Bezpieczeństwo funkcjonalne systemu SECURO™:

I. Wprowadzenie

II. Bezpieczeństwo serwera SecuroBase i jego bezpośredniego otoczenia.
   1. bezpieczeństwo fizyczne
   2. bezpieczeństwo informatyczne
      a. bezpieczeństwo wewnętrzne
      b. bezpieczeństwo zewnętrzne

III. Bezpieczeństwo kanału transmisyjnego
   1. Bezpieczeństwo kanału sterującego
      a. Kryptografia
      b. Routing
   2. Bezpieczeństwo kanału transportowego
      a. Kryptografia
      b. Routing

IV. Bezpieczeństwo terminali abonenckich
   1. Bezpieczeństwo fizyczne
   2. Bezpieczeństwo informatyczne

V. Bezpieczeństwo użytkownika systemu:
   1. zabezpieczenie przekazywanych treści
   2. identyfikacja użytkownika
   3. lokalizacja użytkownika

VI. Przykładowe profile użytkowników
   1. użytkownik z wymogiem bezpieczeństwa standardowego,
   2. użytkownik z wymogiem bezpieczeństwa ponadstandardowego,

VII. Podsumowanie

I. Wprowadzenie

Niniejszy dokument opisuje główne rozwiązania przyjęte przy realizacji systemu Bezpiecznej Komunikacji Cyfrowej **Securo™** określające poziom bezpieczeństwa funkcjonalnego systemu. Priorytetem działania systemu **Securo™** jest osiąganie i utrzymanie najwyższego możliwego poziomu poufności przesyłanych za jego pośrednictwem treści. Głównym wysiłkiem twórców systemu **Securo™** od etapu określania założeń projektowych aż do wdrożenia systemu oraz jego utrzymania w ruchu było dobranie najlepszych, najskuteczniejszych i najbardziej bezpiecznych metod i rozwiązań gwarantujących osiągnięcie założonego celu.

Ze względu na specyficzne założenia projektowe, kładące szczególny nacisk na bezpieczne tworzenie, wdrażanie i eksploatację systemu **Securo™** przyjęto jako podstawę możliwość wykorzystania jedynie oprogramowania Open Source oraz otwartych standardów i protokołów.

Głównymi cechami które zadecydowały o użyciu tego rodzaju oprogramowania do budowy systemu SecuroTM są:

1. publiczna dostępność kodu źródłowego używanych narzędzi, bibliotek i aplikacji. Dostępność ta zwiększa zasadniczo pewność, że w zbudowanym systemie nie będzie ukrytych niepożądanych funkcjonalności i podatności na penetrację i nieuprawniony dostęp do systemu. Dostępność kodu źródłowego daje także możliwość pracy nad jego doskonaleniem przez wiele tysięcy osób z całego świata, co umożliwia użytkowanie oprogramowania dojrzałego i sprawdzonego na wiele sposobów. Podejście takie umożliwia także służbom utrzymującym system na stałe śledzenie wykrywanych przez światową społeczność błędów i podatności używanego oprogramowania i odpowiednie na nie szybkie i samodzielne reagowanie. Nie bez znaczenia ma także fakt, że w razie takiej potrzeby kody źródłowe oprogramowania mogą przejść indywidualny zewnętrzny audyt bezpieczeństwa przeprowadzany na zlecenie użytkowników systemu. Wszystkich powyższych cech pozbawione są systemy pisane na zlecenie pod klucz, do źródeł których nikt poza producentem oprogramowania nie ma dostępu, a bezpieczeństwo i jego utrzymanie zależą głównie od jakości i terminowości pracy producenta oprogramowania i podlegają bardzo ograniczonej kontroli zewnętrznej.

2. Otwarte standardy i protokoły w powiązaniu z oprogramowaniem Open Source pozwalają na zagwarantowanie najwyższej możliwej poufności przesyłanych treści poprzez korzystanie ze sprawdzonych i zalecanych przez międzynarodowe instytucje standaryzujące protokołów, standardów i algorytmów. Z dostępnych standardów, protokołów i algorytmów wybrane zostały te, które najlepiej wg projektantów systemu **Securo™** nadają się do przyjętych założeń równocześnie tworząc spójne, całościowe i bezpieczne rozwiązanie.

