
- pobranie od użytkownika docelowego odbiorcy, któremu zostanie przesłany klucz szyfrujący plik z wykorzystaniem protokołu Diffiego-Hellmana (służy do ustalenia wspólnego tajnego klucza przy użyciu publicznych środków komunikacji);
- zaszyfrowanie klucza do pliku ustalonym wcześniej przez obie strony za pomocą protokołu Diffiego-Hellmana tajnym kluczem;
- odszyfrowanie klucza do pliku w celu skorzystania z udostępnionych zasobów.

Logs - komponent odpowiada za:

- zapisywanie i przechowywanie logów systemowych dostępnych do podglądu dla użytkownika typu Administrator.

Środowisko zabezpieczeń TOE

Aktywa

W tej sekcji opisano wszystko aktywa chronione przez TOE.

A. Dokument

Dokument do szyfrowania/deszyfrowania, który może się składać z:

- pojedynczego dokumentu elektronicznego,
- wielu dokumentów elektronicznych.

Dane zawarte w dokumencie muszą być chronione przed utratą integralności i/lub poufności.

A. Dane do szyfrowania

Dane do szyfrowania są informacją, z którą związany jest szyfrogram. Zawierają one szyfrowany dokument i informacje o atrybutach szyfrogramu.

A. Atrybuty szyfrowane

Atrybuty szyfrowane są to dane, które zostały szyfrowane w tym samym czasie, co dokument. Atrybuty te dostarczają weryfikatorowi informację odnośnie szyfrogramu oraz okoliczności, w jakich został on zrealizowany.

Atrybuty te muszą być chronione przed utratą integralności lub poufności.

A. Rejestr zdarzeń

Informacje zapisane chronologicznie o zdarzeniach i działaniach dotyczących TOE. Wpis w dzienniku zawiera informacje o kodzie błędu, daty i godziny wystąpienia błędu, identyfikator użytkownika i dodatkowe informacje.

A. Szyfrogram

Szyfrogram jest zagregowanym zbiorem danych, zawierającym:

- komplet danych do szyfrowania;
- dodatkowe informacje ułatwiające odszyfrowanie szyfrogramu, w tym atrybuty szyfrogramu.

Aktywa te muszą być chronione przez TOE w trakcie ich tworzenia i przed ich przekazaniem podmiotowi szyfrującemu.

A. Dane logowania

Informacje możliwe do uwierzytelnienia osoby, które są podawane podczas rejestracji/logowania podmiotu. TOE musi zapewnić ochronę przetwarzanych danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną. Bezpieczeństwo informacji należy rozumieć jako zachowanie:

- poufności - zapewnia, że informacja nie jest udostępniania lub ujawniana nieautoryzowanym osobom, podmiotom, procesom;
- integralności - zapewnia, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- dostępności - zapewnia bycie osiągalnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot;
- rozliczalności - zapewnia, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
- autentyczności - zapewnia, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana;
- niezaprzeczalności - oznacza brak możliwości wyparcia się swojego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w wymianie;
- niezawodności - zapewnia spójność zamierzonych zachowań i skutków.

A. Polityka szyfrowania

Polityki szyfrowania definiują reguły, które powinny być stosowane podczas składania szyfrowania danych i ich deszyfrowania. Lista polityk udostępniania, przesyłania klucza deszyfrującego lub szyfrowania przez użytkownika, zarządzana przez administratora TOE, musi być chroniona przed utratą integralności.

Dane te muszą być chronione przed utratą integralności.

A. Zgodność formatu dokumentu z jego przeglądarką

Mechanizmy zaimplementowane w TOE zarządzają parametrami, które pozwalają TOE na uruchomienie właściwej przeglądarki, obsługującej format wskazanego dokumentu i poprawne zaprezentowanie jego treści podmiotowi korzystającemu z systemu, udostępnianemu zasobów, szyfrującemu lub deszyfrującemu.

Parametry te muszą być chronione przed utratą integralności.

A. Dane uwierzytelniające podmiotu systemu

Są to dane, które pozwalają podmiotowi na uwierzytelnienie się (po zalogowaniu się do systemu za pomocą loginu i hasła). Pomyślnie zakończenie uwierzytelnienia upoważnia do korzystania z zasobów dostępnych w systemie.

Dane te muszą być chronione przed utratą integralności i poufności

Podmioty systemu

S. Użytkownicy

Podmiot udostępniający zaszyfrowane zasoby do sieci, przekazujący uprawnienia jak i klucz deszyfrujący innym podmiotom do pobrania dzielonych zasobów w systemie, wykonywanych zgodnie z polityką szyfrowania dla jednego lub kilku dokumentów.

S. Administrator

Administrator posiada niezbędne środki i jest przeszkolony w zakresie wykonywania wszelkich operacji na TOE, za które jest odpowiedzialny: wykonuje stałą obsługę systemu teleinformatycznego, w tym tworzy kopie zapasowe, zdalnie umieszcza kopie archiwów oraz bieżące kopie zapasowe poza podstawowym obszarem lokalizacji TOE. Podmiot posiada pełne zaufanie w odniesieniu do każdej polityki bezpieczeństwa wdrażanej do systemu. Jednostka jest przeszkolona w zakresie wykonywanych operacji na TOE.

Założenia

AE. Konfiguracja TOE

Zakłada się, że TOE jest poprawnie zainstalowany i skonfigurowany (zainstalowana najnowsza wersja systemu operacyjnego, odpowiednio skonfigurowana polityka bezpieczeństwa, aktualna wersja oprogramowania antywirusowego).

AE. Uwierzytelnienie

Zakłada się, że środowisko związane z TOE umożliwia użytkownikom na uwierzytelnienie się poprzez wprowadzenie indywidualnych danych uwierzytelniających.

AE. Bezpieczna komunikacja

Zakłada się, że zapewniona jest poufność i integralność przesyłanych danych w komunikacji między serwerem a klientem.

AE. Rejestracja zdarzeń

Zakłada się, że środowisko TOE rejestruje w dzienniku zdarzeń wszystkie niepoufne zdarzenia istotne z punktu widzenia bezpieczeństwa.

AE. Ochrona danych

Zakłada się, że dane utworzone przez środowisko są zabezpieczone oraz archiwizowane w sposób ciągły.

AE. Aktualizacje zabezpieczeń

Zakłada się, że środowisko jest regularnie aktualizowane w celu wyeliminowania defektów w zabezpieczeniach wykrytych w oprogramowaniu wchodzących w skład środowiska.

Zagrożenia

Ta sekcja opisuje zagrożenia mające wpływ na TOE.

T. Uszkodzenie TOE

Jeszcze przed rozpoczęciem procesu szyfrowania bądź deszyfrowania pliku uszkodzeniu bądź awarii może ulec jedna lub kilka funkcji i/lub jeden lub kilka parametrów TOE.

