T: Prawa użytkowników. Uprawnienia NTFS.

Zadanie1:

Wyszukaj w systemowym Centrum pomocy i obsługi technicznej definicje uprawnień i praw użytkowników.

uprawnienie

Zasada skojarzona z obiektem w celu określenia, którzy użytkownicy i w jaki sposób mogą uzyskać dostęp do obiektu. Uprawnienia są udzielane lub nie są udzielane przez właściciela obiektu.

Zobacz też: obiekt, uprawnienia drukarek, deskryptor zabezpieczeń, uprawnienia folderu udostępnionego, specjalne uprawnienia dostępu

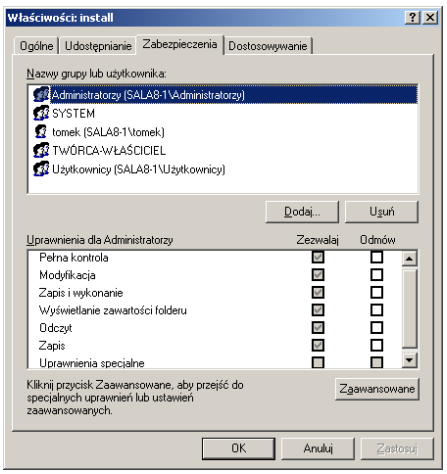
prawa użytkowników

Zadania, które użytkownik może wykonywać w systemie komputerowym lub domenie. Są dwa typy praw użytkownika: przywileje i prawa logowania. Przykładem przywileju jest prawo zamykania systemu. Przykładem prawa logowania jest prawo do lokalnego logowania się na komputerze. Oba typy praw są przypisywane poszczególnym użytkownikom lub grupom przez administratorów jako część ustawień zabezpieczeń komputera.

Zobacz też: administrator, domena, przywilej, grupa

Zadanie2:

Odszukaj w systemie Windows informacje na temat dostępnych uprawnień systemu plików NTFS.



Kłopoty z prawami dostępu do pliku mogą dotyczyć kolejności wpisów kontroli dostępu (ACE, Access Control Entry). Kolejność ta zakłada umieszczanie **odmowy** dostępu przed prawem na **zezwolenie** dostępu. Programy mogą te wpisy mieszać. W związku z tym system może mieć problem z odczytaniem takiej nietypowej listy. Rozwiązaniem jest użycie narzędzia cacls.exe.

```
Start => Run (Uruchom) => cmd
cacls "ścieżka dostępu do pliku/folderu" /E
/G NazwaKonta:F
```

Ta komenda daje pełny dostęp (F= Full Control) dla twojego konta. Jeśli potem chcesz z powrotem usunąć pozwolenie wystarczy ponownie wpisać:

```
cacls "ścieżka dostępu do pliku/folderu" /E /R NazwaKonta
```

Zadanie3:

Zapoznaj się z pomocą systemu Windows na temat polecenia cacls.

Zadanie4:

Utwórz na pulpicie skrót do konsoli tekstowej z uprawnieniami użytkownika asso. Następnie w konsoli załóż w katalogu głównym na dysku c: katalog **asso**. Następnie sprawdź listę kontrolną dla tego katalogu za pomocą polecenia cacls oraz poprzez dostępne narzędzia w trybie tekstowym. Zanotuj w zeszycie odczytane uprawnienia.

W dalszej kolejności dodaj pełne uprawnienia dla wszystkich użytkowników do tego katalogu w trybie tekstowym. Odczytaj uprawnienia i zanotuj powstałe zmiany.

Jako ostatni etap ćwiczenia dokonaj usunięcia uprawnień dla użytkownika asso. Sprawdź dokonane zmiany odczytując konfigurację uprawnień. Zanotuj spostrzeżenia. Usuń katalog.

Zadanie5:

Zaloguj się na lokalne konto administracyjne i utwórz w swoim katalogu domowym w podkatalogu **Send to** plik wsadowy o nazwie **uprawnienia.cmd** o poniższej treści:

```
echo t | cacls %1 /e /g wszyscy:r
```

lub

```
cacls %1 /e /p wszyscy:r
```

Następnie utwórz na pulpicie katalog **asso**. Sprawdź ustawienia zabezpieczeń. Potem kliknij na katalogu prawym klawiszem myszy i wybierz polecenie **Send to => uprawnienia.cmd** i ponownie sprawdź ustawienia zabezpieczeń.

