ARTUR ŻARSKI

Zarządzanie tożsamością

Stopień trudności

Zarządzanie tożsamością jest bardzo szerokim pojęciem, które posiada wiele definicji. Definicje te można sprowadzić do stwierdzenia, które mówi, że jest to zestaw technologii i procedur umożliwiający efektywne zarządzanie cyklem życia tożsamości użytkownika.

Cykl ten składa się z trzech podstawowych elementów, na które składają się usługi:

- Usługi katalogowe, czyli repozytoria przechowujące informację o tożsamościach i uwierzytelnienia oraz uprawnienia;
- *Access management*, czyli procesy weryfikacji uwierzytelnień, kontroli dostępu do zasobów (w tym przyznawania i odbierania dostępu) zgodnie z uprawnieniami stosownymi do roli;
- Identity Lifecycle Management, czyli zestaw zdefiniowanych procesów tworzenia, usuwania oraz modyfikacji ustawień kont, zarządzania zmianami stanu i informacji o tożsamości wraz z informacją o uprawnieniach.

Procesy związane z zarządzaniem tożsamością są powszechnie znane. Wiele firm stosuje własne rozwiązania, ale z drugiej strony znaczna liczba organizacji wdraża gotowe systemy i aplikacje pomagające w codziennej pracy. W chwili obecnej w wielu przedsiębiorstwach można nadal napotkać na problemy związane z zarządzaniem tożsamością, które mogą powodować ogromny chaos dla użytkowników. Na czym polega taki chaos? Ogólnie rzecz biorąc, w każdym przedsiębiorstwie istnieje więcej niż jeden system, który wymaga logowania do niego, oraz więcej niż jeden użytkownik, który ma takie, a nie inne uprawnienia. Każdy z tych użytkowników posiada swoje własne hasło logowania do takiego systemu, a zatem – im więcej systemów, tym większa konieczność pamiętania nazw użytkowników i haseł. Z punktu widzenia administratorów systemy zarządzające użytkownikami w sposób zdecentralizowany również są problematyczne. Co zatem można zrobić? Czy jest jakaś możliwość, aby omawiany proces był łatwiejszy, bezpieczniejszy i przede wszystkim bliższy optymalnemu? Oczywiście, że jest – kwestia kluczowa to wdrożenie systemu zarządzania tożsamością.

Systemy zarządzające tożsamością posiadają wiele funkcji, wśród których można wyróżnić między innymi:

- Zarządzanie nowym użytkownikiem – utworzenie konta, utworzenie uwierzytelnienia, nadanie odpowiednich praw dostępu;
- Kasowanie – kasowanie lub blokada konta, kasowanie lub blokada praw dostępu;
- Zarządzanie hasłami – sprawdzanie *siły* hasła, reset hasła;
- Zmiany typu konta – awanse, transfery, nowe przywileje, zmieniające się atrybuty, etc.

Do tego wszystkiego dochodzi stworzenie metabazy, która będzie te wszystkie informacje gromadzić i synchronizować pomiędzy różnymi

Z ARTYKUŁU DOWIESZ SIĘ

artykuł przedstawia zagadnienia związane z zarządzaniem tożsamością na platformie Microsoft ze szczególnym uwzględnieniem CardSpace.

CO POWINIENEŚ WIEDZIEĆ

nie jest potrzebna żadna szczegółowa wiedza dotycząca technologii. Jest to artykuł wprowadzający w temat zarządzania tożsamością.

systemami, a także będzie posiadać mechanizm raportowania tego, co się aktualnie dzieje w systemie.

