

## ERNW Newsletter 28 / August 2009

Liebe Partner, liebe Kollegen,

willkommen zur 28. Ausgabe des ERNW-Newsletters mit dem Thema:

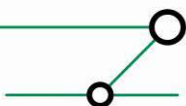
### **Active Directory Security: Sicherheitsbetrachtung des Privilegs “Trusted for delegation”**

Version 1.0 vom 16. August 2009

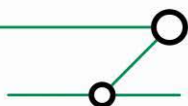
von: Friedwart Kuhn ([fkuhn@ernw.de](mailto:fkuhn@ernw.de))

#### **Abstract**

Dieses Dokument analysiert sicherheitsrelevante Implikationen bei der Verwendung des Privilegs „Trusted for delegation“ im Active Directory und gibt Empfehlungen für die sichere Implementierung dieses Privilegs.



<b>1</b>	<b>MOTIVATION .....</b>	<b>3</b>
<b>2</b>	<b>DAS PRIVILEG „TRUSTED FOR DELEGATION“ .....</b>	<b>3</b>
2.1	„Trusted for delegation“ unter Windows 2000 – ganz oder gar nicht .....	4
2.2	„Trusted for delegation“ und „constrained delegation“ unter Windows Server 2003 und Windows Server 2008 .....	4
<b>3</b>	<b>RISIKOBETRACHTUNG DES PRIVILEGS „TRUSTED FOR DELEGATION“ .....</b>	<b>5</b>
3.1	Bedrohungsszenarien.....	5
3.1.1	Szenario A: Angriff auf das Konto, das delegiert wird.....	5
3.1.2	Szenario B: Ausnutzen des Privilegs „Trusted for delegation“ bei nicht aktivierter „constrained delegation“ .....	5
3.1.3	Szenario C: Angriff auf den Computer, dem das Privileg „Trusted for delegation“ zugewiesen ist .....	5
<b>4</b>	<b>MAßNAHMEN &amp; EMPFEHLUNGEN .....</b>	<b>6</b>
4.1	Starke Authentifizierungsmechanismen .....	6
4.2	Aktivierung von „constrained delegation“ .....	6
4.3	Besonderer Zugriffsschutz für den Computer mit aktiviertem Privileg „Trusted for delegation“ .....	6
4.4	Ausschluss von hochprivilegierten Security Principals von der Delegation.....	7
4.5	Alternative Möglichkeiten.....	7
<b>5</b>	<b>ZUSAMMENFASSUNG UND FAZIT .....</b>	<b>8</b>
<b>6</b>	<b>QUELLEN.....</b>	<b>8</b>



## 1 MOTIVATION

In vielen Active Directory-basierten Umgebungen ist es erforderlich (und gang und gäbe), dass Benutzer über einen Browser auf eine Applikation zugreifen. Ein Teil der Applikation läuft dabei als Webapplikation auf einem Webserver (etwa die Eingabemaske für Daten), während die eigentlichen Daten selbst auf einem Datenbankserver gespeichert werden. Ein solches Szenario wird ebenso durch eine selbst entwickelte (Web-) Applikation wie auch durch den Einsatz eines SharePoint-Servers realisiert. Dabei ist die folgende Design-Frage hinsichtlich von Authentifizierung zu stellen: Wie soll die Authentifizierung des Benutzers gegenüber der Webapplikation und wie die des Webserver, bzw. der Webapplikation gegenüber der Datenbank implementiert werden? Für die vorliegende Untersuchung wird angenommen, dass sich der Benutzer einmal an der Domäne anmeldet und dann über die Webapplikation (oder den SharePoint-Server) transparent (ohne weitere Authentifizierung) auf die Datenbank zugreifen können soll. Dabei sollen alle Authentifizierungen so abgewickelt werden, dass das sichere Kerberosprotokoll verwendet wird und dass Zugriffsberechtigungen für Benutzer zwecks möglicher Audit-Compliance-Anforderungen individuell auf dem Datenbankserver gesetzt werden können. Damit ein solches Single-Sign-On-Szenario mit dem Kerberosprotokoll möglich ist, wird das Privileg „Trusted for delegation“ benötigt. Bei der Verwendung dieses Privilegs stellt sich die Frage, ob das Privileg von Benutzern missbraucht werden kann, um sich dadurch unberechtigten Zugriff auf in der Datenbank gespeicherte Daten anderer Benutzer zu verschaffen, und ob weitere Risiken mit der Verwendung dieses Privilegs verbunden sind.