Uwaga1:

Przed konfiguracją zabezpieczeń w systemie plików NTFS należy w oknie Eksploratora Windows wyłączyć opcję Użyj prostego udostępniania z Narzędzi => Opcji folderów => Widoku. Spowoduje to udostępnienie zakładki Zabezpieczenia z okna Właściwości folderów i plików. Następnie możliwa jest indywidualna konfiguracja uprawnień NTFS do dowolnego pliku bądź katalogu. Ważne: Priorytet uprawnienia Odmów jest wyższy jak Zezwól (kolejność przetwarzania). Dlatego ostrożnie należy przydzielać zabezpieczenia.

Uwaga2:

Prawa użytkownika należy modyfikować za pomocą narzędzi Zasad zabezpieczeń lokalnych (secpol.msc) lub Zasady grup (gpedit.msc). Zaawansowani użytkownicy posługiwać się mogą edytorem rejestru.

Uwaga3:

Na kontrolerze domeny prawa użytkownika można konfigurować w dowolnym obiekcie struktury drzewa Active Directory do którego należy użytkownik.

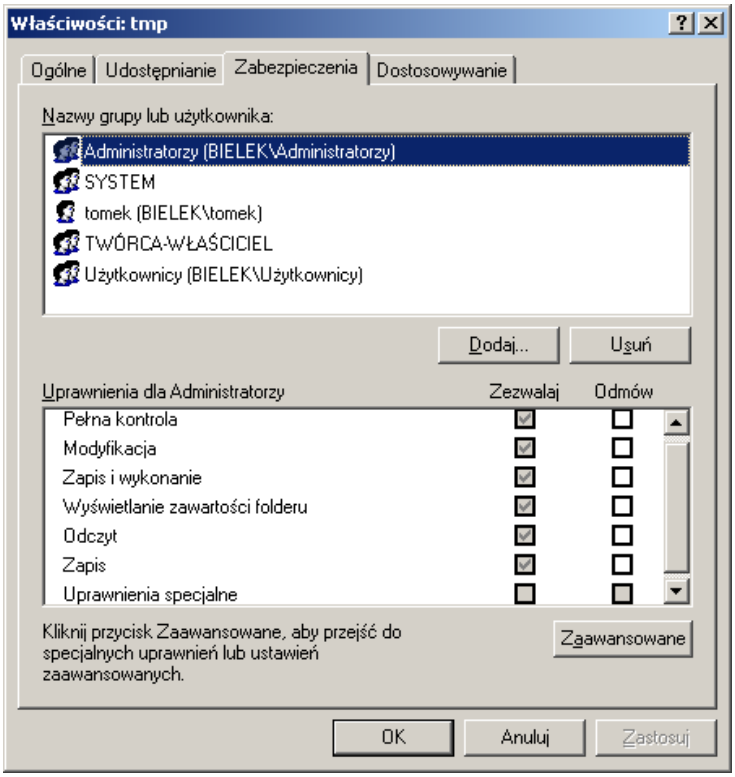
Sekwencja poleceń do wykonania i przeanalizowania:

```
Start => Uruchom => cmd.exe
md test
cacls test
cacls test /e /p wsztscy:w
cacls test
cacls test /t /p wszyscy:r
cacls test
cacls test /e /g administrator:f
cacls test
cacls test /e /p administrator:w
cacls test
cacls test /e /r administrator
cacls test
cacls test /e /d administrator
cacls test
```

Materiały z soisk z klasy I
T: Uprawnienia NTFS do folderów i plików.

Zadanie1:

Zapoznaj się z dostępnym w Pomocy i obsłudze technicznej opisem na temat Ustawiania uprawnień.



W celu konfiguracji uprawnień systemu plików NTFS należy wywołać menu kontekstowe dla danego pliku lub katalogu i wybrać Właściwości. W wyświetlonym oknie przechodzimy na zakładkę **Zabezpieczenia**.

W systemach Windows XP nie pracujących w domenie domyślnie zakładka Zabezpieczenia jest niewyświetlana. W celu wyświetlenia zakładki konfiguracji zabezpieczeń systemu plików należy w Eksploratorze Windows wybrać => Narzędzia => Opcje folderów => Widok i następnie odznaczyć ustawienie Użyj prostego udostępniania plików.

Zadanie 2:

Opisz dostępne uprawnienia dla katalogów i plików w systemie plików NTFS.

