

Entrust Rapid PKI

Metodyka projektowania i wdrażania Infrastruktury Klucza Publicznego

Informacje ogólne

Przygotował:
mgr inż. Mariusz Stawowski
Entrust Certified Consultant

Spis treści

WPROWADZENIE	3
POJĘCIA PODSTAWOWE	4
ETAPY PROJEKTU IKP	5
ETAP 1: ZAPLANOWANIE I ZAINICJOWANIE PROJEKTU	6
ETAP 2: ANALIZA WYMAGAŃ I PROJEKT	8
ETAP 3: PRZYGOTOWANIE I PRZETESTOWANIE OPROGRAMOWANIA	12
ETAP 4: INSTALACJA, INTEGRACJA I TESTOWANIE	13
ETAP 5: WDROŻENIE DOCELOWE	14
ETAP 6: UTRZYMANIE I OBSŁUGA	16
POTENCJALNIE TRUDNOŚCI WDROŻENIOWE	17
PODSUMOWANIE	18

Wprowadzenie

Sieci komputerowe są coraz częściej wykorzystywane jako szkielet strategicznych transakcji elektronicznych i handlowych. Zaletą tych rozwiązań jest błyskawiczny dostęp do ludzi, którzy potrzebują informacji. Wada polega na tym, że kluczowe systemy korporacji są narażone na potencjalne zagrożenia związane z bezpieczeństwem. W rezultacie - sieć zaufana i bezpieczna, która jest w zasięgu firmy to konieczność. Taka sieć daje wiele możliwości korzystania z zalet ważnych z punktu widzenia konkurencyjności oraz wpływa na polepszenie jakości procesów biznesowych w firmie. Coraz częściej, w celu podwyższenia swojej skuteczności na konkurencyjnym rynku globalnym, organizacje biznesowe polegają na bezpiecznej poczcie elektronicznej, elektronicznych formularzach, sieciach intranetowych, sieciach ekstranetowych oraz wirtualnych sieciach prywatnych (VPN).

W dzisiejszym globalnym środowisku e-biznesowym, firmom zależy na zaufaniu do partnerów biznesowych i przekonaniu, że jest zachowana prywatność informacji. W przypadku większych transakcji pieniężnych lub towarowych, klienci muszą wiedzieć, że transakcja jest wiążąca pod względem prawnym oraz towar jest dostarczony w stanie nienaruszonym. **Infrastruktura Klucza Publicznego (IKP)** daje ochronę aplikacjom wykorzystywanym w przedsiębiorstwie, w szczególności tym, które są wykorzystywane w e-biznesie. IKP dostarcza rozwiązania bezpieczeństwa dla szerokiego spektrum aplikacji biznesowych. Są dostępne rozwiązania bezpieczeństwa sieci WWW, e-mail, zdalnego dostępu, formularzy elektronicznych oraz innych aplikacji e-commerce. Mechanizmy bezpieczeństwa wewnątrz aplikacji są przezroczyste dla użytkowników końcowych i łatwe w użytkowaniu.

Tak jak większość implementacji systemów informatycznych wdrożenie IKP wymaga planowania i dodatkowych prac. Entrust, czołowy dostawca rozwiązań IKP na świecie, zapewnia w tym zakresie łatwą administrację i zarządzanie bezpiecznymi aplikacjami biznesowymi. Wymagane jest tylko raz wdrożyć mechanizmy bezpieczeństwa IKP dla wszystkich aplikacji biznesowych i użytkownik końcowy będzie musiał pamiętać tylko jedno hasło dla wszystkich aplikacji. Firma przeznaczając mniej nakładów na utrzymanie i pomoc techniczną oraz ze względu na unikalne możliwości zarządzania IKP, może uzyskać dodatkowe oszczędności.

Entrust oferuje swoim klientom pomoc we wdrożeniu rozwiązania IKP. *Entrust Professional Services* opracował kompleksową metodykę projektowania i wdrażania Infrastruktury Klucza Publicznego w skali korporacyjnej o nazwie *Rapid PKI*. W razie potrzeby Entrust dostarcza także usługi implementacyjne, oparte na doświadczeniach z wielu pomyślnie wykonanych wdrożeń.

Metodyka *Rapid PKI* obejmuje następujące etapy prac:

- 1. Zaplanowanie i zainicjowanie projektu**
- 2. Analiza wymagań i projekt**
- 3. Przygotowanie i przetestowanie oprogramowania**
- 4. Instalacja, integracja i testowanie**
- 5. Wdrożenie docelowe**
- 6. Utrzymanie i obsługa**

Pojęcia podstawowe

Infrastruktura Klucza Publicznego (IKP)

Powszechnie stosowana obecnie w systemach informatycznych kryptografia klucza publicznego daje podstawę bezpieczeństwa sieci poprzez szyfrowanie danych oraz podpisy cyfrowe. Wykorzystanie w systemach zabezpieczeń technik szyfrowania razem z podpisami cyfrowymi zapewnia:

- Uwierzytelnianie: pozwala na udział w e-biznesie zaufanych klientów, partnerów i pracowników.
- Autoryzację: pozwala na definiowanie reguł biznesu określających osoby, które mogą korzystać z określonych zasobów oraz warunki korzystania z tych zasobów.
- Poufność: zabezpiecza poufność ważnych informacji podczas ich przechowywania i przesyłania.
- Integralność: zabezpiecza transakcje przed ingerencją w ich treść i informuje o tym, że nie należy ufać zawartości informacji, jeżeli nastąpiła zmiana w stosunku do oryginalnej treści.
- Brak możliwości wyparcia się: uniemożliwia wyparcie się transakcji e-biznesowej przez dowolną ze stron po jej wykonaniu.
- Kontrolę audytu: umożliwia śledzenie audytu i rejestr ważnych i mniej ważnych zdarzeń, które wydarzyły się wewnątrz infrastruktury IKP.