System SecuroTM w swojej części serwerowej składa się z platformy technologicznej **SecuroBase™**. Platforma ta zbudowana została modułowo i umożliwia płynną rozbudowę elementów składowych rozszerzających jej wydajność a także funkcjonalność. Platforma ta w

podstawowej wersji stanowi wydzielony niepubliczny system telekomunikacyjny typu VPBX (wirtualna abonencka centrala telefoniczna) realizujący bezpieczne połączenia i przesył danych pomiędzy jej abonentami. Istniej także możliwość umieszczenia alternatywnej platformy technologicznej **SecuroBase Private™** w lokalizacji wskazanej przez Abonenta i wtedy jest ona niepublicznym systemem telekomunikacyjnym typu PBX (abonencka centrala telefoniczna) realizującym bezpieczne połączenia i przesył danych jedynie pomiędzy abonentami wskazanymi przez użytkownika systemu (abonenta).

Wszystkie przyjmowane przez projektantów systemu **Securo™** rozwiązania musiały spełniać także założenia dodatkowe, to jest być skalowalne, łatwe w rozbudowie oraz umożliwiać dodawanie nowych funkcjonalności w miarę pojawiania się potrzeb abonentów.

II. Bezpieczeństwo serwera SecuroBase i jego bezpośredniego otoczenia.

1. ***bezpieczeństwo fizyczne***

System SecuroBase™ jest odpowiednio zabezpieczony fizycznie. Dostęp do jego elementów posiadają jedynie osoby do tego uprawnione. System jest objęty monitoringiem wizyjnym i alarmowym.

2. ***bezpieczeństwo informatyczne***

a. *bezpieczeństwo wewnętrzne*

System zrealizowany jest na serwerach umieszczonych w szafie typu Rack. Posiada stabilizowane zasilanie z 2 różnych źródeł oraz system zasilania rezerwowego. Obsługujące system Securo™ macierze dyskowe pracujące w trybie RAID posiadają funkcjonalność hot-swap pozwalającą na wymianę uszkodzonych dysków bez zatrzymywania pracy systemu. Zarządzanie systemem odbywa się bez dostępu do sieci zewnętrznej (Internetu) z indywidualnie uprawnionych terminali posiadających dodatkowe silne zabezpieczenia przez nieuprawnionym dostępem.

b. *bezpieczeństwo zewnętrzne*

Architektura systemu zaprojektowana została tak, aby system Securo™ posiadał odpowiednie zabezpieczenia od strony interfejsów sieci Internet. Wielostopniowe zabezpieczenia pozwalają się komunikować systemowi Securo™ z terminalami abonenckim jedynie w ściśle określony sposób. Każda transmisja dochodząca do systemu, która może pochodzić od terminali jest wieloaspektowo analizowana pod kątem bezpieczeństwa przez ścianę ogniową systemu Securo™, a obce transmisje są

blokowane. Zastosowane zabezpieczenia rozpoznają także nieprawidłowe strumienie danych wysyłane n.p. przez nieprawidłowo działające (n.p. zawieszone) autoryzowane terminale i eleminują z tym związane zagrożenia pracy systemu Securo™.

III. Bezpieczeństwo kanału transmisyjnego

1. ***Bezpieczeństwo kanału sterującego***

a. *Kryptografia*

Do realizacji komunikacji wybrano protokół SIP w wersji 2.0 (http://tools.ietf.org/html/rfc3261). Do szyfrowania komunikacji sterującej wybrano protokół szyfrujący TLS v.1 (http://tools.ietf.org/html/rfc2246) z użyciem algorytmu kryptograficznego RSA (https://tools.ietf.org/html/rfc3447) do wygenerowania kluczy asymetrycznych o ponadstandardowej długości 4096 b z funkcją skrótu realizowaną w oparciu o najbardziej bezpieczny i zalecany obecnie algorytm grupy SHA-2 – SHA512 (https://www.federalregister.gov/articles/2012/03/06/2012-5400/announcing-approval-of-federal-information-processing-standard-fips-publication-180-4-secure-hash). System Securo™ jako jeden z nielicznych cywilnych systemów komunikacyjnych na świecie dokonuje wzajemnej autoryzacji terminala abonenckiego z serwerem komunikacyjnym wykorzystując do tego w każdym przypadku generowane indywidualnie certyfikaty root CA.

