Erweiterte Sicherheit beim Anmeldeprozess

Microsoft hat im Mai 2014 ein Update zur Verbesserung des Schutzes und der Verwaltung von Anmeldeinformationen veröffentlicht. Dieses Update reduziert die Speicherung von Anmeldedaten im Speicher. Unterstützt werden mit diesem Update die Kerberos und AES Authentifizierungen. Behandelt werden die interaktiven sowie Netzwerkanmeldungen.

Wie nun bekannt sein sollte speichert Windows die Anmeldeinformationen im Arbeitsspeicher zwischen.

Die LSA (Local Security Authority) ist ein geschütztes Subsystem von Windows. Die Aufgabe besteht darin, keinen Zugriff auf Ressourcen zu erteilen, ohne dass sich ein Benutzer, ein Dienst oder ein System korrekt authentifiziert hat. Die LSA verarbeitet somit alle Aspekte der lokalen Systemsicherheit LSP (Local Security Policy) und stellt diverse Authentifizierungsdienste (Security Packages) zur Verfügung.

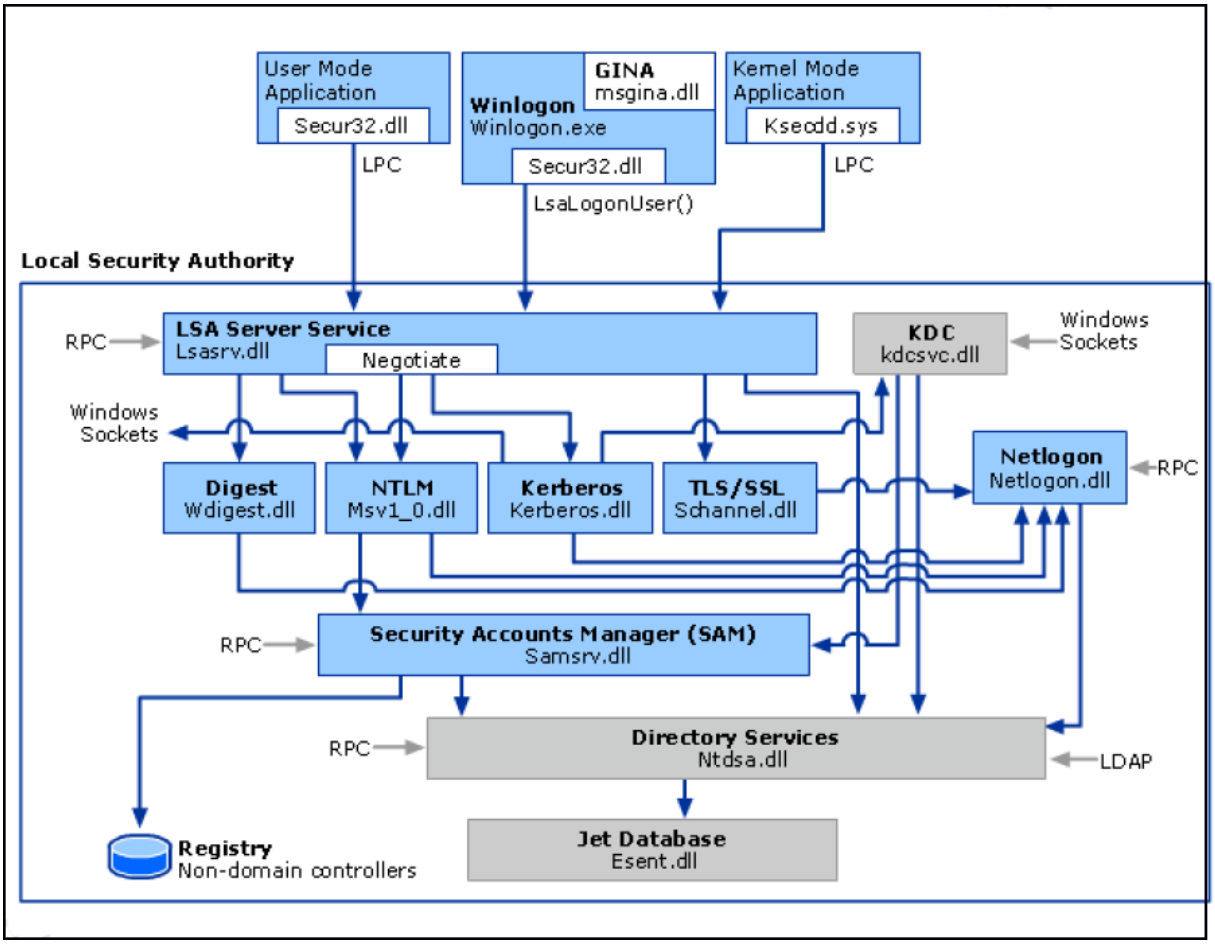
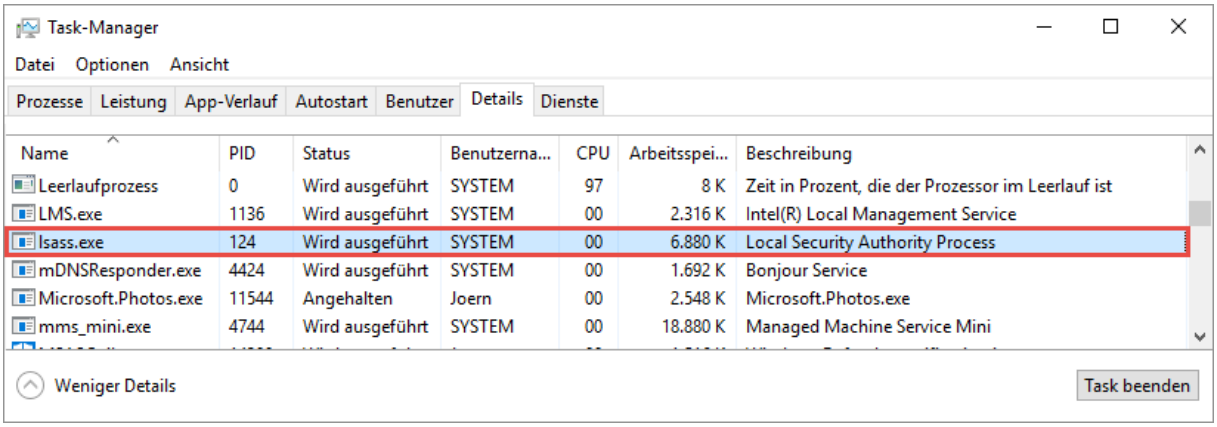
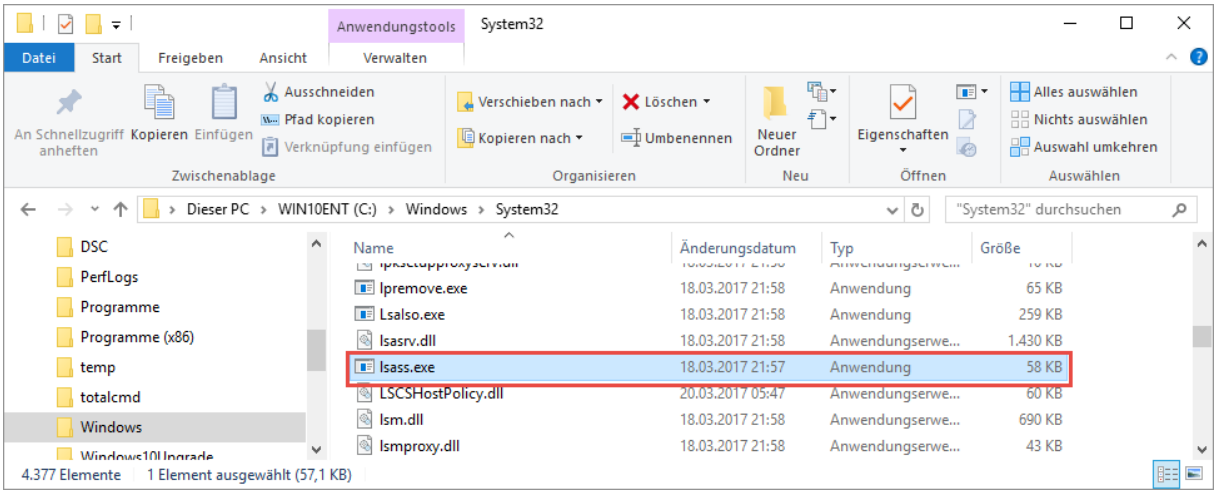


Bild: Microsoft

Nach erfolgtem Bootvorgang, noch bevor der Anmeldebildschirm erscheint wird der Local Security Authority Subsystem Process, bekannt unter dem Namen (lsass.exe) gestartet und validiert die Zugriffsrechte auf etwaige Objekte und überprüft nach der Anmeldung die Privilegien des Benutzers und generiert zeitgleich sicherheitsrelevante Protokolleinträge.