## 2 DAS PRIVILEG „TRUSTED FOR DELEGATION“

Das Privileg „Trusted for delegation“ beinhaltet ein Konto, dessen Credentials ‚delegiert‘ (impersoniert) werden können, und ein weiteres Konto, das die Delegierung (Impersonierung) durchführt. Dann ermöglicht das Privileg „Trusted for delegation“ einem Benutzer- oder Computerkonto, das Beantragen eines Kerberos „Service Tickets“ für einen anderen „Security Principal“ (Computer-, Benutzer-, oder Dienstkonto) unter der Voraussetzung, dass in den Eigenschaften dessen Kontos die Delegierung nicht explizit verboten wurde (siehe Abschnitt 4.4). In der Default-Einstellung kann ein Computer jedoch keine Authentifizierung delegieren (und der transparente Zugriff auf die Webapplikation ist für den Benutzer nicht möglich):

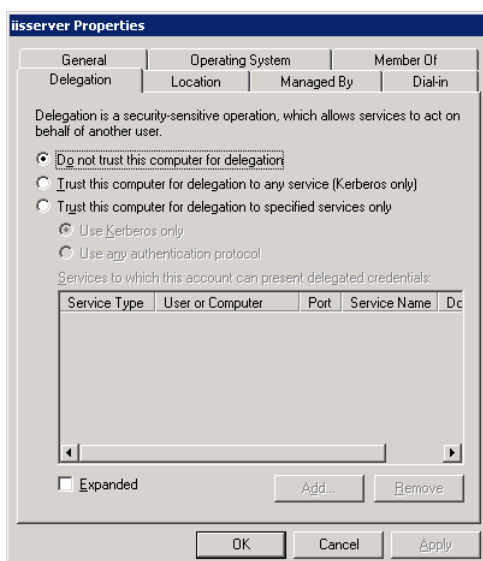
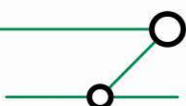


Abbildung 1: Default-Einstellung des Privilegs „Trusted for delegation“ für ein Computer-Konto.



Wenn das Privileg „Trusted for delegation“ etwa für den SharePoint Server gesetzt wurde und auf diesem eine Webapplikation läuft, die mit einer Backend-Datenbank kommuniziert, dann kann ein Benutzer aus seiner Sicht transparent über den Browser auf die Datenbank mit den dort für ihn definierten Zugriffsberechtigungen zugreifen. Der Benutzer kann sich dabei dem SharePoint Server gegenüber mit Kerberos authentifizieren, und der SharePoint Server kann seinerseits im Namen des Benutzers ein Kerberos Service Ticket bei dem Domänencontroller der Domäne für die Authentifizierung gegenüber dem Datenbankserver beantragen. Wird der SharePoint Server dagegen so konfiguriert, dass das Privileg „Trusted for delegation“ nicht vergeben wird, dann kann der Benutzer nicht ohne weitere Authentifizierung auf den Datenbankserver zugreifen.

## 2.1 „Trusted for delegation“ unter Windows 2000 – ganz oder gar nicht

Das Privileg „Trusted for delegation“ ist unter Windows 2000-basiertem Active Directory nur ‚ganz oder gar nicht‘ für einen Security Principal vergebbar: Wird dieses Privileg einem Computer-Konto in einer Windows 2000-basierten Domäne gegeben, dann kann dieser Computer im Namen eines beliebigen Benutzers dieser Domäne Kerberos Service Tickets für den Zugriff auf beliebige Ressourcen beantragen. Gelänge es etwa einem böswilligen Benutzer oder Malware auf einem Windows 2000-basierten Computer mit aktiviertem Privileg „Trusted for delegation“ Schadcode einzuschleusen, dann wäre schlimmstenfalls die gesamte Domäne kompromittiert.

## 2.2 „Trusted for delegation“ und „constrained delegation“ unter Windows Server 2003 und Windows Server 2008

Mit Windows Server 2003<sup>1</sup> wurden Kerberos-Erweiterungen eingeführt, die eine granularere Konfiguration dieses Privilegs gestatten. Damit lässt sich auf einem Computer, dem das Privileg „Trusted for delegation“ gegeben wurde, definieren, für welche Dienste der Domäne der Computer Kerberos Service Tickets im Namen des Benutzers, dessen Konto delegiert wurde, vergeben darf. Diese Einschränkung der Delegierung wird als „constrained delegation“ bezeichnet<sup>2</sup>:

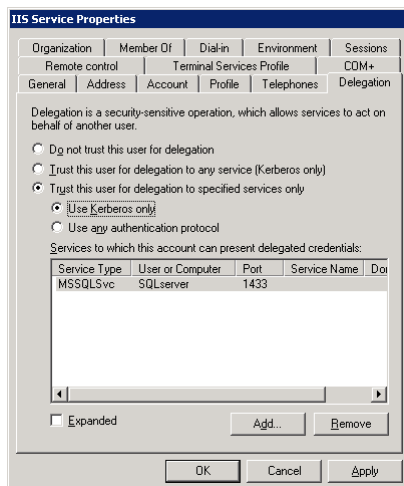
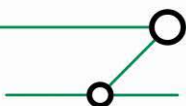


Abbildung 2: Konfiguration von „constrained delegation“.

<sup>1</sup> Windows Server 2008 bringt kleine Veränderungen unter der Haube mit sich: Für Verschlüsselung kann jetzt AES verwendet werden, Kerberos-Authentifizierung findet im Kernel Mode statt, und es gibt ein vernünftig handhabbares Kommando zum Setzen von SPNs (Service Principal Names).

<sup>2</sup> Die Autorisierungsdaten für die Zugriffsart auf die erlaubte Ressource stehen dabei in einer definierten Datenstruktur – dem „PAC“ (Privilege Access Certificate) – innerhalb des Kerberos Service Tickets. Das PAC ist Bestandteil jedes Service Tickets unabhängig davon, ob die Delegierung eingeschränkt wurde oder ob nicht.



### 3 RISIKOBETRACHTUNG DES PRIVILEGS „TRUSTED FOR DELEGATION“

#### 3.1 Bedrohungsszenarien

Es lassen sich die folgenden Bedrohungsszenarien unterscheiden:

Szenario A: Angriff auf das Konto, das Delegiert wird

Szenario B: Ausnutzung des Privilegs „Trusted for delegation“ bei nicht aktivierter „constrained delegation“

Szenario C: Angriff auf den Computer, dem das Privileg „Trusted for delegation“ zugewiesen ist

##### 3.1.1 Szenario A: Angriff auf das Konto, das delegiert wird

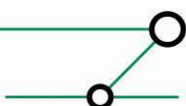
Malware oder ein Angreifer könnten versuchen, das Konto, für das Delegierung gewährt wurde, anzugreifen, um in den Besitz der Credentials für dieses Konto zu gelangen. Dieser Angriff kann auf dem Computer des Benutzers, über „Social Engineering“ des Benutzers, über einen Angriff auf einen Domänencontroller oder einen Angriff auf die Implementierung des Kerberos-Protokolls in Active Directory erfolgen. Dieses Szenario betrifft nicht nur das Konto, das delegiert werden darf, sondern grundsätzlich jeden Security Principal im Active Directory. Gleichwohl muss dieses Szenario genau dann betrachtet werden, wenn über die Vergabe des Privilegs „Trusted for delegation“ entschieden werden soll.

##### 3.1.2 Szenario B: Ausnutzen des Privilegs „Trusted for delegation“ bei nicht aktivierter „constrained delegation“

Wenn die Delegierung von Authentifizierung für ein Konto auf einem Computer mit aktiviertem Privileg „Trusted for delegation“ nicht auf definierte Ressourcen beschränkt wurde, kann ein solches Konto auf alle Ressourcen zugreifen, für die es die dazu notwendigen Zugriffsberechtigungen besitzt. Dies ist besonders dann risikobehaftet, wenn ein solches Konto etwa Mitglied der Gruppe der „Domänen-Benutzer“ ist, der per Default eine Reihe von Zugriffsberechtigungen eingeräumt wird. Dabei gilt es zu beachten: Das PAC enthält die für den Zugriff notwendigen Authorisierungsdaten, ein Benutzer erhält durch die Aktivierung des Privilegs „Trusted for delegation“ damit niemals mehr Berechtigungen als ihm über Gruppenmitgliedschaften und Verzeichniszugriffsberechtigungen von einem Administrator gewährt wurden. Gleichwohl kann der Computer, für den „Trusted for delegation“ aktiviert wurde, Kerberos-Tickets (mit den Authorisierungsdaten des Benutzers) für diesen Benutzer zum Zugriff auf beliebige Ressourcen der Domäne bei einem Domänencontroller anfordern. Das Nicht-Beschränken des Zugriffs auf Domänen-Ressourcen von einem Computer mit aktiviertem Privileg „Trusted for delegation“ kann dann ausgenutzt werden, bzw. zu einem Missbrauch führen, wenn das delegierte Konto oder der Computer mit aktiviertem Privileg kompromittiert sind.

##### 3.1.3 Szenario C: Angriff auf den Computer, dem das Privileg „Trusted for delegation“ zugewiesen ist

Malware oder ein Angreifer könnten versuchen, den Computer mit aktiviertem Privileg „Trusted for delegation“ unter ihre Kontrolle zu bekommen. Gelänge einem Angreifer oder Malware dies, dann könnten schlimmstenfalls Kerberos-Tickets für beliebige delegierte Konten beim Domänencontroller angefordert werden, *wenn* das Kerberos-Protokoll *zusätzlich* erfolgreich angegriffen würde. In einem solchen theoretischen Fall wäre eine Impersonierung eines Kontos durch ein anderes Konto denkbar, d. h. es könnte dann theoretisch ein Benutzer einen anderen Benutzer impersonieren, bzw. in dessen Namen und mit dessen Berechtigungen im Netzwerk agieren. Es sei angemerkt, dass es einen solchen erfolgreichen Angriff bisher nicht in der Kerberos-Implementierung von Active Directory gab.



## 4 MAßNAHMEN & EMPFEHLUNGEN

Die Maßnahmen lassen sich zusammenfassen zu:

### 4.1 Starke Authentifizierungsmechanismen

Durch starke Authentifizierungsmechanismen wird der erfolgreiche Angriff auf delegierte Konten erheblich erschwert. Starke Authentifizierungsmechanismen sollten in jedem Fall eine gute Passwort-Policy enthalten und könnten darüber hinaus Multifaktor-Authentifizierung und Security Awareness-Maßnahmen (etwa Schulung oder Merkblätter) umfassen.

### 4.2 Aktivierung von „constrained delegation“

Durch die Aktivierung von „constrained delegation“ für den Computer mit aktiviertem Privileg „Trusted for delegation“ wird gewährleistet, dass dieser Computer im Namen von Benutzern (mit aktivierter Delegation) nur auf die von einem Administrator definierten Ressourcen zugreifen kann.

Die Voraussetzung für die Verwendung von „constrained delegation“ ist, dass die Domäne, in der der Computer mit dem aktivierten Privileg „Trusted for delegation“ betrieben werden soll, in der Domänenfunktionsebene „Windows Server 2003“ betrieben wird. (Ein Betrieb der Gesamtstruktur mit der Gesamtstrukturfunktionsebene „Windows Server 2003“ ist dagegen nicht notwendig.)