Wszystkie w/w mechanizmy bezpieczeństwa są niezbędne do przeprowadzania rzeczywiście bezpiecznych elektronicznych transakcji handlowych.

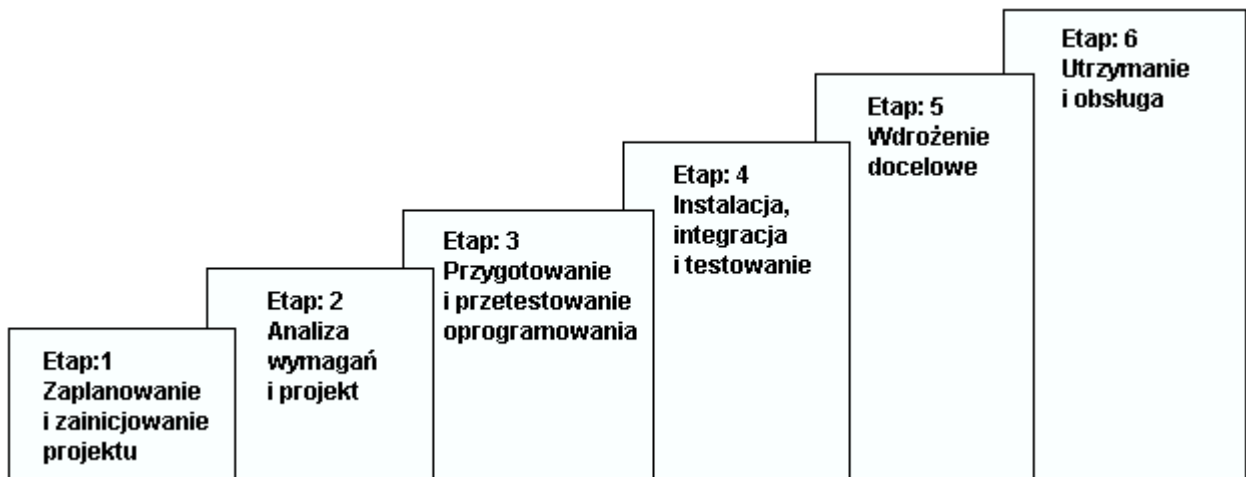
Zarządzalne IKP (Managed PKI)

IKP oferuje dostarcza do systemu informatycznego zabezpieczeń opartych na kryptografii z kluczem publicznym. Zasadniczym zadaniem infrastruktury IKP jest zarządzanie kluczami i certyfikatami wymaganymi przez usługi szyfrowania oraz podpisy cyfrowe w wielu aplikacjach oraz na wielu platformach. Aby spełnić w globalnym zakresie wymagania firm wykorzystujących aplikacje biznesu elektronicznego, infrastruktura IKP powinna oferować rozwiązania samo zarządzalne, jak to ma miejsce w przypadku Entrust. Zarządzalne IKP, to takie, które posiadają możliwości niezbędne do efektywnego, bezpiecznego i przezroczystego zarządzania kluczami i certyfikatami, a przy tym zapewniają szybki zwrot inwestycji oraz minimalny koszt użytkowania. Aby spełnić te wymagania, zarządzalne IKP zawiera zautomatyzowane funkcje, które są łatwe w użyciu, a ich administracja nie jest kosztowana. System Entrust/PKI umożliwia użytkownikom szyfrowanie, składanie podpisów cyfrowych oraz uwierzytelnianie transakcji elektronicznych we wszystkich aplikacjach z wykorzystaniem najlepszych w swojej klasie certyfikowanych mechanizmów bezpieczeństwa (m.in. FIPS 140-1 oraz Common Criteria).

Rozwiązania IKP, które nie umożliwiają automatycznego zarządzania kluczy kryptograficznych i certyfikatów w skali korporacyjnej są bardzo kosztowne i trudne w użytkowaniu. Głównie z tego powodu, że wymagają bardzo rozbudowanego personelu pomocy technicznej (Help Desk), ręcznie wykonującego m.in. generowanie i odświeżanie kluczy. Zarządzalne IKP to wydajne i łatwe w stosowaniu rozwiązania, które automatyzują procesy IKP oraz inne procesy związane z bezpieczeństwem wewnątrz organizacji. Dzięki zastosowaniu systemu Entrust/PKI, użytkownicy nie muszą wiedzieć nic na temat złożonych technik i teorii kryptografii.

Etapy projektu IKP

Skonfigurowanie IKP, które odpowiada celom bezpieczeństwa wymaga podjęcia wielu decyzji. Należy je podjąć przed instalacją jakiegokolwiek oprogramowania. Aby wspomóc podjęcie tych decyzji, firma Entrust opracowała kompleksową metodykę projektowania i wdrażania IKP o nazwie *Rapid PKI*. Metodyka służy jako przewodnik, w jaki sposób przyspieszyć i sprawnie wdrożyć rozwiązania bezpieczeństwa IKP.