Erweiterte Sicherheit beim Anmeldeprozess

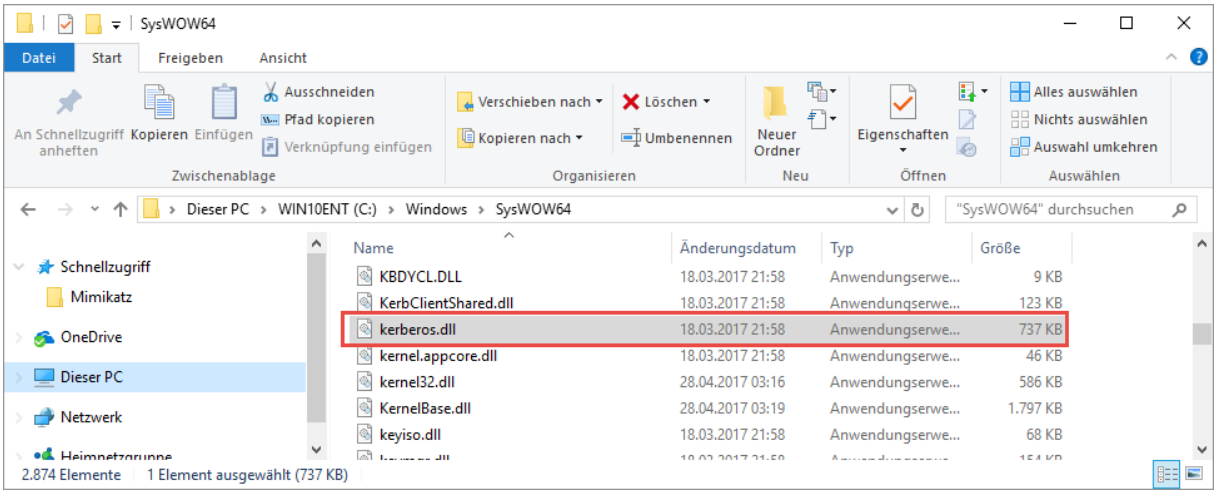




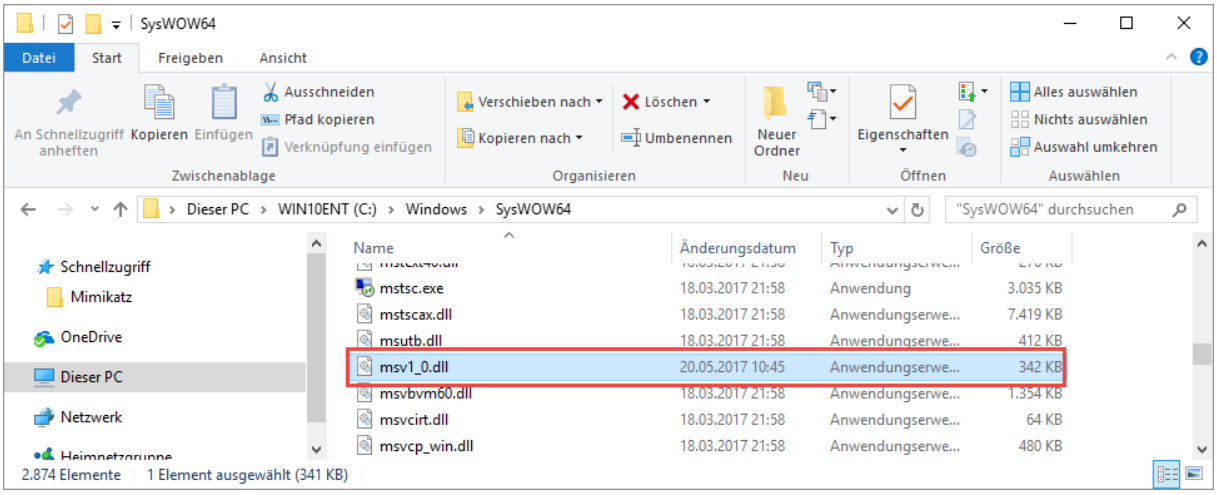
Somit kann der Benutzer nach der Anmeldung (Authentifizierung) ohne wiederholte Eingabe von Benutzername und Passwort auf bereitgestellte Dienste, Webanwendungen und z.B. Netzwerkfreigaben zugreifen.

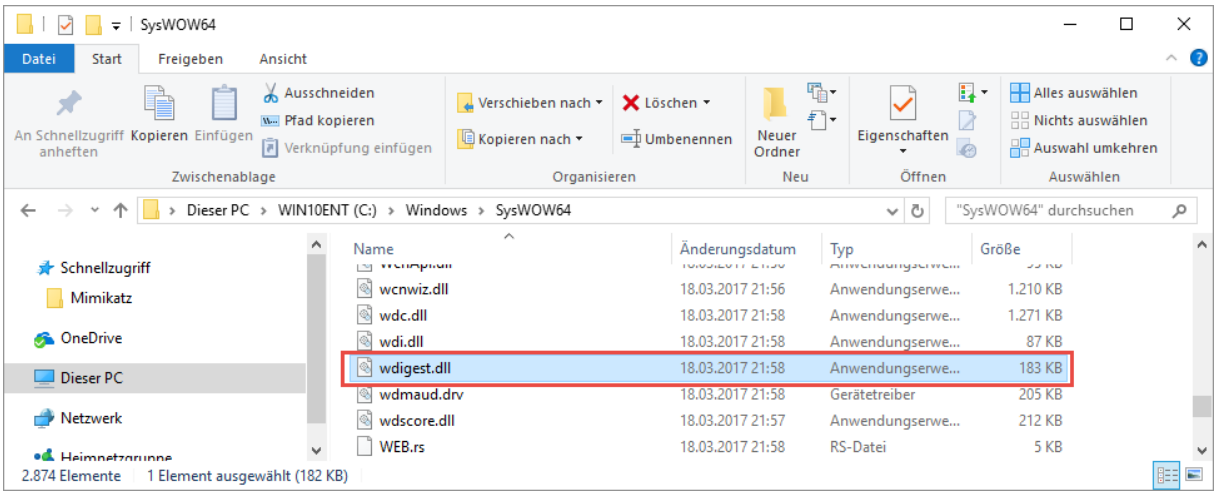
Dieses Konzept nennt sich Single-Sign-On und wird durch LSASS realisiert. Damit SSO überhaupt funktionieren kann, legt Windows das Passwort im Arbeitsspeicher des Systems ab und LSASS greift sich das Passwort dort ab.

LSASS verfügt über eine Vielzahl von Security Packages (Authentifizierungsprotokolle), wie z.B. Kerberos, NTLM TLS/SSL oder Digest Authentication.



Erweiterte Sicherheit beim Anmeldeprozess





Je nach eingesetzte Methode (Security Packages) wir erinnern uns an Kerberos, NTLM oder wDigest wird das Passwort entweder als Hash, verschlüsselt oder in Klartext in den Arbeitsspeicher geschrieben.

Diese Liste zeigt welche Security Packages die Anmeldeinformationen im Arbeitsspeicher zwischenspeichert.

	Primär			Anmeldeinformationsschlüssel				tspkg		wdigest		kerberos				livessp	ssp	dpapi	credman 6
	LM	NTLM	SHA1	NTLM	SHA1	Root	DPAPI	aus	an	aus	an	pass 1	PIN 4	tickets	eKeys				
	Windows XP/2003																		
lokales Konto								2											
Domänen Konto								2					5						
	Windows Vista/2008 & 7/2008r2																		
lokales Konto																			
Domänen-Konto																			
	Windows 8/2012																		
Microsoft Konto																			
lokales Konto																			
Domänen Konto																			
	Windows 8.1/2012R2																		
Microsoft Konto									3		3								
lokales Konto									3		3	7							
Domänen Konto									3		3								
Domänen geschützer B									3		3								

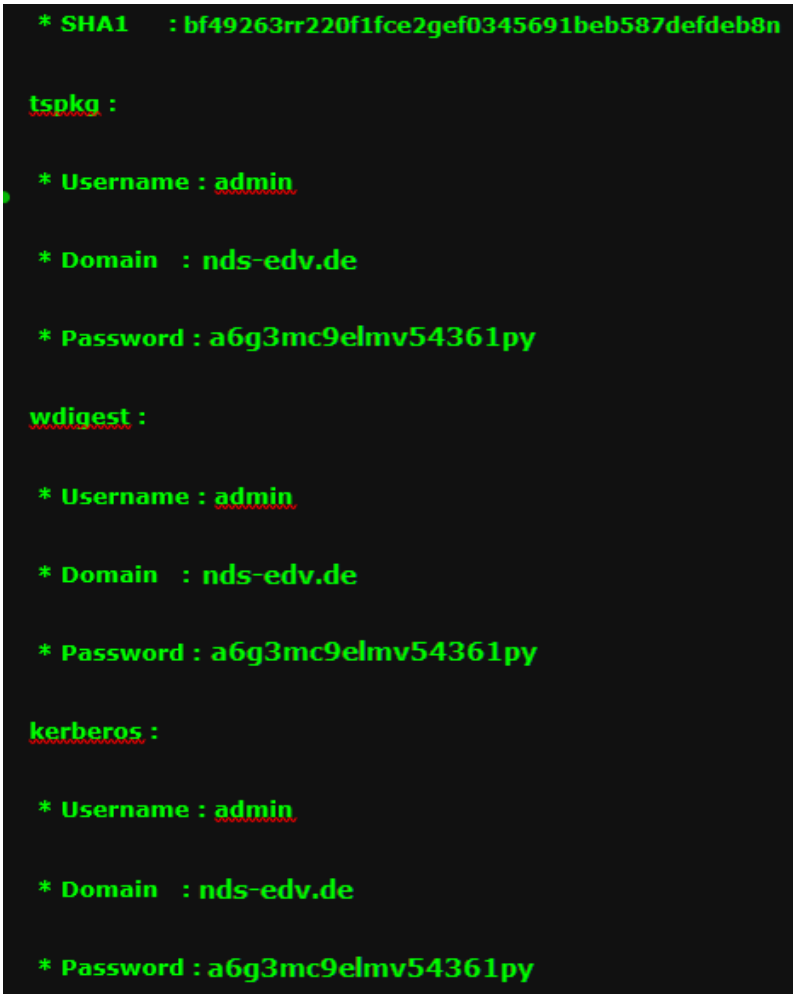
	Windows 8.1 Tresor für Authentifizierungen				
	PIN		Bild		Fingerprint
	Code	Pass	Gesten	Pass	Pass
Microsoft Account					
lokales Konto					

	nicht zutreffend
	im Speicher
	nicht im Speicher

1. Aktivieren unter NT5 und nicht verfügbar für Smartcards
2. tspkg ist kein Standard unter XP und für Server 2003 nicht verfügbar
3. tspkg is standardmäßig aus für SSO und wDigest wird es aber benötigt
   http://technet.microsoft.com/library/dn303404.aspx
4. PIN Code bei nativer Smartcard Nutzung
5. PIN code wird im Speicher nicht verschlüsselt betrifft (XP/2003)
6. Beim Zugriff eines Benutzers
7. Wenn lokaler Admin oder UAC ausgeschaltet

Wie oben beschrieben verwaltet LSASS die Anmeldeinformationen. Eine Interaktion mit diesem Prozess ist nur als lokaler Administrator möglich. Wenn ein System nun

kompromittiert wurde, mimikatz* oder wce zum Einsatz kam, dann ist es ein leichtes Spiel die Anmeldeinformationen auslesen und zu missbrauchen.



