Usługi świadczone na bazie systemu Bezpiecznej Komunikacji Cyfrowej SECURO™

W niniejszym dokumencie tym przedstawiamy Państwu usługi możliwe do zrealizowania na bazie systemu Bezpiecznej Komunikacji Cyfrowej Securo™ - wyjątkowego rozwiązania zapewniającego osiągnięcie najwyższego możliwego bezpieczeństwa przesyłanych treści na rynku rozwiązań cywilnych.

Usługi Bezpiecznej Komunikacji Cyfrowej SECURO™ służą przede wszystkim zapewnieniu bezpiecznej łączności dla osób, których wiedza i posiadane przez nie informacje nie mogą wydostać się poza upoważnione do tego gremia, a równocześnie konieczna jest wymiana tych informacji pomiędzy upoważnionymi do tego osobami. System może realizować także zaawansowane zabezpieczenie danych przesyłanych pomiędzy urządzeniami bez względu na analogowy, czy też cyfrowy sposób ich udostępnienia.

Przyjęte w systemie SecuroTM rozwiązania oparte zostały o najnowocześniejsze standardy, protokoły i algorytmy związane z przesyłaniem i szyfrowaniem danych. Założenia organizacyjno – techniczne projektu zakładają zapewnienie jak najwyższego bezpieczeństwa systemu SecuroTM zarówno w zakresie bezpieczeństwa informatycznego, jak i dostępu fizycznego. Wszystkie działania prowadzone od etapu projektowania systemu, aż do jego wdrożenia i utrzymania w ruchu realizują spójną politykę maksymalnego możliwego do uzyskania bezpieczeństwa systemu dedykowanego do zastosowań cywilnych ze szczególnym uwzględnieniem przesyłanych za jego pomocą treści. Wiecej informacji na temat zastosowanych rozwiązań dotyczących bezpieczeństwa opisane jest w dokumencie „Bezpieczeństwo funkcjonalne systemu SECUROTM".

Postęp w dziedzinie elektroniki i informatyki powoduje coraz większą łatwość w nieuprawnionym pozyskaniu poufnych danych czy to kontrahenta, konkurenta, czy też innej ofiary nielegalnych działań. Dlatego metody zabezpieczania poufności stosowane jeszcze kilka lat temu obecnie okazują się dalece niewystarczajace. Z doświadczenia wynika, że dużym błędem jest lekceważenie bezpieczeństwa firmowych informacji niejawnych, ale jeszcze większym błędem jest stosowanie rozwiązań nieskutecznych w przekonaniu o ich skutecznosci. Ze względu na to zespół ludzi tworzących system SECUROTM dba w sposób ciągły o jego aktualność i stosowanie najnowocześniejszych rozwiązań w dziedzinie bezpieczeństwa przesyłanych treści, służąc utrzymaniu bezpieczeństwa reprezentowanego przez system SECUROTM na najwyższym możliwym poziomie.

Bezpieczna komunikacja jest niezbędna w szeregu branżach, w których zachowanie poufności informacji jest podstawowym wymogiem ich działania. Poufność może wynikać z dbałości o interes firmy, bezpieczeństwo prowadzonych działań, lub wymogów prawnych – n.p. ochrony danych osobowych lub ochrony informacji niejawnych. Do branż, których działania nie można sobie wyobrazić bez zachowania poufności zaliczyć można bankowość i finanse, doradztwo prawne i finansowe, ochronę zdrowia, handel zagraniczny, consulting, ochronę mienia i osób, wymiar sprawiedliwości oraz każdą działalność, w której ujawniając poufne informacje (chociażby nieświadomie) narażamy firmę na poniesienie strat czy to finansowych, czy wizerunkowych.

Im bardziej poufnymi danymi lub większymi kwotami Państwo obracacie, tym większe jest zagrożenie. Czy warto ponosić takie ryzyko?

Usługi systemu SECURO™:

1. **SecuroVoice™** - bezpieczna telefonia realizująca szyfrowane połączenia telefoniczne,
2. **SecuroVideo™** - bezpieczna wideotelefonia realizująca szyfrowane, połączenia wideotelefoniczne,
3. **SecuroSMS™** - bezpieczne przesyłanie SMS-ów realizowane w zaszyfrowanym kanale łączności,
4. **SecuroFax™** - bezpieczne przesyłanie telefaksów realizowane w zaszyfrowanym kanale łączności,
5. **SecuroConference™** - bezpieczna telekonferencja realizująca szyfrowane, równoczesne połączenia maksymalnie 6 uczestników,
6. **SecuroAlarm™** - bezpieczne przesyłanie sygnałów alarmowych do Centrum Monitoringu,
7. **SecuroAlert™*** - bezpieczne przesyłanie wiadomości alarmo-wych realizowane w zaszyfrowanym kanale łączności,
8. **SecuroPTT™*** - bezpieczna komunikacja simpleksowa realizująca szyfrowane połączenia w grupach użytkowników na dużych obszarach