Rys 1) Etapy projektowania i wdrożenia IKP

Etap 1: Zaplanowanie i zainicjowanie projektu

Ogólny plan wdrożenia infrastruktury klucza publicznego Entrust/PKI nie różni się od innych projektów informatycznych. Skuteczne wdrożenie IKP może być stosunkowo łatwe, ale tak jak wszystkie projekty dotyczące dużej infrastruktury, musi być właściwie zaplanowane i wykonane.

Tak jak w przypadku większości projektów informatycznych, należy określić cele i opracować ogólne wymagania, a także strategię wdrożenia, m.in.:

- **Dlaczego to robimy?**
- **Czy wdrożenie ma dotyczyć wykorzystania wewnątrz firmy, na zewnątrz, czy też wewnątrz i na zewnątrz?**
- **Co można osiągnąć już dziś?**
- **Co jest planowane na później?**

Należy określić liczbę osób oraz zakres systemów wykorzystywanych we wdrożeniu pilotażowym oraz we wdrożeniu docelowym. Wyznaczyć kierownika wdrożenia IKP, a w przypadku braków kadrowych zdecydować, czy korzystne jest powierzenie wdrożenia IKP zewnętrznym firmom.

Etap planowania i inicjowania projektu składa się z następujących podetapów:

- **Planowanie projektu**
- **Zaangażowanie sponsorów i kierowników projektu**
- **Określenie zakresu projektu wstępnego**
- **Opracowanie planu zarządzania projektem i sporządzenie odpowiedniej dokumentacji**

Planowanie projektu obejmuje działania związane z określeniem wymagań dotyczących celów oraz zakresu IKP, a także sporządzenie odpowiedniej dokumentacji. Należy zadać sobie pytanie, jakie obecnie istnieją problemy oraz jakie istnieją możliwości ich wyeliminowania poprzez IKP, a także precyzyjnie ustalić, co stanowi motyw wdrożenia IKP.

Przeanalizowanie i udzielenie odpowiedzi na te podstawowe pytania pozwoli na szybkie określenie celów projektu IKP. Określenie tych celów pozwoli na pomyślne wdrożenie IKP. Ponadto, cele te stosunkowo łatwo przekładają się na warunki, które musi zrozumieć zarząd firmy, aby mógł zaangażować się w projekt i zaoferować pomoc.

Jest to etap, w którym należy opracować dokument zwany jako **"business case"**, przeznaczony dla kierownictwa firmy, który odpowie na pytania, dlaczego ważne jest, aby posiadać IKP oraz jakiego rodzaju zwrotu inwestycji należy się spodziewać w przypadku wdrożenia zarządczego IKP.

Zaangażowanie sponsorów i kierowników projektu wewnątrz organizacji jest bardzo ważnym warunkiem, koniecznym do pomyślnego wdrożenia projektu.

- ✓ IKP nie jest same w sobie autonomiczne – dotyczy konkretnego problemu w biznesie.
- ✓ IKP wnosi zmiany w systemie informatycznym, dlatego też będzie potrzebne zrozumienie i pomoc kierownictwa.
- ✓ IKP wymaga czasu i wiedzy, dlatego też będzie potrzebne zaangażowanie wielu wysokiej klasy specjalistów.

Należy utworzyć silny zespół zarządzania projektem. Implementacja IKP jest przedsięwzięciem globalnym na poziomie przedsiębiorstwa, wymagającym użycia nowych technologii oraz procesów i współpracy pomiędzy wieloma komórkami organizacji.

Korporacja planująca wdrożenie IKP powinna utworzyć rdzeń zespołu projektowego złożony z osób o odpowiedniej wiedzy specjalistycznej, doświadczeniu w zarządzaniu projektami oraz posiadających tzw. „zmysł polityczny”. Dedykowany zespół projektowy IKP powinien składać się z przedstawicieli kilku obszarów funkcjonalnych, których będzie dotyczył projekt:

- Informatyków pracujących z użytkownikami,
- projektantów systemowych,
- projektantów aplikacji,
- projektantów strategii oraz twórców procedur,
- operatorów systemu,
- audytorów,
- prawników,
- pracowników serwisu.

Określenie zakresu projektu wstępnego wymaga zdefiniowania rozmiaru populacji użytkowników i aplikacji dla wstępnego wdrożenia pilotażowego.

Wdrożenie IKP przewidziane jest na część pilotażową z ograniczonym zakresem integrowanych aplikacji oraz część wdrożenia docelowego. Część pilotażowa wdrożenia IKP nie jest ewaluacją produktów w warunkach laboratoryjnych. Testy laboratoryjne należy wykonać wcześniej.

Opracowanie i stworzenie dokumentacji planu zarządzania projektem wymaga przygotowania specyfikacji i wymagań systemowych oraz sformułowania programu projektu z określeniem terminów ostatecznych.

Etap 2: Analiza wymagań i projekt

Przed wdrożeniem systemu Entrust/PKI, należy dobrze rozumieć wymagania, jakie powinna spełniać IKP, m.in.:

- Jakie powinna zapewniać bezpieczeństwo (np. integralność, brak możliwości wyparcia się, identyfikację użytkownika, itd., czy też wszystkie z wymienionych cech) i dla jakich zastosowań (aplikacji)?
- Jaka jest planowana polityka bezpieczeństwa?
- Jaka jest preferowana platforma sprzętowa?
- Czy istnieją inne rozwiązania IKP, które podlegają integracji?

Przed opracowaniem i wdrożeniem systemu Entrust/PKI, należy zadać te oraz dodatkowe pytania oraz udzielić na nie odpowiedzi i odpowiednio je przeanalizować.

Czasami, trudno jest określić, które systemy wymagają IKP. Poniższa tabela zawiera wskazówki w tym zakresie.