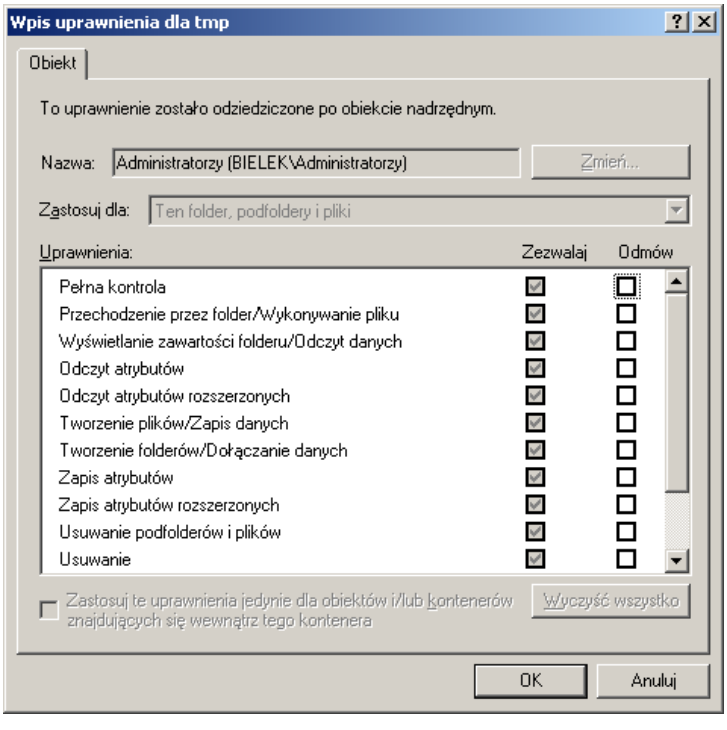
Uprawnienia NTFS przypisywane są dla poszczególnych użytkowników i grup dostępnych w systemie operacyjnym Windows. Uprawnienia dzielą się na dwa rodzaje: Zezwól i Odmów. Kolejności wpisów kontroli dostępu (ACE, Access Control Entry) zakłada umieszczanie odmowy dostępu przed prawem dostępu.

Uprawnienia dla katalogów:

- Pełna kontrola - Przeglądanie, uruchamianie, zmienianie, usuwanie i zmienianie właściciela,
- Modyfikacja - Przeglądanie, uruchamianie, zmienianie i usuwanie,
- Zapis i wykonanie - Przeglądanie i uruchamianie,
- Wyświetlanie zawartości folderu - Przeglądanie,
- Odczyt - Przeglądanie,
- Zapis - Wyświetlanie, uruchamianie, zmienianie i usuwanie,
- Uprawnienia specjalne.

Zadanie 3:

Zapoznaj się z uprawnieniami specjalnymi dostępne po wybraniu opcji Zaawansowane => Edytuj.



Uprawnienia specjalne stosowane są, gdy zachodzi konieczność bardzo precyzyjnego określenia uprawnień użytkowników, zaś uprawnienia standardowe nie są wystarczające. Spośród uprawnień specjalnych najważniejsze są:

- Przechodzenie poprzez folder zezwala lub zabrania na dostęp do pliku w sytuacji, gdy użytkownik ten nie posiada odpowiednich uprawnień do zawierającego ten plik katalogu, ale posiada je w stosunku do samego pliku.