* usługi w trakcie przygotowania

1. **SecuroVoice™** - to bezpieczna telefonia realizująca szyfrowane połączenia telefoniczne

    1. Przeznaczenie:
    usługa przeznaczona jest dla organizacji, osób fizycznych i prawnych prowadzących działalność gospodarczą wymagających wysokiego bezpieczeństwa prowadzonych rozmów telefonicznych.

    2. Zasięg działania:
    każda komputerowa sieć lokalna Ethernet oparta na protokole IP, cały Internet przy założeniu przepływności łącza nie niższej niż 100 kb/s w każdą ze stron, wystarczającej stabilność transferu łącza (jitter <50 ms) oraz braku blokowania pakietów na trasie przez Operatorów pośredniczących,

    3. Bezpieczeństwo:
    bezpieczeństwo przesyłu oparte jest na bardzo bezpiecznych rozwiązaniach szyfrowania z wykorzystaniem protokołu TLS v.1 wykorzystującego system klucza publicznego o ponadstandardowej długości 4096b oraz algorytmie AES256 stosowanym do szyfrowania przesyłanej rozmowy na całej trasie pakietów pomiędzy terminalami Abonentów. System SecuroTM 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.

    4. Terminale abonenckie:
    homologowane i dostarczane przez Operatora systemu telefony i wideotelefony cyfrowe, aplikacje na platformie telefonów komórkowych*,

2. **SecuroVideo™** - to bezpieczna wideotelefonia realizująca szyfrowane, połączenia wideotelefoniczne.

    1. Przeznaczenie:
    usługa przeznaczona jest dla organizacji, osób fizycznych i prawnych prowadzących działalność gospodarczą wymagających wysokiego bezpieczeństwa prowadzonych wideorozmów.

    2. Zasięg działania:
    każda komputerowa lokalna sieć Ethernet oparta na protokole IP, cały Internet przy założeniu przepływności łącza nie niższej niż 500 kb/s w każdą ze stron (w zależności od wybranej jakości

obrazu), wystarczającej stabilność transferu łącza (jitter <10 ms) oraz braku blokowania pakietów na trasie przez Operatorów pośredniczacych,

3. Bezpieczeństwo:
   bezpieczeństwo przesyłu oparte jest na bardzo bezpiecznych rozwiązaniach szyfrowania z wykorzystaniem protokołu TLS v.1 wykorzystującego system klucza publicznego o ponadstandardowej długości 4096b oraz algorytmie AES256 stosowanym do szyfrowania przesyłanej wideorozmowy na całej trasie pakietów pomiędzy terminalami Abonentów. System SecuroTM 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.

4. Urządzenia abonenckie:
   homologowane i dostarczane przez Operatora systemu Videotelefony cyfrowe, aplikacje na platformie telefonów komórkowych*,

3. **SecuroSMS™** - to bezpieczne przesyłanie SMS-ów realizowane w zaszyfrowanym kanale łączności.

   1. Przeznaczenie:
      usługa przeznaczona jest dla organizacji, osób fizycznych i prawnych prowadzących działalność gospodarczą wymagającą wysokiej poufności przesyłanych wiadomości tekstowych.

   2. Zasięg działania:
      każda komputerowa lokalna sieć Ethernet oparta na protokole IP, cały Internet przy założeniu przepływności łącza nie niższej niż 1 kb/s w każdą ze stron, o praktycznie dowolnej stabilność transferu łącza (jitter <1000 ms) oraz braku blokowania pakietów na trasie przez Operatorów pośredniczących,

   3. Bezpieczeństwo:
      bezpieczeństwo przesyłu oparte jest na bardzo bezpiecznych rozwiązaniach szyfrowania z wykorzystaniem protokołu TLS v.1 wykorzystującego system klucza publicznego o ponadstandardowej długości 4096b. Zaszyfrowana transmisja komunikatów SMS odbywa się za pośrednictwem serwera Proxy platformy SecuroBaseTM, który otrzymuje zaszyfrowane komunikaty od jednego z terminali i przekazuje je w sposób zaszyfrowany do drugiego. System SecuroTM 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.

   4. Urządzenia abonenckie:
      homologowane i dostarczane przez Operatora systemu telefony i videotelefony cyfrowe, aplikacje na platformie telefonów komórkowych*,

4. **SecuroFax™** - to bezpieczne przesyłanie telefaksów realizowane w zaszyfrowanym kanale łączności.

