STUDIA INFORMATICA 2006
Volume 27 Number 4 (69)

Michał LEWANDOWSKI
Politechnika Śląska, Instytut Informatyki

KARTY INTELIGENTNE W PROCESIE UWIERZYTELNIANIA UŻYTKOWNIKA W SYSTEMACH OPERACYJNYCH MICROSOFT WINDOWS

Streszczenie. W publikacji opisano proces uwierzytelniania użytkowników w systemach operacyjnych Microsoft Windows. Przedyskutowano obecne możliwości systemów w tym zakresie, ze szczególnym zwróceniem uwagi na możliwość zastosowania kart inteligentnych w procesie uwierzytelniania.

Słowa kluczowe: karta inteligentna, uwierzytelnianie użytkownika, certyfikat, bezpieczeństwo danych, Microsoft Windows

SMART CARDS IN USER AUTHENTICATION PROCESS ON WINDOWS OPERATING SYSTEMS

Summary. The paper presents the process of user authentication on Windows operating systems. What is also discussed are current features of operating systems concerning this matter, with special attention to the possibility of using smart cards in the authentication process.

Keywords: smart card, user authentication, certificate, data security, Microsoft Windows

1. Wstęp

Proces uwierzytelniania (bądź inaczej identyfikacji) użytkownika w systemie operacyjnym jest jednym z ważniejszych elementów polityki bezpieczeństwa. Proces ten polega na sprawdzeniu, czy przedstawiająca się osoba, która żąda dostępu do systemu, jest tą osobą, za którą się podaje. W większości wypadków jest to najczęściej stosowana metoda na zabezpieczenie danych znajdujących się w komputerze, przed niepowołanym dostępem osób trze-

cich. Proces ten poprzedza bezpośrednio autoryzację użytkownika, czyli nadanie mu uprawnień. Jest więc niezwykle istotny, gdyż po pomyślnej identyfikacji osoby system otrzymuje informację, jakie uprawienia należy przypisać osobie, tzn. co osoba może wykonać w systemie i do jakich danych ma prawo dostępu.

W niniejszym artykule zostaną przedyskutowane stosowane obecnie techniki uwierzytelniania użytkownika w systemach Microsoft Windows oraz zostanie zaproponowane rozwiązanie wykorzystujące karty inteligentne jako bezpieczny nośnik informacji identyfikujących użytkownika.

2. Proces uwierzytelniania w systemach Windows

W systemie operacyjnym Windows możemy podzielić konta użytkowników na konta lokalne oraz domenowe. Zależnie od rodzaju konta w algorytmie uwierzytelniania użytkownika stosowane są różne źródła wzorca tożsamości.

2.1. Uwierzytelnianie użytkownika lokalnego

Za interaktywne logowanie użytkownika w systemie jest odpowiedzialny proces *winlogon*, który po starcie systemu ładuje bibliotekę GINA[1] odpowiedzialną za interakcje z użytkownikiem, czyli zebranie niezbędnych danych uwierzytelniających, którymi w najprostszym rozwiązaniu są nazwa użytkownika oraz hasło. Po ich otrzymaniu biblioteka GINA przekazuje dane do serwera LSA[2], który następnie wysyła żądanie identyfikacji do usługi dostawcy zabezpieczeń (SSP[3]), którym jest protokół uwierzytelniania NTLM 2.0 ([8]). Protokół ten szyfruje otrzymane hasło i sprawdza, czy logowanie odbywa się lokalnie, czy też następuje próba logowania do domeny. Jeśli użytkownik korzysta z konta lokalnego, to jego dane uwierzytelniające są przekazywane do lokalnej bazy SAM[4], która dokonuje właściwego sprawdzenia tożsamości użytkownika, porównując otrzymane dane z danymi

[1] *Graphical Identification aNd Authentication* – biblioteka dll odpowiedzialna za pobranie danych uwierzytelniających.