b. *Routing*

Każdy z terminali abonenckich po uruchomieniu, łączy się w szyfrowany, bezpieczny sposób z serwerem systemu Securo™ najkrótszą drogą określoną w tabeli routingu routerów pośredniczących położonych na trasie do serwera SecuroBase™. Nie jest wymagane ingerowanie lub ustawianie innych tras niż domyślne w sieci lokalnej użytkownika, ani też stosowanie jakichkolwiek serwerów pośredniczących na trasie pakietów strumienia sterującego.

2. ***Bezpieczenstwo kanału transportowego***

a. *Kryptografia*

Do szyfrowania sesji transportowej (przesyłającej treść komunikacji) używany jest szyfr blokowy AES 256 o ponadstandardowej w stosunku do powszechnie używanej długości (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf) indywidualnie negocjowany dla każdego połączenia (sesji).

b. *Routing*

W zależności od sytuacji dostępne są różne rozwiązania związane z trasą pakietów sesji transportowej:

a. standardowe; jeżeli uczestniczące w sesji terminale posiadają publiczny adres IP - trasa pakietów nie jest określana przez system SecuroBase™ - wtedy pakiety kierowane są zgodnie z zasadami lokalnego routingu najkrótszą drogą pomiędzy terminalami. Natomiast w sytuacji, kiedy przynajmniej jeden adres korespondujących terminali nie jest adresem publicznym transmisja odbywa się poprzez serwer Media-Proxy systemu SecuroBase™.

b. wymuszony, w którym trasa pakietów kierowana jest zawsze przez zewnętrzny serwer Securo-Proxy™ zazwyczaj umieszczany ze względów bezpieczeństwa u Abonenta. Rozwiązanie takie daje najwyższy poziom bezpieczeństwa przekazywanych w kanale transportowym treści, ale wymaga udostępnienia na ten cel 1 stałego adresu publicznego IP.

IV. Bezpieczeństwo terminali abonenckich

1. ***Bezpieczeństwo fizyczne***

Za bezpieczeństwo fizyczne terminala abonenckiego odpowiada abonent. W przypadku utraty terminala, należy niezwłocznie zawiadomić administratora systemu SECURO™, który unieważnia certyfikat i klucz publiczny terminala oraz zmienia dane dostępowe (login i hasło) uniemożliwiając tym samym nieuprawnione użytkowanie terminala. Po odzyskaniu terminala możliwe jest ponowne jego używanie po wcześniejszym sprawdzeniu i skonfigurowaniu terminala wraz z wczytaniem nowego certyfikatu i klucza prywatnego przez administratora systemu Securo™ w jego siedzibie. Z zasady możliwość konfiguracji terminala zarezerwowana jest dla administratora systemu Securo™, jednakże dane o konfiguracji terminala są dla abonenta dostępne bez ograniczeń.

2. ***Bezpieczeństwo informatyczne***

Administrator systemu Securo™ konfigurując terminal do użytku wczytuje do niego m.in. unikalny certyfikat oraz klucz prywatny, a także hasło do blokowania i odblokowywania terminala, które powinno być zmienione przez użytkownika na własne. W zależności od polityki bezpieczeństwa Abonenta, terminal może mieć dostęp do Internetu i pobierać dane do wybranych przez abonenta aplikacji takich jak prognoza pogody, wiadomości RSS, notowania giełd itp. Istnieje możliwość stałej

deaktywacji w/w oprogramowania tak, aby terminal realizował jedynie transmisje związane z bezpieczną komunikacją.

v. Bezpieczeństwo użytkownika systemu

1. ***zabezpieczenie przekazywanych treści***

W systemie Securo™ treści pomiędzy terminalami przekazywane mogą być dwoma kanałami:

a. w usługach SecuroVoice™, SecuroVideo™, SecuroFax™, SecuroConference™, SecuroAlarm™, SecuroPTT™ treści pomiędzy użytkownikami przekazywane są w kanale transportowym. Treści te są zabezpieczone bardzo mocnym szyfrowaniem z wykorzystaniem symetrycznego algorytmu AES256. W/g relacji szeregu specjalistów kryptologów oraz publikacji naukowych algorytm ten nie został do chwili obecnej złamany.