   1. Przeznaczenie:
      usługa przeznaczona jest dla organizacji, osób fizycznych i prawnych prowadzących działalność gospodarczą wymagających wysokiego bezpieczeństwa przesyłanej komunikacji telefaksowej.

   2. Zasięg działania:
      każda komputerowa lokalna sieć Ethernet oparta na protokole IP, cały Internet przy założeniu przepływności łącza nie niższej niż 100 kb/s w każdą ze stron, o wystarczającej stabilność transferu łącza (jitter <10 ms) oraz braku blokowania pakietów na trasie przez Operatorów pośredniczących,

   3. Bezpieczeństwo:

bezpieczeństwo przesyłu oparte jest na bardzo bezpiecznych rozwiązaniach szyfrowania z wykorzystaniem protokołu TLS v.1 wykorzystującego system klucza publicznego o ponadstandardowej długości 4096b. Zeskanowany obraz przesyłany jest z wykorzystaniem protokołu T.38 i jest zaszyfrowany algorytmem AES128 na całej trasie pakietów pomiędzy terminalami abonenckimi. System SecuroTM 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.

4. Urządzenia abonenckie:
   dowolny telefax Abonenta podłączony do homologowanej i dostarczanej przez Operatora systemu bramki telefonicznej,

5. **SecuroConference™** - to bezpieczna telekonferencja realizująca szyfrowane, równoczesne połączenia maksymalnie 6 uczestników

   1. Przeznaczenie:
      usługa przeznaczona jest dla organizacji, osób fizycznych i prawnych prowadzących działalność gospodarczą wymagających podstawowego lub wysokiego bezpieczeństwa prowadzonych konferencji telefonicznych.

   2. Zasięg działania:
      każda komputerowa sieć lokalna Ethernet oparta na protokole IP, cały Internet przy założeniu przepływności łącza nie niższej niż 100 kb/s w obie strony dla każdego z abonentów, wystarczającej stabilność transferu łącza (jitter <50 ms) oraz braku blokowania pakietów na trasie przez Operatorów pośredniczących,

   3. Bezpieczeństwo:
      bezpieczeństwo przesyłu oparte jest na bardzo bezpiecznych rozwiązaniach szyfrowania z wykorzystaniem protokołu TLS v.1 wykorzystującego system klucza publicznego o ponadstandardowej długości 4096b oraz algorytmie AES256 stosowanym do szyfrowania przesyłanej rozmowy na całej trasie pakietów pomiędzy terminalami Abonentów. System SecuroTM 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.

   4. Urządzenia abonenckie:
      homologowane i dostarczane przez Operatora systemu telefony i wideotelefony cyfrowe, aplikacje na platformie telefonów komórkowych*,

6. **SecuroAlarm™** - to bezpieczne przesyłanie sygnałów alarmowych do Centrum Monitoringu

   1. Przeznaczenie:
      Usługa SecuroAlarm™ przeznaczona jest dla profesjonalnych firm ochrony mienia prowadzących zdalny monitoring obiektów. Usługa SecuroAlarmTM pozwala uzyskać najwyższe bezpieczeństwo transmitowanej sygnalizacji zdarzeń z centralek alarmowych monitorowanych obiektów do Centrum Monitorowania. Sygnał ze standardowego analogowego dialera alarmowego będącego częścią instalacji u klienta podłączony zostaje bezpośrednio do terminala SecuroAlarmTM umieszczanego wraz z centralką alarmową. Terminal przekształca sygnał na zaszyfrowaną postać cyfrową i przesyła do Zestawu Odbiorczego SecuroAlarmTM zlokalizowanego w Centrum Monitorowania. W zależności od wielkości Centrum Monitorowania Zestaw Odbiorczy SecuroAlarmTM posiada od 1 do 120 wyjść analogowych podłączanych jako linie miejskie PSTN do urządzeń Centrum Monitorowania. System nie wymaga wprowadzania żadnych zmian do obecnie eksploatowanych systemów opartych na tradycyjnych liniach telefonicznych (PSTN).

2. Zasięg działania:
   każda komputerowa sieć lokalna Ethernet oparta na protokole IP, cały Internet przy założeniu przepływności łącza nie niższej niż 100 kb/s na każdy kanał transmisyjny, wystarczającej stabilność transferu łącza (jitter <50 ms) oraz braku blokowania pakietów na trasie przez Operatorów pośredniczących,

3. Bezpieczeństwo:
   bezpieczeństwo przesyłu oparte jest na bardzo bezpiecznych rozwiązaniach szyfrowania z wykorzystaniem protokołu TLS v.1 wykorzystującego system klucza publicznego o ponadstandardowej długości 4096b oraz algorytmie AES128 stosowanym do szyfrowania przesyłanej sygnalizacji na całej trasie pakietów pomiędzy terminalem SecuroAlarmTM a Centrum Monitorowania. Dzięki SecuroAlarm™ można mieć pewność, że cała sygnalizacja na trasie od abonenckiej centralki alarmowej do Centrum Monitorowania będzie odporna na podsłuchanie oraz podmianę zawartości przekazywanych sygnałów. Ponadto istnieje możliwość prowadzenia monitorowania stanu traktu komunikacyjnego do terminala SecuroAlarmTM na tablicy synoptycznej lub na ekranie komputera. Możliwe jest też uruchomienie na bazie tego samego terminala SecuroAlarmTM alarmowej bezpiecznej łączności fonicznej (gorącej linii) z dozorem obiektu.

4. Urządzenia i oprogramowanie abonenckie:
   homologowane i dostarczane przez Operatora systemu urzadzenia SecuroAlarmTM dla strony obiektowej, homologowany i dostarczany przez Operatora Zastaw Odbiorczy SecuroAlarmTM dla strony Centrum Monitorowania w wersjach od 1 do 250 równoległych linii odbiorczych, Bezpieczny indywidualny dostęp do systemu monitoringu linii transmisyjnych (https://)

7. **SecuroAlert™*** - to bezpieczne przesyłanie wiadomości alarmowych realizowane w zaszyfrowanym kanale łączności

   1. Przeznaczenie:
      usługa przeznaczona jest dla organizacji, osób fizycznych i prawnych prowadzących działalność gospodarczą wymagającą wysokiej poufności i pewności w dostarczeniu krytycznie ważnych wiadomości. Wiadomość wysyłana z uprawnionego terminala dostarczona zostaje do abonenta, lub grupy abonentów w najkrótszym możliwym czasie (z reguły poniżej 1 s.), odbiór wiadomości sygnalizowany jest głośnym nie dającym się wyciszyć sygnałem wymagającym ręcznego wyłączenia, a otrzymanie oraz przeczytanie wiadomości potwierdzane jest nadawcy automatycznie.

   2. Zasięg działania:
      każda komputerowa sieć lokalna Ethernet oparta na protokole IP, cały Internet przy założeniu przepływności łącza nie niższej niż 100 kb/s w każdą ze stron, wystarczającej stabilność transferu łącza (jitter <50 ms) oraz braku blokowania pakietów na trasie przez Operatorów pośredniczących,

   3. Bezpieczeństwo:
      bezpieczeństwo przesyłu oparte jest na bardzo bezpiecznych rozwiązaniach szyfrowania z wykorzystaniem protokołu TLS v.1 wykorzystującego system klucza publicznego o ponadstandardowej długości 4096b. Zaszyfrowana transmisja wiadomości alarmowych odbywa się za pośrednictwem serwera Proxy platformy SecuroBaseTM, który otrzymuje zaszyfrowane komunikaty z terminala operatorskiego i przekazuje je w sposób zaszyfrowany do wszystkich członków wybranej grupy terminali odbiorczych. System SecuroTM 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.

   4. Urządzenia abonenckie:

terminal operatorski udostępniany przez Operatora systemu SECURO™ za pomocą przeglądarki WWW w połączeniu szyfrowanym HTTPS* , aplikacje na platformie telefonów komórkowych*,

8. **SecuroPTT™*** - to bezpieczna komunikacja simpleksowa realizująca szyfrowane połączenia w grupach użytkowników na dużych obszarach

    1. Przeznaczenie i opis usługi:
    usługa przeznaczona jest dla organizacji, osób fizycznych i prawnych prowadzących działalność gospodarczą wymagających wysokiej poufności prowadzonej komunikacji grupowej podobnej do głosowej simpleksowej łączności radiotelefonicznej. Usługa może obejmować wiele grup użytkowników (od 2 do wielu tysięcy użytkowników w każdej grupie), na praktycznie nieograniczonym obszarze.

    2. Zasięg działania:
    każda komputerowa sieć lokalna Ethernet oparta na protokole IP, cały Internet przy założeniu przepływności łącza nie niższej niż 100 kb/s w każdą ze stron, wystarczającej stabilność transferu łącza (jitter <50 ms) oraz braku blokowania pakietów na trasie przez Operatorów pośredniczących,

    3. Bezpieczeństwo:
    bezpieczeństwo przesyłu oparte jest na bardzo bezpiecznych rozwiązaniach szyfrowania z wykorzystaniem protokołu TLS v.1 wykorzystującego system klucza publicznego o ponadstandardowej długości 4096b. Zaszyfrowana transmisja głosu odbywa się za pośrednictwem serwera Proxy platformy SecuroBaseTM, który otrzymując zaszyfrowany głos z terminala przekazuje je w sposób zaszyfrowany do określonej grupy terminali odbiorczych. System SecuroTM jako jeden z nielicznych cywilnych systemów komunikacyjnych na świecie dokonuje wzajemnej autoryzacji terminali abonenckich z serwerem komunikacyjnym wykorzystując do tego w każdym przypadku generowane indywidualnie certyfikaty root CA.

    4. Urządzenia abonenckie:
    terminal operatorski udostępniany przez Operatora systemu SECURO™ za pomocą przeglądarki WWW w połączeniu szyfrowanym HTTPS*, aplikacje na platformie telefonów komórkowych*,

Terminale abonenckie

Dla realizacji wielu usług Operator dysponuje homologowanymi do użytkowania w usługach Securo™ urządzeniami abonenckimi. Urządzenia te dobierane są spośród poniższych wg potrzeb i preferencji Abonenta. Ze względu na zachowanie najwyższych standardów bezpieczeństwa urządzenia nie homologowane przez Operatora nie mogą być dopuszczone do użytkowania.

1. Bramka Grandstream HT 502 (SecuroFax™, SecuroAlarmTM)
2. Wideotelefon Grandstream GXV3240 (SecuroVoice™, SecuroVideo™, SecuroConferenceTM, SecuroSMS™)
3. Wideotelefon Grandstream GXV3275 (SecuroVoice™, SecuroVideo™, SecuroConferenceTM, SecuroSMS™)
4. Terminal dyspozytorski szyfrowane poł. HTTPS przez przeglądarkę (SecuroAlertTM)*
5. Aplikacja abonencka na telefony komórkowe (SecuroVoice™, SecuroAlert™, SecuroPTT™)*
6. Zestaw Odbiorczy (SecuroAlarmTM- po stronie Centrum Monitorowania)

Platforma technologiczna SecuroBase™

Wszystkie usługi Securo™ realizowane są na bazie platformy sprzętowo – programowej SecuroBase™. Platforma ta zbudowana została modułowo i umożliwia płynną rozbudowę elementów składowych rozszerzających jej wydajność a także funkcjonalność. Platforma ta stanowi wydzielony niepubliczny system telekomunikacyjny realizujący bezpieczne połączenia i przesył danych pomiędzy jej użytkownikami.

Platforma Securo™ została zaprojektowana i wdrożona z uwzględnieniem następujących priorytetów:

1. Zachowania najwyższej poufności informacji przekazywanych za jej pomocą,
2. Zapewnienia najwyższej ciągłości świadczonych usług,
3. Realizowania możliwie najwyższej jakości połączeń,

Najwyższa poufność przekazu zapewniona jest w większości usług poprzez użycie bardzo mocnego szyfrowania połączeń pomiędzy terminalami a platformą SecuroBaseTM zarówno w kanale sterującym (protokół TLS v.1 z szyfrowaniem asymetrycznym z wykorzytaniem technologii klucza publicznego ponadstandardowej długości 4096b) oraz szyfrowania danych transmitowanych w kanale transportowym algorytmem AES256, którego złamanie w chwili obecnej zajmuje miliony lat. Złamanie używanego w usłudze SecuroFax algorytmu AES128 wymaga co najmniej setek tysięcy lat.

Podczas zestawiania bezpiecznego połączenia każdorazowo weryfikowana jest tożsamość obu stron połączenia w oparciu o indywidualne certyfikaty terminali.

W odróżnieniu od innych systemów telekomunikacyjnych najwyższym priorytetem platformy Securo™ jest bezpieczeństwo przesyłanych informacji. Jeżeli z jakichkolwiek przyczyn moduły diagnostyczne systemu wykryłby zagrożenie założonego poziomu bezpieczeństwa transmisji, to tak zagrożone połączenie nie zostanie zrealizowane, a obsługa systemu zostanie poinformowana o wykrytym zagrożeniu.

Szczegóły dotyczące zastosowanych rozwiązań bezpieczeństwa transmisji opisane są w dokumencie „Bezpieczeństwo funkcjonalne systemu SECURO™.

Platforma SECURO™ nie służy do przetwarzania informacji niejawnych w rozumieniu Ustawy z dnia 5.08.2010 r. „O ochronie informacji niejawnych” (Dz. U. z 2010 r. nr 182, poz. 1228).