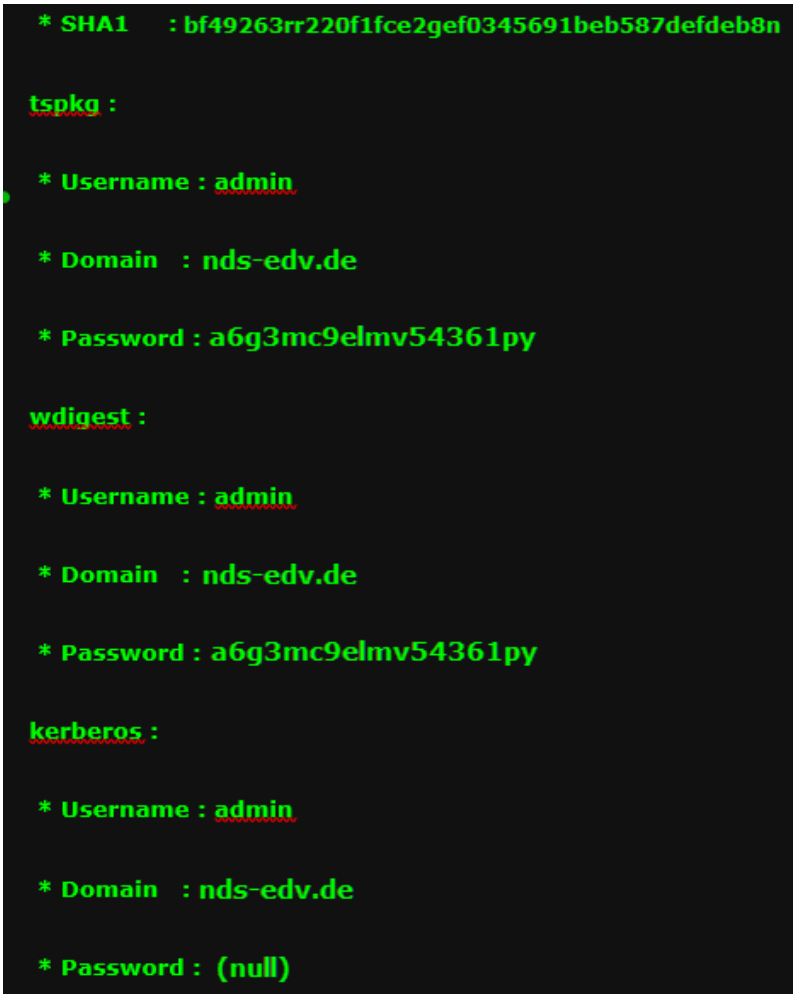
Nach Bekanntwerden hat Microsoft mit dem Security Advisory 2871997

https://technet.microsoft.com/library/security/2871997
https://support.microsoft.com/de-de/help/2871997/microsoft-security-advisory-update-to-improve-credentials-protection-and-management-may-13,-2014

als Gegenmaßnahme reagiert.

Durch Beachtung um Umsetzung des Security Advisory 2871997 wird aus dem LSASS ein geschützter Prozess. Ab diesem Zeitpunkt können nur noch signierte Anwendungen auf diesen Prozess zugreifen und SSO zur Authentifizierung einbinden. Zudem

Durch die Installation des Patches KB2871997 wurde mimikatz leider nur kurzfristig außer Gefecht gesetzt. Der Programmierer von mimikatz hat auf KB2871997 reagiert und sein Produkt entsprechend angepasst. Das Passwort konnte nun doch wieder ausgelesen werden, aber Kerberos blieb standhaft, siehe Bild.



(WCE hingegen brachte bei allen Security Packages nur noch ein NULL Passwort hervor. Der Patch KB2871997* hatte zumindest bei dem Tool WCE eine positive Auswirkung.)

Das Security Package wDigest bleibt weiterhin unsicher und legt das Passwort immer noch in Klartext in den Arbeitsspeicher ab (technisch nicht anders möglich) und kann mithilfe von mimikatz weiterhin ausgelesen werden.

Erweiterte Sicherheit beim Anmeldeprozess

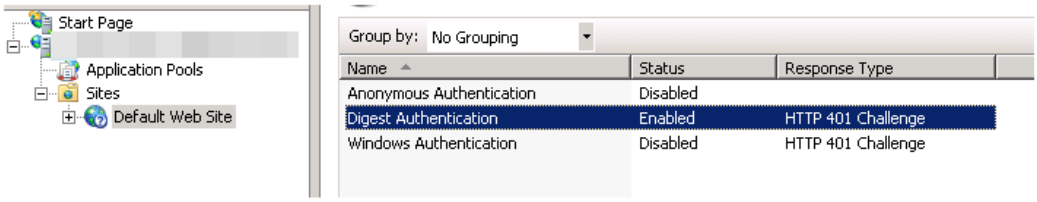
Erfahrungen:

Folgende Fehlermeldung könnten nach der Entfernung z.B. bei der Nutzung von RDP, IIS auftreten. Abhängig von den eingesetzten OS Versionen.

Authentication Error: "The requested security package does not exist"

Standards die wir vorfinden:

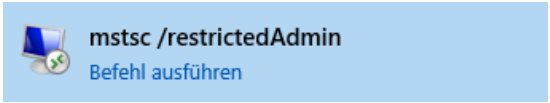
Beim IIS ist die Authentifizierungsmethode wdigest bis Windows Server 2008 R2 standardmäßig aktiviert. Also muss geprüft werden ob dieser genutzt bzw. eingesetzt wird.



Erläuterungen:

*mimikatz liest das Passwort nicht nur aus dem Arbeitsspeicher aus, es ist auch in der Lage das Passwort aus dem Security Account Manager (SAM) zu extrahieren.

*Der Patch KB2984972 bringt beim Einsatz von RDP noch zusätzlich den Schalter RestrictedAdmin mit. Dieser Modus gilt nur für User die auf dem System lokaler Admin sind. Diese Funktion verhindert das auf dem angemeldeten Remote-System das Passwort zwischengespeichert wird. Das bedeutet, dass kein SSO verfügbar ist und somit auch auf keine Freigabe zugegriffen werden kann. Verfügbar ab Windows 7 oder höher.



Am 14. Oktober 2014 veröffentlichte Microsoft die folgenden Updates, um einen eingeschränkten Administratormodus für Remotedesktopverbindung und Remotedesktopprotokoll hinzuzufügen:

2984972 für unterstützte Editionen von Windows 7 und Windows Server 2008 R2

2984976 für unterstützte Editionen von Windows 7 und Windows Server 2008 R2 mit installiertem Update 2592687 (Remote Desktop Protocol 8.0-Update). Kunden, die das Update 2984976 installieren, müssen auch folgendes Update installieren: 2984972 .

2984981 für unterstützte Editionen von Windows 7 und Windows Server 2008 R2 mit installiertem Update 2830477 (Remote Desktop Connection 8.1-Clientupdate). Kunden, die das Update 2984981 installieren, müssen auch folgendes Update installieren: 2984972 .

2973501 für unterstützte Editionen von Windows 8, Windows Server 2012 und Windows RT.

Hinweis Unterstützte Editionen von Windows 8.1, Windows Server 2012 R2 und Windows RT 8.1 enthalten dieses Feature bereits, sodass dies Update hier nicht erforderlich ist.

Am 9. September 2014 veröffentlichte Microsoft Folgendes:

2982378 Microsoft-Sicherheitsempfehlung: Update zur Verbesserung des Schutzes von Anmeldeinformationen und der Verwaltung für Windows 7 und Windows Server 2008 R2: 9. September 2014

Am 8. Juli 2014 veröffentlichte Microsoft Folgendes:

2973351 Microsoft-Sicherheitsempfehlung: Registrierungsupdate zur Verbesserung des Schutzes von Anmeldeinformationen und der Verwaltung von Windows-Systemen, auf denen das Update 2919355 installiert ist: 8. Juli 2014

2975625 Microsoft-Sicherheitsempfehlung: Registrierungsupdate zur Verbesserung des Schutzes von Anmeldeinformationen und der Verwaltung von Windows-Systemen, auf denen das Update 2919355 nicht installiert ist: 8. Juli 2014

Dieses Update enthält konfigurierbare Registrierungseinstellungen für die Verwaltung des eingeschränkten Administratormodus für CredSSP (Credential Security Support Provider).

Hinweis Dieses Update ändert die Funktionalität des eingeschränkten Administratormodus in Windows 8.1, Windows Server 2012 R2 und Windows RT 8.1. Weitere Informationen finden Sie im Abschnitt „Häufig gestellte Fragen" der Empfehlung. Die folgenden Dateien stehen im Microsoft Download Center zum Download zur Verfügung:

Erstellt von Jörn Walter **18.05.2014/23.07.2017**

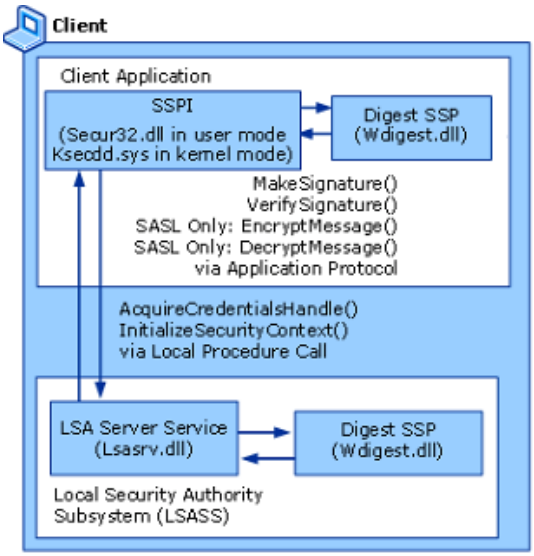
Erweiterte Sicherheit beim Anmeldeprozess

Security Support Provider:

Kerberos zu verstehen als Industriestandard, ist ein Mechanismus für die gegenseitige Authentifizierung zwischen zwei Parteien, wie z.B. Client > Server, Server > Server. Die standardmäßigen Kerberos Implementierungen erfordern ein Active Directory.