Przypadkowe uszkodzenie funkcji i/lub parametrów TOE może nastąpić na przykład wtedy, gdy przesłany plik był niekompletny bądź nastąpiła awaria algorytmu odpowiedzialnego za szyfrowanie. Uszkodzenie może prowadzić do:

- uszkodzenia zaszyfrowanego pliku;
- uszkodzenia deszyfrowanych danych;
- modyfikacji zawartości pliku bez zgody i wiedzy użytkownika.

T. Nieautoryzowany dostęp do zasobów serwera bazodanowego

Atakujący może uzyskać nieautoryzowany dostęp do zasobów serwera bazodanowego w sposób bezpośredni (poprzez interfejs apache sql) bądź z wykorzystaniem luk w aplikacji serwerowej polegającym na modyfikacji zapytania bazodanowego - sql injection.

T. Atak słownikowy i atak metodą pełnego przeglądu

Atakujący może uzyskać hasło do konta użytkownika serwisu, co pozwoli mu na korzystanie ze wszystkich funkcjonalności TOE bez wiedzy i zgody użytkownika.

T. Nieautoryzowane przejęcie sesji użytkownika

Atakujący może uzyskać i przejąć od zalogowanego użytkownika id sesji zalogowania przez co uzyskuje dostęp do udostępnionych plików innym użytkownikom.

T. Nieupoważniony dostęp

Atakujący może korzystać ze wszystkich funkcjonalności TOE pomimo braku zalogowania do systemu.

T. Słaby zestaw algorytmów

Zastosowanie słabych algorytmów szyfrowych podczas tworzenia szyfrogramu.

T. Nieautoryzowany dostęp do prywatnych plików

Atakujący może pobrać prywatne pliki, które nie były dla niego udostępnione.

T. Przypadkowe usunięcie pliku

Użytkownik przypadkowo usuwa udostępniany plik, na skutek czego reszta użytkowników traci dostęp do dzielonych zasobów.

T. Nieautoryzowane podsłuchanie użytkowników podczas operacji dzielenia się kluczem deszyfrującym

Atakujący podsłuchuje komunikaty pomiędzy użytkownikami, którzy dzielą się kluczem deszyfrującym służącym do odszyfrowania pliku.

T. Nieautoryzowane podsłuchiwanie operacji logowania użytkownika do systemu

Atakujący śledzi dane wprowadzane przez użytkownika podczas logowania - login, hasło; które może przechwycić i wykorzystać do nieuprawnionego zalogowania się do systemu.

T. Modyfikacja uprawnień do zasobów

Złośliwy użytkownik może w niedozwolony sposób dodać lub usunąć jednego bądź kilku użytkowników uprawnionych do pobrania określonego pliku.

T. Wyciek danych

W wyniku awarii systemu może dojść do wycieku poufnych i wrażliwych danych - dane logowania, udostępniane pliki, itp.

T. Przejęcie konta administratora

Atakujący może przejąć konto administracyjne poprzez odgadnięcie danych dostępu, np: za pomocą metody brute-force albo w wyniku działania odkrycia luki systemowej.

Polityki bezpieczeństwa

W tym rozdziale określono zasady natury organizacyjnej, mające zastosowanie do TOE.

P. Przerwanie procesu

Podmiot szyfrujący/deszyfrujący musi mieć możliwość przerwania procesu szyfrowania/deszyfrowania przed aktywacją klucza szyfrującego/deszyfrującego.

P. Integralność danych użytkownika

TOE musi chronić integralność wszystkich danych (lista zaszyfrowanych dokumentów, lista uprawnionych do pobrania zasobów), przychodzących od użytkownika.

P. Eksport szyfrogramu

Po zakończeniu procesu szyfrowania powstały w jego wyniku szyfrogram dokumentu musi zostać przekazany przez TOE podmiotowi szyfrującemu/deszyfrującemu.

P. Zarządzanie

TOE musi pozwolić podmiotowi szyfrującemu/deszyfrującemu oraz administratorowi na zarządzanie politykami szyfrowania oraz tabelą wiążącą format dokumentu z jego przeglądarką.

P. Algorytmy kryptograficzne

Do zarządzania kluczami (tj. generowania, udostępniania, niszczenia, korzystania i przechowywania kluczy) oraz udostępniania algorytmów szyfrowych (funkcji szyfrowania, deszyfrowania, podpisywania, obliczania skrótów, wymiany kluczy oraz generowania liczb losowych) stosowane mogą być tylko te algorytmy kryptograficzne (metody i ich implementacje), które spełniają wymagania określone w Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. (Dz. U. Nr 128, poz.1094 z dnia 12 sierpnia 2002 r.) oraz w Ustawie z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. 1999 nr 11 poz. 95, wersja ujednolicona) i

zatwierdzona przez odpowiednie instytucje certyfikujące przy wysokim poziomie siły funkcji zabezpieczającej lub przynajmniej zgodne z FIPS 140 poziom 2 lub wyższy.

Cele zabezpieczeń

Cele zabezpieczeń dla TOE

O. Ochrona kanału komunikacyjnego

TOE zapewnia, że dane przesyłane między serwerem WWW a przeglądarką są chronione przed nieautoryzowanym dostępem. TOE musi zagwarantować, że nie ulegną modyfikacji w trakcie przbywania drobi między węzłami końcowymi kanału komunikacyjnego.

O. Uwierzytelnienie użytkownika

TOE powinien zapewnić, aby użytkownik miał możliwość wprowadzenia danych uwierzytelniających (uwierzytelnienia się) przed uzyskaniem dostępu do prywatnych oraz udostępnionych plików.

O. Integralność danych do szyfrowania

TOE musi zapewnić integralność różnych reprezentacji danych przeznaczonych do zaszyfrowanie od momentu ich sformatowania do momentu utworzenia szyfrogramu.

O. Ochrona procesów

TOE musi zapewnić ochronę przed ingerencją dowolnych niezaufanych procesów, urządzeń peryferyjnych i kanałów komunikacyjnych oraz intruzuów w pracę tych procesów, które wykorzystywane są podczas szyfrowania/deszyfrowania, zgodnie ze wskazaniem zawartym w żądaniu utworzenia szyfrogramu.

O. Poufność danych uwierzytelniających

TOE musi zapewnić poufność danych uwierzytelniających należących do podmiotu szyfrującego/deszyfrującego.

O. Zatwierdzone algorytmy

TOE powinien zapewnić, aby były stosowane tylko te algorytmy szyfrowe, które należą do zbioru zatwierdzonych algorytmów i parametrów stosowanych podczas tworzenia szyfrogramu; w szczególności, aby format był zgodny z formatami wskazanymi w Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. (Dz. U. Nr 128, poz.1094 z dnia 12 sierpnia 2002 r.).