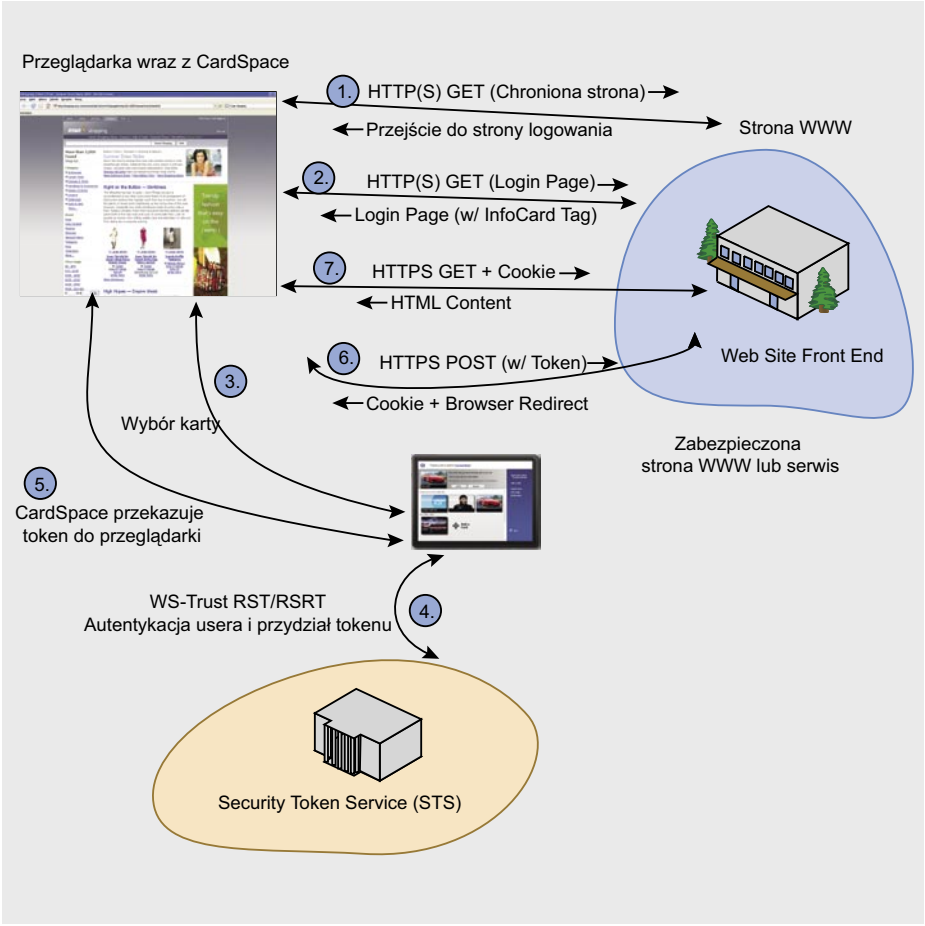
Na czym polega w takim razie synchronizacja? Do jej zadań należy między innymi automatyzacja zarządzania życiem obiektów (*provisioning* oraz *deprovisioning*), przepływ danych pomiędzy katalogami, przechowywanie informacji o relacjach pomiędzy obiektami odpowiadającymi tej samej tożsamości, które znajdują się w różnych katalogach. Proces synchronizacji zapewnia, że będziemy posiadać spójne dane w zintegrowanych katalogach, że podstawowe informacje będą replikowane do wszystkich katalogów oraz że dysponujemy aktualnymi danymi.

Przy opisywaniu procesu synchronizacji spotykamy dwa nowe hasła: provisioning oraz proces odwrotny, czyli *deprovisioning*.