- Uprawnienie Wykonanie pliku przyznaje lub odmawia użytkownikowi prawa do uruchamiania plików zawierających programy. Prawo to stosuje się jedynie do plików.
- Odczyt atrybutów - Zezwala lub odmawia przeglądania atrybutów pliku lub folderu.
- Odczyt atrybutów rozszerzonych - Zezwala bądź odmawia przeglądania rozszerzonych atrybutów pliku bądź folderu. Niektóre rozszerzone atrybuty definiują same aplikacje we właściwy dla siebie sposób. Należą do nich również dwa atrybuty NTFS - kompresji i szyfrowania.
- Tworzenie plików/Zapis danych - Zezwala bądź odmawia prawa do tworzenia plików wewnątrz folderu. Zapis danych zezwala bądź odmawia prawa do dokonywania zmian w plikach i nadpisywania ich bieżącej zawartości. Prawo to stosuje się jedynie do plików.
- Tworzenie folderów/Dołączanie danych - Zezwala bądź odmawia prawa tworzenia podkatalogów wewnątrz folderu. Dołączanie danych zezwala bądź odmawia do dopisywania danych na końcu istniejącego pliku, lecz nie do zmiany, usuwania lub nadpisywania istniejących już w nim danych.
- Zapis atrybutów - Zezwala bądź odmawia prawa do zmieniania atrybutów pliku lub folderu.
- Zapis rozszerzonych atrybutów - Zezwala bądź odmawia prawa do zmieniania rozszerzonych atrybutów pliku lub folderu.
- Usuwanie podfolderów i plików - Zezwala bądź odmawia prawa do usuwania znajdujących się wewnątrz folderu plików zabezpieczeń podkatalogów, nawet jeżeli użytkownik nie posiada uprawnienia Usuwanie do usuwanego pliku lub podkatalogu.
- Usuwanie - Zezwala bądź odmawia prawa do usuwania plików i katalogów. Jeżeli użytkownik nie posiada uprawnienia Usuwanie do pliku lub katalogu, ciągle może je usunąć o ile posiada uprawnienie Usuwanie podfolderów i plików w stosunku do folderu nadrzędnego.
- Odczyt uprawnień - Zezwala bądź odmawia prawa do odczytywania uprawnień zastosowanych do pliku lub folderu, takich jak Pełna kontrola, Zapis, Odczyt.
- Zmiana uprawnień - Zezwala bądź odmawia prawa do zmieniania uprawnień zastosowanych do pliku lub folderu takich jak Pełna kontrola, Zapis, Odczyt.
- Przejęcie na własność- Zezwala bądź odmawia prawa do przejęcia pliku lub folderu na własność. Właściciel pliku lub folderu może zawsze zmienić jego uprawnienia, niezależnie od tego, jakie zastosowano uprawnienia w celu jego ochrony.
- Synchronizacja - Zezwala bądź odmawia prawa do tego, aby różne wątki mogły oczekiwać na zwolnienie uchwytu do pliku zabezpieczeń w ten sposób synchronizować się z innymi, sygnalizującymi to wątkami. Ten rodzaj uprawnienia ma zastosowanie jedynie dla programów wielowątkowych i wieloprocesorowych.

Lista kontroli dostępu (Access Control List) jest listą zapisów kontroli dostępu (Access Control Entries - ACEs), przechowywaną razem z obiektem, który chroni. W Windows XP ACL jest przechowywana jako wartość binarna, zwana deskryptorem bezpieczeństwa (Security Descriptor). Każdy ACE zawiera identyfikator bezpieczeństwa (Security Identifier - SID), który identyfikuje głównego (użytkownika bądź grupę), do którego odnosi się ACE, oraz informacje, jaki rodzaj dostępu ACE ma przyznany lub zabroniony.

Dziedziczenie ACL (ACL Inheritance) pozwala danemu ACE uzyskać rozszerzenie uprawnień z kontenera, do którego się podłączył na wszystkie dzieci tego kontenera. Dziedziczenie może być łączone z uprawnieniami do administrowania całym poddrzewem bazy danych przy pojedynczej operacji aktualizacji. Prawa do delegacji dostępu odnoszą się do kontenera w zakresie delegacji.

Konfiguracji uprawnień do plików w trybie tekstowym na partycjach NTFS dokonujemy poleceniem **cacls**.

Informacje dodatkowe

Konfigurowanie skrótów do programów, które chcemy uruchamiać ze specjalnymi uprawnieniami, dodatkowo przełącznik interactive uruchomi proces z pełnymi prawami tylko lokalnie:

```
at hh:mm /interactive regedit.exe
```

Każdy zaalokowany sektor na woluminie NTFS należy do pliku. Wszystkie pliki i katalogi są traktowane jako zestawy atrybutów, do których należą m.in. nazwa, informacje o zabezpieczeniach, a także same dane przechowywane w pliku. Każdy atrybut jest identyfikowany przez kod, a opcjonalnie także przez nazwę. Atrybuty, które są zapisane w rekordzie pliku w MFT, są nazywane atrybutami rezydującymi, a te, które się nie mieszczą, zapisywane są poza MFT, w przestrzeni dyskowej i noszą nazwę nierezydujących. W atrybutach rezydujących zostaje utworzona lista atrybutów (która także jest atrybutem) zawierająca wskazania na położenie atrybutów nierezydujących w celu odnalezienia wszytskich atrybutów

pliku. Nazwa pliku oraz znaczniki czasu są zawsze rezydujące. Rekordy katalogów zawierają informacje indeksujące i podobnie jak w przypadku plików, atrybuty katalogów mogą się nie zmieścić w jednym rekordzie. Duże katalogi są wtedy organizowane w postaci posortowanego drzewa zrównoważonego (balanced tree, B-tree) i posiadają rekordy ze wskaźnikami do zewnętrznych klastrów (buforów indeksowych, index buffers), zawierających wpisy w folderze, które nie mieszczą się w MFT. Przeszukiwanie drzewa zrównoważonego jest dużo szybsze niż listy, szczególnie przy dużej ilości elementów. W przypadku drzewa obszar poszukiwań za każdym razem zmniejsza się kilkukrotnie, zależnie od ilości elementów w węźle. W systemie plików FAT, gdzie stosowana była lista, wpisy w katalogu przeszukiwane były po kolei, dopóki nie został odnaleziony poszukiwany plik/katalog. Co prawda w nowszych systemach korzystających z FAT, takich jak Windows 98, wprowadzono podobne optymalizowanie przeszukiwania, jednak nadal stosowane było liniowe ułożenie wpisów.

Atrybuty plików i katalogów

Typ atrybutu	Kod	Numer	Opis
Informacje standardowe	$STANDARD_INFORMATION	#16 0x10	Zawiera informacje takie jak znaczniki czasu i liczba łączy, w NTFS5.1 także prawa dostępu.
Lista atrybutów	$ATTRIBUTE_LIST	#32 0x20	Zawiera lokalizacje rekordów atrybutów, które nie zmieściły się w MFT.
Nazwa pliku	$FILE_NAME	#48 0x30	Atrybut powtarzalny dla długich i krótkich nazw plików. Dodatkowe nazwy lub twarde łącza mogą być zapisywane jako dodatkowe atrybuty tego typu.
Wersja woluminu	$VOLUME_VERSION	#64 0x40	Wersja woluminu, atrybut usunięty wraz z NTFS 5.0, wcześniej istniał, ale był nieużywany.
ID obiektu	$OBJECT_ID	#64 0x40	Identyfikator unikalny w obrębie woluminu, wykorzystywany przez usługę śledzenia łączy, wprowadzony w NTFS 5.0.
Deskryptor zabezpieczeń	$SECURITY_DESCRIPTOR	#80 0x50	Identyfikuje właściciela pliku oraz użytkowników, którzy mogą korzystać z pliku, nie znajduje się w NTFS 5.1.
Nazwa woluminu	$VOLUME_NAME	#96 0x60	Etykieta woluminu, brak w NTFS 5.1.
Informacje o woluminie	$VOLUME_INFORMATION	#112 0x70	Wersja woluminu, w NTFS 5.1 także nazwa.
Dane	$DATA	#128 0x80	Dane pliku, jeśli plik posiada strumienie wielokrotne, takich atrybutów ma więcej.
Indeks główny	$INDEX_ROOT	#144 0x90	Używany do implementowania katalogów i indeksów.
Alokacje indeksu	$INDEX_ALLOCATION	#160 0xA0	Używany w B-drzewie w dużych katalogach i indeksach.
Mapa bitowa	$BITMAP	#176 0xB0	Określa użycie struktur B-drzewa.
Łącze symboliczne	$SYMBOLIC_LINK	#192 0xC0	Używany do łączy symbolicznych, usunięty w NTFS 5.0, wcześniej istniał, ale nie był używany.
Punkt ponownej analizy	$REPARSE_POINT	#192 0xC0	Używany przez punkty ponownej analizy, wprowadzony w NTFS 5.0.
Informacje o atrybucie rozszerzonym	$EA_INFORMATION	#208 0xD0	Używany dla zgodności z OS/2.
Atrybut rozszerzony	$EA	#224 0xE0	j.w.
Zestaw właściwości	$PROPERTY_SET	#240 0xF0	Miał służyć do wspierania Native Structure Storage (NSS). Istniał krótko w NTFS 5.0, został usunięty podczas betatestów.
Rejestrowany strumień pomocniczy	$LOGGED_UTILITY_STREAM ($LOGGED_TOOL_STREAM)	#256 0x100	Rejestrowany do dziennika ($LogFile) strumień danych używany przez EFS, pojawił się w NTFS 5.0.

Lista kontroli dostępu (Access Control List) - jest listą zapisów kontroli dostępu (Access Control Entries - ACEs), przechowywaną razem z obiektem, który chroni.

Dziedziczenie ACL (ACL Inheritance) - pozwala danemu ACE uzyskać rozszerzenie uprawnień z kontenera, do którego się podłączył na wszystkie dzieci tego kontenera.
Active Directory automatycznie propaguje prawa dziedziczenia dostępu do wszystkich podkontenerów i obiektów wewnątrz poddrzewa. Powielanie praw delegowanego dostępu tylko kopiuje zmiany do jednego obiektu, kontenera, w którym prawa zostały określone, a nie do całego poddrzewa. Każda replika Active Directory automatycznie stosuje kontrolę odziedziczonego dostępu z wpływem odnoszącym się do całego poddrzewa.

Delegacja (Delegation) (Access Control List)	Delegacja pozwala wyższemu autorytetowi administracyjnemu uzyskać specjalne prawa administracyjne do kontenerów i poddrzew dla jednostek i grup
Dziedziczenie (Inheritance)	Dziedziczenie pozwala danemu ACE rozszerzyć zakres z kontenera, z którego korzysta, na wszystkie dzieci tego kontenera
Autorytet Świadczący (Certificate Authority)	Autorytet świadczący (CA) jest to po prostu jednostka lub instytucja, która wydaje świadectwo
System utajniania plików (Encrypting File System - EFS)	EFS wprowadza technologię szyfrowania plików magnetycznych, aby zapisywać na dysku zaszyfrowane pliki systemu plików Windows NT (NTFS)

Delegacja (Delegation) - Delegacja jest jedną z najważniejszych cech bezpieczeństwa Active Directory. Delegacja pozwala wyższemu autorytetowi administracyjnemu uzyskać specjalne prawa administracyjne do kontenerów i poddrzew dla jednostek i grup. Eliminuje to potrzebę administratorów domen z szerokimi uprawnieniami w stosunku do wielkich segmentów populacji użytkowników. ACE mogą uzyskać specjalne prawa administracyjne do obiektów w kontenerze dla użytkowników lub grup. Prawa uzyskuje się do specjalnych operacji na specjalnych klasach obiektów za pośrednictwem ACE w ACL kontenera. Na przykład, żeby pozwolić użytkownikowi "James Smith" być administratorem jednostki organizacyjnej "Corporate Accounting", powinieneś dodać ACE do ACL w "Corporate Accounting" jak to pokazano poniżej:
"James Smith";Grant ;Create, Modify, Delete;Object-Class User
"James Smith";Grant ;Create, Modify, Delete;Object-Class Group
"James Smith";Grant ;Write;Object-Class User; Attribute Password
Teraz James Smith może stworzyć nowych użytkowników i grupy w Corporate Accounting i ustalić hasło dla istniejących użytkowników, ale nie może stworzyć żadnej innej klasy obiektów i nie może wpływać na użytkowników w żadnym innym kontenerze (jeżeli nie jest, oczywiście, upoważniony do takiego dostępy przez ACE w innych kontenerach).
Dziedziczenie (Inheritance) - Dziedziczenie pozwala danemu ACE rozszerzyć zakres z kontenera, z którego korzysta, na wszystkie dzieci tego kontenera. Dziedziczenie może być łączone z delegacją na uzyskanie praw administracyjnych w całym poddrzewie obiektowej bazy danych za jedna operacją.
Świadectwo (Certificate) - Świadectwo jest szczególnym typem polecenia podpisanego cyfrowo; przedmiotem świadectwa jest szczególny temat klucza publicznego i świadectwo jest podpisywane przez jego wydawcę (posiadającego inną parę prywatnych i publicznych kluczy). Zwykle świadectwa zawierają także inne informacje odnoszące się do tematu kluczy publicznych, takich jak informacja tożsamościowa o jednostce, która ma dostęp do odpowiedniego klucza prywatnego. I tak, wydając świadectwo wydawca poświadcza aktualność związku między tematem kluczy publicznych a tematem informacji tożsamościowej.
Autorytet Świadczący (Certificate Authority) - Autorytet świadczący (CA) jest to po prostu jednostka lub instytucja, która wydaje świadectwo. CA występuje w roli gwaranta związku między tematem kluczy publicznych a tematem informacji tożsamościowej, zawartej w świadectwie, które wydał. Różne CA mogą postanowić zweryfikować ten związek różnymi środkami, dlatego jest tak ważne, aby zrozumieć politykę i działanie autorytetów przed postanowieniem zaufania temu autorytetowi na kredyt za klucze publiczne.
Kryptografia (Cryptography) - Kryptografia jest nauką o ochronie danych. Algorytmy kryptograficzne matematycznie łączą wprowadzanie danych jawnym tekstem i klucz szyfrowy, aby wygenerować dane zaszyfrowane (tekst zaszyfrowany). Dobry algorytm kryptograficzny ma taką właściwość, że jest niemożliwe obliczeniowo odwrócić proces szyfrowania i otrzymać dane jawnym tekstem, startując od samego tekstu zaszyfrowanego. Pewne dane dodatkowe, klucz odszyfrowujący, są potrzebne, aby wykonać przekształcenie.
System utajniania plików (Encrypting File System - EFS) - EFS wprowadza technologię szyfrowania plików magnetycznych, aby zapisywać na dysku zaszyfrowane pliki systemu plików Windows NT (NTFS). EFS w szczególności wypowiada rady dotyczące bezpieczeństwa, wspomagane przez narzędzia dostępne w innych systemach operacyjnych, co pozwala użytkownikom na dostęp do plików z woluminów NTFS bez kontroli dostępu. Z EFS, dane w plikach NTFS są szyfrowane na dysku. Używana technologia szyfrowania oparta jest na kluczach publicznych i działa jak zintegrowana usługa systemowa, co czyni ją łatwą w obsłudze, trudną do zaatakowania i przejrzystą dla użytkowników. Jeżeli użytkownik usiłujący dostać się do zaszyfrowanego pliku NTFS ma prywatny klucz do tego pliku, będzie mógł otworzyć plik i pracować z nimi przezroczyście jak z normalnym dokumentem. Użytkownik bez prywatnego klucza do pliku po prostu będzie miał dostęp zabroniony.