Bezpieczeństwo nie jest wymagane	Typowe wymagania bezpieczeństwa	Wysokie wymagania bezpieczeństwa
<ul style="list-style-type: none"> • Osobista poczta elektroniczna • Informacje WWW dostępne publicznie • Ogłoszenia o zatrudnieniu • Informacje o produktach • Informacje o kapitale firmy/ rozmiarze inwestycji 	<ul style="list-style-type: none"> • Korporacyjna poczta elektroniczna • Zamówienia o niskich kosztach • Transakcje na niewielką skalę • Status zamówień • Monitorowanie zapasów 	<ul style="list-style-type: none"> • Listy płac • Prognozy dotyczące produktów oraz sprzedaży • Umowy, dokumenty prawne • Raporty rządowe • Zamówienia na dużą skalę • Informacje uniemożliwiające wyparcie się • B2B/B2C

Tabela 1) Wskazówki do ustalenia zakresu IKP

Zdefiniowanie wymagań obejmuje także określenie zasobów (m.in. ludzkich), koniecznych do implementacji systemu Entrust/PKI. Akcent kładzie się na:

- Opracowanie „Polityki Certyfikacji” (**Certificate Policy**) oraz „Regulaminu pracy Urzędu Certyfikacji” (**Certification Practice Statements**).
- Inicjatywy dotyczące edukacji oraz współpracy pomiędzy oddziałami firmy.
- Opracowanie dokumentacji wymagań systemu IKP oraz projektu.
- Opracowanie dokumentacji wymagań dla komponentów IKP.
- Ustalenie potrzeb kadrowych oraz szkoleniowych.
- Zabezpieczenie (zakup) sprzętu i oprogramowania.

„Polityka Certyfikacji” oraz „Regulamin pracy Urzędu Certyfikacji” są podstawą współdziałania i zaufania pomiędzy różnymi podmiotami w systemie informatycznym oraz stanowią część polityki prawnej instytucji. Entrust dostarcza kompleksową listę elementów, które należy rozważyć przy tworzeniu tych dokumentów oraz zestaw wzorcowej dokumentacji.

Celem tworzenia dokumentów polityki bezpieczeństwa IKP jest opisanie procedur wewnątrz organizacji, które z wykorzystaniem technik kryptograficznych zabezpieczają wykonywanie operacji biznesowych. Polityka bezpieczeństwa utrzymuje i wspomaga realizację bieżących zadań w zakresie bezpieczeństwa i jakości usług systemu informatycznego dla działań handlowych organizacji. Ta polityka bezpieczeństwa nie jest specyfikacją wymagań planowanych mechanizmów bezpieczeństwa, ale definicją minimalnego zestawu reguł, które ustanowią wymagania bezpieczeństwa późniejszych mechanizmów. Połączenie bezpieczeństwa komputerowego, bezpieczeństwa łączności, bezpieczeństwa promieniowania ujawniającego, bezpieczeństwa osobowego, bezpieczeństwa fizycznego, bezpieczeństwa działania oraz bezpieczeństwa administracji stanowi obowiązującą politykę bezpieczeństwa.

"Polityka Certyfikacji" ustala najważniejsze zasady ochrony informacji w IKP w instytucji oraz zasady i metody stosowania w tym celu kryptografii. Zawiera ustalenia, w jaki sposób firma ma zarządzać materiałem kryptograficznym i wyznacza ich poziom należytej ochrony. „Regulamin pracy Urzędu Certyfikacji” to szczegółowy dokument opisujący procedury operacyjne IKP m.in. obsługa Urzędu Certyfikatów, generowanie, rejestrowanie i certyfikowanie kluczy, sposób i miejsce ich przechowywania, jak również metody dystrybucji certyfikatów.

Proces definiowania polityki rozpoczyna się w chwili, gdy kierownictwo organizacji identyfikuje potrzebę opracowania polityki bezpieczeństwa, określa odpowiedzialność za zarządzanie bezpieczeństwem poprzez ustanowienie kierownictwa bezpieczeństwa wewnątrz organizacji i zatwierdza ogólny koszt wdrożenia w organizacji oraz związanej z wdrożeniem obsługi. Istotnym czynnikiem pomyślnego ustanowienia polityki oraz jej wdrożenia jest utworzenie programu uświadamiania zagadnień bezpieczeństwa z odpowiednim dialogiem z użytkownikami.

Inicjatywy dotyczące edukacji oraz współpracy pomiędzy oddziałami firmy to spotkania oraz wewnętrzne kampanie na temat IKP, które uświadamiają ważność polityki bezpieczeństwa w przedsiębiorstwie. Najlepiej przeprowadzić wewnętrzne spotkania z każdą grupą wydziałową i objaśnić na nich zasady polityki bezpieczeństwa.

Opracowanie dokumentacji wymagań systemu IKP oraz projektu – IKP obejmuje swoim zasięgiem bardzo wiele elementów: osoby, informacje i systemy; pracowników, współpracowników, zleceniobiorców, klientów, partnerów; zasoby ludzkie, bezpieczeństwo fizyczne, aplikacje biznesowe, zarządzanie systemami i sieciami. Należy opracować proces sprawnej integracji tych elementów. Należy przy tym zrozumieć następujące wymagania:

- Gdzie są kluczowe elementy biznesu (*business drivers*), jaki poziom bezpieczeństwa dla nich jest odpowiedni?
- Gdzie są słabe punkty systemu, jakie są ograniczenia prawne i regulaminowe?