O. Hashowanie hasła wraz z domieszką

TOE powinien szyfrować wrażliwe dane logowania użytkowników hashem bcrypt wraz z zastosowaniem domieszki (salt).

O. Szyfrowane dokumenty

TOE powinien przechowywać w bazie danych jedynie dokumenty w formie zaszyfrowanej za pomocą algorytmu AES-256. Klucz deszyfrujący znany jest jedynie użytkownikowi, który jest właścicielem pliku.

O. Zgoda użytkownika

TOE powinien udostępnić podmiotowi szyfrującemu/deszyfrującemu mechanizm umożliwiający mu (w sposób dobrowolny i jednoznaczny) wyrażenie zgody na zainicjowanie procesu wyboru dokumentu w celu utworzenia szyfrogramu bądź pobrania i odszyfrowania.

TOE powinien zażądać od podmiotu szyfrującego/deszyfrującego nietrywialnego zainicjowania procesu, wykluczającego jakąkolwiek przypadkowość tej decyzji; żaden inny proces w systemie nie może zainicjować tego procesu.

O. Udostępnienie pliku innemu użytkownikowi

TOE powinien zapewnić podmiotowi będącemu właścicielem danego pliku na udostępnienie wybranego zasobu odbiorcy wskazanego przez nadawcę.

O. Przesyłanie klucza deszyfrującego

TOE powienien zapewnić bezpieczne przekazanie klucza szyfrującego wskazanemu przez niego odbiorcy. Proces przekazania klucza powinien być uzgadniany pomiędzy nadawcą a odbiorcą algorytmem Diffie-Hellmana, natomiast TOE ma zapewnić bezpieczny kanał transmisyjny.

O. Ustawienie czasu wygaśnięcia pliku

TOE powinien zapewnić uprawnienia właściciela pliku na jednoznaczne wskazanie terminu wygaśnięcia pliku. Po upływie czasu wygaśnięcia TOE powinien przeprowadzić operację trwałego usunięcia pliku.

O. Zbiór dokumentów

Po wyrażeniu przez podmiot szyfrujący zgody na szyfrowanie, TOE musi gwarantować, że przetwarzany dokument rzeczywiście odpowiada dokładnie wybranemu dokumentowi przeznaczonego do szyfrowania.

O. Blokowanie ataków na TOE

TOE musi zapewnić mechanizm blokowania ataków (wiele nieudanych prób logowania, DDoS) poprzez oflagowanie adresu IP bądź identyfikatora atakującego i zablokowanie kanału komunikacyjnego z podmiotem atakującym.

O. Zgodność uprawnień do dokumentów

TOE musi zapewnić zgodność, która potwierdza uprawnienia użytkownika do pobrania wybranego dokumentu.

Cele zabezpieczeń dla środowiska

OE. Bezpieczna komunikacja

W celu ustanowienia bezpiecznego kanału komunikacji, komunikacja pomiędzy serwerem WWW, a przeglądarką WWW odbywa się z zastosowaniem protokołu HTTPS z TLS.

OE. Wiarygodni użytkownicy

Upoważnieni użytkownicy rzetelnie wykonują swoje zadania.

OE. Wiarygodni administratorzy

Upoważnieni administratorzy rzetelnie wykonują swoje zadania.

OE. Konfiguracja TOE

TOE musi być poprawnie zainstalowany i skonfigurowany tak, aby zaraz po uruchomieniu przechodził w bezpieczny stan.

OE. Moduły kryptograficzne

TOE musi korzystać tylko z tych usług kryptograficznych, udostępnianych przez środowisko teleinformatyczne, które spełniają wymagania określone w Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. (Dz. U. Nr 128, poz.1094 z dnia 12 sierpnia 2002 r.) oraz Ustawie z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. 1999 nr 11 poz. 95, wersja ujednolicona) i zatwierdzone przez odpowiednie instytucje certyfikujące przy wysokim poziomie siły funkcji zabezpieczającej lub przynajmniej zgodne z FIPS 140 poziom 2 lub wyższy.

OE. Bezpieczeństwo fizyczne

Środowisko musi zapewniać akceptowalny poziom bezpieczeństwa fizycznego tak, aby nie było możliwe manipulowanie TOE.

OE. Obecność użytkownika

Podmiot szyfrujący/deszyfrujący powinien pozostać obecny między momentem wyrażenia przez niego zamiaru szyfrowania, a momentem kiedy wprowadza dane szyfrujące.

OE. Tworzenie danych na potrzeby audytu

Środowisko związane z TOE zapewni możliwość zapisywania zdarzeń związanych z bezpieczeństwem TOE w rejestrze zdarzeń w sposób jednoznacznie wiążący zdarzenie z użytkownikiem, który był przyczyną wystąpienia tego zdarzenia lub zdarzenie nastąpiło podczas korzystania przez niego z TOE.

OE. Ochrona danych rejestrowanych na potrzeby audytu

Środowisko związane z TOE zapewni możliwość ochrony informacji gromadzonej na potrzeby audytu.

OE. Przeglądanie danych rejestrowanych na potrzeby audytu

Środowisko związane z TOE zapewni możliwość selektywnego przeglądania informacji zgromadzonej w rejestrze zdarzeń.

OE. Aktualizacje zabezpieczeń

Środowisko jest automatycznie aktualizowane w celu wyeliminowania defektów w zabezpieczeniach wykrytych w oprogramowaniu wchodzących w skład środowiska.

Wymagania bezpieczeństwa

Funkcjonalne wymagania bezpieczeństwa

W niniejszej części dokumentu wymagania funkcjonalne systemu zostały sprecyzowane pod kątem bezpieczeństwa.

Dane audytowe

FAU_GEN - Rejestrowanie zagrożeń bezpieczeństwa

```
FAU_GEN.1 - Generowanie danych na temat bezpieczeństwa
        FAU_GEN.1.1 - System musi rejestrować wszystkie potencjalnie niebezpieczne
zdarzenia, takich jak nieudane próby logowania, nieoczekiwane wywołania funkcji
systemowych, nieobsłużone wyjątki i zapisywać je w postaci logów systemowych.

FAU_GEN.2 - Przypisywanie zdarzeń do konkretnych podmiotów
        FAU_GEN.2.1 - Każde zdarzenie rejestrowane przez system powinno posiadać
znacznik czasu, typ zdarzenia, oraz identyfikator podmiotu, który wywołał dane
zdarzenie.
```

FAU_ARP - Powiadomienia systemu w przypadku wykrycia potencjalnych zagrożeń bezpieczeństwa.

```
FAU_ARP.1 -  Alarmy bezpieczeństwa.
        FAU_ARP.1.1 - W przypadku wykrycia przez system potencjalnego krytycznego
zagrożenia bezpieczeństwa, powinien on powiadomić administratora za pomocą
stosownego komunikatu oraz zapisać zdarzenie w rejestrze logów systemowych.
        FAU_ARP.1.2 - System powinien zablokować dostęp do systemu użytkownikowi,
stwarzającemu krytyczne zagrożenie.
```