IPSec (Access Control List)	IPSEC określa protokół do szyfrowania sieciowego na poziomie protokołu IP
Kerberos	Przechodni i hierarchiczny protokół bezpieczeństwa, który jest standardem bezpieczeństwa Internetu
Infrastruktura Klucza Publicznego (Public Key Infrastructure - PKI)	Zintegrowany zbiór usług i narzędzi administracyjnych do tworzenia, instalacji i zarządzania aplikacjami opartymi na kluczach publicznych

IPSec - IPSEC określa protokół do szyfrowania sieciowego na poziomie protokołu IP. IPSEC nie wymaga technologii opartej na kluczach publicznych i może używać wspólnych tajnych kluczy, bezpiecznie korespondujących przez mechanizm bez granic, do szyfrowania na punktach końcowych sieci. Grupa robocza IETF IPSEC uznała jednakże, że technologia oparta na kluczach publicznych oferuje praktyczne rozwiązanie do tworzenia architektury zaufania rozłożonego w różnej skali. W szczególności to, że urządzenia IPSEC mogą wzajemnie poświadczać się i zgoda na klucze szyfrujące bez polegania na wcześniej zaaranżowanych wspólnych tajemnicach.

Kerberos - Przechodni i hierarchiczny protokół bezpieczeństwa, który jest standardem bezpieczeństwa Internetu. Protokół Kerberos jest głównym mechanizmem poświadczenia w systemie operacyjnym Microsoft® Windows 2000. W sercu protokołu jest zaufany serwer, zwany Centrum Dystrybucji Kluczy (Key Distribution Center - KDC). Gdy użytkownik loguje się do sieci, KDC sprawdza tożsamość użytkownika i dostarcza dokumenty zwane "biletami", jeden na każdą usługę sieciową, z której użytkownik chce skorzystać. Każdy bilet wprowadza użytkownika do właściwej usługi i, opcjonalnie, przenosi informację, która wskazuje na przywileje użytkownika przy usłudze.

Infrastruktura Klucza Publicznego (Public Key Infrastructure - PKI) - zintegrowany zbiór usług i narzędzi administracyjnych do tworzenia, instalacji i zarządzania aplikacjami opartymi na kluczach publicznych.

Replikacja (powielanie) (Replication) (Access Control List)	Active Directory zapewnia replikacje typu wiele-głównych (multi-master). Replikacja wiele-głównych oznacza, że wszystkie repliki danej partycji dają się zapisywać
Numer kolejności uaktualnienia (Update Sequence Number)	USN jest 64-bitową liczbą utrzymywaną przez każdy serwer Directory

ISM - ISM to Intersite Messaging Service (usługa przesyłania informacji międzymiejscowych). Wspomaga on dające się włączać ("pluggable") (uwzględniając definicje ISV) asynchroniczne przesyłanie informacji z miejsca do miejsca ("site-to-site"). Każde przesłanie służy dwóm głównym rzeczom -wysłaniu/odebraniu i topologii zapytań (tj. jakie różne miejsca łączy to przesłanie i po jakich kosztach?). W Windows 2000 realizuje się dwie usługi przesyłania informacji międzymiejscowych, RPC i SMTP (mail).

Czas oczekiwania (Latency) - Czas oczekiwania jest nieodłączną cecha charakterystyczną replikacji w Active Directory. Czas oczekiwania jest opóźnieniem między czasem uaktualnienia danej repliki i czasem przeniesienia tego uaktualnienia na jakąś inną replikę. Czasem czas oczekiwania nazywa się opóźnieniem przeniesienia.

Opóźnienie przeniesienia (Propagation Delay) - patrz "Czas oczekiwania".

Częściowe uaktualnienie (Partial Update) - Częściowe uaktualnienie występuje, gdy aplikacje czytają ten sam zbiór obiektów z różnych replik, podczas gdy trwa proces replikacji. Aplikacja w odległej replice widzi niektóre zmiany, ale nie wszystkie. Zauważ, że znajduje się tu małe okno, w którym częściowe uaktualnienie może wpływać na aplikację: aplikacja musi rozpocząć czytanie obiektów, podczas gdy trwa przychodząca replikacja, następnie jeden lub kilka powiązanych, zmienionych obiektów zostanie przyjętych lecz zanim zostaną przyjęte wszystkie. Czas pomiędzy uaktualnieniem repliki do źródła wpływa bezpośrednio na wielkość tego okna.

- Uaktualnienia, które występują ściśle w jednym czasie, będą replikowane ściśle w jednym czasie. Częściowe uaktualnienie występuje, jeżeli aplikacje używają powiązanych zbiorów obiektów.
- Na przykład, usługa zdalnego dostępu może używać obiektowej bazy danych do zachowania informacji o polityce (działaniach) i profilu. Informacja o polityce zachowywana jest w jednym zbiorze obiektów, a profil w innym zbiorze. Gdy użytkownik łączy się z usługą zdalnego dostępu, usługa ta czyta politykę, aby ustalić, czy użytkownik ma prawo do połączenia, a jeśli tak, to jaki profil zastosować podczas jego sesji. Częściowe uaktualnienie może wpływać na usługę zdalnego dostępu w różny sposób:
- Jeżeli polityka jest złożona i składa się z wielu obiektów, usługa zdalnego dostępu może czytać częściowo uaktualnioną politykę, co może spowodować niewłaściwą odmowę lub zgodę na usługę dla użytkownika, niemożność przetworzenia polityki ze względu na wewnętrzna niespójność, itp.
- Jeżeli zarówno polityka jak i profile zostały uaktualnione, usługa może prawidłowo przetworzyć politykę, ale zastosować przestarzały profil, ponieważ obiekty polityki już zostały zreplikowane, a profile jeszcze nie.

Jeżeli profil jest złożony i składa się z wielu obiektów, usługa może prawidłowo przetworzyć politykę, lecz zastosować częściowo uaktualniony profil, ponieważ zostały już zreplikowane obiekty polityki, ale tylko niektóre obiekty profilu.

Replikacja (powielanie) (Replication) - Active Directory zapewnia replikacje typu wiele-głównych (multi-master). Replikacja wiele-głównych oznacza, że wszystkie repliki danej partycji dają się zapisywać. Pozwala to na zastosowanie uaktualnień do dowolnej repliki danej partycji. System replikacji Active Directory upowszechnia zmiany z danej repliki na wszystkie inne repliki. Replikacja jest automatyczna i przechodnia.

Numer kolejności uaktualnienia (Update Sequence Number) - USN jest 64-bitową liczbą utrzymywaną przez każdy serwer Directory. Gdy serwer zapisuje jakąś właściwość do Active Directory, USN jest zwiększany i zachowywany z zapisaną właściwością. Operacja jest wykonywana atomowo - to znaczy, że zwiększenie i zachowanie USN i zapisanie właściwości powodzi się lub nie jako jedna jednostka pracy.
Skrzywienie wersji (Version Skew) - Skrzywienie wersji następuje, gdy aplikacje czytają ten sam obiekt (obiekty) z różnych replik, zanim zostaną powielone zmiany. Aplikacje czytając odległe repliki widzą obiekty niezmienione. Skrzywienie wersji staje się sprawą, gdy dana aplikacja albo zbiór aplikacji spowoduje, że informacje w obiektowej bazie danych staną się niekompatybilne.