b. w usługach SecuroSMS™ oraz SecuroAlert™ treści pomiędzy użytkownikami przekazywane są w kanale sterującym za pośrednictwem serwera proxy wbudowanego w platformę SecuroBase™. Ponieważ serwer ten działa jako „lustro" przekazujące dane pomiędzy terminalami abonenckimi żadne informacje w ten sposób przesyłane nie są rejestrowane. Dane te szyfrowane są łącznie z informacjami sterujacymi transmisją z wykorzystaniem najnowocześniejszych i najmocniejszych dostępnych algorytmów używanych w komunikacji realizowanej przy użyciu technologii klucza publicznego. Zastosowano tu algorytmy o zwielokrotnionej długości kluczy w stosunku np. do analogicznych rozwiązań n.p. w szyfrowanym dostępie do kont bankowych przez Internet (https). Rozwiązanie takie z dużym zapasem bezpieczeństwa zabezpiecza przesyłaną treść przed przejęciem przez nieuprawnione osoby.

2. ***identyfikacja użytkownika***

Każde konto abonenckie skonfigurowane na terminalu w systemie Securo™ posiada swój unikalny identyfikator który jest odpowiednikiem numeru połączeniowego w tradycyjnej telefonii. System nie posiada żadnych innych informacji pozwalających identyfikować użytkownika, ani też narzędzi ku temu. W chwili obecnej nie ma możliwości logowania się różnych użytkowników do terminala i rozróżniania tego przez system Securo™.

3. ***lokalizacja użytkownika***

System nie posiada możliwości lokalizacji użytkownika, ani narzędzi do tego służących. Dedykowane terminale systemu Securo™ można użyć do bezpiecznego przesyłania tego typu danych, ale z wykorzystaniem zewnętrznych względem systemu i terminali urządzeń określających położenie terminala (na przykład GPS). Jedyną przesłanką do ewentualnej lokalizacji terminala może być adres IP terminala, którym się on komunikuje z systemem Securo™. Możliwość ta nie jest jednak zaimplementowana w systemie.

VI. Przykładowe profile użytkowników

1. ***użytkownik z wymogiem bezpieczeństwa standardowego***

Użytkownik ten wymaga od systemu bezpiecznego i sprawnego przekazywania treści wymagając zabezpieczenia poufności przekazywanych danych na drodze transmisji pomiędzy każdym z uczestników połączenia najkrótszą skuteczną trasą internetową/intranetową.

2. ***użytkownik z wymogiem bezpieczeństwa ponadstandardowego***

Użytkownik ten wymaga od systemu bezpiecznego i sprawnego przekazywania treści wymagając zabezpieczenia poufności przekazywanych danych na drodze transmisji pomiędzy każdym z uczestników połączenia za pośrednictwem serwera SecuroProxy™ umieszczonego we wskazanym przez niego miejscu i gwarantującego przechodzenie przez ten serwer wszystkich transmisji kanału transportowego.

VII. Podsumowanie

W/g autorów niniejszego opracowania, wszystkie działania podejmowane przy tworzeniu systemu Securo™ od etapu założeń projektowych do wdrożenia i ciągłego procesu utrzymania systemu w ruchu stanowią spójny ciąg gwarantujący osiągnięcie założonego celu jakim jest uzyskanie najwyższego możliwego bezpieczeństwa przekazywanych za jego pomocą treści. Zakres przyjętego w systemie Securo™ poziomu zabezpieczeń znacząco przekracza poziom przyjety w innych cywilnych zastosowaniach komunikacyjnych.

Wykorzystanie istniejących, publicznie dostepnych standardów, norm i algorytmów pozwoliło stworzyć unikalny na skalę europejską system bezpiecznej komunikacji do zastosowań cywilnych dostępny dla każdego zainteresowanego podmiotu gospodarczego.

Autorom nie jest znany inny system prywatnej bezpiecznej komunikacji porównywalny pod względem gamy oferowanych usług, elastyczności konfiguracyjnej i przejrzystości zastosowanych rozwiązań,