Analiza kosztów i przewidywanych korzyści dla biznesu są integralnie związane z analizą i projektem IKP. Po określeniu przez organizację wymagań systemowych, można przystąpić do procesu projektowania. Pierwszym krokiem jest opracowanie architektury wysoko-poziomowej, dla której określa się wysoko-poziomowe wymagania odpowiadające blokom funkcjonalnym systemu. Na podstawie tego projektu, projektant systemu może określić komponenty potrzebne do implementacji rozwiązania. Komponentami systemu mogą być produkty dostarczone przez firmę Entrust oraz firmy trzecie lub wytworzone we własnym zakresie.

Projekt architektury IKP w dużym stopniu zależy od wielu złożonych czynników takich jak dostęp wewnętrzny w porównaniu z zewnętrznym, rozkład obciążenia, strefy bezpieczeństwa, administracja, itp. W trakcie implementacji IKP należy rozważyć standardowy zbiór wskazówek/dobrych praktyk. Poniższy schemat przedstawia podstawowe komponenty architektury IKP.



Rys 2) Podstawowe komponenty architektury IKP

Opracowanie dokumentacji wymagań dla komponentów IKP. Należy zminimalizować ryzyko zagrożeń dla systemów informatycznych poprzez wybór lokalizacji obiektów z uwzględnieniem takich zagrożeń jak: powódzie, zakłócenia elektromagnetyczne oraz emisja elektromagnetyczna, przestępczość oraz wypadki przemysłowe. Należy także rozważyć łatwość i efektywność kontroli dostępu w budynkach z wieloma gospodarzami oraz budynkach publicznych. Zewnętrzne miejsca przechowywania danych lub kopii zapasowych nie powinny być narażone na te same zagrożenia fizyczne oraz środowiskowe, co zasadnicze obiekty (tzn. nie powinny znajdować się w obrębie tego samego budynku lub w bezpośrednim sąsiedztwie obiektu zasadniczego). Jeżeli istnieją zagrożenia pożarowe lub środowiskowe, należy stosować odpowiednie pojemniki przechowywania kluczowych nośników informacji zarówno wewnątrz systemu jak w miejscu przechowywania kopii zapasowych.

Definiowanie potrzeb kadrowych i szkoleniowych. Zazwyczaj obsługą systemu Entrust/PKI może zająć się personel informatyczny firmy w ramach swoich obowiązków. Zautomatyzowane procesy rejestrowania pracowników mogą wpłynąć na minimalizację nakładów pracy związanej z obsługą. Wewnątrz organizacji istnieje kilka osób, które uczestniczą we wdrożeniu oraz obsłudze systemu Entrust (fazy konfiguracji, wdrożenia i obsługi IKP).

Personel obsługi IKP zazwyczaj wymaga istnienia następujących osób funkcyjnych:

- administratorzy systemów (Windows NT, Novell i Unix),
- administratorzy sieci,
- programiści i projektanci aplikacji (oraz ich kierownicy),
- personel „Help Desk” i serwisowy, który zarządza instalacją i wspomaga działanie aplikacji biurowych.
- administratorzy usług katalogowych (np. Microsoft Active Directory, Netscape Directory lub innych usług katalogowych),
- administratorzy systemów aplikacyjnych (np. SAP/R3),
- pracownicy zarządzania zasobami ludzkimi i kadrami, którzy utrzymują bazę danych o wszystkich pracownikach organizacji,
- pracownicy ochrony,
- pomocniczy personel administracyjny,
- administratorzy Entrust.

W modelu Entrust/PKI istnieją cztery główne osoby funkcyjne:

- Administrator główny (Master User): utrzymuje centralne środowisko Entrust/PKI.
- Oficer bezpieczeństwa: określa politykę bezpieczeństwa i obsługuje kluczowe zagadnienia zaufania.
- Administrator Entrust: obsługuje codzienne zadania jak np. zarządzanie kluczami i użytkownikami.
- Administrator katalogu: dodaje użytkowników do katalogu.

Zakup sprzętu i oprogramowania jest kluczowy ze względu na określenie całkowitego kosztu użytkowania (TCO). Należy zdefiniować sprzęt wymagany przez system Entrust/PKI. Jakie jest bieżące środowisko i jakim sprzętem dysponują wydziały informatyki? Jaki ma być rozmiar docelowego systemu sprzętowego? Czy system będzie zdolny do osiągnięcia rozmiaru środowisk B2B oraz B2C?

Etap 3: Przygotowanie i przetestowanie oprogramowania

Etap 3 ma za zadanie przygotowanie niezbędnego oprogramowania oraz przetestowanie aplikacji systemu przed wykonaniem instalacji IKP. Opracowanie i przetestowanie własnych komponentów IKP pod względem odpowiednich wskaźników (użyteczność, nakład prac administracyjnych, obciążenie systemu, itp.) może także okazać się konieczne.

Bardzo ważne jest opracowanie podręcznika administrowania IKP w organizacji oraz przeprowadzenie szkoleń personelu IKP. Szkolenie jest przeznaczone dla personelu obsługującego IKP, władz rejestracyjnych oraz personelu pomocy technicznej (Help Desk).

W doprowadzeniu do akceptacji IKP w firmie kluczową rolę spełnia odpowiednio silne wsparcie dla użytkowników. Technicy pomocy technicznej (Help Desk) spełniają tu istotną rolę. Należy ich przygotować zarówno w zakresie wdrażania i rozwoju technologii IKP, jak i procesów wsparcia. Zazwyczaj obsługą systemu Entrust/PKI może zająć się personel informatyczny firmy w ramach swoich obowiązków.