FAU_SAR - Wymagania dotyczące narzędzi audytu, dostępnych dla osób uprawnionych w celu przeglądu danych.

```
FAU_SAR.1 Przegląd audytu, możliwość odczytywania rejestrowanych danych.
        FAU_SAR.1.1 - System musi zapewnić możliwość odczytu zarejestrowanych
danych audytu.
        FAU_SAR.1.2 - System musi zapewnić możliwość odczytu danych w formie
możliwej do interpretacji przez użytkownika.
```

FAU_SAR.2 - Systemowa kontrola dostępu do danych audytu.

```
FAU_SAR.2.1 - System musi zapewnić kontrolę odczytu danych audytu. Dane audytowe
mogą być odczytywane tylko przez podmioty do tego uprawnione.
```

FAU_STG - Wymagania System dotyczące przechowywania zbioru rejestrowanych zdarzeń.

```
FAU_STG.1 - Miejsce przechowywania rejestrowanych danych.
        FAU_STG.1.1 - System musi być w stanie wykonać kopię zapasową oraz
ewentualne przywrócenie danych audytu.

FAU_STG.2 - Gwarancja dostępności rejestrowanych danych przez system.
        FAU_STG.2.1 - System musi zapewnić kopiowanie danych (w ramach kopii
zapasowej) do innej części TOE.
```

Weryfikacja

FDP_ACC - Polityka kontroli dostępu.

```
FDP_ACC.1 - kontrola dostępu do poszczególnych funkcjonalności TOE.
        FDP_ACC.1.1 - System na podstawie kontroli dostępu SFP (ang. Security.
Function Policies, zbiór zasad bezpieczeństwa które muszą być przestrzegane w
ramach TOE) musi egzekwować kontrolę dostępu do poszczególnych funkcji oraz
zasobów TOE zdefiniowanych w SFP.
```

FDP_ACF - funkcje kontroli dostępu.

```
FDP_ACF.1 - atrybuty kontroli dostępu.
        FDP_ACF.1.1 - System musi wymuszać kontrolę dostępu zdefiniowaną w SFP
bazującą na rolach przypisanych do poszczególnych podmiotów w ramach TOE.
        FDP_ACF.1.2 - System musi egzekwować poniższe zasady w celu weryfikacji
czy dany podmiot powinien uzyskać dostęp do wybranej funkcjonalności:
        - podmiot musi być autoryzowanym podmiotem występującym w ramach TOE,
        - system musi zweryfikować rolę danego podmiotu,
        - na podstawie atrybutów dostępu przypisanych do poszczególnych ról,
System powinien udzieli lub odmówić dostępu do danej funkcji TOE dla danego
podmiotu.
```

Uwierzytelnianie i identyfikacja

```
FIA_AFL - błędy uwierzytelniania.

FIA_AFL.1- obsługa błędów uwierzytelniania.
        FIA_AFL.1.1 - System musi wykrywać błędne próby logowania użytkowników (w
ilości zdefiniowanej przez administratora).
        FIA_AFL.1.2 - w przypadku wykrycia zdefiniowanej ilości niepoprawnych prób
logowania danego użytkownika, system musi wykonać następujące czynności:
        - zapisać dokładne informacje na temat adresu logowania, ilości
niepoprawnych prób logowania, oraz podmiotu którego dotyczyły zdarzenie w logach
systemu,
        - zablokować możliwość logowania dla danego użytkownika na określony,
zdefiniowany przez administratora okres czasu,
        - poinformować podmiot o nieudanych próbach logowania.
```

FIA_UAU - uwierzytelnianie użytkowników.

```
FIA_UAU.1 - uwierzytelnianie użytkowników przed każdym działaniem.
        FIA_UAU.1.1 - System wymaga, aby każdy użytkownik aplikacji klienckiej i
serwer został pomyślnie uwierzytelniony, zanim zdecyduje się na inne operacje
związane z systemem w imieniu tego użytkownika.
        FIA_UAU.1.2 - System wymaga, aby każdy użytkownik aplikacji klienckiej i
serwer został zidentyfikowany przed umożliwieniem w imieniu tego użytkownika
jakichkolwiek innych działań z udziałem systemu.
```

EXT_FIA_VC_LOGIN - logowanie użytkowników.

```
EXT_FIA_VC_LOGIN.1 - żądanie logowania użytkownika serwera.
        EXT_FIA_VC_LOGIN.1.1 - serwer bazy danych musi zażądać identyfikacji i
uwierzytelniania z środowiska serwera dla użytkownika serwera i otrzymać
powiadomienie o sukcesie, przed wykonaniem w imieniu u»ytkownika jakichkolwiek
innych działań z udziałem TSF.
```

FIA_UID - identyfikacja użytkowników.

```
FIA_UID.1 - identyfikacja użytkownika przed jakimkolwiek działaniem.
        FIA_UID.1.1 - System wymaga, aby każdy użytkownik aplikacji został
zidentyfikowany przed umożliwieniem w imieniu tego użytkownika jakichkolwiek
innych działań z udziałem systemu.
```

Przerwanie procesu

FDP_IFF - funkcje kontrolujące przepływ informacji.

```
FDP_IFF.1 - proste atrybuty zabezpieczeń
        FDP_IFF.1.1 - TSF zezwala na przepływ informacji pomiędzy kontrolowanym
podmiotem a kontrolowanymi informacjami za po±rednictwem kontrolowanej operacji,
jeżli spełnione są następujące warunki:
        1. jeżeli pakiet danych pochodzi z uznanego i autoryzowanego interfejsu
sieci fizycznej lub wirtualnego interfejsu sieciowego VM,
        2. identyfikowanego przez identyfikator interfejsu lub Identyfikator sieci
VLAN (jeżli ma to zastosowanie) wskazany przez identyfikator źródłowy zdefiniowany
w tej specyfikacji SFP i jest adresowany do uznanego i autoryzowanego odbiorcy
wskazanego przez identyfikator docelowy zdefiniowany w tej SFP,
        3. a następnie umo»liwia przepływ informacji, w przeciwnym razie odmawia
przepływu informacji.
```

Ochrona

FMT_MSA - zarządzanie atrybutami bezpieczeństwa.

```
FMT_MSA.1 - inicjowanie atrybutu statycznego.
        FMT_MSA.1.1 - TSF musi egzekwować wirtualny i rozproszony przełącznik
sterowania przepływem informacji SFP do ograniczania możliwości dodawania,
modyfkowania i usuwania atrybutów bezpieczeństwa. TSF będzie wymuszać politykę
wirtualnej i rozproszonej zasady kontroli przepływu informacji.
```