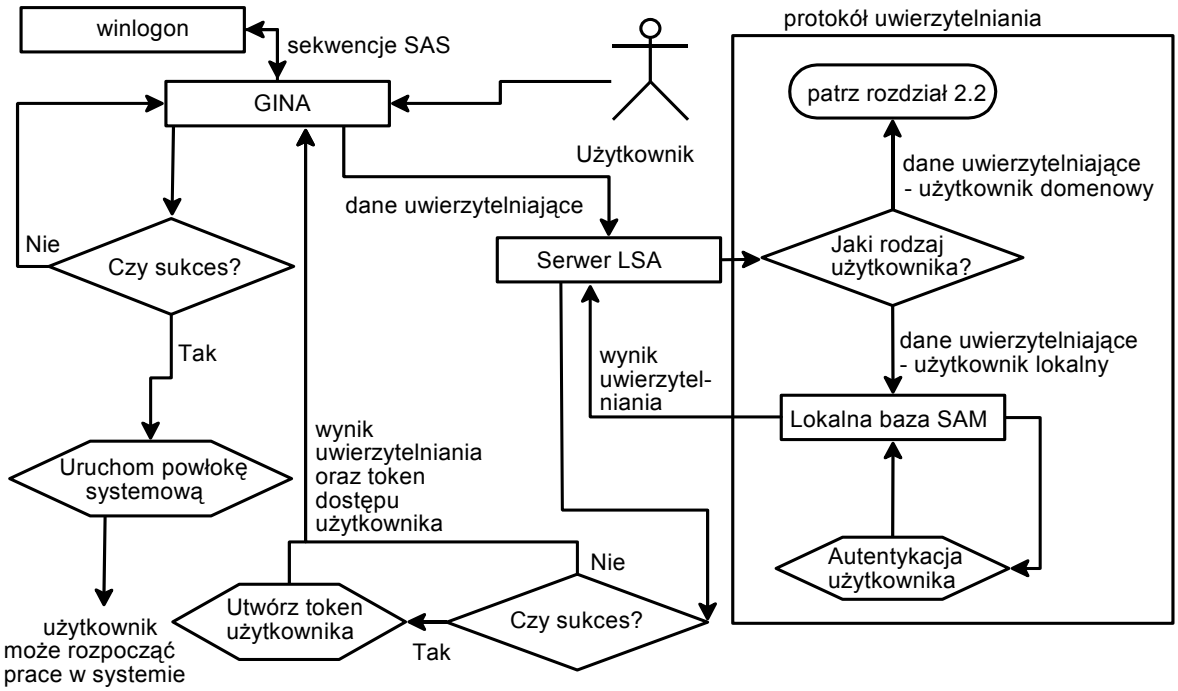
[2] *Local Security Authority* – urząd zabezpieczeń lokalnych będący podsystemem zabezpieczeń, odpowiedzialnym za wszystkie usługi interakcyjnego uwierzytelniania i autoryzacji użytkowników w komputerze lokalnym (zarządzanie dostępem i uprawnieniami).

[3] *Security Service Provider* – usługa dostawcy zabezpieczeń, biblioteka dll implementująca sposób uwierzytelniania użytkownika w systemie.

[4] *Security Account Manager* – usługa windows odpowiedzialna za zarządzanie kontami, grupami użytkowników oraz deskryptorami zabezpieczeń, używana do autentykacji użytkownika.

zapisanymi w bazie. W przypadku odnalezienia prawidłowego wpisu w bazie następuje odczytanie deskryptorów bezpieczeństwa skojarzonych z kontem użytkownika.

Informacja o odczytanych deskryptorach bezpieczeństwa jest przekazywana z powrotem do serwera LSA, który wykonuje autoryzację użytkownika. Sprawdzane jest przy tym, czy użytkownik ma prawo do używanego typu logowania i w przypadku sukcesu tworzony jest podstawowy token sesji logowania (przepustka/sygnatura dostępu – ang. *access token*) na podstawie otrzymanych deskryptorów bezpieczeństwa z bazy. Jeśli deskryptory bezpieczeństwa zostały pomyślnie odnalezione i odczytane oraz autoryzacja użytkownika zakończyła się sukcesem, to cały proces uwierzytelniana kończy się również sukcesem.



Rys. 1. Procedura uwierzytelniania użytkownika lokalnego
Fig. 1. Procedure of local user identification

Sygnatura dostępu to zespół danych wykorzystywanych później przy ubieganiu się użytkownika o dostęp do zasobów systemu. Znajduje się w niej m.in. identyfikator SID[5] użytkownika, nazwa użytkownika oraz identyfikatory SID i nazwy wszystkich grup, do których użytkownik należy. Przepustka dostępu identyfikuje użytkownika w sieci przez cały czas trwania sesji. Po utworzeniu przepustki jej kopia jest dołączana do każdego procesu oraz wątku uruchomionego w kontekście konta użytkownika. Jeśli proces lub wątek zażąda dostępu do jakiegoś obiektu, sygnatura jest wykorzystywana do sprawdzenia, jakie uprawnienia do tego obiektu ma użytkownik. Porównuje się w tym celu identyfikatory użytkownika

[5] *Security Identification Number* – identyfikator zabezpieczeń generowany podczas tworzenia konta (którym może być użytkownik, grupa, komputer), który jednoznacznie identyfikuje konto przez cały okres istnienia.

oraz grup, do których przynależy, z listą arbitralnej kontroli dostępu (DACL[6]) posiadaną przez każdy obiekt w systemie.