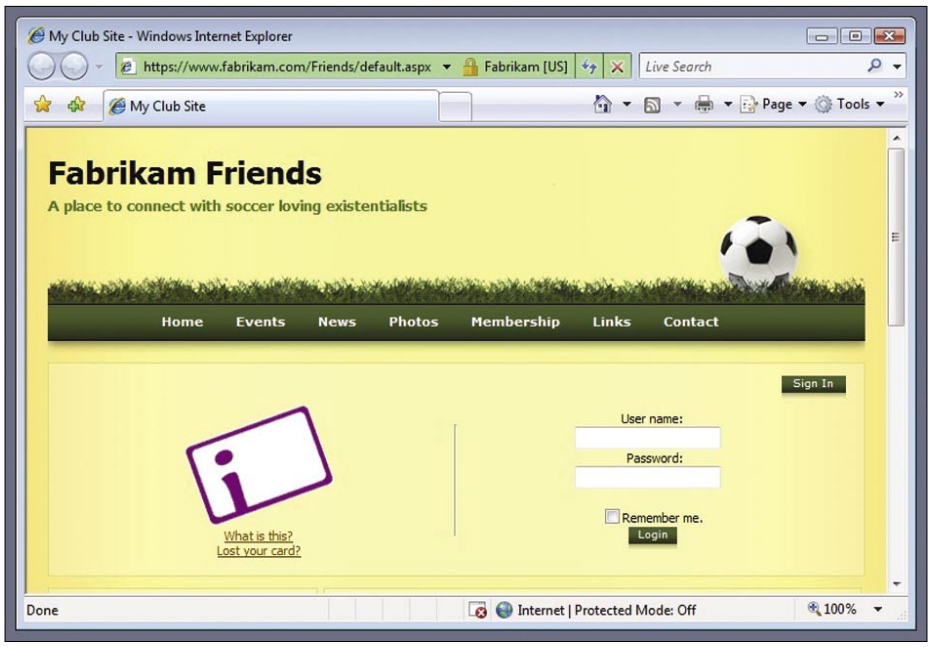
Pierwsze z tych pojęć to automatyzacja procesu dostępu do zasobów, w których użytkownik otrzymuje swoje własne uprawnienia w sposób zupełnie automatyczny na bazie danych wejściowych.

Zestaw reguł definiuje, w jakich repozytoriach i na jakich zasadach użytkownik powinien mieć dostęp do zasobów. Provisioning to nie tylko tworzenie kont, ale również tworzenie unikalnego loginu i innych atrybutów, które są zgodne z zadanymi konwencjami nazewnictwa, przypisanie do odpowiednich ról lub grup, do kontenerów zgodnie ze stanowiskiem, ustawienie i przekazanie pierwszego hasła dostępowego, wysłanie wiadomości powitalnej, etc. *Deprovisioning* to proces odwrotny.

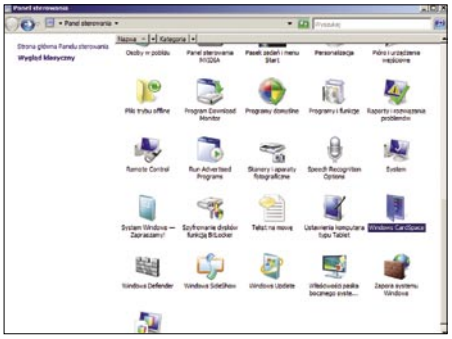
Przejdźmy zatem do głównego tematu artykułu, czyli zarządzania tożsamością przy wykorzystaniu produktów Microsoft i dokładniejszego omówienia jednego z nich. Microsoft w swoim katalogu rozwiązań posiada wiele produktów lub technologii, które umożliwiają zarządzanie tożsamością. W dalszej części tekstu postaram się je wszystkie przedstawić.



Rysunek 1. *Schemat działania CardSpace*



Rysunek 2. *Logowanie do strony przy użyciu CardSpace*



Rysunek 3. *CardSpace w Panelu Sterowanie*

Do rozwiązań związanych z zarządzaniem tożsamością należą między innymi:

- Access Control List – lista kontroli dostępu, skojarzona z plikiem lub obiektem, zawierająca informacje o użytkownikach, procesach lub obiektach, które mogą uzyskiwać do niego dostęp.
- Active Directory – usługi katalogowe dla systemu Windows Server;
- ADAM (AD LDS), ADFS – *Active Directory Application Mode* oraz *Active Directory Federation Services*, czyli specjalne tryby pracy dla Active Directory, które nie wymagają zależności wymaganych w przypadku usługi katalogowej (np. nie wymagają wdrażania domen ani kontrolerów domen);
- CardSpace – omawiany w dalszej części artykułu;
- Kerberos – protokół, który do autoryzacji wykorzystuje centrum dystrybucji kluczy;
- MIIS (*Microsoft Identity Integration Server*) – stanowi najważniejszy komponent w systemach zarządzania tożsamością. Jest narzędziem, którego zadaniem jest kontrola operacji provisioningu nowych tożsamości i deprovisioningu już istniejących, zarządzanie hasłami i synchronizowanie danych pomiędzy podłączonymi źródłami danych;
- ILM (*Identity Lifecycle Manager*) – jest platformą dla synchronizacji tożsamości, certyfikatów i zarządzania hasłami oraz użytkowników (następca MIIS).
- LiveID – *Windows Live ID* (dawniej Microsoft Passport lub .NET Passport) to ogólnodostępny, jednolity system, umożliwiający dowolnym użytkownikom (nie tylko klientom Microsoft) korzystanie ze wszystkich stron Microsoft wymagających logowania.

Rysunek 4. *Pusta lista kart*

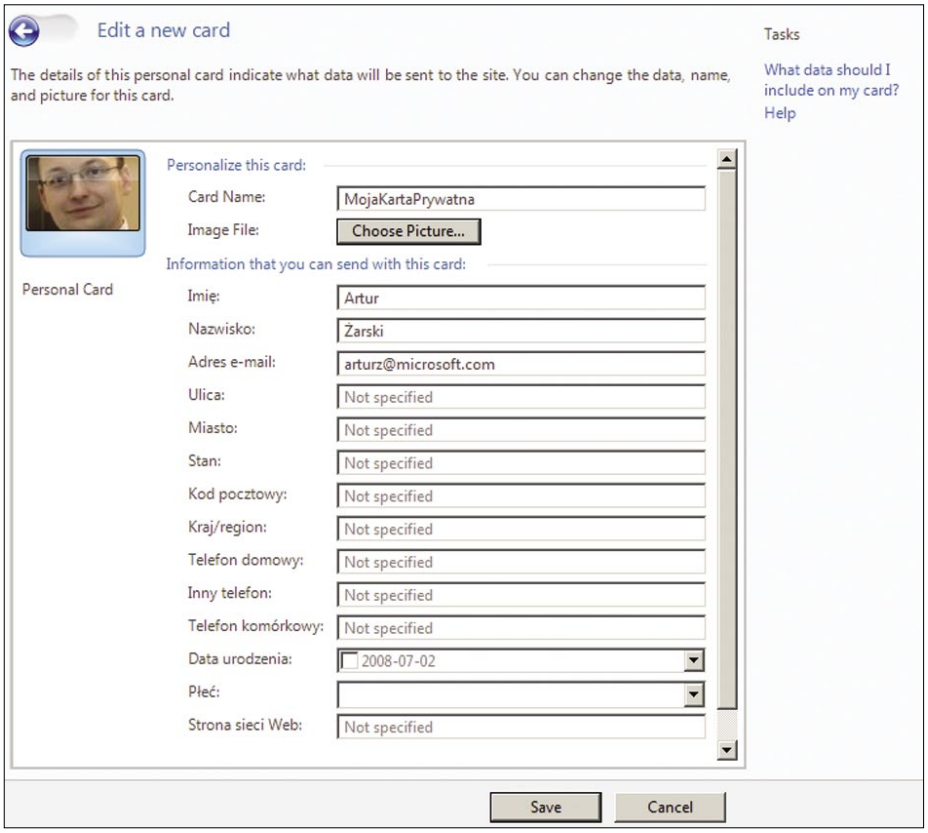
CardSpace

CardSpace to technologia identyfikacji i zarządzania tożsamością zaimplementowana w Windows Vista (dostępna także w Windows XP jako część .NET Framework 3.0). Poprzednia nazwa tej technologii to InfoCard. W Cardspace poszczególni wystawcy tożsamości są prezentowani użytkownikowi w postaci kart. Na karcie zapisywane są metadane reprezentujące możliwości wystawcy takiej tożsamości. Wśród nich możemy wyróżnić: rodzaje dostarczanych stwierdzeń, formaty tokenów, lokalizację STS. Karta jest reprezentowana przez dokument XML zawierający metadane i obrazek podpisany przez wystawcę przy użyciu XMLDSIG (XML *digital signature*). Dokument ten (w postaci pliku **.crd*) stanowi kartę informacyjną (ang. *Information Card*), która reprezentuje relację użytkownika z wystawcą tożsamości. Istnieją dwa rodzaje kart:

- osobiste – przypominające wizytówki, mają one kilkanaście pól zawierających podstawowe dane, karty te tworzy sam użytkownik,

Listing 1. *Uruchomienie CardSpace w aplikacji ASP.NET 2.0*

```
<form name="logon page" method="post"
   …
   <object type="application/x-informationcard" name="xmlToken">
      <param name="tokenType" value="urn:oasis:names:tc:SAML:1.0:assertion">
      <param name="issuer" value="http://schemas/.../identity/issuer/self">
      <param name="requiredClaims"value=
        "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
          http://"http://schemas/.../identity/claims/privatepersonalidentifier">
   </object>
</form>
```



Rysunek 5. *Tworzenie nowej karty*

- zarządzane – wydawane przez instytucje (np. pracodawcę), zawierające dowolną liczbę pól, są one przechowywane na serwerze instytucji, która je wydała.

Użytkownicy autentykują się do stron WWW oraz różnych serwisów przez wybranie z zestawu wirtualnych identyfikatorów (kart) tej, która identyfikuje użytkownika. Użytkownik może mieć kilka kart, które mogą mu służyć do autoryzacji w różnych serwisach lub stronach.

Założenia dla CardSpace są następujące:

- Niezależne od przeglądarki – zdefiniowane są mechanizmy wspierające implementację dla dowolnej przeglądarki i na dowolnej platformie;
- Niezależne od serwera WWW – protokoły komunikacyjne wspierane są przez dowolną stronę WWW oraz platformę;
- Minimalna ingerencja w stronę WWW – udogodniona adaptacja mechanizmu przez minimalne zmiany w istniejącej stronie;
- Brak stałej integracji z przeglądarką – obsługa kart ma być plugin'em do przeglądarki, a nie jej częścią integralną;
- Praca z przeglądarką przy wysokim poziomie bezpieczeństwa – dostarczany mechanizm aktywacji wyboru pozwala na pracę również wtedy, gdy przeglądarka ma ustawiony poziom bezpieczeństwa *Wysoki*.

Przepływ pracy użytkownika i poszczególnych elementów systemu przedstawiony został na Rysunku 1. Jak widać z tego rysunku, pierwszym krokiem użytkownika po wejściu na stronę, która wykorzystuje CardSpace, jest przejście na stronę logowania. W momencie, kiedy użytkownik ma się zalogować do strony, zostaje poproszony o podanie hasła lub wybór karty (Rysunek 2). Po wyborze karty przez użytkownika zostaje ona przekazana do centrum autoryzacji w celu potwierdzenia tożsamości. Dzieje się to zupełnie automatycznie, bez wiedzy użytkownika.

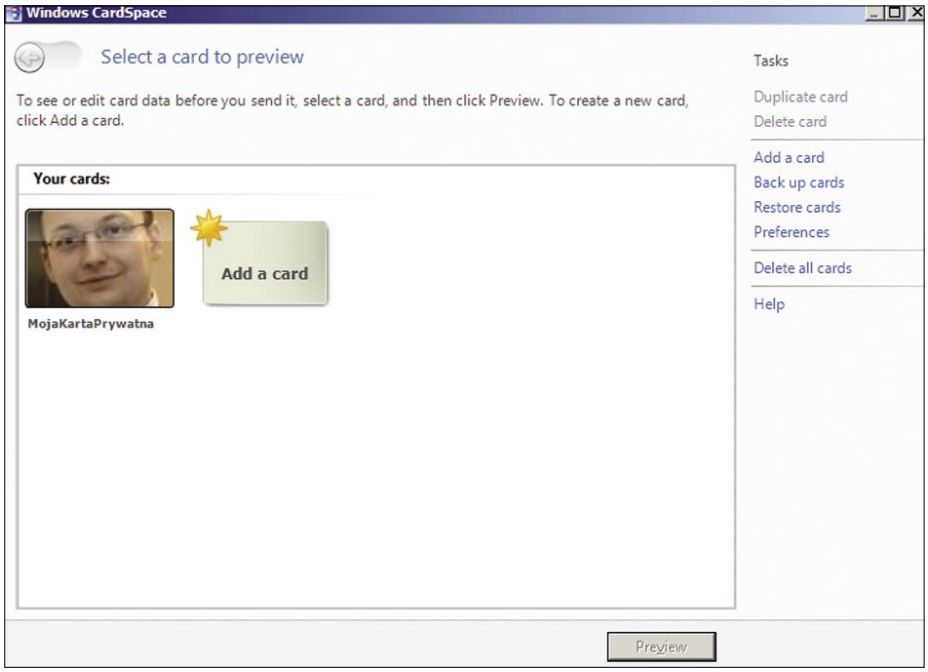
Jeśli użytkownik zostanie zweryfikowany poprawnie, otrzymuje token, którym następnie posługuje się przeglądarka w komunikacji z wybraną stroną WWW.

Z punktu widzenia użytkownika końcowego praca z CardSpace jest bardzo prosta. Na przykładzie Windows Vista prześledźmy proces tworzenia takiej karty. W Panelu Sterowania znajdujemy opcję odpowiedzialną za CardSpace (Rysunek 3). Następnie uruchamiamy tę opcję i dostajemy listę stworzonych kart. W naszym przypadku lista jest pusta (Rysunek 4). Wybieramy opcję Utwórz nową kartę i zostajemy poproszenie o wybranie rodzaju karty. Wybieramy karta osobista i wypełniamy ją danymi (Rysunek 5). Po zapisaniu danych nasza lista z karatami została wzbogacona o nowo utworzoną kartę (Rysunek 6).

We wcześniejszym fragmencie tekstu dotyczącym założeń napisałem, że kwestia integracji aplikacji Web z mechanizmem kart ma być prosta. Jak zatem wygląda taka integracja? Generalnie należy dodać fragment kodu HTML, który będzie odpowiadał za pokazanie selektora kart. Jest to jasno zdefiniowany typ aplikacji, który osadzamy jako obiekt na stronie. Poniżej fragment kodu HTML odpowiedzialny za ten proces.

Z punktu widzenia programisty to w zasadzie wszystko. Ze strony konfiguracji witryny wymagane jest włączenie protokołu HTTPS oraz obsługi Extended Validation dla certyfikatów.

Jeśli chodzi o implementację InfoCard, to nie tylko Microsoft jest tutaj dostawcą rozwiązania. Jest wiele inicjatyw i projektów Open Source, które również je wspierają. Są to rozwiązania wspierane między innymi przez IBM, Novell, Red Hat, Sun, VeriSign i innych, dla których Microsoft oferuje pełne wsparcie technologiczne. Interoperacyjność poprzez opublikowane w sieci protokoły została pokazana na przykładzie gotowych rozwiązań, które służą między innymi do wyboru identyfikatorów, systemów sprawdzających tożsamość oraz dostawców tożsamości. W Internecie opublikowana jest pełna dokumentacja dla CardSpace wraz z przykładami użycia, implementacji, technologii, protokołów.



Rysunek 6. *Nowo utworzona karta na liście kart*

Artur Żarski
Jest pracownikiem firmy Microsoft. Na co dzień zajmuje się m.in. tworzeniem rozwiązań w oparciu o SQL Server w różnych aspektach – bazy relacyjne, usługi integracyjne, usługi analityczne. Jest certyfikowanym administratorem baz danych (MCDBA).
Kontakt z autorem: *arturz@microsoft.com*