Dostępne w Entrust/PKI zautomatyzowane procesy rejestrowania użytkowników oraz obsługi kluczy i certyfikatów mogą zminimalizować nakłady pracy administratorów. Nie znaczy to jednak, że personel obsługi nie musi być w pełni przeszkolony w zakresie administracji IKP. Obowiązkiem personelu obsługi jest administracja Entrust/PKI i systemów usług katalogowych (Active Directory, X.500) oraz pomoc techniczna (Help Desk).

Dostępne są szkolenia organizowane przez CLICO (kursy jednodniowe) oraz szkolenia autoryzowane Entrust (kursy pięciodniowe):

(szkolenia CLICO)

- 1/ Instalacja i konfiguracja Urzędu Certyfikacji na bazie technologii Entrust.
- 2/ Konfiguracja Check Point VPN-1/FireWall-1 w infrastrukturze PKI opartej na technologii Entrust.
- 3/ Instalacja i konfiguracja Entrust Web Connector i jego integracja z serwerami iPlanet i MS IIS.

(szkolenia autoryzowane Entrust)

- 1/ Entrust Authority Administrator Training.
- 2/ Entrust PKI Deployment Planning.
- 3/ Entrust/PKI Management.
- 4/ PKI Policies and Procedures.
- 5/ Securing Web-Business Solutions.
- 6/ InJoin LiveContent Directory Training.
- 7/ getAccess Fundamentals and Installations.

Zalecane jest, aby personel odpowiedzialny za zarządzanie Entrust/PKI przeszedł drogę certyfikacji: ***Entrust-Certified RA Specialist*** i ***Entrust-Certified Consultant***.

Etap 4: Instalacja, integracja i testowanie

W tej fazie prac następuje instalacja wszystkich komponentów IKP w organizacji. Wszystkie potencjalne problemy, jakie mogą wystąpić w docelowym wdrożeniu IKP są poddane wnikliwej analizie.

Etap 4 obejmuje następujące prace:

- Instalację urządzeń sieciowych, systemu zaporowego Firewall, sprzętu IKP, systemów operacyjnych oraz innych wymaganych komponentów oprogramowania (np. Active Directory).
- Instalację oprogramowania Entrust oraz pomocniczych systemów (np. sprzętowe repozytorium materiału kryptograficznego IKP).
- Testowanie wszystkich komponentów i funkcji IKP.

W tym etapie prac realizowane jest zespolenie wszystkich komponentów IKP. Wykonuje się testowanie integracji aplikacji systemu informatycznego, dla których usługi IKP będą dostępne m.in. integrację z serwerami WWW (np. iPlanet, IIS), urządzeniami VPN, bazami danych (np. Oracle), systemami aplikacyjnymi (np. SAP R/3), wdrożenie IKP na stacjach PC użytkowników. Tworzone są szczegółowe plany pilotażowego i docelowego wdrożenia systemu.

W trakcie etapu 4 odbywają się szkolenia dla personelu „Help Desk”.

Etap 5: Wdrożenie docelowe

Etap 5 rozpoczyna się to od wdrożenia pilotażowego dla ściśle ustalonego i kontrolowanego zakresu IKP. Po zakończeniu wdrożenia pilotażowego następuje wdrożenie IKP w poszczególnych działach organizacji.

Wdrożenie IKP w korporacji przebiega w następującej kolejności:

- ***Zaangażowanie społeczności użytkowników pilotażowych.***
- ***Uruchomienie systemu pilotażowego w czasie od czterech do sześciu tygodni.***
- ***Stopniowe (przyrostowe) wdrażanie IKP w przedsiębiorstwie.***

Wdrożenia pilotażowe można stosować wielokrotnie dla różnych obszarów systemu informatycznego (np. ochrona stacji PC, dostęp do aplikacji). Po wdrożeniu pilotażowym (4-6 tygodni) powinno następować stopniowe wdrożenie właściwe IKP.

Celem ostatecznym jest wdrożenie IKP w całym przedsiębiorstwie, ale należy stosunkowo wcześniej i z odpowiednią częstotliwością stosować pilotażowe wdrożenia dla małych grup użytkowników. Rozmiar grupy pilotażowej jest ograniczony do 50-500 użytkowników. Wybranie właściwej grupy pilotażowej ma znaczenie kluczowe. Jak wspomniano wcześniej, należy zidentyfikować „najlepszych” użytkowników w firmie (np. zdolnych, otwartych na zmiany pracowników). Użytkowników należy przygotować za pomocą biuletynu przesyłanego środkami informatycznymi. Wdrożenie IKP jest dla użytkowników istotną zmianą, dlatego należy przeszkolić ich z zagadnień bezpieczeństwa oraz wyjaśnić, dlaczego te zagadnienia są dla nich ważne. Wspólny dialog jest niezbędnym. To właśnie oni pomogą „sprzedać” IKP pozostałym pracownikom firmy. Czas trwania wdrożenia pilotażowego w dużej mierze zależy od rozmiaru początkowego sukcesu. Niezbędne jest przeanalizowanie wniosków z wdrożenia pilotażowego i wykorzystanie tych informacji w celu maksymalnego podniesienia jakości usług IKP.

W trakcie wdrożenia IKP należy zwrócić uwagę na dwie sprawy - dystrybucję oprogramowania oraz wstępną konfigurację klientów.

