Glossar

A

Active Directory

Active Directory ist der vom Betriebssystem Windows 2000 verwendete LDAP-Verzeichnisdienst.

Anmeldeinformationen

Anmeldeinformationen sind eine Sammlung von Elementen, die ein Principal zum Nachweis seiner Identität verwendet. Benutzername und Kennwort sind ein geläufiges Beispiel für Anmeldeinformationen.

Anmeldesitzung

Eine Anmeldesitzung definiert den Sicherheitskontext, in dem jeder Prozess ausgeführt wird. Wenn Sie sich interaktiv an einem Computer anmelden, wird eine interaktive Anmeldesitzung erstellt, die als Host für die Windows-Shell und jeden Prozess dient, den Sie möglicherweise interaktiv starten. Wenn ein Prozess in Ihrem Namen auf einen Remotecomputer zugreift, werden Ihre Anmeldeinformationen (die von der lokalen Anmeldesitzung gecacht werden) verwendet, um Authentifizierungsanforderungen des Remotecomputers zu beantworten. Wenn der Authentifizierungsprozess erfolgreich abläuft, wird eine Netzwerkanmeldesitzung auf dem Remotecomputer eröffnet, in deren Rahmen die Prozesse laufen, die in Ihrem Namen auf dem Remotecomputer ausgeführt werden.

Anonyme Authentifizierung

Die anonyme Authentifizierung ist eine Art der IIS-Authentifizierung, bei der IIS keinen Versuch unternimmt, die Identität des Clients zu bestätigen. Die anonyme Authentifizierung ist mit keiner Authentifizierung gleichzusetzen. Sie wird häufig in Verbindung mit der Formularauthentifizierung von ASP.NET verwendet, bei der ein HTML-Formular für die Erfassung der Anmeldeinformationen des Clients herangezogen wird.

Anwendungsserver

Ein Anwendungsserver ist ein dedizierter Servercomputer, der vom Front-End-Webserver getrennt ist. Der Anwendungsserver fungiert in der Regel als Host für Webdienste, Remotekomponenten und/oder Enterprise Services-Anwendungen, die den Hauptteil der Geschäftslogik einer Anwendung enthalten.

Authentifizierung

Die Authentifizierung ist der Prozess des Identitätsnachweises. Wenn Sie sich beispielsweise bei Windows anmelden, werden Sie vom Betriebssystem authentifiziert, indem Ihre Anmeldeinformationen, also Benutzername und Kennwort, abgefragt werden. Wenn ein Prozess (eine Art von Principal) in Ihrem Namen die Verbindung zu einem Remotecomputer herstellt, werden die Authentifizierungsaufforderungen aus dem Netzwerk mithilfe einer im Cache befindlichen Sammlung von Anmeldeinformationen beantwortet.

Autorisierung

Bei der Autorisierung wird festgestellt, ob eine authentifizierte Identität über die erforderlichen Rechte für den Zugriff auf die angeforderte Ressource oder das Durchführen des angeforderten Vorgangs verfügt.

Autorität

Eine Autorität ist eine vertrauenswürdige Entität (eine Organisation oder ein Computer), die Authentifizierungsdienste bereitstellt.

B

Base-64-Codierung

Die Base-64-Codierung ist eine gut definierte Methode für die Darstellung von Binärdaten als druckbaren ASCII-Text, der für den Einsatz in Verbindung mit textbasierten Protokollen wie HTTP geeignet ist. Hierbei handelt es sich nicht um eine Verschlüsselungsmethode.

Benutzerprofil

Mit Benutzerprofilen werden die Konfigurationsinformationen eines Benutzers verwaltet. Hierzu gehört die Gestaltung des Desktops ebenso wie persönliche Programmgruppen, Programmelemente, Bildschirmfarben, Bildschirmschoner, Netzwerkverbindungen usw. Wenn sich ein Benutzer interaktiv anmeldet, lädt das System das Profil des Benutzers und konfiguriert die Umgebung gemäß den Informationen im Profil.

Die **LoadUserProfile**-API kann verwendet werden, um ein Benutzerprofil programmgesteuert zu laden. Nicht interaktive Konten wie beispielsweise das lokale ASPNET-Konto, das zum Ausführen von ASP.NET-Webanwendungen verwendet wird, verfügen nicht über ein Benutzerprofil.

C

Clientzertifikat

Ein Clientzertifikat ist ein von Clients verwendetes Zertifikat, das eine positive Identifikation der jeweiligen Identität gegenüber Serveranwendungen ermöglicht.

Codezugriffssicherheit

Die Codezugriffssicherheit ist eine Form der .NET-Sicherheit, mit der die Zugriffsrechte von Code auf geschützte Ressourcen kontrolliert werden.

D

Datenschutz

Der Datenschutz sorgt dafür, dass Daten geheim und vertraulich bleiben und nicht mit einer Netzwerküberwachungssoftware von Lauschern angezeigt werden können. Datenschutz wird in der Regel durch Verschlüsselung ermöglicht.

Deklarative Autorisierung

Die deklarative Autorisierung ist eine Art der Autorisierung, die mithilfe von Attributen realisiert wird. Beispielsweise stellt .NET die **PrincipalPermissionAttribute**-Klasse bereit, die zum Notieren von Methoden für die Bereitstellung von deklarativer Autorisierung herangezogen werden kann.

Die nachstehende deklarative Autorisierung stellt beispielsweise sicher, dass die Methode **DoPrivMethod** nur von Mitgliedern der Rollen **Manager** oder **Teller** ausgeführt werden kann.

```
[PrincipalPermissionAttribute(SecurityAction.Demand, Role="Teller"),
 PrincipalPermissionAttribute(SecurityAction.Demand, Role="Manager")]
public void DoPrivMethod()
{
}
```

Delegierung

Die Delegierung ist eine erweiterte Form des Identitätswechsels, mit der ein Serverprozess, der eine Aufgabe im Namen eines Clients ausführt, auf die Ressourcen eines Remotecomputers zugreifen kann. Diese Fähigkeit wird durch die Kerberos-Integration in Windows 2000 und späteren Betriebssystemen bereitgestellt. Bei einem herkömmlichen Identitätswechsel (z. B. durch NTLM) ist lediglich ein einziger Netzwerkhop möglich. Wenn der NTLM-Identitätswechsel verwendet wird, erfolgt dieser eine Hop zwischen dem Client und den Servercomputern, sodass der Server bei einem Identitätswechsel auf den Zugriff auf lokale Ressourcen beschränkt ist.

DES

Bei DES (Data Encryption Standard) handelt es sich um eine Blockverschlüsselung, bei der Daten in 64-Bit-Blocks verschlüsselt werden. DES ist ein symmetrischer Algorithmus, bei dem der gleiche Algorithmus und der gleiche Schlüssel für die Ver- und Entschlüsselung verwendet wird. DES wurde durch Dreifach-DES (Triple DES) ersetzt.

Dienstkonto

Ein Dienstkonto ist ein speziell konfiguriertes Konto (auch als Proxykonto bezeichnet), das ausschließlich zum Zwecke des Zugriffs auf eine nachgeordnete Ressource (häufig eine Datenbank) in einer auf mehreren Ebenen verteilten Anwendung verwendet wird. Die Komponenten der mittleren Ebene verwenden häufig eine begrenzte Anzahl Dienstkonten für die Herstellung der Verbindung zu einer Datenbank, um das Verbindungspooling zu unterstützen. Dienstkonten können Windows-Konten sein, die in Active Directory oder der SAM-Datenbank verwaltet werden, oder SQL-Konten, die von SQL Server verwaltet werden.

Digest

Siehe Hash.

Digestauthentifizierung

Die Digestauthentifizierung wird mit dem HTTP-Protokoll 1.1 definiert, ist jedoch nicht weit verbreitet. Bei dieser Form der Authentifizierung wird ein Kennwort nicht im Klartext über das Netzwerk übertragen. Stattdessen wird ein Kennwort-Hash oder Digest übergeben. Diese Authentifizierungsform ist zwar sicherer als die Standardauthentifizierung, setzt jedoch Internet Explorer 5.0 oder höher auf dem Client sowie einen Windows 2000-Computer als Server voraus, bei dem IIS 5.0 mit Active Directory ausgeführt wird.

Digitale Signatur

Eine digitale Signatur wird für die Nachrichtenauthentifizierung verwendet, um zum einen die Gültigkeit der Identität des Senders der Nachricht und zum anderen die Integrität der Nachricht sicherzustellen, d. h. um zu gewährleisten, dass die Daten während der Übertragung nicht geändert wurden. Beim Signieren der Daten werden diese nicht geändert. Hierbei wird lediglich eine digitale Signaturzeichenfolge erzeugt, die mit den Daten übertragen wird.

Digitale Signaturen werden unter Verwendung von Signaturalgorithmen mit öffentlichen Schlüsseln wie z. B. der Verschlüsselungsmethode RSA erstellt.

Digitale XML-Signatur

Eine digitale XML-Signatur ist eine digitale Signatur, die für ein XML-Dokument verwendet wird.

Domänenkonten

Domänenkonten sind Windows- oder Gruppenkonten, die zentral in der SAM-Datenbank eines Domänencontrollers oder in Active Directory verwaltet werden.

DPAPI

Die DPAPI (Data Protection API) ist eine Win32-API, die unter Windows 2000 und nachfolgenden Betriebssystemen zur Verfügung steht und zum Ver- und Entschlüsseln von Daten verwendet wird. Mit der DPAPI wird das Schlüsselverwaltungsproblem, das generell mit Verschlüsselungstechniken einhergeht, an das Betriebssystem ausgelagert, da hierbei die Kennwörter von Windows-Konten zum Erzeugen von Verschlüsselungsschlüsseln verwendet werden.

E

EFS

Das verschlüsselnde Dateisystem (Encrypting File System oder EFS) wird von Windows 2000 und nachfolgenden Betriebssystemen bereitgestellt und bietet Dateiverschlüsselungs-funktionen für NTFS-Datenträger.

Entropie

Die Entropie ist eine Maßnahme zur Schaffung von Ungewissheit. Sie wird in Verbindung mit einigen Verschlüsselungstechnologien verwendet, um einen gewissen Grad an Zufälligkeit in den Verschlüsselungsprozess einzubringen. Wird zusätzlich zum Verschlüsselungsschlüssel ein Entropiewert zum Verschlüsseln von Daten verwendet, muss dieser auch zum Entschlüsseln verwendet werden.

F

Fester Identitätswechsel des Principals

Der feste Identitätswechsel des Principals ist eine von ASP.NET verwendete Form des Identitätswechsels, bei der die gewechselte Identität ungeachtet der Identität des authentifizierten Aufrufers konstant bleibt. Normalerweise wird die gewechselte Identität von der Identität des Aufrufers bestimmt. Die für den festen Identitätswechsel des Principals verwendete Identität wird hingegen festgelegt, indem die Attribute **userName** und **password** des <**identity**>-Elements in **Web.config** herangezogen werden. Nachstehend ein Beispiel:

```
<identity userName="Bob" password="password" />
```

Formularauthentifizierung

Die Formularauthentifizierung ist eine von ASP.NET unterstützte Form der Authentifizierung, die voraussetzt, dass sich die Benutzer über die Eingabe von Anmeldeinformationen in ein HTML-Formular anmelden.

Freigegebene Zugriffssteuerungsliste

Eine freigegebene Zugriffssteuerungsliste (Discretionary Access Control List oder DACL) ist mit einem sicherungsfähigen Objekt verknüpft (unter Verwendung eines Sicherheitsdeskriptors) und gibt die Sammlung der Zugriffsrechte an, die Benutzern und Benutzergruppen gewährt werden. Die DACL wird vom Besitzer eines Objekts kontrolliert und besteht aus einer geordneten Liste mit Zugriffssteuerungseinträgen (Access Control Entries oder ACEs), die die Arten der Operationen festlegen, die ein Benutzer oder eine Benutzergruppe mit einem Objekt durchführen können.

G

Gatekeeper

Ein Gatekeeper ist eine Technologie oder ein Subsystem, die bzw. das für die Bereitstellung von Zugriffssteuerung verwendet wird. Beispiele für Gatekeeper sind IIS sowie **UrlAuthorizationModule** und **FileAuthorizationModule** von ASP.NET.

Gegenseitige Authentifizierung

Bei der gegenseitigen Authentifizierung authentifiziert der Client den Server und der Server den Client. Diese Art der Authentifizierung wird nicht von NTLM, sondern von Kerberos unterstützt. Darüber hinaus kann auch SSL verwendet werden, wenn der Server Clientzertifikate akzeptiert bzw. fordert.

GenericIdentity

GenericIdentity ist eine Implementierung der **IIdentity**-Schnittstelle, die von ASP.NET in Verbindung mit den Authentifizierungsmechanismen Formularauthentifizierung und Passport-Authentifizierung (und manchmal benutzerdefinierter Authentifizierungsmechanismen) verwendet wird. Das **GenericPrincipal**-Objekt enthält ein **GenericIdentity**-Objekt.

GenericPrincipal

GenericPrincipal ist eine Implementierung der **IPrincipal**-Schnittstelle, die von ASP.NET in Verbindung mit den Authentifizierungsmechanismen Formularauthentifizierung und Passport-Authentifizierung (und möglicherweise auch benutzerdefinierter Authentifizierungsmechanismen) verwendet wird. Es enthält die Liste der Rollen, denen der Benutzer angehört (und die von der Anwendung aus einem benutzerdefinierten Datenspeicher abgerufen wurde).

Das **GenericPrincipal**-Objekt ist mit dem Kontext von Webanforderungen verknüpft und wird für die Autorisierung verwendet. Es enthält ein **GenericIdentity**-Objekt.

H

Hash

Ein Hash ist ein numerischer Wert fester Länge, anhand dessen Daten eindeutig identifiziert werden können. Hashwerte sind nützlich, um die Integrität von Daten zu prüfen, die über unsichere Kanäle gesendet wurden. Hierbei kann der Hashwert der empfangenen Daten mit dem Hashwert der Daten beim Versand verglichen werden, um festzustellen, ob die Daten verändert wurden.

Hashwerte werden zudem in Verbindung mit digitalen Signaturen verwendet. Da die kleineren Hashwerte verwendet werden können, um wesentlich umfangreichere Datenmengen zu repräsentieren, muss nur der Hash einer Nachricht und nicht die gesamte Nachrichten-datenmenge signiert werden.

HTTP-Handler

ASP.NET ordnet HTTP-Anforderungen HTTP-Handlern zu. ASP.NET ordnet zudem auch einzelne URLs oder Gruppen aus URL-Erweiterungen bestimmten HTTP-Handlern zu. HTTP-Handler sind die funktionellen Entsprechungen von ISAPI-Erweiterungen, weisen jedoch ein wesentlich einfacheres Programmierungsmodell auf. Ein HTTP-Handler ist eine Assembly, die die Schnittstellen **IHttpHandler** und **IHttpAsyncHandler** implementiert.

HTTP-Kontext

Der HTTP-Kontext ist der Kontext oder die Eigenschaftenauflistung, die mit der aktuellen Webanforderung verbunden ist (und diese beschreibt).

HTTP-Modul

Ein HTTP-Modul wird von ASP.NET verwendet, um Webanforderungen zu verarbeiten. Ein HTTP-Modul ist eine Assembly, die die **IHttpModule**-Schnittstelle implementiert und Ereignisse verarbeitet. ASP.Net verwendet eine Reihe von integrierten Modulen wie die Authentifizierungsmodule, das Sitzungsstatusmodul und das Global Cache-Modul. Darüber hinaus können benutzerdefinierte HTTP-Module entwickelt und in die HTTP-Verarbeitungspipeline von ASP.NET integriert werden.

I

Identität

Die Identität bezieht sich auf ein Merkmal eines Benutzers oder Dienstes, anhand dessen eine eindeutige Identifizierung möglich ist. Oftmals handelt es sich hierbei um einen Anzeigenamen, in der Regel in der Form "Autorität/Benutzername".

Identitätswechsel

Der Identitätswechsel ist eine Technik, die von einer Serveranwendung verwendet wird, um im Namen des Clients auf Ressourcen zuzugreifen, indem eine Kopie des Zugriffstokens des Clients verwendet wird. Um die Erzeugung des Zugriffstokens eines Clients auf dem Servercomputer zu vereinfachen, muss der Client seine Identität über das Netzwerk an die Serveranwendung übermitteln.

Siehe auch Fester Identitätswechsel des Principals.

Identitätswechseltoken

Siehe Threadtoken.

Imperative Autorisierung

Die imperative Autorisierung ist eine Form der Autorisierung, die mit Methodencode implementiert wird. Beispielsweise stellt .NET die **PrincipalPermissionAttribute**-Klasse bereit, die – wie im nachstehenden Code gezeigt – für die Implementierung von imperativer Autorisierung herangezogen werden kann. Der Code fordert, dass der Aufrufer der Rolle **Teller** angehört. Wenn der Aufrufer dieser Rolle nicht angehört, wird eine Sicherheitsausnahmebedingung erzeugt, und der mit erweiterten Rechten ausgestattete Code (der Code, der auf den Aufruf der **Demand**-Methode folgt) wird nicht ausgeführt.

```
public UsePrivilege()
{
  PrincipalPermission permCheck = new PrincipalPermission(null,"Teller");
  permCheck.Demand();
  // privileged code
}
```

Integrität

Sichere Kommunikationskanäle müssen auch sicherstellen, dass die Daten bei der Übertragung vor versehentlichen oder absichtlichen (böswilligen) Änderungen geschützt werden. Die Integrität wird normalerweise durch Nachrichtenauthentifizierungscodes (Message Authentication Codes oder MACs) bereitgestellt.

IPSec

IPSec (Internet Protocol Security) ist eine Form der Sicherheit auf Transportebene. IPSec verschlüsselt Daten auf dem Übertragungsweg zwischen zwei Computern und schützt sie auf diese Weise vor Änderung und Ausspähen.

J

K

Kerberos

Kerberos ist ein Authentifizierungsprotokoll, das von Windows 2000 und nachfolgenden Betriebssystemen unterstützt wird. Kerberos unterstützt die erweiterte Form des Identitätswechsels, die sogenannte Delegierung, die es dem Sicherheitskontext des Aufrufers ermöglicht, auf Netzwerkressourcen ebenso zuzugreifen wie auf Ressourcen, die das Serverbetriebssystem als lokale Ressourcen verwaltet.

Klartext

Unverschlüsselte Daten liegen im Klartext vor.

Konto

Ein Konto ist ein Eintrag in der Sicherheitsdatenbank, der die Sicherheitsattribute eines einzelnen Principals enthält. Bei der Sicherheitsdatenbank kann es sich entweder um die SAM-Datenbank oder um Active Directory handeln.

Konten können entweder Domänenkonten oder lokale Konten sein.

Kryptografie

Die Kryptografie ist die Kunst und die Wissenschaft der Informationssicherheit. Sie umfasst Datensicherheit und -vertraulichkeit, Integrität und Authentifizierung.

L

LDAP

LDAP (Lightweight Directory Access Protocol) ist ein Protokoll für den Zugriff auf Verzeichnisdienste wie Active Directory.

LogonUser

LogonUser ist eine Win32-API zum Erstellen einer Anmeldesitzung (und eines Zugriffstokens) für ein angegebenes Windows-Konto. Code, der **LogonUser** aufruft, muss Teil der TCB (Trusted Computing Basis) des Computers sein, was bedeutet, dass er innerhalb eines Prozesses ausgeführt werden muss, dessen Windows-Konto über das Recht **Als Teil des Betriebssystems handeln** verfügt.

Lokales Konto

Ein lokales Konto ist ein Windows-Konto, das in der lokalen SAM-Datenbank des jeweiligen Computers gespeichert ist und verwaltet wird. Lokale Konten können (im Gegensatz zu Domänekonten) nicht für den Zugriff auf Netzwerkressourcen verwendet werden, es sei denn, auf dem Remotecomputer wurde das gleiche lokale Konto (mit dem gleichen Benutzernamen und Kennwort) noch einmal eingerichtet.

LSA

Die LSA (Lokale Sicherheitsautorität) ist ein lokales Windows-Subsystem, das für die Bereitstellung von Authentifizierungsdiensten zuständig ist.

M

MAC

Der Nachrichtenauthentifizierungscode (Message Authentication Code, MAC) ist ein Hashwert, der an eine Nachricht angefügt wird, um deren Integrität sicherzustellen. Bei der Verwendung eines MAC-Algorithmus zur Erzeugung eines Hashwertes muss die empfangende Anwendung ebenfalls über den Sitzungsschlüssel verfügen, um den Hashwert neu zu berechnen, sodass sichergestellt werden kann, dass die Nachrichtendaten nicht geändert wurden.

Modell der vertrauenswürdigen Subsysteme

Das Modell der vertrauenswürdigen Subsysteme ist ein von Webanwendungen verwendetes Ressourcenzugriffsmodell, bei dem die Anwendung eine feste "vertrauenswürdige" Identität verwendet, um auf nachgeordnete Ressourcen-Manager wie Datenbanken zuzugreifen.

Der Datenbankadministrator definiert innerhalb der Datenbank Sicherheitsrollen und Berechtigungen für die spezifische "vertrauenswürdige" Identität. Dieses Modell unterstützt das Datenbankverbindungspooling, wodurch die Skalierungsfähigkeit einer Anwendung wesentlich erhöht wird. Diese Modell steht im Gegensatz zum Modell mit Identitätswechsel/Delegierung.

Modell mit Identitätswechsel/Delegierung

Ein Modell mit Identitätswechsel/Delegierung ist ein Ressourcenzugriffsmodell, bei dem der Sicherheitskontext des ursprünglichen Aufrufers über aufeinander folgende Anwendungsebenen an die Back-End-Ressourcen-Manager weitergegeben wird. Auf diese Weise sind die Ressourcen-Manager in der Lage, Autorisierungsentscheidungen basierend auf der Identität des ursprünglichen Aufrufers zu treffen.

Dies steht im Gegensatz zum Modell der vertrauenswürdigen Subsysteme, bei dem feste "vertrauenswürdige" Identitäten für den Zugriff auf Ressourcen verwendet werden.

N

Nachweisbarkeit

Unter Nachweisbarkeit versteht man die Möglichkeit, den Benutzer zu identifizieren, der bestimmte Aktionen durchgeführt hat, sodass dessen Verantwortung unwiderlegbar bewiesen werden kann. Beispielsweise kann ein System immer dann die Kennung eines Benutzers protokollieren, wenn eine Datei gelöscht wird.

NTLM

NTLM (Windows NT LAN Manager) ist ein Abfrage-/Antwort-Authentifizierungsprotokoll, das in Netzwerken mit Windows NT-Betriebssystemversionen vor Windows 2000 und auf eigenständigen Systemen zum Einsatz kommt.

O

Öffentlicher Schlüssel

Der öffentliche Schlüssel ist die öffentlich zugängliche Hälfte des aus einem öffentlichen und einem privaten Schlüssel bestehenden Schlüsselpaares. Der öffentliche Schlüssel wird in der Regel verwendet, um einen Sitzungsschlüssel oder eine digitale Signatur zu entschlüsseln. Der öffentliche Schlüssel kann auch verwendet werden, um eine Nachricht zu verschlüsseln, womit sichergestellt wird, dass nur die Person, die über den entsprechenden privaten Schlüssel verfügt, die Nachricht wieder entschlüsseln kann.

P

PKCS

Unter PKCS (Public-Key Cryptography Standards) versteht man eine Reihe von Syntaxstandards für die Verschlüsselung mit öffentlichen Schlüsseln, die Sicherheitsfunktionen einschließlich Methoden für das Signieren von Daten, den Austausch von Schlüsseln, die Anforderung von Zertifikaten, die Ver- und Entschlüsselung mit öffentlichen Schlüsseln und weitere Sicherheitsfunktionen umfassen.

Principal

Ein Principal ist eine Entität (in der Regel eine Person, ein Computer, eine Anwendung oder ein Dienst), die versucht, auf eine gesicherte Ressource oder Anwendung zuzugreifen. Ein Principal verfügt über einen eindeutigen Namen und diverse Möglichkeiten, seine Identität gegenüber anderen Principals in einem System nachzuweisen.

Prinzip der minimalen Rechte

Beim Prinzip der minimalen Rechte wird versucht, ausführbaren Code unter Verwendung einer Prozessidentität auszuführen, die über so wenig Rechte wie nur möglich verfügt. Der Zweck dieser Vorgehensweise besteht darin, den potenziellen Schaden, der mit einer möglichen Gefährdung des Prozesses einhergeht, so weit wie möglich einzugrenzen.

Wenn ein böswilliger Benutzer es schafft, Code in einen Serverprozess einzubringen, bestimmen die Rechte, die dem betreffenden Prozess gewährt wurden, im Wesentlichen den Typ der Operationen, die der Benutzer ausführen kann.

Privater Schlüssel

Der private Schlüssel ist die geheime Hälfte des Schlüsselpaares, das bei einem Algorithmus mit öffentlichem Schlüssel zum Einsatz kommt. Private Schlüssel werden in der Regel verwendet, um einen symmetrischen Sitzungsschlüssel zu verschlüsseln, um ein Nachricht digital zu signieren oder eine Nachricht zu entschlüsseln, die mit dem zugehörigen öffentlichen Schlüssel verschlüsselt wurde.

Proxykonto

Siehe Dienstkonto.

Prozessidentität

Die Prozessidentität wird von dem Windows-Konto bestimmt, das zum Ausführen eines ausführbaren Prozesses verwendet wird. Beispielsweise ist ASPNET (ein lokales, mit minimalen Rechten ausgestattetes Windows-Konto) die standardmäßige Prozessidentität des ASP.NET-Workerprozesses (**Aspnet_wp.exe**).

Die Prozessidentität bestimmt zudem auch den zu verwendenden Sicherheitskontext, wenn Code innerhalb des Prozesses auf lokale oder Remoteressourcen zugreift. Nimmt der Code einen Identitätswechsel vor, stellt die Threadidentität (die vom Threadtoken bestimmt wird) den Sicherheitskontext für den Ressourcenzugriff bereit.

Q

R

RC2

RC2 ist der CryptoAPI-Algorithmusname für den RC2-Algorithmus.

RC4

RC4 ist der CryptoAPI-Algorithmusname für den RC4-Algorithmus.

Recht

Unter einem Recht wird die Fähigkeit eines Benutzers verstanden, bestimmte mit dem System zusammenhängende Operationen auszuführen, wie beispielsweise Herunterfahren des Systems, Laden von Gerätetreibern oder Ändern der Systemzeit. Das Zugriffstoken eines Benutzers enthält eine Liste der Rechte, die dem Benutzer oder der Benutzergruppe, der der Benutzer angehört, gewährt wurden.

Rollen

Rollen sind logische Bezeichner (wie beispielsweise "Manager" oder "Mitarbeiter"), die von einer Anwendung verwendet werden, um Benutzer mit denselben Sicherheitsrechten innerhalb der Anwendung zu gruppieren. Beispiele für Rollen sind .NET-Rollen, Enterprise Services- (COM+-) Rollen und die von SQL Server verwendeten Datenbankrollen.

RSA

Die RSA Data Security, Inc., ist eine bedeutende Entwicklerin und Herausgeberin von Kryptografiestandards für die Verschlüsselung mit öffentlichen Schlüsseln. RSA steht für die Namen der drei Entwickler und Eigentümer des Unternehmens: Rivest, Shamir und Adleman.

S

SACL

Eine Systemzugriffssteuerungsliste (System Access Control List oder SACL) ist mit einem sicherungsfähigen Objekt verknüpft (unter Verwendung eines Sicherheitsdeskriptors) und gibt die Arten der Operationen eines bestimmten Benutzers an, die Überwachungsmeldungen erzeugen sollen.

Salt-Wert

Der Salt-Wert ist eine Zufallszahl, die in Verbindung mit verschlüsselten oder per Hash-algorithmus transformierten Daten verwendet werden kann, um den Aufwand zu erhöhen, der mit einem Brute-Force-Verzeichnisangriff (Wörterbuchangriff) auf die geschützten Daten verbunden ist. Dieser Wert wird in der Regel vor verschlüsselte oder per Hashalgorithmus transformierte Daten gesetzt.

SAM-Datenbank

Bei der SAM-Datenbank handelt es sich um die von Windows NT und Windows 2000 (ohne Active Directory) verwendete Datenbank für die Verwaltung von Benutzer- und Gruppenkonten.

Schlüssel

Ein Schlüssel ist ein Wert, der an einen Ver- oder Entschlüsselungsalgorithmus übergeben wird, mit dem Daten ver- oder entschlüsselt werden. Bei symmetrischen Verschlüsselungsalgorithmen wird für die Ver- und Entschlüsselung von Daten derselbe Schlüssel, bei asymmetrischen Algorithmen ein aus einem öffentlichen und einem privaten Schlüssel bestehendes Schlüsselpaar verwendet.

Schlüsselpaar

Ein Schlüsselpaar setzt sich aus einem öffentlichen und einem privaten Schlüssel zusammen, die zu einer Einheit gehören und zum Ver- und Entschlüsseln von Daten verwendet werden.

Schlüsselspeicher

Ein Schlüsselspeicher ist der Speicherort, an dem die Microsoft Cryptography API (CryptoAPI) Schlüsselpaare speichert (in der Regel in einer Datei oder als Registrierungsschlüssel). Schlüsselspeicher sind entweder benutzerspezifisch oder spezifisch für den Computer, auf dem sie erzeugt wurden.

SHA

SHA (Secure Hash Algorithm) ist ein Algorithmus zum Erzeugen eines Nachrichtendigests oder -hashs. Der ursprüngliche SHA-Algorithmus wurde durch den verbesserten SHA1-Algorithmus ersetzt.

Sichere Kommunikation

Bei der sicheren Kommunikation geht es um die Bereitstellung von Nachrichtenintegrität und Datenschutz beim Transfer von Daten durch ein Netzwerk. Als Technologien für die Bereitstellung einer sicheren Kommunikation kommen u. a. SSL und IPSec zum Einsatz.

Sicherheitsdeskriptor

Ein Sicherheitsdeskriptor (Security Descriptor oder SD) enthält Sicherheitsinformationen, die mit einem sicherungsfähigen Objekt wie beispielsweise einer Datei oder einem Prozess verbunden sind. So umfasst der Sicherheitsdeskriptor z. B. Attribute wie die Identifikation des Besitzers eines Objekts, der Sicherheitsgruppen, denen der Besitzer angehört, sowie zwei Zugriffssteuerungslisten (Access Control Lists oder ACLs), und zwar die freigegebene Zugriffssteuerungsliste (Discretionary Access Control List oder DACL), die die Zugriffsrechte einzelner Benutzer und Benutzergruppen definiert, und die Systemzugriffssteuerungsliste (System Access Control List oder SACL), die die Arten der Operationen definiert, die, wenn sie an einem Objekt vorgenommen werden, Überwachungsmeldungen erzeugen sollen.

Sicherheitskontext

Sicherheitskontext ist ein generischer Begriff, mit dem die Gesamtheit der Sicherheits-einstellungen bezeichnet wird, die das sicherheitsrelevante Verhalten eines Prozesses oder Threads beeinflussen. Die Attribute der Anmeldesitzung und des Zugriffstokens eines Prozesses bilden zusammen den Sicherheitskontext des Prozesses.

SID

Anhand der Sicherheitskennung (Security Identifier oder SID) wird ein Benutzer oder eine Benutzergruppe in einer Domäne eindeutig identifiziert. Eine SID ist ein Wert mit variabler Länge, der eine Revisionsstufe, einen Wert für die authentifizierende Autorität (den Aussteller der SID, normalerweise Windows), eine Reihe von Werten für untergeordnete Autoritäten (die in der Regel für die Netzwerkdomäne stehen) und eine relative ID (RID) umfasst, die in der Kombination aus authentifizierender Autorität/untergeordneter Autorität eindeutig ist.

SIDs werden niemals erneut verwendet, auch dann nicht, wenn ein Benutzerkonto gelöscht und mit der gleichen Kombination aus Name und Kennwort neu erstellt wird.

Sitzungsschlüssel

Der Sitzungsschlüssel ist ein als Zufallszahl erzeugter symmetrischer Schlüssel, der zum Verschlüsseln von Daten verwendet wird, die zwischen zwei Parteien übertragen werden. Sitzungsschlüssel werden nur einmal (für eine einzige Sitzung) verwendet und danach verworfen.

SOAP

SOAP ist ein einfaches XML-basiertes Protokoll für den Datenaustausch in einer verteilten Umgebung. SOAP wird von Webdiensten verwendet.

SOAP-Erweiterung

Eine SOAP-Erweiterung ist ein von ASP.NET unterstützter Erweiterungsmechanismus, der es ermöglicht, die SOAP-Nachrichtenverarbeitung zu erweitern. Mit einer SOAP-Erweiterung können Sie eine Nachricht in bestimmten Stadien des Verarbeitungslebenszyklus entweder auf dem Client oder auf dem Server prüfen oder ändern.

SSL

SSL (Secure Sockets Layer) ist ein Protokoll für die sichere Netzwerkkommunikation, bei dem eine Kombination aus öffentlichem und geheimem Schlüssel verwendet wird.

SSPI

SSPI (Security Support Provider Interface) ist eine gemeinsame Schnittstelle zwischen Anwendungen auf der Transportebene, wie z. B. Microsoft RPC (Remote Procedure Call oder Remoteprozeduraufruf) und Sicherheitsprovidern, wie z. B. der integrierten Windows-Authentifizierung. Mit SSPI kann eine Transportanwendung einen aus einer Reihe von Sicherheitsprovidern aufrufen, um in einheitlicher Weise eine authentifizierte Verbindung aufzubauen.

Standardauthentifizierung

Die Standardauthentifizierung ist Teil des Protokolls HTTP 1.0. Diese Art der Authentifizierung ist weit verbreitet, da sie in praktisch allen Webservern und Webbrowsern implementiert ist. Die Standardauthentifizierung ist ein einfacher Authentifizierungsmechanismus, der weder Kryptografie noch Anfrage-/Antwort-Handshaking umfasst. Stattdessen werden die Anmeldeinformationen eines Principals (Benutzername und Kennwort) direkt vom Client an den Server übergeben. Diese Authentifizierungsmethode stellt ein Sicherheitsrisiko dar, sofern sie nicht in Verbindung mit SSL eingesetzt wird, da das Kennwort vor der Übermittlung über das Netzwerk nicht verschlüsselt wird. Es wird unter Verwendung der Base-64-Codierung übermittelt, sodass das im Klartext vorliegende Kennwort einfach ausgespäht werden kann.

Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung wird für das Ver- und Entschlüsseln von Daten der gleiche Schlüssel verwendet. Hierbei müssen sowohl der Sender als auch der Empfänger der verschlüsselten Daten über den gleichen Schlüssel verfügen.

T

TCB

Eine TCB (Trusted Computing Basis oder vertrauenswürdige Computerbasis) ist eine Grenze, die einen vertrauenswürdigen Teil innerhalb eines Systems definiert, um Sicherheitsrichtlinien durchzusetzen. Ausführbarer Code, der innerhalb der TCB ausgeführt wird, kann Operationen durchführen, ohne dass die normalen Sicherheitsüberprüfungen vorgenommen werden. Beispielsweise werden Gerätetreiber innerhalb der TCB ausgeführt. Benutzercode wird innerhalb der TCB ausgeführt, wenn dem hiermit verbundenen Prozesskonto das Recht **Als Teil des Betriebssystems handeln** gewährt wurde. Benutzercode, der unter dem lokalen SYSTEM-Konto ausgeführt wird, wird ebenfalls innerhalb der Grenzen der TCB ausgeführt.

Temporäres Token

Siehe Threadtoken.

Threadtoken

Ein Threadtoken ist ein temporäres Zugriffstoken, das mit einem bestimmten Thread verknüpft ist. Wenn ein Thread erstellt wird, verfügt dieser nicht über ein Zugriffstoken, und alle sicheren Operationen, die von diesem Thread durchgeführt werden, verwenden Informationen aus dem Prozesstoken. Eine klassische Situation, in der ein Thread ein Zugriffstoken erhält, ist, wenn ein Thread in einem Serverprozess eine Aufgabe im Namen eines Clients durchführen möchte. In diesem Fall führt der Thread einen Identitätswechsel des Clients durch, indem er ein Zugriffstoken erhält, das den Client repräsentiert.

Threadtoken werden auch als temporäre Token oder Identitätswechseltoken bezeichnet.

Token

Siehe Zugriffstoken.

Transitive Vertrauensstellung

Eine transitive Vertrauensstellung ist ein bidirektionales Vertrauensverhältnis zwischen Computern oder Domänen. Transitiv bedeutet, dass, wenn Autorität A Autorität B und Autorität B Autorität C vertraut, Autorität A implizit auch Autorität C vertraut (ohne dass zwischen A und C ein explizites Vertrauensverhältnis bestehen muss). Transitive Vertrauensstellungen werden unter Windows 2000 von Active Directory unterstützt.

Dreifach-DES

Dies ist der Dreifach-DES-Verschlüsselungsalgorithmus (Triple DES, 3DES). Hierbei handelt es sich um eine Variation des DES-Blockverschlüsselungsalgorithmus, bei dem der Klartext mit dem ersten Schlüssel, der hieraus resultierende verschlüsselte Text mit einem zweiten Schlüssel und das Ergebnis der zweiten Verschlüsselung schließlich mit einem dritten Schlüssel verschlüsselt wird. Dreifach-DES ist ein symmetrischer Algorithmus, bei dem der gleiche Algorithmus und die gleichen Schlüssel für die Ver- und Entschlüsselung verwendet werden.

U

Unverschlüsselter Text

Siehe Klartext.

V

Verschlüsselter Text

Verschlüsselter Text sind Daten, die verschlüsselt wurden.

Verschlüsselung

Als Verschlüsselung wird der Prozess des Umwandelns von Daten (im einfachen Textformat) in ein Format bezeichnet, das wie zufällig und bedeutungslos erscheint (verschlüsselter Text) und das ohne einen geheimen Schlüssel nur schwer entschlüsselt werden kann. Verschlüsselung wird verwendet, um die Vertraulichkeit von Nachrichten sicherzustellen.

Verschlüsselung

Verschlüsselung ist ein kryptografischer Algorithmus, der zum Verschlüsseln von Daten verwendet wird.

Verschlüsselung mit öffentlichem und privatem Schlüssel

Die Verschlüsselung mit öffentlichem und privatem Schlüssel ist eine asymmetrische Form der Verschlüsselung, die auf ein kryptografisch erzeugtes Schlüsselpaar bestehend aus einem öffentlichen und einem privaten Schlüssel aufsetzt. Daten, die mit dem privaten Schlüssel verschlüsselt wurden, können nur mit dem zugehörigen öffentlichen Schlüssel wieder entschlüsselt werden und umgekehrt.

Vertrauensstellung

Sichere Systeme setzen bis zu einem gewissen Grad auf Vertrauensstellungen. Beispielsweise muss Benutzern, die über Administratorrechte verfügen (also den Administratoren) das adäquate Vertrauen entgegengebracht werden, dass diese ein System in korrekter Weise verwalten und es nicht in böswilliger Absicht schädigen. In ähnlicher Weise muss Code, der mit erweiterten Rechten ausgeführt wird, wie beispielsweise Gerätetreibern, und Code, der als LocalSystem läuft, vertraut werden. Code, der implizit eine derartige Vertrauensstellung benötigt, wird innerhalb der TCB (Trusted Computing Base oder vertrauenswürdige Computerbasis) des Computers ausgeführt. Code, dem nicht in vollem Umfang vertraut werden kann, darf nicht gestattet werden, innerhalb der TCB zu laufen.

Vertrauensstellungen sind auch für das Modell der vertrauenswürdigen Subsysteme von Bedeutung, bei dem einer Anwendung oder einem Dienst vertraut wird.

Vertraulichkeit

Siehe Datenschutz.

Verzeichnisangriff

Ein Verzeichnisangriff (Wörterbuchangriff) ist ein Brute-Force-Angriff, bei dem der Angreifer versucht, mit jedem nur vorstellbaren geheimen Schlüssel verschlüsselte Daten zu entschlüsseln. Das Risiko solcher Angriffsarten können Sie vermindern, indem Sie einen Salt-Wert in Verbindung mit verschlüsselten (oder per Hashalgorithmus transformierten) Daten verwenden.

W

WindowsIdentity

WindowsIdentity ist eine Implementierung der **IIdentity**-Schnittstelle, die von ASP.NET in Verbindung mit der Windows-Authentifizierung verwendet wird. Ein **WindowsIdentity**-Objekt stellt das Windows-Zugriffstoken des Benutzers zusammen mit dem Benutzernamen bereit. Das **WindowsPrincipal**-Objekt enthält ein **WindowsIdentity**-Objekt.

WindowsPrincipal

WindowsPrincipal ist eine Implementierung der **IPrincipal**-Schnittstelle, die von ASP.NET in Verbindung mit der Windows-Authentifizierung verwendet wird. ASP.NET fügt ein **WindowsPrincipal**-Objekt an den Kontext der aktuellen Webanforderung an, um den authentifizierten Aufrufer zu repräsentieren. Dies wird zum Zwecke der Autorisierung verwendet.

Das **WindowsPrincipal**-Objekt enthält die Liste der Rollen (Windows-Gruppen), denen der Benutzer angehört. Darüber hinaus enthält es das **WindowsIdentity**-Objekt, das Informationen zur Identität des Aufrufers bereitstellt.

X

Y

Z

Zertifikat

Ein Zertifikat ist eine digital signierte Datenstruktur, die Informationen über ein Subjekt (eine Person oder eine Anwendung) sowie den öffentlichen Schlüssel des Subjekts enthält. Zertifikate werden von vertrauenswürdigen Organisationen, sogenannten Zertifizierungsstellen (Certification Authority oder CA), ausgestellt, nachdem die jeweilige Zertifizierungsstelle die Identität des Subjekts überprüft hat.

Zertifikatsauthentifizierung

Die Zertifikatsauthentifizierung ist eine Art der IIS-Authentifizierung, bei der IIS Clientzertifikate akzeptiert, die zum Nachweis der Identität des Clients verwendet werden. Bei dieser Form der Authentifizierung kann IIS ein Clientzertifikat optional auch einem Windows-Benutzerkonto zuordnen, indem auf eine interne Zuordnungstabelle oder auf Active Directory zurückgegriffen wird.

Zertifikatspeicher

Ein Zertifikatspeicher ist ein Speicherort für Zertifikate, Zertifikatsperrlisten (Certificate Revocation List oder CRL) und Zertifikatvertrauenslisten (Certificate Trust List oder CTL).

Zertifikatsperrliste

Eine Zertifikatsperrliste (Certificate Revocation List oder CRL) ist ein Dokument, das von einer Zertifizierungsstelle verwaltet und veröffentlich wird und in dem die von der Zertifizierungsstelle ausgestellten Zertifikate aufgeführt sind, die keine Gültigkeit mehr besitzen.

Zertifizierungsstelle

Eine Zertifizierungsstelle (Certification Authority oder CA) ist eine vertrauenswürdige Organisation oder Entität, die Zertifikate ausstellt.

Zugriffsrecht

Ein Zugriffsrecht ist ein Attribut eines Zugriffstokens, das die Art der Operation festlegt, die eine bestimmte Windows-Gruppe oder ein Benutzer mit einem gesicherten Objekt vornehmen kann. Beispiele für Zugriffsrechte sind Lesen, Schreiben, Löschen, Ausführen usw.

Zugriffssteuerungseintrag

Ein Zugriffssteuerungseintrag (Access Control Entries oder ACEs) identifiziert einen bestimmten Benutzer oder eine Benutzergruppe innerhalb einer Zugriffssteuerungsliste (Access Control List oder ACL) und gibt die Zugriffsrechte dieses Benutzers oder der Gruppe an. Mit einem einzelnen Zugriffssteuerungseintrag können Rechte explizit gewährt oder verweigert werden.

Zugriffssteuerungsliste

Eine Zugriffssteuerungsliste (Access Control List oder ACL) ist eine geordnete Liste mit Zugriffssteuerungseinträgen (Access Control Entries oder ACEs), die einem sicherungsfähigen Objekt zugeordnet wird. Das Betriebssystem Windows verwendet zwei Arten von Zugriffssteuerungslisten, die freigegebene Zugriffssteuerungsliste (Discretionary Access Control List oder DACL), mit der die Zugriffsrechte eines Benutzers oder einer Benutzergruppe festgelegt werden, und die Systemzugriffssteuerungsliste (System Access Control List oder SACL), mit der festgelegt wird, wann bestimmte Zugriffsarten Überwachungsmeldungen erzeugen sollen.

Zugriffstoken

Ein Zugriffstoken ist eine Datenstruktur, die jedem Windows-Prozess zugeordnet ist. Hiermit werden die Informationen zum Sicherheitskontext des Prozesses verwaltet, wozu eine Benutzer-SID gehört, die den Principal der Anmeldesitzung identifiziert, sowie die Autorisierungsattribute einschließlich der Gruppen-SIDs und der Rechte des Benutzers.

Jedes Zugriffstoken ist mit exakt einer Anmeldesitzung verknüpft, während eine Anmeldesitzung mehrere Zugriffstoken enthalten kann, nämlich eines für jeden Prozess, der innerhalb der Anmeldesitzung gestartet wurde, und optional weitere Threadtoken, die mit einzelnen Threads verbunden sind.