Jeżeli logowanie odbyło się pomyślnie, biblioteka GINA uruchamia powłokę systemową (ang. *shell*) w kontekście użytkownika (najczęściej explorer.exe) i dołącza do niej kopie otrzymanego tokenu dostępu z serwera LSA. Token dostępu jest przekazywany również do procesu *winlogon*, który wiąże go z zawieszonym procesem użytkownika, a następnie tworzy w ramach tego procesu pulpit użytkownika oraz pulpit wygaszacza ekranu oraz modyfikuje ich DACL, tak aby zalogowany użytkownik oraz pulpit systemowy mieli do nich dostęp. Od tego momentu proces użytkownika jest gotowy, aby rozpocząć normalną pracę.

Proces *winlogon* pełni rolę nadzorcy całej procedury uwierzytelniania i współpracuje z biblioteką GINA, wymieniając dane i komunikaty SAS[7]. Standardowa współpraca opiera się na schemacie:

- proces *winlogon* wykrywa sekwencje SAS,
- proces *winlogon* sprawdza, w jakim jest stanie (zalogowanym, niezalogowanym lub zablokowanym), kiedy zdarzenie SAS wystąpiło,
- proces *winlogon* na tej podstawie określa, którą funkcję z biblioteki GINA należy wywołać,
- proces *winlogon* przełącza bieżący pulpit na pulpit systemowy, do którego nikt inny nie ma dostępu,
- uruchomiona funkcja z biblioteki GINA wykonuje niezbędne operacje i zwraca wynik do procesu *winlogon*.

Alternatywny sposób współpracy pomiędzy procesem *winlogon* a biblioteką GINA może przebiegać według schematu nakreślonego poniżej:

- biblioteka GINA wykrywa nowy rodzaj SAS, jaki by chciała obsłużyć (na przykład włożenie/wyciągnięcie karty inteligentnej z czytnika),
- biblioteka GINA informuje proces *winlogon* o sekwencji SAS,
- proces *winlogon* sprawdza, w jakim jest stanie (zalogowanym, niezalogowanym lub zablokowanym), kiedy zdarzenie SAS wystąpiło,
- proces *winlogon* na tej podstawie określa, którą funkcję z biblioteki GINA należy wywołać,

[6] *Discretionary Access Control List* – lista arbitralnej kontroli dostępu identyfikuje użytkowników i grupy, którym udzielono lub odmówiono uprawnień dostępu do obiektu. Domyślnie listę kontroluje właściciel lub twórca obiektu i zawiera ona wpisy kontroli dostępu (ACE), które określają poziom dostępu użytkownika do obiektu.

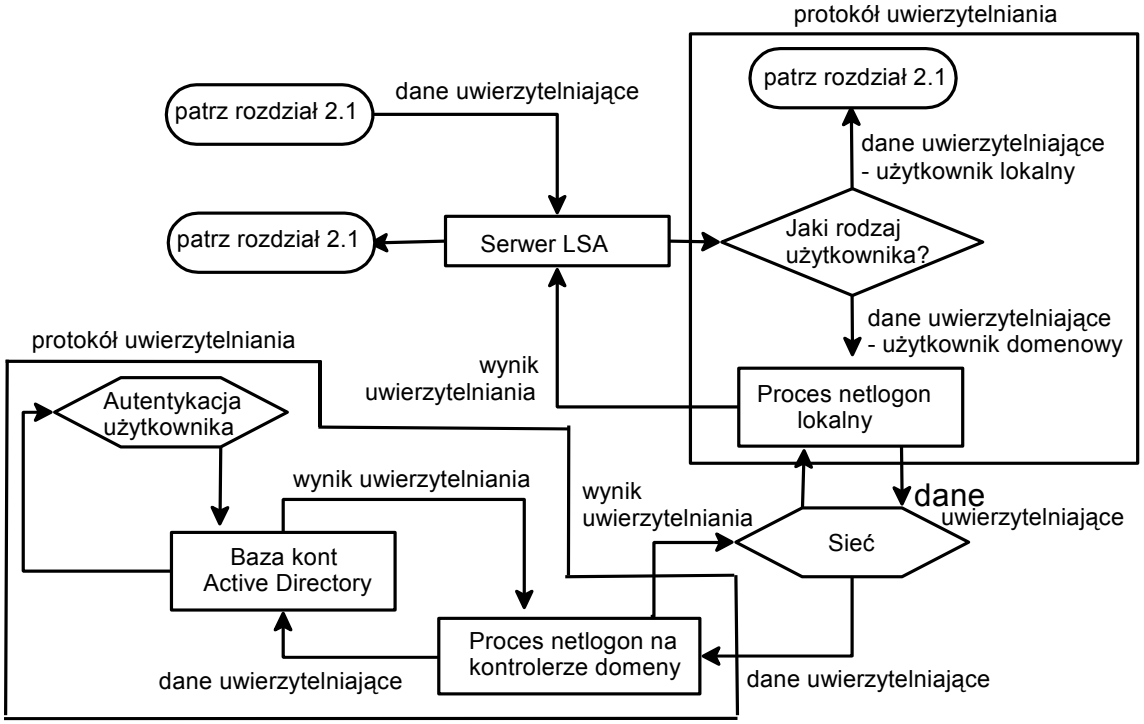
[7] *Secure Action Sequence* – bezpieczna sekwencja, standardowo jest to sekwencja klawiszy: Ctrl+Alt+Del.

- proces *winlogon* przełącza bieżący pulpit na pulpit systemowy, do którego nikt inny nie ma dostępu,
- uruchomiona funkcja z biblioteki GINA wykonuje niezbędne operacje i zwraca wynik do procesu *winlogon*.

Tak więc implementacja własnej biblioteki GINA pozwala obsłużyć jakikolwiek nośnik informacji uwierzytelniających, jaki będzie potrzebny, począwszy od standardowej tekstowej wersji nazwy użytkownika i hasła, przez odczytanie zawartości chronionej karty inteligentnej i wykorzystanie certyfikatów, po pobranie cech biometrycznych użytkownika.

2.2. Uwierzytelnianie użytkownika domenowego

Uwierzytelnianie użytkownika domenowego odbywa się na podobnych zasadach, jak już opisana identyfikacja użytkownika lokalnego, z tą różnicą że weryfikacja tożsamości użytkownika nie odbywa się w komputerze lokalnym, ale w komputerze podłączonym do sieci, który pełni funkcję kontrolera domeny.



Rys. 2. Procedura uwierzytelniania użytkownika domeny
Fig. 2. Procedure of domain user identification

Jako usługa dostawcy zabezpieczeń (SSP) w tym wypadku używany jest domyślnie protokół *kerberos* 5.0 ([7]), a protokół NTLM 2.0 ([8]) jest stosowany tylko wtedy, jeśli z jakiś względów protokół *kerberos* nie jest dostępny (na przykład w poprzednikach systemu operacyjnego Windows 2000). Protokół uwierzytelniania szyfruje hasło i jeśli stwierdzi, że

ma do czynienia z użytkownikiem domeny, to przekazuje dane uwierzytelniające do lokalnej usługi *netlogon*.

Usługa *netlogon* wyszukuje z kolei żądany kontroler domeny w sieci i łączy się z nim używając bezpiecznego kanału komunikacyjnego, a konkretniej dokonuje połączenia z procesem *netlogon* na znalezionej maszynie. Następnie dane uwierzytelniające są przekazywane przez sieć za pomocą utworzonego kanału wprost do bazy obiektów kont w usłudze katalogowej *Active Directory*, która dokonuje właściwego uwierzytelnienia użytkownika. W przypadku sukcesu pobierane są deskryptory bezpieczeństwa, skojarzone z kontem użytkownika i zwracane tą samą drogą do systemu, na którym zostało zainicjowane żądanie logowania. Otrzymane dane lokalny proces *netlogon* zwraca do serwera LSA i dalszy schemat postępowania jest taki sam jak w przypadku użytkownika lokalnego. Różnicą polega na tym, że użytkownik posiada w sygnaturze dostępu dwa zestawy SID-ów, czyli dwa poziomy uprawnień: jeden poziom dotyczy praw dostępu do zasobów domeny, drugi natomiast do stacji lokalnej, na której użytkownik pracuję.

3. Wady tradycyjnego systemu uwierzytelniania

Standardowa procedura uwierzytelniania za pomocą nazwy użytkownika i hasła w systemach Windows staje się niewystarczająca i mało bezpieczna na skutek kilku czynników. Według badań przeciętny pracownik korzystający w pracy z komputera musi pamiętać około 10 różnych haseł. Ponieważ pracownik ma ograniczone zdolności zapamiętywania dużej liczby haseł, więc stosowane hasła są najczęściej niezbyt skomplikowane, aby ułatwić ich zapamiętanie. Dlatego też stosowane są rozwinięcia standardowej procedury uwierzytelniania o:

- ustawienie minimalnej długości hasła akceptowanego przez systemu, zaleca się użycie minimum 8 znaków,
- wymóg okresowej zmiany haseł,
- ustawienie stopnia złożoności hasła – można określić reguły dla bezpiecznego hasła (konieczność użycia małych/dużych liter, cyfr, innych znaków specjalnych), poza tym system odrzuci hasła będące prostym ciągiem znaków,
- możliwość zablokowania konta użytkownika po zadanej liczbie niepowodzeń prób logowania na określony czas, w szczególności konto może zostać zablokowane aż do interwencji administratora.

Stosując się do wymienionych wyżej reguł, bezpieczeństwo systemu komputerowego rośnie, ale należy pamiętać, że najsłabszym ogniwem każdej przyjętej polityki bezpieczeństwa jest człowiek. Jeżeli więc będzie wymóg, aby użytkownik pamiętał zbyt długie i/lub

zbyt skomplikowane hasło, to najprawdopodobniej użytkownik po prostu zapisze sobie gdzieś to hasło i umieści w pobliżu komputera. Podobna sytuacja wystąpi, jeśli hasła będą zbyt często zmieniane, wskutek czego użytkownik nie zdąży przywyknąć i ich zapamiętać.

4. Wykorzystanie kart inteligentnych w procesie uwierzytelniania

Rozwiązaniem problemów zarysowanych w poprzednim rozdziale może być wykorzystanie kart inteligentnych w procesie uwierzytelniania jako bezpiecznego nośnika informacji. Takie podejście umożliwia zbudowanie bardziej bezpiecznej i pewniejszej procedury uwierzytelniania, gdyż wprowadzanie kart udostępnia dwustopniowe uwierzytelnianie:

- własna karta (identyfikacja za pomocą unikalnego urządzenia),
- PIN[8] (identyfikacja przez unikalną wiedzę).

Poza tym użycie kart absorbuje uwagę użytkownika do niezbędnego minimum, czyli pamiętania PIN-u oraz konieczności posiadania karty przy sobie, gdyż wszelkie potrzebne dane uwierzytelniające znajdują się w chronionym obszarze pamięci karty. Takie rozwiązanie wydaje się być idealne, ale jednak niesie ze sobą potrzebę pewnych inwestycji, czyli zakupu kart, czytników i niekiedy specjalnego oprogramowania.

Karta inteligentna, inaczej karta elektroniczna, to urządzenie wielkości karty kredytowej z wbudowanym programowalnym układem scalonym zawierającym pamięć z chronionym dostępem. Komunikacja karty z komputerem jest realizowana przy użyciu czytnika kart, który jest najczęściej urządzeniem zewnętrznym, a transfer informacji pomiędzy czytnikiem a komputerem odbywa się z wykorzystaniem portu USB lub portu RS232. Istnieją również komputery z wbudowanym czytnikiem – standard TP/TPM. Więcej informacji na temat kart inteligentnych można odnaleźć w pozycjach [1 i 2] literatury.

4.1. Zastosowania kart inteligentnych w komputerach będących częścią domeny *Active Directory* zbudowanej na bazie systemu operacyjnego Windows 2003 Server

Systemy operacyjne Windows Server 2003, Windows 2000 oraz Windows XP Professional z SP2 zostały rozszerzone o wbudowaną obsługę kart inteligentnych w procesie uwierzytelniania. Można z niej skorzystać tylko wtedy, jeśli komputery są częścią domeny *Active Directory* zbudowanej z wykorzystaniem systemu Windows Server 2003, który pełni rolę kontrolera domeny.

[8] *Personal Identification Number* – osobisty numer identyfikujący służący do uwierzytelnienia użytkownika na karcie.

W takim rozwiązaniu do uwierzytelnienia użytkownika jest wykorzystywany certyfikat wystawiany przez zaufany urząd certyfikacji, który tym samym poświadcza autentyczność tożsamości użytkownika. Certyfikat jest zapisywany na karcie i generowany na potrzeby konkretnego konta użytkownika w domenie, dlatego charakteryzuje się pewnymi dodatkowymi atrybutami. Podczas procesu uwierzytelniania weryfikowana jest ważność i poprawność certyfikatu zapisanego na karcie i w przypadku gdy certyfikat jest zaufany, to na podstawie danych zapisanych w certyfikacie jest on odwzorowywany na konkretne konto użytkownika domeny, a proces uwierzytelniania kończy się sukcesem.

Aby skorzystać z możliwości wykorzystania kart elektronicznych, najpierw trzeba odpowiednio skonfigurować system. Przede wszystkim w domenie Active Directory musi istnieć niezależny urząd certyfikacji i może być nim urząd certyfikacji Microsoftu bądź też urząd jakieś innej firmy. Drugim niezbędnym czynnikiem jest konieczność udostępnienia listy odwołanych certyfikatów (CRL) przy użyciu protokołu HTTP lub LDAP. W tym celu najprościej skorzystać z serwera IIS[9] dostarczonego z systemem operacyjnym Windows Server 2003, który umożliwi publikacje list CRL urzędu certyfikacji w sieci.

4.1.1. Wykorzystanie oprogramowania urzędu certyfikacji wbudowanego w system operacyjny Windows 2003 Serwer

Oprogramowanie urzędu certyfikacji Microsoft jest dostarczone razem z systemem operacyjnym Windows Server 2003 (również 2000) i wymaga ręcznego do instalowania z poziomu panelu sterowania (Dodaj/usuń składniki systemu Windows). Atutem tego oprogramowania jest duża kompatybilność urzędu z systemem operacyjnym, przez co część operacji da się zautomatyzować, co czyni rozwiązanie wygodnym i bardzo użytecznym. Wraz z instalacją oprogramowania tworzony jest również główny certyfikat urzędu na potrzeby domeny. Domyślnie wspomniany certyfikat jest instalowany w magazynie NTAuth domeny *Active Directory,* co jest niezbędne, aby użytkownicy mogli być uwierzytelniani w domenie. Istnieje możliwość skonfigurowania domeny w ten sposób, aby certyfikat urzędu automatycznie rozpowszechnił się wśród członków domeny i instalował w ich lokalnym głównym magazynie zaufanych urzędów certyfikacji. Po prawidłowej instalacji urzędu jest również generowany automatycznie certyfikat kontrolera domeny i instalowany w systemie.

Kolejnym krokiem jest stworzenie odpowiedniego szablonu certyfikatu na potrzeby logowania przy użyciu karty i konfiguracja serwera, aby umożliwiał automatyczne wydawanie certyfikatów oraz ich odnawianie na żądanie klienta dla wszystkich użytkowników domeny. Jeżeli użytkownik posiada swoje konto w domenie oraz ma podłączony czytnik z kartą inteligentną do komputera, z którego korzysta, to po udanym logowaniu system spróbuje

[9] *Internet Information Sernice* – internetowe usługi informacyjne, serwer WWW firmy Microsoft.

automatycznie wygenerować certyfikat na karcie. W tym celu poprosi użytkownika o podanie PIN-u do karty i rozpocznie proces, które potrwa pewien okres czasu, podczas którego karta elektroniczna zostanie spersonalizowana. Po pomyślnym wygenerowaniu certyfikatu użytkownik może korzystać z karty, aby uzyskać dostęp do systemu. Aby uniemożliwić logowanie za pomocą nazwy użytkownika i hasła, konieczna jest jeszcze interwencja administratora, który musi zmienić domyślny sposób uwierzytelniania użytkownika w systemie na metodę dopuszczającą logowanie tylko przy użyciu karty.

Szczegóły na temat konfiguracji systemu operacyjnego Windows 2003 Server w rozważanym zastosowaniu można odnaleźć w pozycjach [3], [4] i [5].

4.2. Propozycja usprawnienia mechanizmu stosowania kart inteligentnych w systemach operacyjnych Microsoft Windows

Przeprowadzone testy z wykorzystaniem przedstawionego w poprzednim rozdziale rozwiązania z użyciem urzędu certyfikacji Microsoft wykazały, że zasadnicza wadą jest brak obsługi komputerów, które nie są częścią domeny zbudowanej w oparciu o usługę katalogową *Active Directory*. Tak więc oprogramowanie urzędu certyfikacji Microsoftu nie można zastosować tam, gdzie nie ma rozbudowanej infrastruktury informatycznej i wobec tego usługa katalogowa *Active Directory* również nie została wdrożona. Ponadto logowanie przy użyciu kart inteligentnych staje się niemożliwe w komputerach domowych, czy też na komputerach przenośnych, które z oczywistych względów pracują większość czasu poza domeną.

Rozwiązaniem problemów jest propozycja utworzenia aplikacji, która połączyłaby w sobie funkcję urzędu certyfikacji, urzędu rejestracji oraz aplikacji personalizacji kart inteligentnych. Stworzenie natomiast własnej implementacji biblioteki GINA pozwoliłoby obsłużyć zarówno uwierzytelnianie użytkownika w domenie, jak i lokalnie.

Rozwiązanie powinno być kompatybilne z usługą *Active Directory*, dlatego certyfikaty generowane przez stworzony urząd muszą spełniać wszystkie wymogi certyfikatów przeznaczonych do logowania w domenie, czyli zawierać wszystkie rozszerzenia (więcej w pozycji [6]). Dodatkowo, w pamięci karty powinno być przechowywane hasło konta użytkownika zabezpieczone PIN-em. Tak spersonalizowana karta umożliwi wykonanie uwierzytelniania użytkownika zarówno w domenie, jak i lokalnie.

Aplikacja powinna integrować w sobie wszystkie aspekty procedury wydawania karty, czyli administrator systemu w jednym miejscu może stworzyć konto użytkownika domenowego (określając jego wszystkie atrybuty), następnie na podstawie tego konta zostałby wydany automatycznie odpowiednio przygotowany i podpisany certyfikat, a na koniec certyfikat zostałby wgrany na kartę inteligentną. Wszystkie informacje o użytkowniku, jego certyfikacie, użytej karcie przechowywane byłyby w repozytorium w celu łatwiejszej administracji

systemem. Aplikacja powinna pozwolić odnawiać certyfikaty, jak również je odwoływać, przy czym aktualizacja list CRL urzędu odbywałaby się automatycznie na podstawie stanu bazy danych, a dostęp do list CRL byłby możliwy poprzez protokół HTTP.

W przypadku wykorzystania kart inteligentnych w komputerach nie podłączonych do domeny, aplikacją nie może stworzyć od razu użytkownika lokalnego w systemie docelowym podczas personalizacji karty, ale może wgrać wszystkie niezbędne informacje do utworzenia użytkownika na kartę i zabezpieczyć je PIN-em. W takim wypadku po zainstalowaniu rozszerzonej biblioteki GINA w stacji klienckiej, zanim zostanie wykonana próba logowania, użytkownik otrzymałby możliwość stworzenia swojego konta w systemie na podstawie danych zapisanych w karcie. Przy logowaniu lokalnym do uwierzytelnienia wykorzystywana byłaby nazwa użytkownika pobrana z certyfikatu oraz hasło użytkownika zapisane również w karcie. Aby zwiększyć bezpieczeństwo, to w ramach własnej implementacji biblioteki GINA można przewidzieć sprawdzenie, czy certyfikat zainstalowany w karcie jest zaufany dla stacji roboczej. Ponieważ komputer nie jest członkiem odpowiednio skonfigurowanej domeny, więc certyfikat urzędu certyfikacji nie instaluje się automatycznie do lokalnego magazynu, ale można rozważyć inne sposoby jego pozyskania. Certyfikat urzędu można by udostępnić w serwerze WWW lub poprzez wgranie certyfikatu bezpośrednio na kartę i w trakcie tworzenia konta użytkownika lokalnego zainstalować również certyfikat urzędu do lokalnego głównego magazynu zaufanych urzędów certyfikacji. Utworzone konto użytkownika lokalnego, przypisane do zadanej grupy użytkowników podczas jego tworzenia, miałoby odpowiednio skomplikowane i długie hasło oraz brak możliwości zmiany tego hasła.

Ostatnim możliwym wariantem zastosowania jest użycie spersonalizowanej karty inteligentnej w komputerze przenośnym, na którym można wyobrazić sobie konieczność istnienia uwierzytelniania użytkownika lokalnego i/lub domenowego, zależnie od tego czy komputer ma dostęp do domeny, czy też jest używany poza nią. Rozszerzona biblioteka GINA zainstalowana w stacji roboczej sprawdzałaby, czy maszyna jest aktualnie członkiem domeny i na tej podstawie wykonywałaby automatycznie logowanie a pomocą certyfikatu w domenie lub uwierzytelnianie za pomocą hasła i nazwy użytkownika pobranego z karty elektronicznej, po pomyślnej weryfikacji certyfikatu podczas logowania lokalnego.

Ostatnią rzeczą, na jaką powinniśmy zwrócić uwagę, jest fakt, że jeśli komputer nie jest członkiem domeny, to nie otrzymuje on automatycznie komunikatów o zdarzeniu włożenia/wyciągnięcia karty z czytnika, która została wykorzystana do uwierzytelniania. Dlatego też w ramach własnej implementacji biblioteki GINA należy monitorować stan czytników oraz kart w nich się znajdujących, aby odpowiednio zareagować na zdarzenia tego typu.

5. Podsumowanie

W artykule opisano sposób działania algorytmu uwierzytelniającego zaimplementowanego w systemach operacyjnych Microsoft Windows oraz przedstawiono podstawowe ograniczenia i zalety wykorzystania kart inteligentnych w procesie uwierzytelniania. Zostało również zaproponowane rozwinięcie wbudowanego mechanizmu uwierzytelniania użytkownika (za pomocą karty inteligentnej) o możliwość korzystania z karty przy identyfikacji tożsamości użytkownika w komputerach niebędących członkami domeny. Propozycja usprawnienia, która opiera się na wykonaniu aplikacji administracyjnej i własnej implementacji biblioteki GINA, została wykonana w znacznym stopniu w ramach realizacji pracy magisterskiej.

LITERATURA

1. Nazimek P.: Inżyniera programowania kart inteligentnych. Politechnika Warszawska, Warszawa 2005.
2. Molski M., Glinkowska M.: Karta elektroniczna – bezpieczny nośnik informacji. Mikom, Warszawa 2002.
3. Cross D. B., Kinder C. B.: Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure. Microsoft Corporation 2004 – witryna WWW: http://technet2.microsoft.com/WindowsServer/en/Library/091cda67-79ec-481d-8a96-03e0be-7374ed1033.mspx?mfr=true.
4. Cross D. B., Kinder C. B.: Advanced Certificate Enrollment and Management. Microsoft Corporation 2004 – witryna WWW: http://www.microsoft.com/technet/prodtechnol/-windowsserver2003/technologies/security/advcert.mspx.
5. Cross D. B., AlRashed A.: Windows Server 2003 PKI Operations Guide. Microsoft Corporation 2004 – witryna WWW: http://technet2.microsoft.com/WindowsServer/en-/Library/e1d5a892-10e1-417c-be13-99d7147989a91033.mspx?mfr=true.
6. Guidelines for enabling smart card logon with third-party certification authorities. Microsoft Corporation 2006 – witryna WWW: http://support.microsoft.com/kb/281245.
7. Microsoft Kerberos. Microsoft Corporation – witryna WWW: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secauthn/security/microsoft_ntlm.asp.
8. Microsoft NTLM. Microsoft Corporation – witryna WWW: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secauthn/security/microsoft_ntlm.asp.

Recenzent: Dr inż. Krzysztof Nałęcki

Wpłynęło do Redakcji 20 lipca 2006 r.

Abstract

In this paper was discussed various possibilities of user authentication on Windows operating systems with special attention to the usage of smart card in such processes, basing on author's experience. After short introduction the authentication procedure is described in details. Such procedure can be considered in two ways which are described in section 2.1 (local user authentication) and 2.2 (domain user authentication). Both ways are also illustrated in figure 1 and figure 2. Next chapter concentrates on problems with standard authentication of user, which is based on username and password. After that the solution is shown in chapter 4. The solution relies on using smart card as a secure data storage on which all necessary authentic data could be saved. Then section 4.1 describes a way of using smart card to authenticate user which is by default built-in into some of Windows operating systems. Finally section 4.2 presents a short explanation how to improve built-in solution also based on smart card but with possibility to logon on computer which is not a member of domain. And at the end, chapter 5 contains small summary about article.

Adres

Michał LEWANDOWSKI: Politechnika Śląska, Instytut Informatyki, ul. Akademicka 16, 44-101 Gliwice, Polska, m.lewandowski@polsl.pl.