Dystrybucja oprogramowania

W przedsiębiorstwie należy rozprowadzić i wdrożyć oprogramowanie strony klienta Entrust/PKI. Ze względu na złożoność oprogramowania, jego rozmiar zazwyczaj przekracza pojemność standardowej dyskietki. W związku z tym, firma Entrust zaleca stosowanie innych metod dystrybucji oprogramowania. Metody te obejmują umieszczenie oprogramowania na centralnym serwerze do bezpośredniej instalacji, umieszczenie oprogramowania w ośrodku WWW do pobrania/installacji, przygotowanie dystrybucji na płytach CD, bądź zastosowanie istniejącego systemu automatycznej instalacji (np. MS SMS).

Aby uprościć proces instalacji oprogramowania przez użytkowników końcowych, zminimalizować liczbę decyzji podejmowanych w czasie instalacji oraz wymusić zastosowanie zalecanych parametrów konfiguracyjnych zdefiniowanych przez specjalistów informatyków oraz specjalistów z dziedziny bezpieczeństwa firma Entrust zaleca, aby jak najwięcej parametrów konfiguracyjnych oprogramowania klienckiego było ustawiane w pakiecie dystrybucji.

Produkty takie jak Entrust Desktop Suite zawierają swoje narzędzia konfiguracji. Ten rodzaj konfiguracji można jednak umieścić w dedykowanym pakiecie instalacyjnym.

Chociaż większość rozwiązań bezpieczeństwa w przedsiębiorstwie wymaga oprogramowania klienckiego, istnieje rozwiązanie oparte na WWW - Entrust/TruePass, nie wymagające instalacji i konfiguracji oprogramowania klienckiego na komputerach użytkowników. Dzięki temu Entrust/TruePass daje unikalne połączenie funkcji zarządzania ryzykiem oraz bezpieczeństwa z przezroczystością dla użytkownika i łatwością wdrożenia. System Entrust/TruePass jest rozwiązaniem bezpieczeństwa sieci WWW zabezpieczającym prywatność oraz dostarczającym związków zaufania pomiędzy firmami oferującymi usługi on-line oraz ich klientami, dostawcami i partnerami. System Entrust/TruePass wykracza poza ramy tradycyjnego rozwiązania bezpieczeństwa sieci WWW, ponieważ udostępnia funkcje tworzenia rejestru transakcji, ochronę kluczowych danych biznesu oraz ochronę prywatności.

Definiowanie użytkowników / inicjowanie oprogramowania klienckiego

Definiowanie użytkowników to w zasadzie proces złożony z trzech etapów, który obejmuje inicjowanie użytkowników, dystrybucję haseł dostępu oraz rejestrację użytkowników. Każdy użytkownik systemu Entrust/PKI musi być zainicjowany przez administratora. Administratorzy mogą wykonać inicjalizację ręcznie, poprzez wprowadzenie danych o użytkowniku lub za pomocą procesu zautomatyzowanego, gdzie do systemu Entrust/PKI jest systematycznie ładowana istniejąca baza danych o użytkownikach. Automatyzacja procesu jest zazwyczaj wymagana w przypadku istnienia obszernej społeczności użytkowników końcowych, których w efektywny sposób należy załadować do systemu.

Po wykonaniu inicjalizacji użytkowników przez administratora przypisuje się im hasła. W typowym środowisku Entrust/PKI hasło dostępu składa się z numeru referencyjnego oraz kodu autoryzacji. Problemem do rozwiązania w przypadku haseł jest ich efektywna dystrybucja do dużej populacji użytkowników końcowych. Do dystrybucji haseł można użyć np. koperty z „ślepej drukarki”, sieć WWW (SSL) lub interaktywny system rozpoznawania głosu.

W systemie Entrust/PKI klient generuje własną parę kluczy do tworzenia podpisu cyfrowego (tzw. klucze uwierzytelniania) i wysyła publiczny klucz weryfikacji do IKP (klucz prywatny do uwierzytelniania nigdy nie opuszcza klienta). Z kolei IKP generuje parę kluczy szyfrowania dla użytkownika. Dzięki temu nie ma problemów z archiwizowaniem kluczy użytkowników (Backup) przy jednoczesnym zachowaniu wysokiego poziomu bezpieczeństwa (np. w razie potrzeby korporacja może odtworzyć klucz deszyfrowania danych).

Istotne jest stopniowe i konsekwentne wdrażanie IKP w przedsiębiorstwie. Należy utrzymywać przy tym odpowiednią częstość wewnętrznego dialogu z użytkownikami. Będzie potrzebny taki sam zespół jak zespół przed wdrożeniem pilotażowym z większym naciskiem na zespół operacyjny. Rozmiar zespołu operacyjnego jest zmienny i zależy od:

- metody inicjalizacji użytkowników,
- zaangażowania użytkowników,
- wiedzy użytkowników.

Etap 6: Utrzymanie i obsługa

Po zakończeniu wdrożenia, przy działającym IKP, organizacja powinna zapewnić ciągłe działanie i obsługę systemu. Utrzymanie i obsługa obejmuje:

- prowadzenie ciągłej pielęgnacji systemu,
- wsparcie techniczne,
- sterowanie IKP.

Wykonywanie usług ciągłej pielęgnacji i wsparcia odbywa się za pomocą personelu operacyjnego. Usługi te obejmują:

- 1/ Administrację użytkownikami końcowymi (inicjalizację, odtwarzanie, unieważnianie).
- 2/ Przeglądanie logów systemowych.
- 3/ Wykonywanie kopii zapasowych systemu.
- 4/ Monitorowanie systemu i odtwarzanie.
- 5/ Pomoc techniczną.
- 6/ Raportowanie.
- 7/ Audyty bezpieczeństwa.
- 8/ Zbieranie uwag od użytkowników.
- 9/ Ciągłe monitorowanie zmian.

Potencjalnie trudności wdrożeniowe

- **Potrzeba aplikacji Entrust-Ready**

Aby zaspokoić potrzeby biznesu należy wybrać odpowiednie oprogramowanie klienckie przygotowane do pracy z systemem Entrust. Istnieje wiele takich aplikacji. Firma Entrust, w celu tworzenia produktów przygotowanych do pracy z systemem Entrust współpracuje z bardzo wieloma partnerami OEM. Oferuje także szkolenia z zakresu Entrust/Toolkit, które pozwala klientom tworzenie własnych aplikacji przygotowanych do współpracy z systemem Entrust.

- **Dystrybucja oprogramowania**

Dystrybucja oprogramowania stanowi istotny element każdej implementacji klient/serwer. W chwili obecnej dostępna jest dystrybucja w oparciu o ośrodki WWW, serwery sieciowe, instalacje poprzez systemy zarządzania aplikacjami oraz dystrybucja na płycie CD. System Entrust Desktop Suite umożliwia wybór pojedynczego źródła instalacji z parametrami domyślnymi możliwymi do konfiguracji przez klienta.

- **Dystrybucja haseł dostępu**

Dystrybucja haseł musi być efektywna i skuteczna. System Entrust/Authority zawiera mechanizmy, które umożliwiają zautomatyzowaną dystrybucję haseł. Popularne systemy dystrybucji opierają się o WWW, interaktywną odpowiedź głosem (IVR) oraz "ślepe drukarki" (*blind printers*).

- **Akceptacja użytkowników**

Akceptacja użytkowników jest kluczem do sukcesu wdrożenia systemu Entrust/PKI. Firma Entrust dostarcza materiały szkoleniowe końcowym użytkownikom np. dla Entrust/Entelligence, Entrust/Express oraz Entrust/ICE. Entrust/Entelligence umożliwia także logowanie Entrust na 32-bitowej platformie Windows, ułatwiając logowanie końcowych użytkowników. Spójny dialog z użytkownikami końcowymi IKP jest także ważnym elementem dla sukcesu wdrożenia IKP.

- **Potrzeba polityki i procedur**

Ważnym zagadnieniem jest opracowanie przez firmę dokumentów polityki bezpieczeństwa o nazwie „Polityka Certyfikacji” oraz „Regulamin pracy Urzędu Certyfikacji”. Większość klientów nie posiada doświadczenia, aby móc opracować te dokumenty. Entrust oferuje usługi konsultingowe i szkolenia, które pomagają klientom w opracowaniu dokumentów polityki bezpieczeństwa PKI.

Podsumowanie

Przedsiębiorstwa są pod ciągłym naciskiem prezentowania należytej pilności w ochronie informacji dotyczących klientów/partnerów oraz własnych, wewnętrznych dóbr intelektualnych. Ze względu na ciągły wzrost liczby transakcji on-line B2B oraz B2C, rośnie także odpowiedzialność przedsiębiorstw, co rodzi potrzebę zapewnienia odpowiedniego poziomu bezpieczeństwa i odporności na zagrożenia i ataki. Oprócz wymiernych strat finansowych związanych z niebezpieczeństwem, przedsiębiorstwo ponosi ryzyko utraty klientów ze względu na utratę dobrego imienia lub wiarygodności w oczach klientów. IKP daje ochronę aplikacjom wykorzystywanym w przedsiębiorstwie, w szczególności tym, które są wykorzystywane w e-biznesie. IKP dostarcza rozwiązań bezpieczeństwa dla szerokiego spektrum aplikacji biznesowych. Są dostępne rozwiązania bezpieczeństwa sieci WWW, e-mail, zdalnego dostępu, formularzy elektronicznych oraz innych aplikacji e-commerce. Mechanizmy bezpieczeństwa wewnątrz aplikacji są przezroczyste dla użytkowników końcowych i łatwe w użytkowaniu.

Tak jak większość implementacji systemów informatycznych wdrożenie IKP wymaga planowania i zastosowania sprawdzonej, kompleksowej metodyki. Entrust oferuje swoim klientom pomoc we wdrożeniu rozwiązania IKP. *Entrust Professional Services* opracował kompleksową metodykę wdrażania IKP w skali korporacyjnej o nazwie *Rapid PKI*. W razie potrzeby Entrust dostarcza także usługi implementacyjne, oparte na doświadczeniach z wielu pomyślnie wykonanych wdrożeń.

Dodatkowo, system Entrust/PKI zapewnia w odróżnieniu od rozwiązań konkurencyjnych łatwą administrację i zarządzanie bezpiecznymi aplikacjami biznesowymi. Wymagane jest tylko raz wdrożyć mechanizmy bezpieczeństwa IKP dla wszystkich aplikacji biznesowych i użytkownik końcowy będzie musiał pamiętać tylko jedno hasło dostępu dla wszystkich aplikacji (zwykle hasło dostępu do materiału kryptograficznego przechowywanego w bezpieczny sposób na karcie Smart Card lub USB Token). Firma przeznaczona dzięki temu mniej nakładów na utrzymanie i pomoc techniczną oraz ze względu na unikalne możliwości zarządzania IKP, może uzyskać dodatkowe oszczędności.