FMT_SMR - podział na role

```
FMT_SMR.1 - role bezpieczeństwa
        FMT_SMR.1.1 - system musi przechowywać następujące role użytkowników
aplikacji:
        - użytkownik,
        - administrator.

        FMT_SMR.1.2</b> - system musi zachowywać role użytkowników aplikacji takie
jak:
        - administrator,
        - użytkownik.

FMT_SMR.2 - ograniczenia bezpieczeństwa dla ról.
        FMT_SMR.2.1 - system musi być w stanie powiązać użytkowników aplikacji z
wyżej wymienionymi rolami.
        FMR_SMR.2.2 - system musi być w stanie powiązać użytkowników aplikacji
klienckiej z wyżej wymienionymi rolami.
```

FPT_STM - znaczniki czasu.

```
FPT_STM.1 - niezawodność znaczników czasu.
        FPT_STM.1.1 - system musi niezawodnie generować znaczniki czasu.

FPT_STM.2 System powinien rejestrować wszystkie akcje użytkowników w postaci logów
systemowych i przypisywać im znaczniki czasu.
```

FCS_CKM - zarządzanie klucza kryptograficznego.

```
FCS_CKM.1 - generowanie kluczy kryptograficznych; wymaga wygenerowanie klucza
kryptograficznego zgodnie z określonym algorytmem i rozmiarem klucza zgodnie ze
standardami.
FCS_CKM.2 - dostarczanie klucza kryptograficznego; wymaga klucza
kryptograficznego, który będzie dostarczony zgodnie z określoną metodą przesyłu
zgodną z przyjętymi standardami.
FCS_CKM.3 -  dostęp do klucza kryptograficznego; wymagany dostęp do klucza
zgodnego z określoną metodą dostępu zgodną z przyjętymi standardami.
FCS_CKM.4 - usuwanie klucza kryptograficznego; wymagane niszczenie klucza
kryptograficznego zgodnej z przyjętymi standarami.
```

FCS_COP Operacja szyfrowania

```
FCS_COP.1 - TSF powinien zapewnić zgodnie z określonym algorytmem kryptograficznym
i rozmiaru klucza operację szyfrowania zgodną z przyjętymi standardami.
```

Specyfikacja funkcjonalna TOE

W tym rozdziale zawarto opis funkcji TOE spełniających wymagania zdefiniowane w poprzednich rozdziałach dokumentu.

Funkcje bezpieczeństwa TOE

Każde wymaganie bezpieczeństwa i związane z nimi opisy odpowiadają funkcjom bezpieczeństwa. Każda funkcja jest opisywana przez to, w jaki sposób spełnia swoje wymagania.

Funkcja bezpieczeństwa TOE	**SFR ID**
Alarm bezpieczeństwa	FAU_ARP.1
Audyt bezpieczeństwa	FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.2

Funkcja bezpieczeństwa TOE	SFR ID
Idetyfikacja i uwierzytelnianie	FIA_AFL.1, FIA_UAU.1, FIA_UID.1, EXT_FIA_VC_LOGIN
Ochrona danych użytkownika	FDP_IFF.1
Zarządzanie bezpieczeństwem	FMT_MSA.1, FMT_SMR.1, FMT_SMR.2, FPT_STM.1, FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4, FCS_COP.1

Uzasadnienie celów zabezpieczenia

W niniejszym rozdziale zawarto uzasadnienie, dlaczego zidentyfikowane cele zabezpieczeń są odpowiednie do przeciwdziałania zidentyfikowanym zagrożeniom i spełniają określone polityki bezpieczeństwa.

Odwzorowanie zagrożeń TOE na cele zabezpieczeń

Zagrożenie	Cele zabezpieczeń TOE
T. Atak słownikowy i atak metodą pełnego przeglądu	O. Hashowanie hasła wraz z domieszką, O. Blokowanie ataków na TOE
T. Uszkodzenie TOE	O. Konfiguracja TOE, O. Bezpieczeństwo fizyczne, Aktualizacje zabezpieczeń
T. Nieautoryzowany dostęp do zasobów serwera bazodanowego	O. Ochrona procesów, O. Aktualizacje zabezpieczeń, O. Hashowanie hasła wraz z domieszką, O. Szyfrowane dokumenty
T. Nieautoryzowane przejęcie sesji użytkownika	O. Wiarygodni administratorzy, O. Wiarygodni użytkownicy, O. Uwierzytelnienie użytkownika
T. Nieupoważniony dostęp	O. Uwierzytelnienie użytkownika, O. Ochrona procesów, O. Szyfrowane dokumenty
T. Słaby zestaw algorytmów	O. Integralność danych do szyfrowania, O. Zatwierdzone algorytmy, O. Moduły kryptograficzne, O. Szyfrowane dokumenty, O. Hashowanie hasła wraz z domieszką
T. Nieautoryzowany dostęp do prywatnych plików	O. Uwierzytelnienie użytkownika, O. Zgodność uprawnień do dokumentów, O. Szyfrowane dokumenty
T. Przypadkowe usunięcie pliku	O. Zgoda użytkownika, O. Obecność użytkownika
T. Nieautoryzowane podsłuchanie użytkowników podczas operacji dzielenia się kluczem deszyfrującym	O. Ochrona kanału komunikacyjnego, O. Uwierzytelnienie użytkownika
T. Nieautoryzowane podsłuchiwanie operacji logowania użytkownika do systemu	O. Ochrona kanału komunikacyjnego

Zagrożenie	Cele zabezpieczeń TOE
T. Modyfikacja uprawnień do zasobów	O. Konfiguracja TOE, O. Bezpieczeństwo fizyczne, O. Aktualizacje zabezpieczeń
T. Wyciek danych	O. Ochrona procesów, O. Aktualizacje zabezpieczeń, O. Szyfrowane dokumenty, O. Hashowanie hasła wraz z domieszką
T. Przejęcie konta administratora	O. Wiarygodni administratorzy, O. Uwierzytelnienie użytkownika, O. Aktualizacje zabezpieczeń

Odwzorowanie polityki zabezpieczeń TOE na cele zabezpieczeń

Polityka	Cele zabezpieczeń TOE
P. Przerwanie procesu	O. Ochrona procesów, O. Konfiguracja TOE, O. Bezpieczeństwo fizyczne
P. Integralność danych użytkownika	O. Zgodność uprawnień do dokumentów, O. Wiarygodni użytkownicy, O. Zbiór dokumentów
P. Eksport szyfrogramu	O. Poufność danych uwierzytelniających, O. Bezpieczeństwo fizyczne, O. Obecność użytkownika,
P. Zarządzanie	O. Ochrona kanału komunikacyjnego, O. Udostępnienie pliku innemu użytkownikowi, O. Ustawienie czasu wygaśnięcia pliku, O. Zbiór dokumentów, O. Tworzenie danych na potrzeby audytu, O. Ochrona danych rejestrowanych na potrzeby audytu, O. Przeglądanie danych rejestrowanych na potrzeby audytu, O. Aktualizacje zabezpieczeń
P. Algorytmy kryptograficzne	O. Zatwierdzone algorytmy, O. Moduły kryptograficzne