NTLM, NT LAN Manager gibt es seit der ersten Windows Netzwerk Unterstützung. NTLM gibt es in der Version 1 und 2, wobei der Authentifizierungsprozess der gleiche ist. Der Unterschied liegt in der Dichte der Verschlüsselung. Der hier eingesetzte Mechanismus basiert auf dem Challenge-Response-Mechanismus. Hier muss bewiesen werden das jemand (Benutzer/Server) auch er/es ist für den er/es sich ausgibt.

Die Digest-Authentifizierung ist wie soll ich sagen ein branchenübergreifendes Authentifizierungsprotokoll und wird vom LDAP (Lightweight Directory Access Protocol) und für die Web-Authentifizierung benutzt.



TLS/SSL ist ein standarisiertes Internet Authentifizierungsprotokoll und wird zum Verschlüsseln von Nachrichten eingesetzt. Die Authentifizierung funktioniert im Client-Server-Mode. Die Kryptografie basiert auf einem öffentlichen Schlüssel (public key cryptography).

Ein Digest:

Ein Digest ist ein Extrakt aus binären Daten basierend auf einen Algorithmus. Zum Einsatz kommt MD5 und SHA. MD5 erzeugt einen ein 128 Bit bzw. 16 Byte langes Muster. SHA erzeugt aus dem Datum ein 160 Bit bzw. 20 Byte langes Muster. Das Resultat ist eine Einweg Funktion und nicht umkehrbar.

Die Digest Authentication besteht im Wesentlichen darin, das Client und Server zweimal eines Digest mit Hilfe eines Passworts berechnen. Der Client macht das mit dem vom Benutzer eingegebenen Passwort und sendet diesen Digest mit dem Benutzernamen an den Server. Der Server kann das Passwort nicht errechnen, weil ein Digest nicht umkehrbar ist, aus diesem Grund ermittelt der Server mithilfe des Benutzernamen das Passwort aus der Datenbank. Der Server errechnet aus dem Passwort ein Digest und vergleicht dieses mit dem vom Client übertragenden Digest. Sind diese gleich ist der Authentifizierungsvorgang abgeschlossen.

Erweiterte Sicherheit beim Anmeldeprozess

Weiterführende Informationen:

https://msdn.microsoft.com/en-us/library/windows/desktop/ms721625(v=vs.85).aspx#_security_security_package_gly

https://msdn.microsoft.com/de-de/library/windows/desktop/aa379392(v=vs.85).aspx

https://msdn.microsoft.com/en-us/library/aa375200(VS.85).aspx

https://support.microsoft.com/de-de/help/2871997/microsoft-security-advisory-update-to-improve-credentials-protection-and-management-may-13,-2014

https://support.microsoft.com/de-de/help/3126593/ms16-014-description-of-the-security-update-for-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-server-2012,-windows-8.1,-and-windows-server-2012-r2-february-9,-2016

Erstellt von Jörn Walter **18.05.2014/23.07.2017**

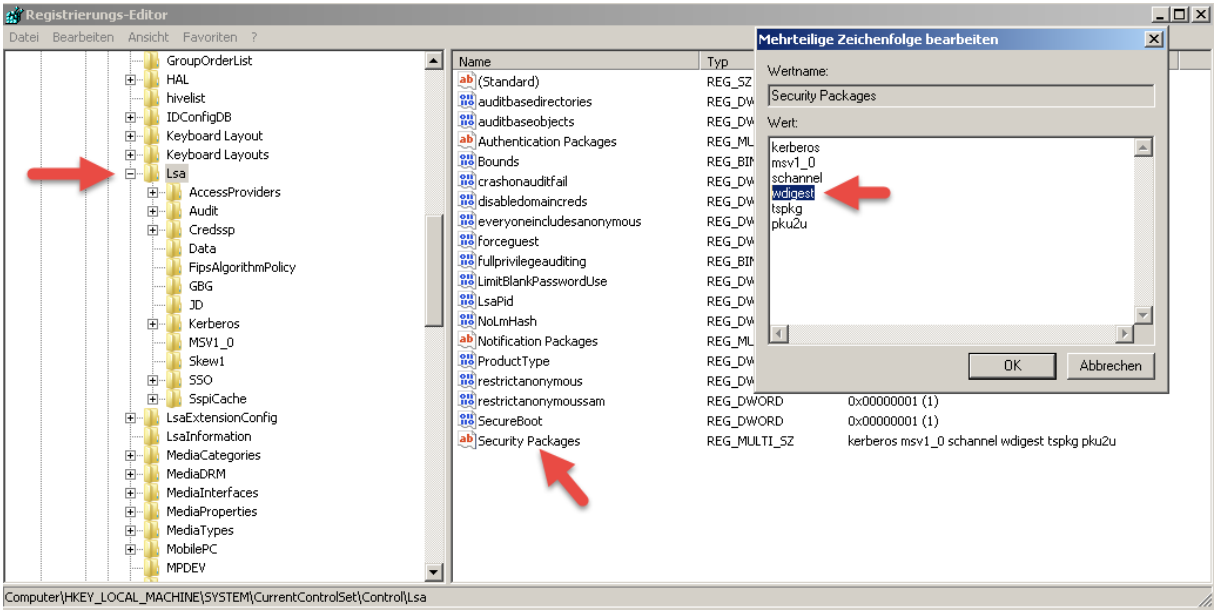
Erweiterte Sicherheit beim Anmeldeprozess

Meine Empfehlung, die Entfernung des Protokolls:

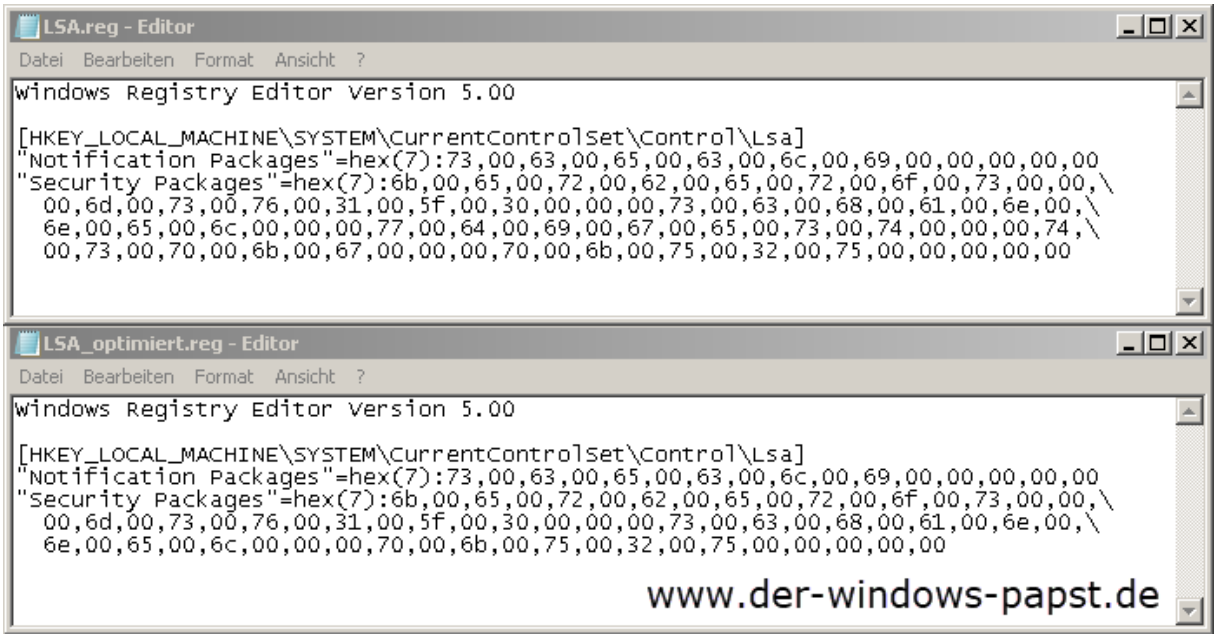
Die Digest Authentication wurde mit Windows XP eingeführt und wird von dem Hypertext Transfer Protokoll (http) und gern vom IIS verwendet. Das Security Package wDigest ist bis Windows 8 standardmäßig aktiviert und erst ab Windows 8.1 bis Server 2016 standardmäßig wieder deaktiviert.

Die Deaktivierung für Windows 7/8/2008R2/2012 erfolgt über die Registry. Falls das Package wdigest und TSpkg (Web Service Security Package) nicht mehr benötigt wird sollte es unter

HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages entfernt werden:



LSA_Security Packages_optimiert:



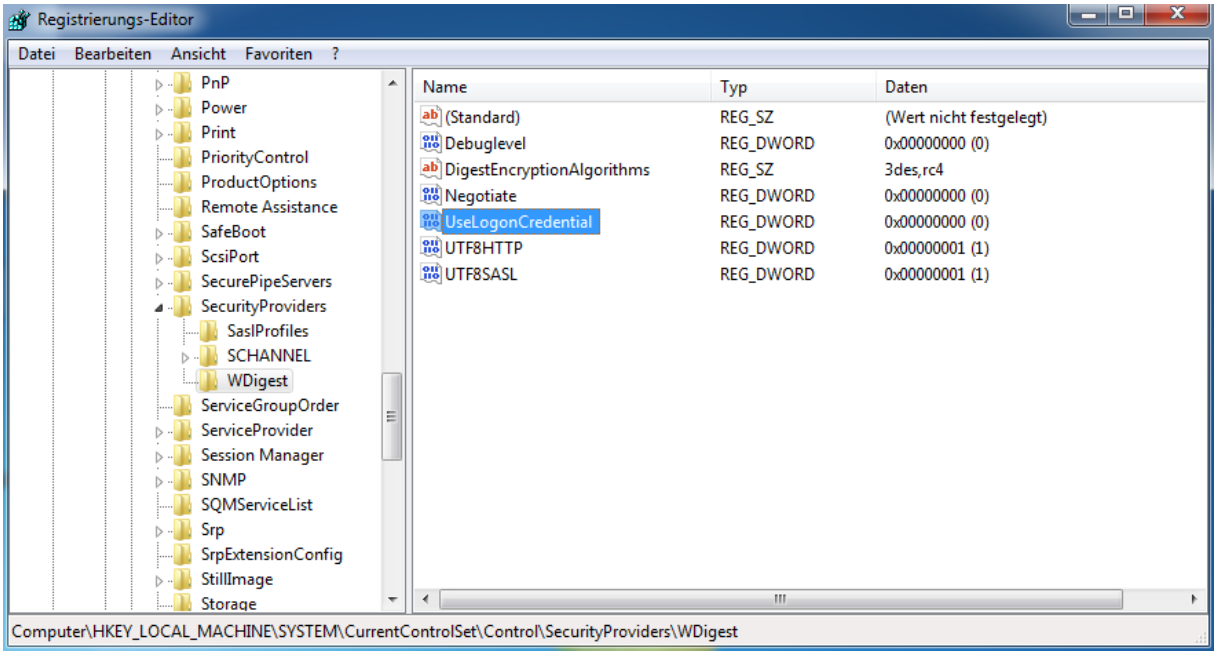
Erweiterte Sicherheit beim Anmeldeprozess

