Fundusze Europejskie – dla rozwoju innowacyjnej gospodarki

# Bezpieczny System Autoryzacji Transakcji Internetowych Oparty o Urządzenie Zewnętrzne

**Projekt współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka Działanie 1.4 – 4.1**

## Główny cel projektu:

Celem projektu jest rozbudowa aktualnej oferty firmy w zakresie systemów autoryzujących dokonywanie transakcji. Wynikiem projektu ma być opracowanie nowego, kompleksowego rozwiązania odpornego na istotne zagrożenia, jakie ograniczają bezpieczeństwo transakcji w aktualnie istniejących systemach. Lista najważniejszych, aktualnych zagrożeń została określona poprzez analizy przeprowadzone z udziałem aktualnych i potencjalnych klientów firmy Comarch oraz biorąc pod uwagę analizy dostępne powszechnie w prasie specjalistycznej i Internecie. W związku z rosnącym rynkiem bankowości internetowej oraz innych rozwiązań wykorzystujących Internet, a wymagających bezpiecznego przesyłu i potwierdzenia kluczowych danych, innowacyjne i unikalne rozwiązanie, jakim jest „Bezpieczny System Autoryzacji Transakcji Internetowych Oparty o Urządzenie Zewnętrzne T-PRO - Transaction Protector Token", powinno znaleźć szeroką gamę potencjalnych odbiorców.

## Opis:

Technicznie projekt polega na przeprowadzeniu szeregu badań, projektowaniu i stworzeniu prototypu fizycznego urządzenia T-PRO, obsługującej go części klienta oraz części serwerowej rozwiązania, odpowiedzialnej za stworzenie bezpiecznego tunelu do przesłania danych i weryfikację ich integralności. Rozwiązanie ma być zgodne z powszechnie przyjętymi standardami, wykorzystywać najnowsze i najpewniejsze algorytmy kryptograficzne oraz posiadać innowacyjny schemat architektury i scenariusza działań systemu. Projekt wymaga przeprowadzenia prac badawczo-rozwojowych, w celu uzyskania niezbędnej wiedzy do stworzenia prototypu, w tym wielu eksperymentów w zakresie implementacji silnych algorytmów kryptograficznych za pomocą tanich układów mikrokontrolerowych, tworzenia tuneli oraz zapewnienia poufności i integralności zestawionego kanału komunikacji.

W części wdrożeniowo-inwestycyjnej projektu głównym celem jest stworzenie finalnej, optymalnej wersji produktu, wykorzystując wiedzę uzyskaną podczas tworzenia jego prototypu i wywiadów przeprowadzonych z potencjalnymi klientami.

Firma planuje realizować projekt własnymi zasobami, w szczególności wykorzystując dział B+R działu bezpieczeństwa, posiłkując się usługami podmiotów zewnętrznych w zakresie wykonania elektronicznych i plastikowych elementów wchodzących w skład fizycznego urządzenia T-PRO.

Po zakończeniu projektu spółka powinna posiadać najbardziej zaawansowaną, innowacyjną i kompletną rodzinę produktów wspomagających dokonywanie transakcji. Pozwoli to na zbudowanie przewagi konkurencyjnej i zyskanie szansy na zwiększenie udziału rynkowego w Polsce, w krajach Unii Europejskiej i na świecie. Konsekwencją tego powinien być wzrost przychodów i dalszy rozwój działu bezpieczeństwa firmy Comarch, w szczególności jego komórki B+R. Wsparcie ze środków unijnych gra tu kluczową rolę, gdyż jednym z głównych czynników warunkującym uzyskanie liczącej się pozycji na rynku jest poziom bezpieczeństwa rozwiązania oraz jego cena. Dodatkowe fundusze pozyskane z PARP pozwolą na wykonanie szerzej zakrojonych badań przemysłowych, które umożliwią opracowanie i wykorzystanie bardziej zaawansowanych schematów bezpieczeństwa. Pozwolą także na zaimplementowanie rozwiązań, które zmniejszą koszt urządzenia, a tym samym jego konkurencyjność na rynku.

Innowacyjność projektu dotyczy innowacji produktowej na poziomie międzynarodowym, poprzez wprowadzenie na rynek nowego produktu o nazwie T-PRO, z rodziny rozwiązań do autoryzacji transakcji, który w sposób istotny wpłynie na uatrakcyjnienie oferty firmy Comarch.

Wnioskodawca od lat jest zaangażowany w dostarczanie klientom gotowych rozwiązań, które w wymierny sposób zwiększają bezpieczeństwo wykorzystywanych przez nich systemów i aplikacji. Szczególną klasę klientów stanowią tu banki i inne instytucje finansowe, dla których krytyczne jest zapewnienie integralności wykonywanych transakcji. Zadanie to staje się szczególne trudne, jeśli operacje wykonywane przy wykorzystaniu Internetu, medium, które ze swojej natury należy uznać za niezaufane. Banki udostępniając odpowiednie platformy swoim klientom mogą zapewnić wysoki stopień bezpieczeństwa wewnątrz swojej infrastruktury, ale platformy internetowe zawsze będą musiały korzystać z zasobów stacji klienta i ta część architektury niezmiennie stanowić będzie najsłabsze ogniwo rozwiązania. Największym zagrożeniem dla finansowych rozwiązań internetowych w dzisiejszych czasach są ataki typu *Men-In-The-Browser* oraz *KeyLoggers*. Ataki MITB polegają na podmianę danych zlecenia, wprowadzonych przez użytkownika, zanim jeszcze dane mogą zostać one ochronione przez system bankowy. Ataki *KeyLoggers* polegają na monitorowaniu zarówno przy pomocy fizycznego urządzenia, jak i specjalistycznych programów, wszystkich przycisków wciśniętych przez użytkownika. Pozwala to na podsłuchanie haseł do aplikacji,

kodów autoryzujących oraz kodów PIN do kart kryptograficznych. Przeciwdziałanie tym atakom jest bardzo trudne, a nawet niemożliwe, jeśli strona odpowiedzialna za architekturę rozwiązania nie ma bezpośredniego nadzoru nad stacją klienta, który korzysta z tego systemu. Produkt T-PRO pozwala na bezpieczną autoryzację transakcji, także w przypadku, gdy stacja klienta nie może być uznana za godną zaufania. Mechanizm tego rozwiązania pozwala skutecznie przeciwdziałać atakom MITB i *KeyLoggers*, o których wcześniej była mowa.

Innowacyjny charakter rozwiązania T-PRO opiera się przede wszystkim na pełnej realizacji wytycznych WYSIWYS, w architekturze, która nie może zostać skompromitowana niezależnie od tego czy stacja kliencka jest zaufana, czy też znajduje się tam wrogie oprogramowanie. Charakter tego rozwiązania sprawia, że może zostać ono wykorzystane w usługach realizujących krytyczne operacje finansowe z wykorzystaniem Internetu, tym samym znacząco zwiększając ich bezpieczeństwo.

Obecnie nie ma dostępnego na rynku urządzenia realizującego wytyczne WYSIWYS (ang. *What You See Is What You Sign*) w bankowości elektronicznej. Funkcjonalność ta, która jest dostarczana poprzez T-PRO, nie jest dostarczana przez żadnego innego producenta. Założenia WYSIWYS to bardzo istotne wymagania przy realizacji podpisów cyfrowych. Opisują one zachowanie systemu, w którym semantyczna zawartość podpisywanej wiadomości, nie może być w żaden sposób zmieniona, zarówno w przypadkowy jak i intencjonalny sposób. Te wymagania są w pełni realizowane poprzez T-PRO.

Innowacyjny charakter realizowany poprzez następujące cechy produktu:

1. Krytyczne dane transakcji (np.: konto docelowe, kwota transakcji) przekazane do instytucji finansowej, zostają jeszcze raz zweryfikowane przez użytkownika systemu z wykorzystaniem fizycznego urządzenia T-PRO. Weryfikacja odbywa się w oparciu o dane przekazane poza domyślnym kanałem – prezentowane są na wyświetlaczu urządzenia.
2. Użytkownik aktywnie uczestniczy w procesie weryfikacji.
3. Bezpieczeństwa weryfikacji w żaden sposób nie jest pochodną zaufania, jakim system darzy docelową stację kliencką. Tunel kryptograficzny (end-to-end) jest zestawiany bezpośrednio pomiędzy urządzeniem T-PRO, a serwerem działającym w infrastrukturze dostawcy usługi. Wszelkie zmiany dokonane w danych transakcji na stacji klienckiej czy też w wewnętrznej infrastrukturze sieci Internet, są w łatwy sposób wykrywane podczas operacji weryfikacji.
4. Komponenty działające na stacji klienckiej nie mają możliwości podmienienia danych transakcji przesłanych do weryfikacji. Połączenie nie jest rozszyfrowywane na stacji klienckiej.
5. Do podpisania danych transakcji może zostać wykorzystana istniejąca infrastruktura PKI istniejąca w organizacji. Urządzenia wspiera wykonywanie podpisów wykorzystujących klucze osadzone na kartach kryptograficznych.
6. Rozwiązanie zwiększa bezpieczeństwo wykorzystania kart inteligentnych poprzez dostarczenie bezpiecznego sposobu wprowadzenia PIN.

7. Urządzenie nie zmusza klienta do ponownego wprowadzenia danych transakcji, czy też do wprowadzania ich li tylko użyciem niewygodnej klawiatury osadzonej na urządzeniu. Dane mogą być wprowadzone raz, z użyciem wygodnego interface'u strony WWW, użytkownik na urządzeniu tylko potwierdza ich prawdziwość, ewentualnie odrzuca wykonanie transakcji.
8. Zostanie zastosowany innowacyjny sposób ochrony urządzenia przed typowymi atakami na urządzenia kryptograficzne. T-PRO nie będzie widziane w systemie, jako czytnik kart czy inne urządzenia bezpieczeństwa, ale jako klawiatura. Mimo to zostanie opracowany mechanizm umożliwiający, wspierania przez nie kryptograficznych usług systemy operacyjnego, takich jak zestawienie tunelu SSL z uwierzytelnieniem klienta.
9. Urządzenie jest niewielkich rozmiarów, tak, więc daje możliwość by użytkownik przenosił je ze sobą.
10. Jest podłączane do portu USB, tak, więc jest w stanie działać praktycznie z każdym aktualnie obecnym na rynku zestawem komputerowym.
11. Dane autoryzacyjne są w pełni powiązane z danymi transakcji. Nie ma możliwości podmiany danych transakcji i wykorzystania przechwyconych wcześniej danych autoryzacyjnych jak ma to miejsce w przypadku kodów sms czy też kodów pochodzących z urządzeń OTP.