Odwzorowanie celów zabezpieczń TOE na politykę i zagrożenie

Cele zabezpieczeń TOE	Polityka/Zagrożenia
Ochrona kanału komunikacyjnego	P. Zarządzanie; Nieautoryzowane podsłuchiwanie operacji logowania użytkownika do systemu, T. Nieautoryzowane podsłuchanie użytkowników podczas operacji dzielenia się kluczem deszyfrującym, T. Przejęcie konta administratora
Uwierzytelnienie użytkownika	P. Integralność danych użytkownika; T. Nieautoryzowane przejęcie sesji użytkownika, T. Nieupoważniony dostęp, T. Przejęcie konta administratora
Integralność danych do szyfrowania	P. Algorytmy kryptograficzne, P. Integralność danych użytkownika, P. Eksport szyfrogramu; T. Uszkodzenie TOE, T. Słaby zestaw algorytmów, T. Przypadkowe usunięcie pliku, T. Wyciek danych
Ochrona procesów	P. Przerwanie procesu; T. Uszkodzenie TOE, T. Nieautoryzowany dostęp do zasobów serwera bazodanowego, T. Nieupoważniony dostęp, T. Nieautoryzowany dostęp do prywatnych plików, T. Przypadkowe usunięcie pliku, T. Wyciek danych

Cele zabezpieczeń TOE	Polityka/Zagrożenia
Poufność danych uwierzytelniających	P. Algorytmy kryptograficzne, P. Zarządzanie; Nieautoryzowane przejęcie sesji użytkownika, T. Nieupoważniony dostęp, T. Przypadkowe usunięcie pliku, T. Wyciek danych
Zatwierdzone algorytmy	P. Algorytmy kryptograficzne; T. Uszkodzenie TOE
Ochrona procesów	P. Integralność danych danych użytkownika, P. Zarządzanie; T. Modyfikacja uprawnień do zasobów, T. Wyciek danych, T. Przypadkowe usunięcie pliku
Zgoda użytkownika	P. Integralność danych użytkownika, P. Zarządzanie; T. Przypadkowe usunięcie pliku, T. Przejęcie konta administratora
Udostępnienie pliku innemu użytkownikowi	P. Eksport szyfrogramu, P. Integralność danych użytkownika; T. Nieautoryzowane przejęcie sesji użytkownika, T. Nieupoważniony dostęp, T. Nieautoryzowany dostęp do prywatnych plików, T. Przypadkowe usunięcie pliku, T. Nieautoryzowane podsłuchanie użytkowników podczas operacji dzielenia się kluczem deszyfrującym, T. Wyciek danych
Przesyłanie klucza deszyfrującego	P. Eksport szyfrogramu; T. Nieautoryzowane T. podsłuchanie użytkowników podczas operacji dzielenia się kluczem, T. Modyfikacja uprawnień do zasobów
Ustawienie czasu wygaśnięcia pliku	P. Zarządzanie; T. Przypadkowe usunięcie pliku, T. Nieupoważniony dostęp, T. Nieautoryzowany dostęp do prywatnych plików, T. Modyfikacja uprawnień do zasobów
Zbiór dokumentów	P. Zarządzanie, P. Integralność danych użytkownika; T. Wyciek danych, T. Przypadkowe usunięcie pliku, T. Nieupoważniony dostęp
Zgodność uprawnień do dokumentów	P. Zarządzanie, P. Integralność danych użytkownika; T. Nieupoważniony dostęp, T. Nieautoryzowany dostęp do prywatnych plików, T. Przypadkowe usunięcie pliku
Bezpieczna komunikacja	P. Zarządzanie, P. Eksport szyfrogramu; T. Nieautoryzowane przejęcie sesji użytkownika, T. Nieautoryzowane podsłuchanie użytkowników podczas operacji dzielenia się kluczem deszyfrującym, T. Nieautoryzowane podsłuchiwanie operacji logowania użytkownika do systemu
Wiarygodni użytkownicy	P. Integralność danych użytkownika; T. Nieautoryzowane przejęcie sesji użytkownika, T. Nieautoryzowane podsłuchiwanie operacji logowania użytkownika do systemu
Wiarygodni administratorzy	P. Integralność danych użytkownika; T. Nieautoryzowane przejęcie sesji użytkownika, T. Nieautoryzowane podsłuchiwanie operacji logowania użytkownika do systemu
Konfiguracja TOE	P. Zarządzanie; T. Uszkodzenie TOE
Moduły kryptograficzne	P. Algorytmy kryptograficzne; T. Słaby zestaw algorytmów; T. Nieautoryzowane podsłuchanie użytkowników podczas operacji dzielenia się kluczem deszyfrującym

Cele zabezpieczeń TOE	Polityka/Zagrożenia
Bezpieczeństwo fizyczne	P. Zarządzanie; T. Wyciek danych, T. Modyfikacja uprawnień do zasobów
Obecność użytkownika	P. Integralność danych użytkownika, P. Zarządzanie; T. Nieupoważniony dostęp, T. Nieautoryzowany dostęp do prywatnych plików, T. Nieautoryzowane przejęcie sesji użytkownika
Tworzenie danych na potrzeby audytu	P. Zarządzanie, P. Integralność danych użytkownika; T. Uszkodzenie TOE, T. Nieautoryzowany dostęp do zasobów serwera bazodanowego, T. Nieupoważniony dostęp
Ochrona danych rejestrowanych na potrzeby audytu	P. Zarządzanie; T. Uszkodzenie TOE, T. Wyciek danych
Przeglądanie danych rejestrowanych na potrzeby audytu	P. Zarządzanie; T. Nieautoryzowany dostęp do prywatnych plików
Aktualizacje zabezpieczeń	P. Zarządzanie; T. Uszkodzenie TOE, T. Modyfikacja uprawnień do zasobów, T. Wyciek danych

Zapobieganie zagrożeń

T. Uszkodzenie TOE

Zagrożeniu T. Uszkodzenie TOE zapobiegają następujące cele zabezpieczeń:

O. Konfiguracja TOE

Konfiguracja wymaga, by były prawidłowo skonfigurowane ustawienia aplikacji, uprawnień użytkowników oraz

O. Bezpieczeństwo fizyczne

Bezpieczeństwo wymaga, aby TOE zapewnił bezpieczeństwo znajdującego się w obrębie środowiska aplikacji, tak aby infrastruktura była zabezpieczona przed atakami wewnątrz.

O. Aktualizacje zabezpieczeń

Bezpieczeństwo wymaga, aby TOE zapewnił aktualizację zabezpieczeń mającej na celu załatanie wykrytych luk i błędów w systemie.

T. Nieautoryzowany dostęp do zasobów serwera bazodanowego

Zagrożeniu T. Nieautoryzowany dostęp do zasobów serwera bazodanowego zapobiegają następujące cele zabezpieczeń:

O. Ochrona procesów

Ochrona procesów wymaga, aby TOE zapewnił ochronę procesów w celu zniwelowania ryzyka związanego z wyciekiem danych. Spreparowane zapywania bazodanowe powinny być zweryfikowane i zwalidowane pod względem podatności na atak typu SQL-injection. Ochrona procesów wymaga, aby TOE był odporny na atak typu SQL-injection.

O. Aktualizacje zabezpieczeń

Aktualizacje zabezpieczeń wymagają, aby TOE zapewnił automatyczną aktualizację serwera bazodanowego do najnowszej wersji oprogramowania w celu eliminacji wykrytych błędów i luk w systemie bazodanowym.

O. Hashowanie hasła wraz z domieszką

TOE powinien szyfrować wrażliwe dane logowania użytkowników hashem bcrypt wraz z zastosowaniem domieszki (salt).

O. Szyfrowane dokumenty

TOE powinien przechowywać w bazie danych jedynie dokumenty w formie zaszyfrowanej za pomocą algorytmu AES-256. Klucz deszyfrujący znany jest jedynie użytkownikowi, który jest właścicielem pliku.

T. Atak słownikowy i atak metodą pełnego przeglądu

Zagrożeniu T. Atak słownikowy i atak metodą pełnego przeglądu zapobiegają następujące cele zabezpieczeń:

O. Hashowanie hasła wraz z domieszką

TOE powinien szyfrować wrażliwe dane logowania użytkowników hashem bcrypt wraz z zastosowaniem domieszki (salt).

O. Blokowanie ataków na TOE

TOE musi zapewnić mechanizm blokowania ataków (wiele nieudanych prób logowania, DDoS) poprzez oflagowanie adresu IP bądź identyfikatora atakującego i zablokowanie kanału komunikacyjnego z podmiotem atakującym.

T. Nieautoryzowane przejęcie sesji użytkownika

Zagrożeniu T. Nieautoryzowane przejęcie sesji użytkownika zapobiegają następujące cele zabezpieczeń:

O. Wiarygodni administratorzy

Środowisko TOE wymaga by, upoważnieni administratorzy rzetelnie wykonują swoje zadania oraz byli przeszkoleni w zakresie bezpieczeństwa przechowywania danych.

O. Wiarygodni użytkownicy

Środowisko TOE wymaga, by użytkownicy znali zasady związane z bezpieczeństwem przechowywania danych.

O. Uwierzytelnienie użytkownika

TOE musi zapewnić poprawne uwierzytelnienie się użytkownika przed wykonaniem określonej akcji użytkownika.

T. Nieupoważniony dostęp

Zagrożeniu T. Nieupoważniony dostęp zapobiegają następujące cele zabezpieczeń:

O. Uwierzytelnienie użytkownika

TOE musi zapewnić poprawne uwierzytelnienie się użytkownika przed wykonaniem określonej akcji użytkownika.

O. Ochrona procesów

Ochrona procesów wymaga, aby TOE zapewnił ochronę przed ingerencją dowolnych, niezaufanych procesów, kanałów komunikacyjnych oraz intruzów w działanie tych procesów, które wykorzystywane są podczas wysyłania poufnych danych.

T. Słaby zestaw algorytmów

Zagrożeniu T. Słaby zestaw algorytmów zapobiegają następujące cele zabezpieczeń:

O. Integralność danych do szyfrowania

TOE musi zapewnić integralność różnych reprezentacji danych przeznaczonych do zaszyfrowanie od momentu ich sformatowania do momentu utworzenia szyfrogramu.

O. Zatwierdzone algorytmy

TOE powinien zapewnić, aby były stosowane tylko te algorytmy szyfrowe, które należą do zbioru zatwierdzonych algorytmów i parametrów stosowanych podczas tworzenia szyfrogramu; w szczególności, aby format był zgodny z formatami wskazanymi w Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. (Dz. U. Nr 128, poz.1094 z dnia 12 sierpnia 2002 r.).

O. Moduły kryptograficzne

TOE musi korzystać tylko z tych usług kryptograficznych, udostępnianych przez środowisko teleinformatyczne, które spełniają wymagania określone w Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. (Dz. U. Nr 128, poz.1094 z dnia 12 sierpnia 2002 r.) oraz Ustawie z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. 1999 nr 11 poz. 95, wersja ujednolicona) i zatwierdzone przez odpowiednie instytucje certyfikujące przy wysokim poziomie siły funkcji zabezpieczającej lub przynajmniej zgodne z FIPS 140 poziom 2 lub wyższy.

T. Nieautoryzowany dostęp do prywatnych plików

Zagrożeniu T. Nieautoryzowany dostęp do prywatnych plików zapobiegają następujące cele zabezpieczeń:

O. Uwierzytelnienie użytkownika

TOE musi zapewnić poprawne uwierzytelnienie się użytkownika przed uzyskaniem dostępu do prywatnych bądź udostępnionych jemu dokumentów.

O. Zgodność uprawnien do dokumentów

TOE musi zapewnić zgodność, która potwierdza uprawnienia użytkownika do pobrania wybranego dokumentu.

O. Szyfrowane dokumenty

TOE powinien przechowywać w bazie danych jedynie dokumenty w formie zaszyfrowanej za pomocą algorytmu AES-256. Klucz deszyfrujący znany jest jedynie użytkownikowi, który jest właścicielem pliku.

T. Przypadkowe usunięcie pliku

Zagrożeniu T. Przypadkowe usunięcie pliku zapobiegają następujące cele zabezpieczeń:

O. Zgoda użytkownika

TOE musi zapewnić, że operacja usunięcia pliku przez użytkownika jest poprzedzona odpowiednim komunikatem: "Czy chcesz usunąć plik XXXXXX", wraz z opcjami do wyboru "TAK", "NIE". Po świadomym uzyskaniu zgodny przez użytkownika plik jest kasowany z systemu.

O. Obecność użytkownika

TOE wymaga, by operacja usuwania pliku należącego do użytkownika odbywała się przy jego udziale.

T. Nieautoryzowane podsłuchanie użytkowników podczas operacji dzielenia się kluczem deszyfrującym

Zagrożeniu T. Nieautoryzowane podsłuchanie użytkowników podczas operacji dzielenia się kluczem deszyfrującym zapobiegają następujące cele zabezpieczeń:

O. Ochrona kanału komunikacyjnego

TOE musi zapewnić bezpieczne połączenie pomiędzy użytkownikami podczas operacji dzielenia się kluczem deszyfrującym. W tym celu zastosowany jest Protokół Diffie-Hellmana oraz protokół HTTPS.

O. Uwierzytelnienie użytkownika

Przed przeprowadzeniem operacji dzielenia się kluczem deszyfrującym, TOE wymaga aby każda ze stron przeszła pomyślnie operację uwierzytelnienia się.

T. Nieautoryzowane podsłuchiwanie operacji logowania użytkownika do systemu

Zagrożeniu T. Nieautoryzowane podsłuchiwanie operacji logowania użytkownika do systemu zapobiegają następujące cele zabezpieczeń:

O. Ochrona kanału komunikacyjnego

TOE musi zapewnić bezpieczny kanał komunikacyjny systemu z użytkownikiem. W tym celu zastosowano protokół HTTPS.

T. Modyfikacja uprawnień do zasobów

Zagrożeniu T. Modyfikacja uprawnień do zasobów zapobiegają następujące cele zabezpieczeń:

O. Konfiguracja TOE

Prawidłowa konfiguracja uprawnień, polityki dostępowej TOE zapobiega nieupoważnionym modifikacjom uprawnień do zasobów.

O. Bezpieczeństwo fizyczne

Środowisko musi zapewniać akceptowalny poziom bezpieczeństwa fizycznego tak, aby nie było możliwe manipulowanie TOE.

O. Aktualizacje zabezpieczeń

TOE musi zapewnić automatycznie aktualizowanie zabezpieczeń w celu wyeliminowania defektów w zabezpieczeniach wykrytych w oprogramowaniu wchodzących w skład środowiska.

T. Wyciek danych

Zagrożeniu T. Wyciek danych zapobiegają następujące cele zabezpieczeń:

O. Ochrona procesów

Ochrona procesów wymaga, aby TOE zapewnił ochronę przed ingerencją dowolnych, niezaufanych procesów, kanałów komunikacyjnych oraz intruzów w działanie tych procesów, które wykorzystywane są podczas wysyłania poufnych danych.

W przypadku awarii systemu i wycieku danych wrażliwe dane są zabezpieczone przed nieuprawnionym dostępem:

- hasło - zabezpieczone hashem **bcrypt** z domieszką salt;
- dokumenty - zaszyfrowane kluczem symetrycznym AES-256, klucz deszyfrujący nie jest przechowywany w systemie.

O. Aktualizacje zabezpieczeń

TOE musi zapewnić automatycznie aktualizowanie zabezpieczeń w celu wyeliminowania defektów w zabezpieczeniach wykrytych w oprogramowaniu wchodzących w skład środowiska.

O. Hashowanie hasła wraz z domieszką

TOE powinien szyfrować wrażliwe dane logowania użytkowników hashem bcrypt wraz z zastosowaniem domieszki (salt).

O. Szyfrowane dokumenty

TOE powinien przechowywać w bazie danych jedynie dokumenty w formie zaszyfrowanej za pomocą algorytmu AES-256. Klucz deszyfrujący znany jest jedynie użytkownikowi, który jest właścicielem pliku.

T. Przejęcie konta administratora

Zagrożeniu T. Przejęcie konta administratora zapobiegają następujące cele zabezpieczeń:

O. Wiarygodni administratorzy

Środowisko TOE wymaga by, upoważnieni administratorzy rzetelnie wykonują swoje zadania oraz byli przeszkoleni w zakresie bezpieczeństwa przechowywania danych.

O. Uwierzytelnienie użytkownika

TOE musi zapewnić poprawne uwierzytelnienie się użytkownika przed wykonaniem określonej akcji użytkownika.

O. Aktualizacje zabezpieczeń

TOE musi zapewnić automatycznie aktualizowanie zabezpieczeń w celu wyeliminowania defektów w zabezpieczeniach wykrytych w oprogramowaniu wchodzących w skład środowiska.

Uzasadnienie funkcjonalnych wymagań bezpieczeństwa

Cele zabezpieczeń TOE	Wymagania funkcjonalne dla TOE
O. Ochrona kanału komunikacyjnego	FDP_IFF.1 - proste atrybuty zabezpieczeń, FMT_MSA.1 - inicjowanie atrybutu statycznego
O. Uwierzytelnienie użytkownika	FIA_AFL.1- obsługa błędów uwierzytelniania, FIA_UAU.1 - uwierzytelnianie użytkowników przed każdym działaniem, EXT_FIA_VC_LOGIN.1 - żądanie logowania użytkownika serwera, FIA_UID.1 - identyfikacja użytkownika przed jakimkolwiek działaniem, FMT_SMR.1 - role bezpieczeństwa
O. Integralność danych do szyfrowania	FPT_STM.1 - niezawodność znaczników czasu, FCS_CKM.1 - generowanie kluczy kryptograficznych, FCS_CKM.2 - dostarczanie klucza kryptograficznego, FCS_CKM.3 - dostęp do klucza kryptograficznego, FCS_CKM.4 - usuwanie klucza kryptograficznego, FCS_COP.1 - operacja szyfrowania
O. Ochrona procesów	FMT_MSA.1 - inicjowanie atrybutu statycznego, FMT_SMR.1 - role bezpieczeństwa, FMT_SMR.2 - ograniczenia bezpieczeństwa dla ról

Cele zabezpieczeń TOE	Wymagania funkcjonalne dla TOE
O. Poufność danych uwierzytelniających	FMT_SMR.2 - ograniczenia bezpieczeństwa dla ról, FDP_IFF.1 - proste atrybuty zabezpieczeń, FIA_UID.1 - identyfikacja użytkownika przed jakimkolwiek działaniem, FDP_ACC.1 - kontrola dostępu do poszczególnych funkcjonalności TOE
O. Zatwierdzone algorytmy	FCS_COP.1 - operacja szyfrowania, FCS_CKM.1 - generowanie kluczy kryptograficznych
O. Zgoda użytkownika	FIA_UID.1 - identyfikacja użytkownika przed jakimkolwiek działaniem, EXT_FIA_VC_LOGIN.1 - żądanie logowania użytkownika serwera,
O. Udostępnienie pliku innemu użytkownikowi	FIA_UAU.1 - uwierzytelnianie użytkowników przed każdym działaniem
O. Przesyłanie klucza deszyfrującego	FCS_CKM.2 - dostarczanie klucza kryptograficznego, FCS_CKM.3 - dostęp do klucza kryptograficznego,
O. Ustawienie czasu wygaśnięcia pliku	FPT_STM.1 - niezawodność znaczników czasu,
O. Zbiór dokumentów	FIA_UAU.1 - uwierzytelnianie użytkowników przed każdym działaniem, EXT_FIA_VC_LOGIN.1 - żądanie logowania użytkownika serwera, FIA_UID.1 - identyfikacja użytkownika przed jakimkolwiek działaniem
O. Zgodność uprawnień do dokumentów	FMT_SMR.1 - role bezpieczeństwa, FMT_SMR.2 - ograniczenia bezpieczeństwa dla ról