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
"Security Packages"=hex(7):6b,00,65,00,72,00,62,00,65,00,72,00,6f,00,73,00,00,\
00,6d,00,73,00,76,00,31,00,5f,00,30,00,00,00,73,00,63,00,68,00,61,00,6e,00,\
6e,00,65,00,6c,00,00,00,74,00,73,00,70,00,6b,00,67,00,00,00,70,00,6b,00,75,\
00,32,00,75,00,00,00,00,00
```

Nachdem das Package entfernt wurde konnte auch mit mimikatz das Passwort nicht mehr ausgelesen werden.

Zusätzlich sollte dieser REG-KEY ausgerollt bzw. wenn bereits geschehen, dann den DWORD-Wert UseLogonCredential auf = **0** setzen und den TokenLeakDetectDelaySecs Eintrag neu anlegen. TokenLeakDetectDelaySecs = **30** sagt aus, das 30 Sekunden nach der Abmeldung die Anmeldeinformationen gelöscht werden. Das entspricht dem Standardverhalten von Windows 8 und Windows 10.

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest]
"UseLogonCredential"=dword:00000000
"TokenLeakDetectDelaySecs"=dword:00000030
```



Erweiterte Sicherheit beim Anmeldeprozess

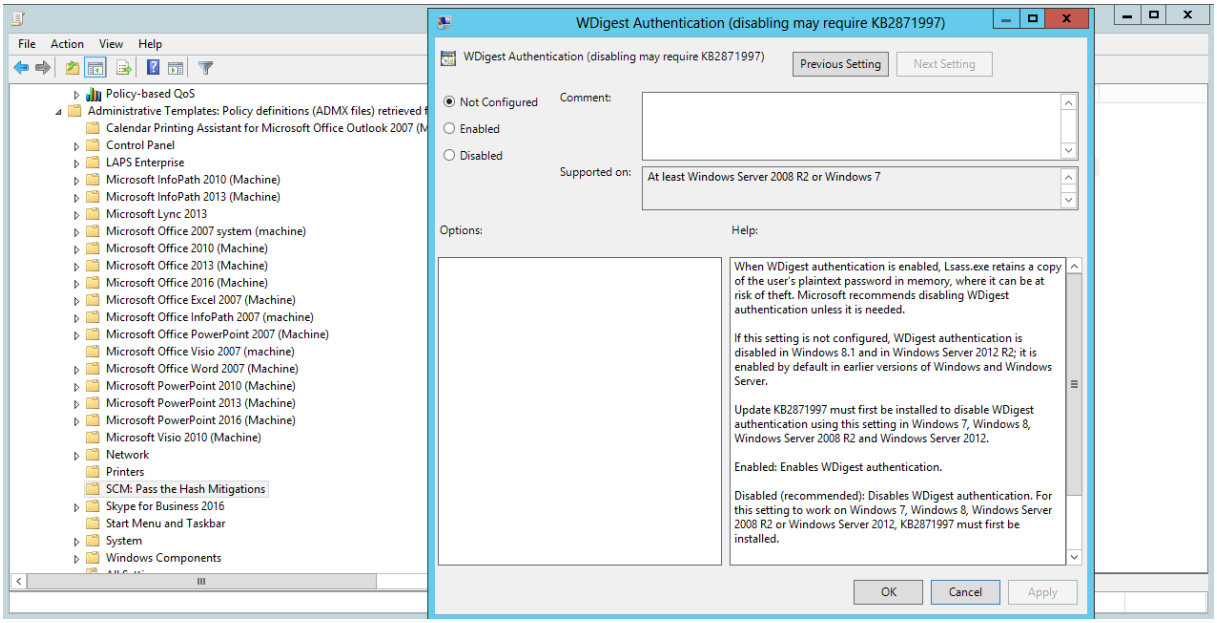
Was ist Zusammengefasst nun zu tun?

Es muss sichergestellt werden, dass die aufgeführten Patche für die Aktvierung von TokenLeakDetectDelaySecs und UseLogonCredential ausgerollt sind:

- KB3126593 Win7/2008R2/2012/2012R2 = TokenLeakDetectDelaySecs
- KB3126593 abgelöst durch KB3126587
- KB2871997 Win7/Win8/2008R2/2012 = UseLogonCredential

Um den Schalter UseLogonCredential per GPO zu verteilen und anzuwenden, muss ein neues GPO erstellt und auf die entsprechenden OUs verlinkt werden.

Achtung: Die Umsetzung ist nicht rückkehrbar!



Manuell abfragen:

REG QUERY "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest" /v "UseLogonCredential"

Manuell setzen:

REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest" /f /v "UseLogonCredential" /t REG_DWORD /d 0x0

Powershell setzen:

New-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest -Name UseLogonCredential -Type DWORD –Value 0

Erstellt von Jörn Walter **18.05.2014/23.07.2017**

Erweiterte Sicherheit beim Anmeldeprozess

Für die Aktivierung des eingeschränkten Administratormodus (Restricted Admin) muss diese Tabelle beachtet werden.

KB-Nummer des Sicherheitsupdates	Betriebssystem
2973351	Windows 8.1- und Windows Server 2012 R2-Systeme, auf denen Update 2919355 installiert wurde
2975625	Windows 8.1- und Windows Server 2012 R2-Systeme, auf denen Update 2919355 nicht installiert wurde
2973501	Windows 8, Windows Server 2012 und Windows RT
2871997	Windows 7, Windows Server 2008 R2, Windows 8 und Windows Server 2012
2973351	Windows 7, Windows Server 2008 R2, Windows 8 und Windows Server 2012
2982378	Windows 7 und Windows Server 2008 R2
2984972	Windows 7 und Windows Server 2008 R2
2984976	Windows 7 und Windows Server 2008 R2 mit installiertem Update 2592687. 2984972 muss ebenfalls installiert sein.
2984981	Windows 7 und Windows Server 2008 R2 mit installiertem Update 2830477. 2984972 muss ebenfalls installiert sein.

Alternative zu WDIGEST:

Es kommt die Security Group Protected Users zum Einsatz. Mitglieder dieser Gruppe können sich dann nur noch über Kerberos authentifizieren. Die Methoden über NTLM, Digest Authentication oder CredSSP bleiben außen vor.

Bei der ausschließlichen Nutzung des Kerberos Protokolls muss sichergestellt werden, das AES Cipher Suites unterstützt werden, weil DES oder RC4 von Kerberos nicht unterstützt werden.

Nachteil bei der Nutzung ist, das keine Constrained oder Unconstrained Delegation mehr möglich sind.

Kerberos Sicherheit:

Seit Windows 7 arbeitet Kerberos nicht mehr mit DES sondern nur noch mit AES und RC4. Alle Anfragen und Antworten (TGT als auch Session Keys) werden mit den zuletzt genannten Verschlüsselungsstufen verarbeitet.

Fallback:

Computer Configuration\ Windows Settings\ Security Settings\ Local Policies\ Security Options “Network security: Configure encryption types allowed for Kerberos”

Erstellt von Jörn Walter **18.05.2014/23.07.2017**

Erweiterte Sicherheit beim Anmeldeprozess

Zur Härtung einer RDP Sitzung sollte folgender Registry-Key erstellt werden:

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
"DisableRestrictedAdmin"=dword:00000000

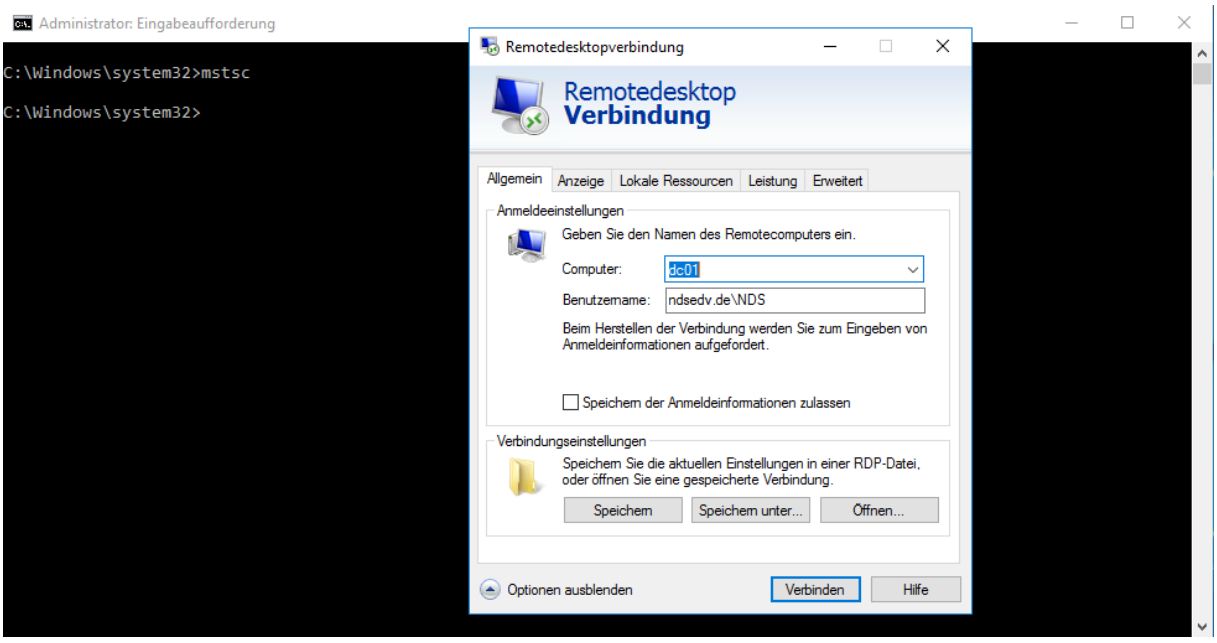
reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v DisableRestrictedAdmin /d 0 /t REG_DWORD

Dieser Key sorgt dafür, dass bei einer Remoteanmeldung an einen Server, die Anmeldeinformationen nicht weitergereicht werden um z.B. auf ein File-Share zuzugreifen oder andere Ressourcen.