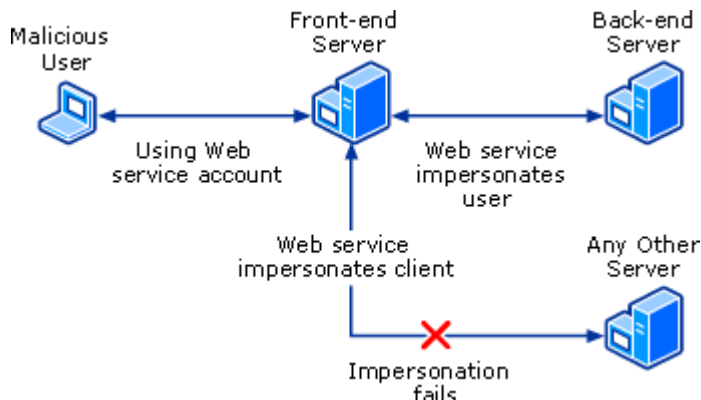


Abbildung 3: Bei aktivierter „constrained delegation“, kann ein kompromittierter Webserver (hier als Front-end Server dargestellt) Benutzer-Credentials *nicht* zum Zugriff auf anderer Ressourcen der Domäne verwenden.<sup>3</sup>

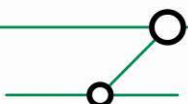
### 4.3 Besonderer Zugriffsschutz für den Computer mit aktiviertem Privileg „Trusted for delegation“

Ein Computer mit aktiviertem Privileg „Trusted for delegation“ darf sicherheitssensitive Operationen durchführen (i. e. Kerberos-Tickets für delegierte Konten bei einem Domänencontroller anfordern). Daher sollten für diesen Computer ähnlich hohe Sicherheitsanforderungen wie für einen Domänencontroller gelten. Die besonderen Sicherheitsanforderungen betreffen in erster Linie den physischen und logischen Zugriffsschutz. So sollten etwa für hochprivilegierten Konten die Benutzerrechte

- „Auf diesen Computer vom Netzwerk aus zugreifen“
- „Lokal anmelden zulassen“

deaktiviert werden, um Kerberos-Tickets solcher Konten gar nicht erst in den Besitz dieses Computer gelangen zu lassen. Außerdem sollte der Computer an einem mit einer physischen Zugangskontrolle versehenem Ort stehen. Darüber hinaus sollte für einen solchen Computer in

<sup>3</sup> Die Abbildung entstammt [4].



besonderem Maße gelten, dass auf ihm nur die notwendigen Dienste und Software installiert sind und sich der Computer auf dem aktuellen Patchstand befindet.

#### 4.4 Ausschluss von hochprivilegierten Security Principals von der Delegation

Security Principals können von der Delegation explizit ausgeschlossen werden. Ist dieses Attribut in den Kontoeigenschaften eines Security Principals gesetzt, dann kann kein anderer Security Principal Kerberos-Tickets im Namen des ersten Security Principals anfordern, d. h. ein Computer mit aktiviertem Privileg „Trusted for delegation“ kann einen solchen Security Principal nicht impersonieren. Bei einem Benutzer wird dies über eine Einstellung in dessen Kontoeigenschaften im Active Directory gewährleistet werden : „Account is sensitive and cannot be delegated“

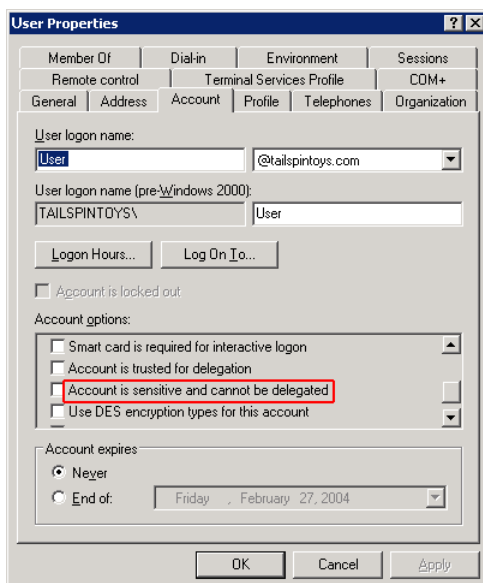


Abbildung 4: Explizites Verbot der Delegation von Credentials für ein Benutzer-Konto.<sup>4</sup>

Von der Delegation auszuschließende Konten (Security Principals) sind in jedem Fall:

- Organisations-Admins
- Schema-Admins
- Domänen-Admins

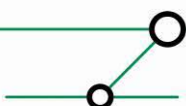
und darüber hinaus weitere hochprivilegierte Konten von Benutzern oder Diensten.

#### 4.5 Alternative Möglichkeiten

Eine begleitende Möglichkeit für eine granulare Zugriffssteuerung und Rechteverwaltung von Benutzern, die auf den SharePoint Server (mit aktiviertem Privileg „Trusted for delegation“) zugreifen sollen, soll nicht unerwähnt bleiben:

ADFS oder Active Directory Federation Services: Für Webbasiertes-SSO kann Mitarbeitern einer anderen Organisation und/mit einer eigenen/anderen Benutzerverwaltung dediziert Zugriff auf Webanwendungen (SharePoint Server 2007 ist für die Zusammenarbeit mit ADFS geeignet) gewährt werden. Dieses Szenario eignet sich dann, wenn relativ viele Benutzer einer Organisation auf Web-basierte Ressourcen einer anderen Organisation sicher zugreifen können sollen.

<sup>4</sup> Die Abbildung entstammt [4].



## 5 ZUSAMMENFASSUNG UND FAZIT

Relevante Bedrohungsszenarien für Computer mit aktiviertem Privileg „Trusted for delegation“ und delegierbaren Security Principals zielen im Wesentlichen auf zwei Dinge: Auf einen Angriff auf das Kerberos-Protokoll und – wenn dieser erfolgreich wäre – auf den Missbrauch des Privilegs „Trusted for delegation“, um auf beliebige Ressourcen der Domäne zugreifen zu können. Da zum einen das Kerberos-Protokoll an sich, zum anderen die Implementierung von Kerberos durch Microsoft in Active Directory sehr wenig Schwachstellen und keine bekannte Impersonierungslücke aufweisen, ist die missbräuchliche Ausnutzung des Privilegs „Trusted for delegation“ nach aktuellem Sicherheitsstand sehr unwahrscheinlich. Sollte es hier eine Lücke geben, dann würden die genannten Maßnahmen greifen: Durch Aktivierung der „constrained delegation“ nur für definierte Ressourcen sowie durch den Ausschluss der Delegation für hochprivilegierte Konten würde ein Zugriff auf beliebige Ressourcen der Domäne wie auch ein Zugriff durch hochprivilegierte Konten effektiv unterbunden werden. Flankierende Maßnahmen dazu betreffen den genannten besonderen Zugriffsschutz. Die weiteren genannten Maßnahmen (starke Authentifizierung und besondere Systemhärtung) entsprechen allgemeinen Security Best Practices.

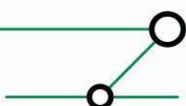
## 6 QUELLEN

[1] Dasco, Mark und Penev, Boyan: Enhanced Security and Integration of Microsoft BI Solutions with Kerberos, 27.11.2008, <http://bp-msbi.blogspot.com/2009/04/enhanced-security-and-integration-of.html>.

[2] Smith, Martin: Kerberos authentication and troubleshooting delegation issues, Review vom 05.02.2009, <http://support.microsoft.com/kb/907272/en-us>.

[3] Yermakhovo, Max: Implementing Kerberos for SharePoint running on Windows Server 2008 and IIS7, 01.08.2008, <http://blogs.objectsharp.com/cs/blogs/max/archive/2008/08/01/implementing-kerberos-in-sharepoint-running-on-windows-server-2008.aspx>.

[4] Windows Server 2003. Troubleshooting Kerberos Delegation, Microsoft Corporation, 2004, <http://www.microsoft.com/downloads/details.aspx?familyid=99b0f94f-e28a-4726-bffe-2f64ae2f59a2&displaylang=en>.



Für Fragen zu Planung und Implementierung auch zu weiteren sicherheitsrelevanten Aspekten in und um Active Directory steht Ihnen das Team von ERNW-Deutschland und ERNW-Portugal gern zur Verfügung.

Mit freundlichen Grüßen,

Friedwart Kuhn.

ERNW GmbH  
Friedwart Kuhn  
Senior Security Consultant

ERNW Enno Rey Netzwerke GmbH  
Breslauer Str. 28  
69124 Heidelberg  
Tel. +49 6221 480390  
Fax +49 6221 419008  
Mobil +49 15152411855  
Mobil (Portugal): +351 91 8763637  
[www.ernw.de](http://www.ernw.de)

