Wirtualna tożsamość w realnym świecie w obliczu nowych usług zaufania i identyfikacji elektronicznej

26.09.2013

PWPW
POLSKA WYTWÓRNIA PAPIERÓW WARTOŚCIOWYCH

Agenda

1. Wprowadzenie do wirtualnej tożsamości

2. Wirtualna tożsamość z perspektywy PKI

3. Skuteczne zarządzanie tożsamością

4. PWPW jako gwarant niezaprzeczalności

5. Wirtualna tożsamość w świetle nowych usług zaufania i identyfikacji elektronicznej

Wprowadzenie do wirtualnej tożsamości

Wirtualna tożsamość:

- istnieje potencjalnie;
- nie wyklucza rzeczywistej tożsamości;
- stanowi „tożsamość zastępczą" będąc jednocześnie jej źródłem;
- nie istnieje bez Internetu;
- wiąże ze sobą miliony ludzi;
- odwzorowuje nasze myśli i fantazje;
- pozwala na kreowanie i istnienie w innym świecie – świecie wirtualnym, który jest obecnie częścią naszej codzienności

Wprowadzenie do wirtualnej tożsamości

Wirtualna tożsamość jest poniekąd światem wyobraźni, iluzji stworzonej przez człowieka za pomocą różnych sposobów i metod

Problem:

Jak stwierdzić prawdziwą tożsamość osoby w wirtualnym świecie?

Rozwiązanie:

Zaproponowanie koncepcji otwartej na różne technologie i usługi w dziedzinie elektronicznego uwierzytelnienia, nadążającej za rozwojem technologicznym o globalnym charakterze

Wirtualna tożsamość z perspektywy PKI

PKI (Public Key Infrastructure) *jest przykładem otwartej koncepcji, która doskonale nadaje się do stwierdzenia tożsamości w sieci Internet poprzez wydawane na jej bazie certyfikaty elektroniczne.*

Z certyfikatu dowiadujemy się m.in. :

- o **właścicielu** certyfikatu (Subskrybencie);
- o **kluczu publicznym** właściciela certyfikatu;
- o **przeznaczeniu** certyfikatu (podpis, szyfrowanie);
- o **okresie ważności** certyfikatu
- o **wystawcy** certyfikatu (Urzędzie certyfikacji);
- o **numerze seryjnym** certyfikatu

Wirtualna tożsamość z perspektywy PKI

*Certyfikat elektroniczny poprzez podpisanie go przez zaufanego wystawcę gwarantuje nam jego autentyczność i stanowi naszą **wirtualną tożsamość** w Internecie.*

Cechy wirtualnej tożsamości PKI:

- powinna być porcją danych;
- powinna być jednoznacznie opisana (unormowana);
- powinna zawierać jednoznaczne wskazanie na jej posiadacza;
- powinna wykorzystywać mechanizmy kryptografii w celu zagwarantowania integralności i poufności informacji;
- powinna zawierać klucz publiczny;
- powinna być potwierdzona przez organ cieszący się powszechnym zaufaniem;
- powinna być uplasowana prawnie;
- powinna być ogólnie przyjęta i zaakceptowana

Wirtualna tożsamość z perspektywy PKI

Problem:

Kradzież tożsamości – raz skradziona wirtualna tożsamość pozwala na zarządzanie nią przez hackera w całym wirtualnym świecie

Rozwiązanie:

Skuteczny sposób na uniknięcie kradzieży tożsamości w wirtualnym świecie to PKI i certyfikaty elektroniczne, których domeną są:

- *Identyfikacja;*
- *Autoryzacja;*
- *Uwierzytelnienie;*
- *Niezaprzeczalność.*

Skuteczne zarządzanie tożsamością

Fakt:

Nie unikniemym wirtualnej tożsamości, ale bądźmy świadomi szans i zagrożeń z nią związanych, zarządzajmy tożsamością

Jak zarządzać tożsamością:

•wykorzystać mechanizmy systemów zarządzania tożsamością;

•zarządzać dostępem zgodnie z obowiązującymi regułami polityki bezpieczeństwa (np. przydzielanie certyfikatów cyfrowych, którym umożliwia się dostęp do najbardziej sekretnych danych);

•ułatwianie dostępu do różnych systemów przez możliwość jednokrotnej rejestracji;

•zarządzanie uprawnieniami centralizując administrację uprawnieniami użytkowników;

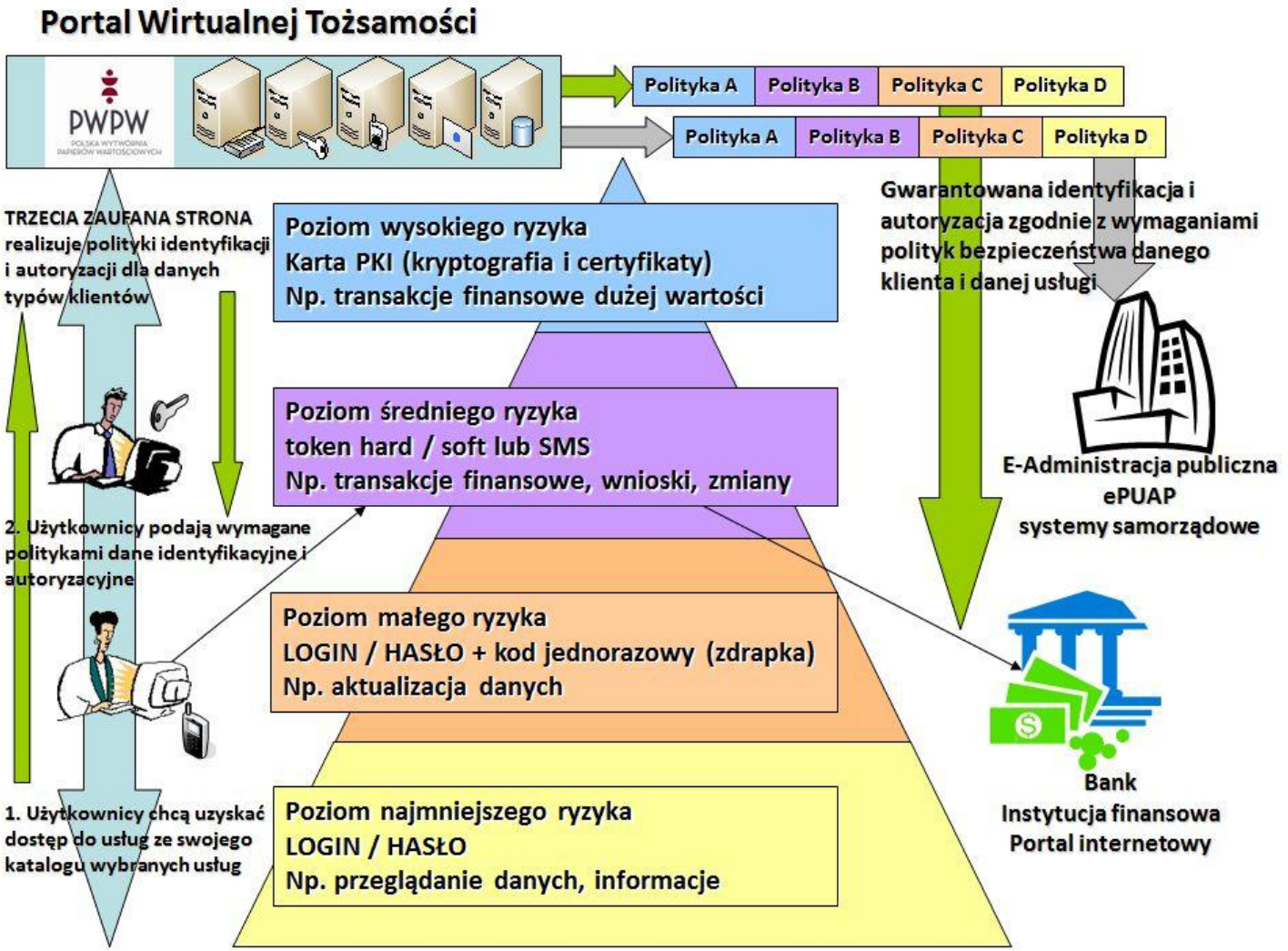
PWPW jako gwarant niezaprzeczalności

- **PWPW S.A. jako Trzecia Zaufana Strona może być gwarantem niezaprzeczalności wirtualnej tożsamości;**

Propozycja: Portal Zarządzania Tożsamością

- identyfikacja użytkownika na żądanie;
- jednolita metoda logowania użytkownika;
- autoryzacja operacji logowania przez zaufany podmiot np. PWPW;
- ustalanie polityki zarzadzania tożsamością np. identyfikator i hasło;
- uzyskanie przez użytkownika listy możliwych dla siebie dostępów do usług (firma pracodawca, bank, towarzystwo emerytalne, ubezpieczyciel, ZUS, urząd gminy, urząd skarbowy itd.);
- podmiot obsługujący taki Portal sprawdza zgodność żądanego dostępu z określoną polityką identyfikacji;
- system klienta zachowuje własne mechanizmy uwierzytelnienia i weryfikacji danych użytkownika,
- nie nakłada ograniczeń biznesowych lub technologicznych na klienta;

PWPW jako gwarant niezaprzeczalności



Wirtualna tożsamość w świetle nowych usług zaufania i identyfikacji elektronicznej

Lipiec 2012 – *projekt rozporządzenia w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym* (eIDAS);

Założenia:

- idea przewodnia eIDAS – harmonizacja rynku cyfrowego UE w oparciu o trzy kluczowe elementy: podpis elektroniczny, elektroniczną identyfikację i usługi zaufania;
- forma Rozporządzenia w celu zapewnienia jednolitej interpretacji zapisów przez kraje członkowskie; wiążące i obowiązuje natychmiast po wejściu w życie w prawie wewnętrznym państw członkowskich;
- zapewnienie transgranicznego uznawania i akceptacji elektronicznej identyfikacji (eID);
- ujednolicenie ram prawnych świadczenia usług zaufania oraz nadzoru nad dostawcami usług eID w UE;
- wprowadzenie nazwanych usług zaufania związanych z elektronicznymi transakcjami, tj. podpisami elektronicznymi, pieczęciami elektronicznymi, znakowaniem czasem, dokumentami elektronicznymi, archiwizacją dokumentów elektronicznych, usługami przekazu elektronicznego oraz uwierzytelnianiem witryn internetowych.

Wirtualna tożsamość w świetle nowych usług zaufania i identyfikacji elektronicznej

Zagrożenia:

•przekazuje uprawnienia do przygotowania odpowiednich aktów delegowanych oraz aktów wykonawczych, które w chwili obecnej nie istnieją i nie wiemy jaki będzie ich kształt;

•nakazuje uznawać i akceptować notyfikowane środki identyfikacji elektronicznej dla tych usług w przypadku których zgodnie z prawem tego państwa dostęp do usługi elektronicznej wymaga identyfikacji elektronicznej;

•nie precyzuje wymagań, które muszą być spełnione, aby dostawca mógł być uznany za kwalifikowanego dostawcę usług.

Podsumowanie

- Korelacja z różnymi poziomami identyfikacji i autoryzacji (Portal Wirtualnej Tożsamości) a planowanymi nowymi usługami (eIDAS) - im dane bardziej newralgiczne tym mocniejsze zabezpieczenie należy zastosować
- Dzięki planowanym, jednolitym i uznanym mechanizmom identyfikacji i autoryzacji w ramach UE, jest szansa na współpracę ze sobą instytucji wzajemnie sobie ufających (np. poprzez centralny Portal)

Cel do osiągnięcia:

- Należy dążyć z jednej strony do ograniczenia ryzyka płynącego z wykorzystania wirtualnej tożsamości, z drugiej zaś strony umożliwić podmiotom elastyczne działanie w świecie wirtualnym - uzyskanie maksimum bezpieczeństwa przy utrzymaniu maksimum prywatności

Dziękuję

Artur Miękina
Channel Sales Manager
a.miekina@pwpw.pl

Tel. (22) 324 30 11; 693 100 949
00-225 Warszawa, Zakroczymska 13
Pion Rozwiązań Informatycznych
Polska Wytwórnia Papierów Wartościowych S.A.