Ein kleines Beispiel wie es sich mit dem mstsc /restrictedadmin verhält.

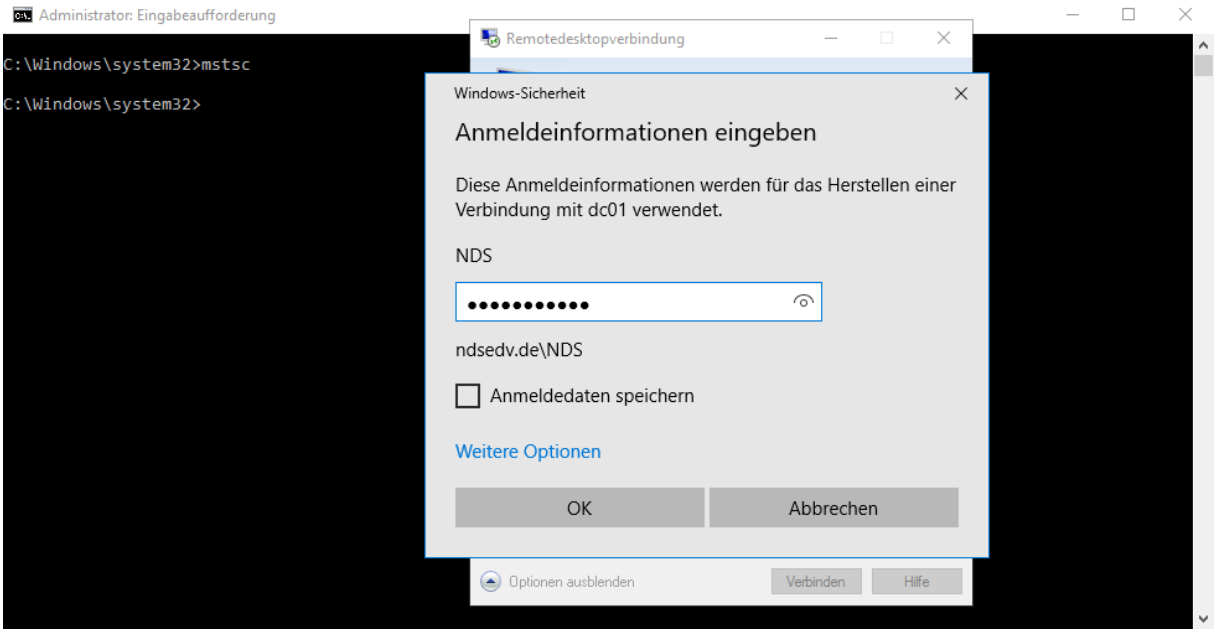
Ich stelle jetzt eine RDP Sitzung von dem Server rootCA zum DC01 her und von dort aus versuche ich das Laufwerk issuingca\c$ zu öffnen. Der User mit dem ich das teste ist Domänen-Admin und hat auf allen Maschinen volle Rechte.

Im Moment habe ich die Option restrictedadmin nur auf dem DC01 aktiviert, der jetzt als Jumphost fungiert, auf sonst keiner anderen Maschine, der Zugriff sollte mit nur mstsc funktionieren.

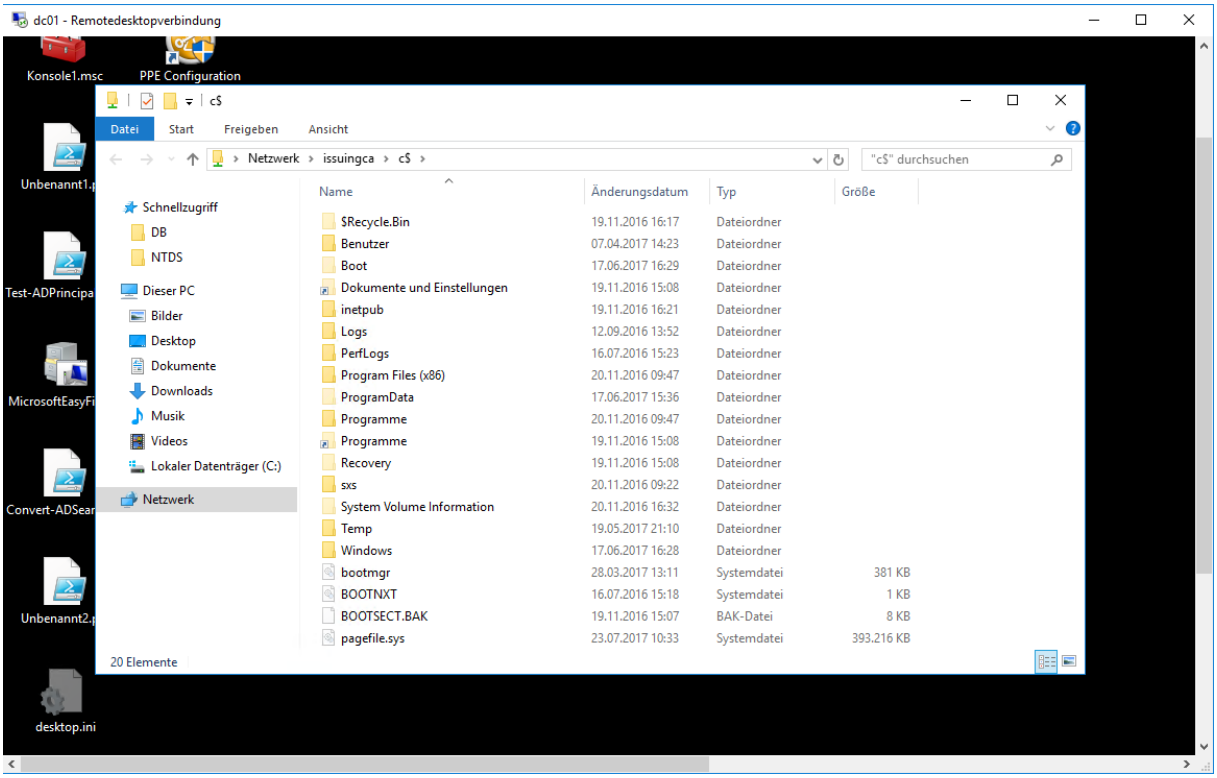


Erweiterte Sicherheit beim Anmeldeprozess

Gebe meine Anmeldeinformationen ein:

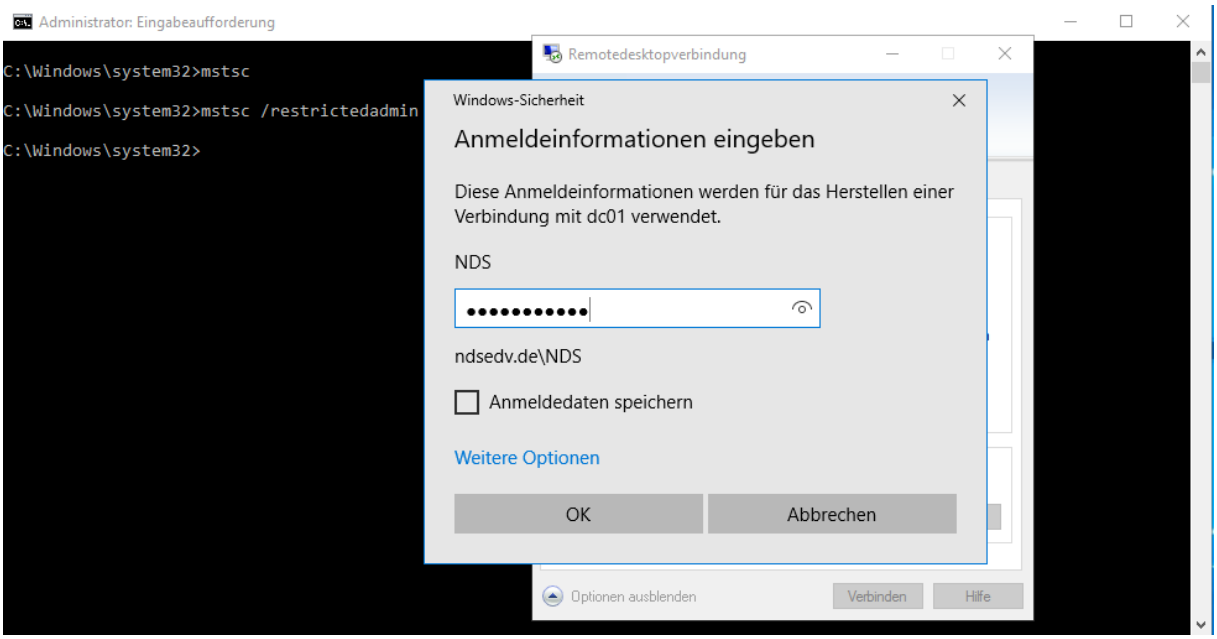


Korrekt, meine Anmeldeinformationen werden vom Server DC01 zum Server IssuingCA durchgereicht (SSO). Der Zugriff auf die Ressource ist gegeben.



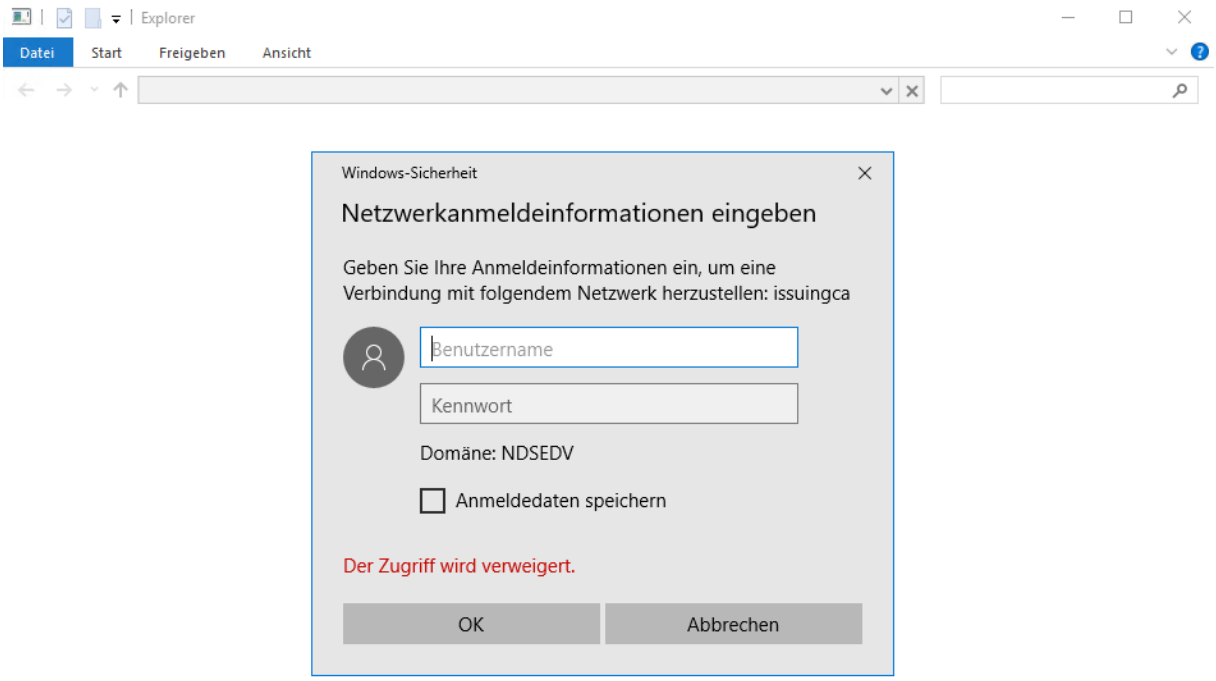
Erweiterte Sicherheit beim Anmeldeprozess

Stelle die gleiche Verbindungsreihenfolge wieder her. Jetzt nutze ich den Optionsschalter /restrictedAdmin. Der Zugriff auf die Ressource C$ des Servers IssuingCA sollte jetzt vom Server DC01 geblockt werden.



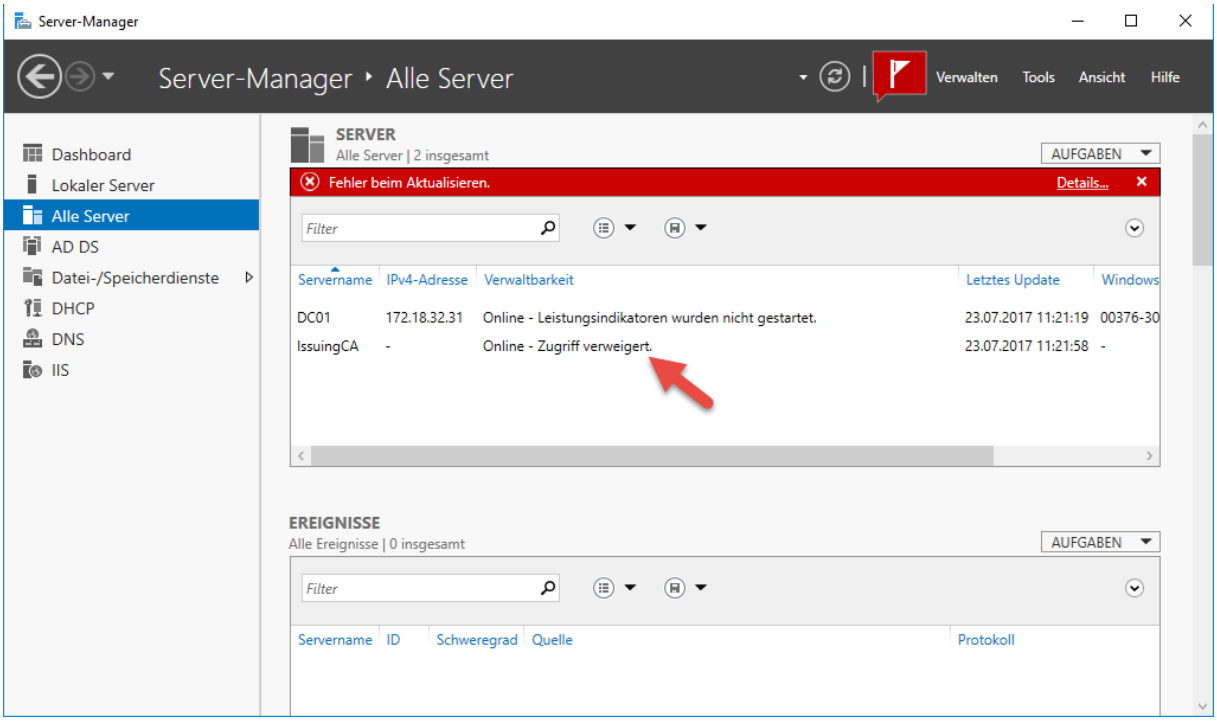
Korrekt, der Server DC01 nutzt jetzt nicht mehr die ihm bekannten Anmeldeinformationen zur Authentifizierung an die Ressource C$ des Servers IssuingCA, sondern versucht es aus dem Maschinenkontext heraus, und deshalb erscheint die Meldung „Der Zugriff wird verweigert".

Eine erneute Benutzer-Authentifizierung ist erforderlich!



Erweiterte Sicherheit beim Anmeldeprozess

Auch das Hinzufügen des Servers IssuingCA auf dem Server DC01 (Server-Manager) funktioniert somit nicht mehr.



Jetzt sollte noch folgendes erwähnt werden. Wir haben gesehen, das die Anmeldedaten des Benutzers zur Authentifizierung nicht weitergereicht werden, sobald der Optionsschalter /restricedadmin eingesetzt wird. Aber was ist, wenn der Server DC01 lokale Admin-Rechte auf dem Server IssuingCA besitzt?

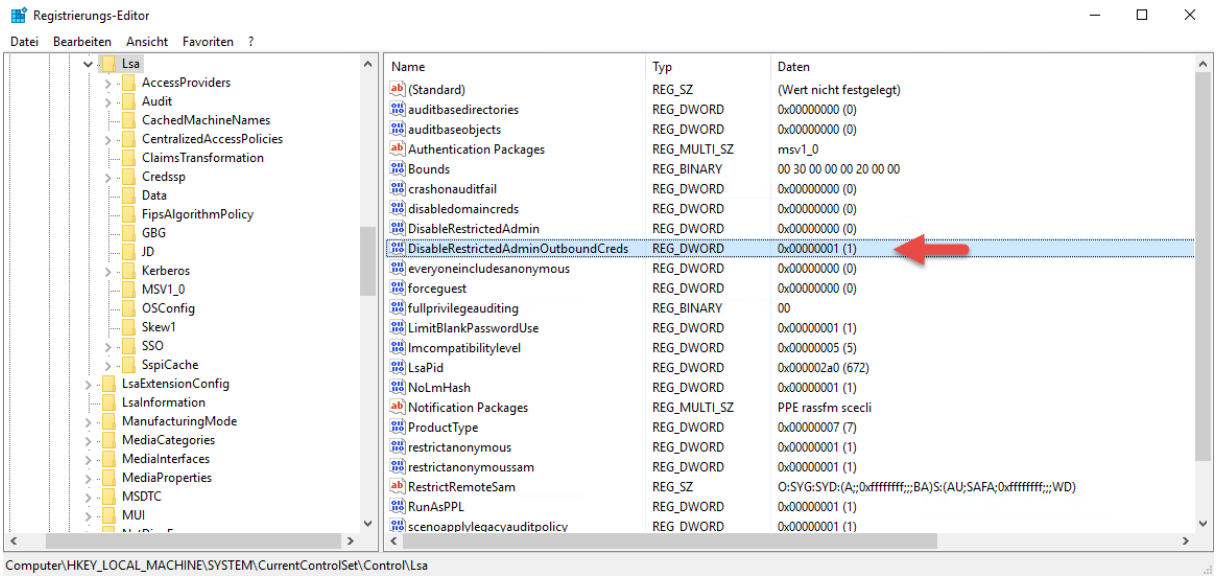
Richtig, dann bekommt der User doch wieder Zugriff auf die Ressource C$ des Servers IssungCA, weil der Zugriff im Fallbackmode im Maschinenkontext versucht wird. Siehe Bild auf der vorherigen Seite.

Auch das sollte unterbunden werden. Aber Achtung, damit schaltet man auch gewollte Delegierungen ab!

Erweiterte Sicherheit beim Anmeldeprozess

Und so geht’s:

Ich erstelle auf dem Server DC01 einen weiteren Eintrag:

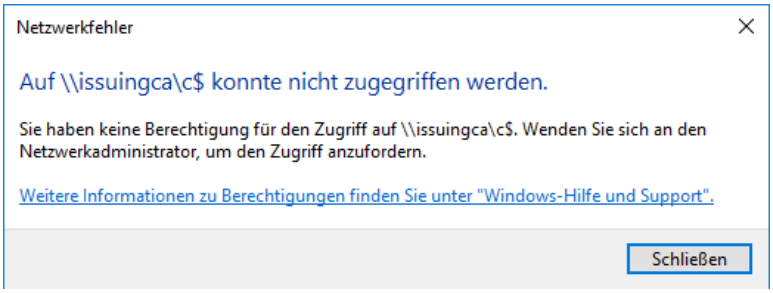


Dieser Eintrag verhindert die Authentifizierung im Kontext des Servers DC01.

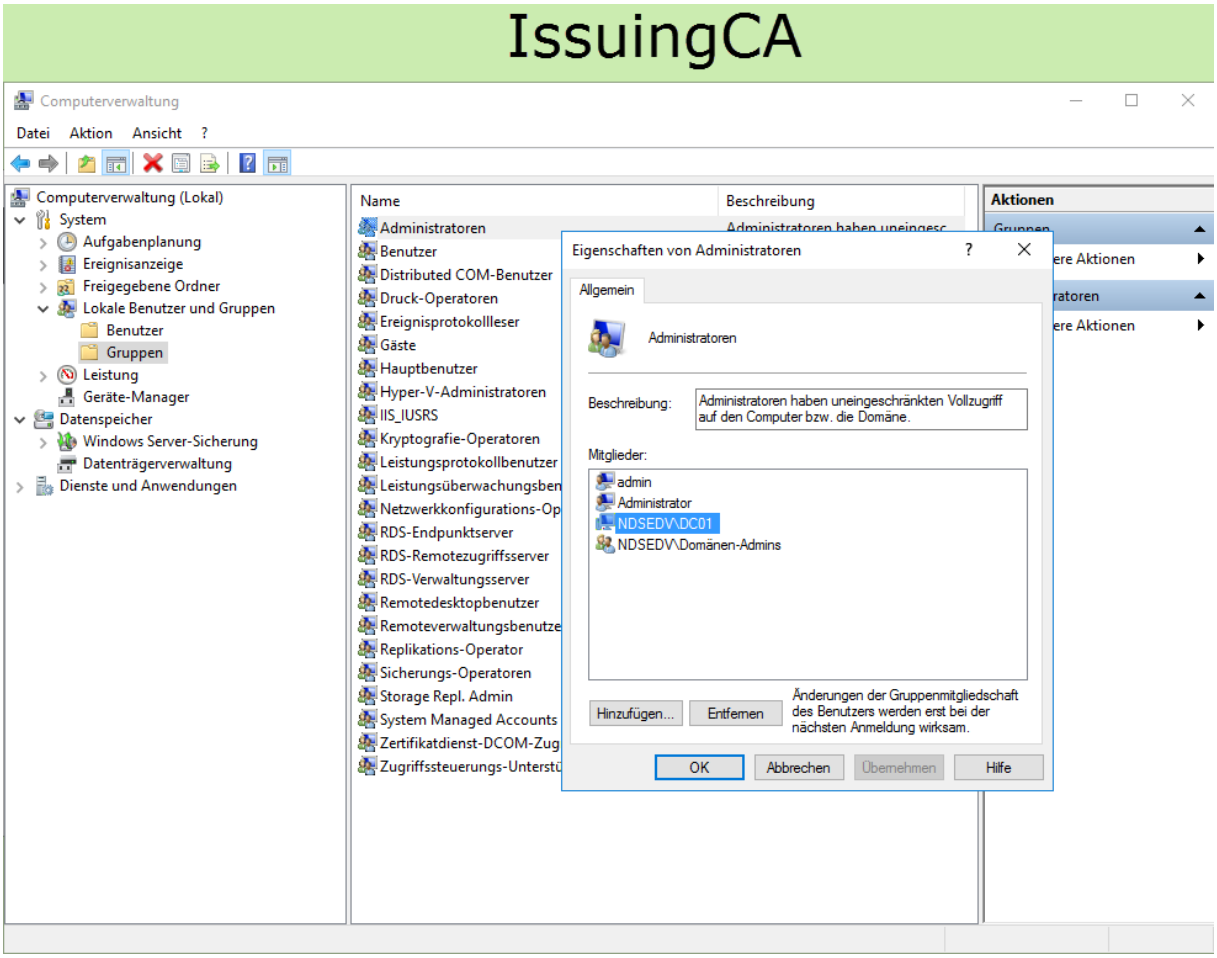
```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
"DisableRestrictedAdmin"=dword:00000000
"DisableRestrictedAdminOutboundCreds"=dword:00000001
```

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v
DisableRestrictedAdminOutboundCreds /d 1 /t REG_DWORD
```

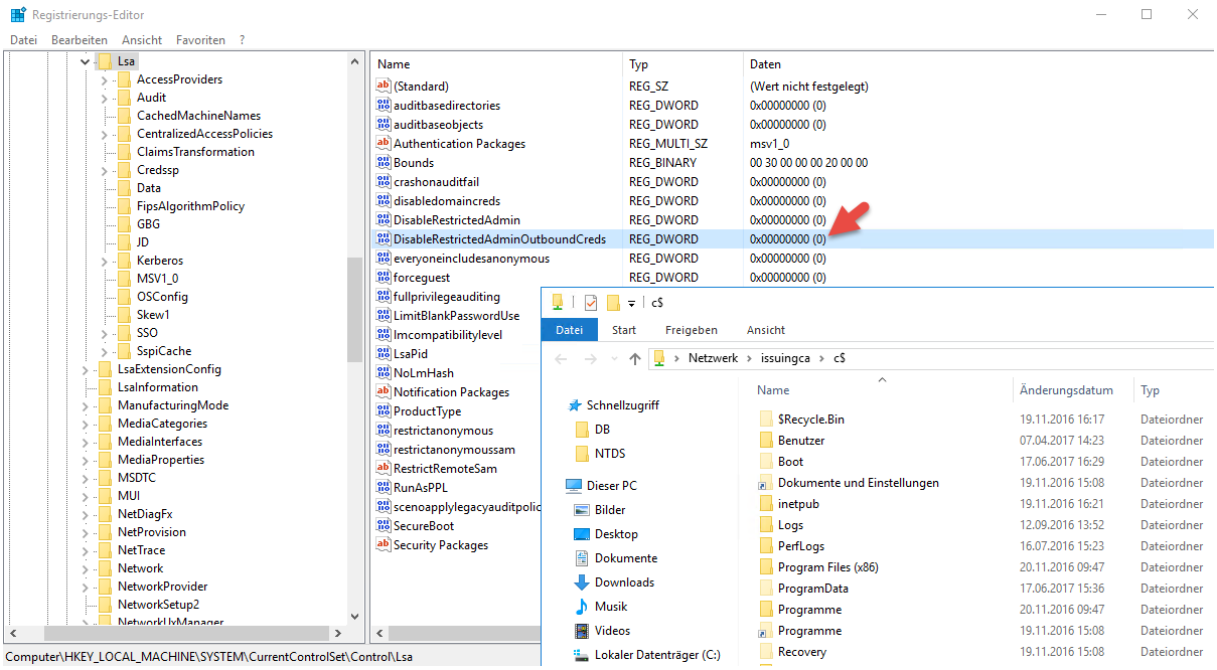
Folgende Meldung erscheint obwohl der Server DC01 lokale Admin-Rechte besitzt.



Erweiterte Sicherheit beim Anmeldeprozess



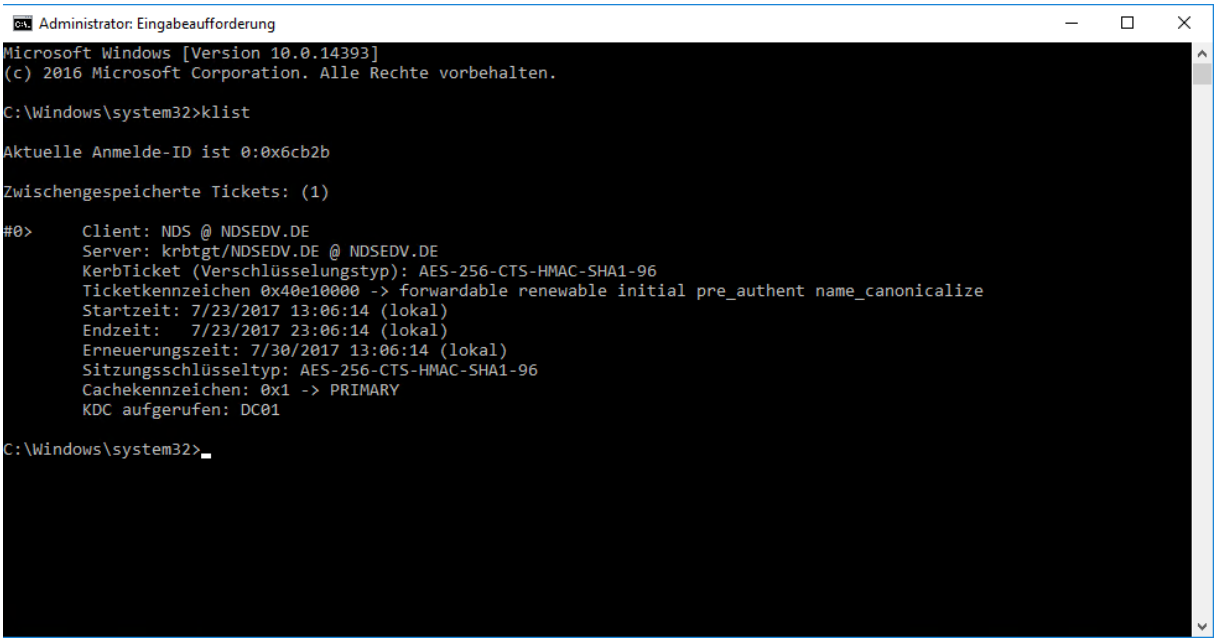
Setze ich den Wert = 0 ist die Funktion deaktiviert und der Zugriff funktioniert auch wieder im Kontext der Maschine.



Erweiterte Sicherheit beim Anmeldeprozess

An diesem Beispiel können wir es noch einmal ganz klar erkennen, wann die Anmeldeinformationen zwischengespeichert werden und wann nicht:

MSTSC:



MSTSC /RESTRICTEDADMIN: