

HCL Domino

Certificates Key Rollover

Ein detaillierter Leitfaden für Domino Administratoren

Autor Manfred Dillmann

Inhaltsverzeichnis

1. Einführung	4
1.1. Motivation	5
1.2. Rechtliche Hinweise	
2. Begriffe und der Status Quo	7
2.1. Begriffe und Abkürzungen	8
2.2. Überprüfung der Zertifikate auf der Ebene: Organisation	
2.2.1. Im Domino Directory	
2.2.2. Durch die Zertifizierer-ID	
2.3. Überprüfung der Zertifikate auf der Ebene: Abteilung	13
2.3.1. Im Domino Directory	
2.3.2. Durch die Zertifizierer-ID	
2.4. Überprüfung der Zertifikate eines Domino Servers	
2.4.1. Im Domino Directory	
2.4.2. Durch die Server-ID	
2.5. Überprüfung der Zertifikate eines Notes Anwenders	
2.5.1. Im Domino Directory	
2.5.2. Durch die User-ID	18
3. Key Rollover Einführung	21
3.1. Voraussetzungen	
3.2. Was gibt es nach einem Key Rollover zu beachten?	
3.2.1. Agenten	24
3.2.2. Execution Contro Lists (ECL's)	
3.2.3. Gegenzertifikate	
3.2.4. Policies	
3.2.5. Templates	
4. Key Rollover der Organisation (O)	
4.1. Durchführung des Key Rollovers	
4.2. Überprüfung der geänderten Schlüssellängen	
4.2.1. Zertifikatsdokument im Domino Directory	33
4.2.2. Zertifizierer-ID	
5. Key Rollover der Abteilungen (OUs)	
5.1. Durchführung des Key Rollovers	38
5.2. Überprüfung der geänderten Schlüssellängen	
5.2.1. Zertifikatsdokument im Domino Directory	
5.2.2. Zertifizierer-ID	
6. Key Rollover der Domino Server	
6.1. Durchführung des Key Rollovers	
6.2. Überprüfung der geänderten Schlüssellängen	
6.2.1. Serverdokument im Domino Directory	
6.2.2. Server-ID	
6.3. Alternative: Rezertifizierung eines Domino Servers	

7. Key Rollover der Notes Anwender	
7.1. Schlüsselüberprüfung im Serverdokument deaktivieren!	
7.2. ID Vault - warum ist der wichtig?	<u></u> 63
7.3. Keinen ID Vault im Einsatz? Sofort ändern!	
7.4. notes.ini Parameter für den ID Vault	
7.5. Durchführung des Key Rollovers	
7.6. Überprüfung der geänderten Schlüssellängen	
7.6.1. Personendokument im Domino Directory	
7.6.2. User-ID	
7.7. Alternative: Rezertifizierung eines Notes Users	
8. ID Vault	
8.1. Mögliche Probleme	
8.1.1. Rücksetzung des Passworts	
8.1.2. Registrierung von Anwendern	
8.1.3. Automatischer Upload von User-IDs	
8.2. Aktuellen Stand der ID Vaults erfassen	
8.3. Austausch der Vault Trust und Password Reset Zertifikate	
8.3.1. Bestehende Zertifikatsdokumete löschen	
8.3.2. Neue Zertifikatsdokumente erstellen	
9. Optional: Einen neuen ID Vault erstellen	
9.1. Motivation	
9.2. Einen neuen ID Vault erstellen	
9.2.1. Schritt 1	
9.2.2. Schritt 2	100
9.2.3. Schritt 3	101
9.2.4. Schritt 4	102
9.2.5. Schritt 5	103
9.2.6. Schritt 6	104
9.2.7. Schritt 7	106
9.2.8. Schritt 8	107
9.2.9. Schritt 9	108
9.2.10. Schritt 10	
9.3. Überprüfung der durchgeführten Aktivitäten	110
9.4. Überprüfung der Policies	
9.5. Anpassung der Settings Dokumente	
9.6. Was passiert jetzt noch?	

1. Einführung

1.1. Motivation

Wer schon länger eine Notes/Domino Umgebung betreibt, ist »damals« mit kleinen Schlüssellängen in den Zertifizierern als auch Server- und User-IDs gestartet (630 Bit), welche heute als unsicher gelten und schnellstmöglich ausgetauscht werden sollten. Sichere Schlüssel haben eine Länge von 2048 - 4096 Bit.

Der »Domino Certificate Authority Key Rollover« Prozess ermöglicht es einer Organisation, ihrer Domino-Zertifizierungsstelle sowie ihren Organisationseinheiten, Servern und Benutzern neue private und öffentliche Schlüssel zuzuweisen. Der Vorgang der Bereitstellung neuer privater und öffentlicher Schlüssel ist allgemein als »Key Rollover« bekannt und wird im weiteren Verlauf dieser Dokumentation als solcher bezeichnet.

Die primäre Zielsetzung dieses Buchs ist es, Ihnen eine praxistaugliche Anleitung für die Durchführung eines Key Rollover in Ihrer eigenen Domino-Umgebung zu geben. Zusätzlich finden Sie auch einige Hintergrundinformationen zu den Zertifizierern sowie Server- und User-IDs, welche in der offiziellen Dokumentation von HCL zu diesem Thema nicht vorhanden oder schwer zu finden sind.

✓ Diese Buch ist sehr detailliert und mit vielen Screenshots ausgestattet. Dies soll auch Administratoren, welche sich im Bereich des Zertifikatsmanagements nicht so gut auskennen, eine fehlerfreie Umsetzung eines Key Rollover in Ihrer Domino-Umgebung ermöglichen.

Als Beispiel wird eine Notes/Domino Umgebung verwendet, welche mit 1024 Bit Schlüssellänge für private und öffentliche Schlüssel erstellt wurde. Die Schlüssel von Organisationen und Abteilungen sollen auf 4096 Bit und die Schlüssel von Server- und User-IDs auf 2048 Bit (Maximum bei Domino 12) erweitert werden.

Hinweis

Falls Sie selbst in einer Testumgebung mit 1024 Bit Schlüssellänge starten möchten, können Sie dies durch folgenden notes.ini Eintrag des Domino Servers erzwingen:

SETUP_FIRST_SERVER_PUBLIC_KEY_WIDTH=1024

Dieser Eintrag muss **nach** der Installation und **vor** der Konfiguration des 1. Domino Servers der Testumgebung gesetzt werden.

Diese Dokumentation wurde unter Nutzung der Notes/Domino Version 12.0.1 FP1 erstellt und mit dieser Version die einzelnen Schritte umgesetzt und auch die Screenshots erstellt. Für ältere Versionen bis zurück zur Version 8.5 sollten die Schritte ähnlich verlaufen - das wurde aber nicht explizit verifiziert.

Wichtig

Die gesamte Dokumentation bezieht sich ausschließlich auf die Nutzung von Zulassungsstellen-, Server- und User-ID **Dateien**.

Ein Key Rollover bei Nutzung des Domino **CA-Prozesses** wird **nicht** besprochen.

1.2. Rechtliche Hinweise

Autor

Dipl.-Ing. Manfred Dillmann https://www.madicon.de

Ausgabe

Ausgabe 1 vom 2022-08-22

Copyright – Urheberrechtshinweise

Alle Inhalte dieser Dokumentation, insbesondere Texte, Fotografien und Grafiken, sind urheberrechtlich geschützt. Das Urheberrecht liegt, soweit nicht ausdrücklich anders gekennzeichnet, bei Manfred Dillmann.

Bitte fragen Sie mich, falls Sie die Inhalte dieser Dokumentation verwenden möchten.

© Manfred Dillmann. Alle Rechte vorbehalten.

Hinweise

Der Autor dieser Dokumentation ist nicht verantwortlich für die Funktion oder Fehler der in dieser Dokumentation beschriebenen Software.

Bei der Erstellung von Texten und Abbildungen wurde mit grösster Sorgfalt vorgegangen - trotzdem können Fehler nicht vollständig ausgeschlossen werden.

Der Autor kann für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen. Für Verbesserungsvorschläge und Hinweise auf Fehler ist der Autor dankbar.

In dieser Dokumentation werden Warennamen ohne die Gewährleistung der freien Verwendbarkeit und ohne besondere Kennzeichnung benutzt. Es ist jedoch davon auszugehen, dass viele der Warennamen gleichzeitig eingetragene Warenzeichnen oder als solche zu betrachten sind.

2. Begriffe und der Status Quo

2.1. Begriffe und Abkürzungen

In dieser Dokumentation werden die folgenden Begriffe und mögliche Abkürzungen verwendet.

• Domino Directory

Der offizielle Titel der names.nsf Datenbank in Ihrer Notes/Domino Umgebung.

• Domino Certificate Trust Hierarchy

Das Vertrauen auf der Zertifikatsebene reicht von der Zertifizierungsstelle der Organisation bis hin zum Zertifikat eines einzelnen Benutzers. Die Vertrauenswürdigkeit kann durch die Untersuchung der ID-Eigenschaften jeder Datei in der Hierarchie und den Vergleich der Kennungen der öffentlichen Schlüssel festgestellt werden.

• Organization Certifier (0)

Der erste Zertifizierer, der bei der Installation des ersten Domino Servers einer neuen Notes/Domino Umgebung erstellt wird und aus dem alle weiteren Zertifikate generiert werden.

• Organizational Unit (OU)

Zertifizierer, die in Domino erstellt werden können, um Server und Benutzer in logischen Unterabteilungen zu gruppieren, z. B. nach Abteilung oder geografischem Gebiet, und die die Hierarchie einer Organisation nachahmen.

Key Rollover

Der Vorgang, bei dem einem Zertifizierer neue öffentliche und private Schlüssel zugewiesen werden, was häufig geschieht, um die Schlüsselstärke eines Zertifizierers zu erhöhen. Key Rollover wird normalerweise von oben nach unten durchgeführt (wie dies auch in dieser Dokumentation gezeigt wird), aber eine Firma kann sich auch dafür entscheiden, dies z.B. nur für ihre Anwender umzusetzen.

• Rollover Certificate

Zertifikat, das bei einem Rollover erstellt wird, um eine Verbindung zwischen dem alten und dem neuen öffentlichen Schlüsselsatz für ein Zertifikat herzustellen.

Recertify

Die Verlängerung der ID eines Anwenders, um zu verhindern, dass sie abläuft.

• Certify

Der Vorgang des »Stempelns« einer physischen ID-Datei, die in der Regel zu einer OU oder einem Server gehört, um zu verhindern, dass die ID abläuft, oder um in einigen Fällen eine andere Sprache, einen alternativen Namen hinzuzufügen, oder um die Vertrauenshierarchie des Zertifikats wiederherzustellen.

2.2. Überprüfung der Zertifikate auf der Ebene: Organisation

2.2.1. Im Domino Directory

Öffnen Sie im Domino Administrator den Tab »Configuration« und wählen Sie links in der Navigation den Punkt »Security« \rightarrow »Certificates« \rightarrow »Certificates«.



Wählen Sie das Dokument des Zertifizierers auf der obersten Ebene (im Beispiel: /Training) in der Kategorie »Notes Certifiers« und öffnen Sie das Dokument mit einem Doppelklick.

Edit Certifier 🔗 Examine Notes Certificate(s) 🛞 Cancel						
DOMINO DIRECT	ORY - Certifier [NOTES CERTIFIER] :/Training					
Basics Recovery Configuration	on Contact Information Other Administration					
Certifier type:	Notes Certifier					
Certifier name:	/Training					
Issued by:	/Training					
Issued to:	O=Training					
Alternate names:	-					
Primary key identifier:	1JCFG 9KXT5 VW7N9 37R8D SGV7C R74FD					
International key identifier:	1JCFG 9KXT5 VW7N9 37R8D SGV7C R74FD					
Current key strength:	Compatible with 6.0 and later (1024 Bits)					
Current key creation date:	09.08.2022 12:26:13					
Certified public key:	0400AE01 F4EC4A84 0AG0160A G002E9F4 90C71803 G0030200 0120A200 34553900 998825G0 0280G002 36553900 98882500 36553900 45172600 01A0G001 34553900 998825G0 06365539 0098825 00365539 00451726 004F3D54 7261696E 696E674F 3D547261 696E696E 6730819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281 8100EFF1 DDFF8182 99A039B2					

Im Feld »Current key strength« wird die aktuelle Länge des Schlüssels angezeigt.

2.2.2. Durch die Zertifizierer-ID

Öffnen Sie im Domino Administrator den Tab »Configuration« und selektieren Sie rechts das Tool »Certification«.



🚾 Choose ID Fi	ile to Examine			×
Suchen in:	certs	~	G 🤌 📂 🛄 -	
Schnellzugriff Desktop Bibliotheken	Name Cert - Kopie.i Cert.id TrainingEL TrainingEL	d DV - Kopie.id DV.id	Änderungsdatum 09.08.2022 12:26 09.08.2022 12:26 09.08.2022 12:47 09.08.2022 12:47	Typ ID-Datei ID-Datei ID-Datei ID-Datei
Dieser PC	Datei <u>n</u> ame: Dateityp:	cert.id		 ✓ Öffnen ✓ Abbrechen

Klicken Sie auf »ID Properties...«.

Selektieren Sie den gewünschten Zertifizierer und bestätigen Sie den Dialog mit »Öffnen«.



Geben Sie das Passwort ein und bestätigen Sie den Dialog durch »OK«.

ID Properties					? 🗙			
	Certificates	Certificates in your ID file						
Security Basics	Your certifica	Your certificates provide a secure way to identify you to Notes and other programs. Your ID may contain						
🔮 🖃 Your Identity	certificates u	certificates used to secure Notes communications as well as certificates used with the Internet.						
Your Names								
Your Certificates	All Notes Certi	All Notes Certificates V Includes your Notes certificates, and certificates for the certificate authorities that issued your certificates.						
Type Issued To ♀ Issued By ♀ Get Certificates								
	ER /Train	ning	/ Ira	ining				
	Other Actions							
	- Selected iten	1						
	Issued to	/Training						
	Issued by	/Training						
	Activated	08.08.2022	Туре	Notes certificate authority				
	Expires	09.08.2122	Key identifier	1JCFG 9KXT5 VW7N9 37F	R8D SGV7C R74FD			
	Advan	ced Details						
					OK Close			

Wählen Sie links in der Navigation den Punkt »Your Identity« → »Your Certificates«. Wählen Sie einen der beiden Einträge und klicken Sie auf die Schaltfläche »Advanced Details…«.

Notes Certific	ate Advance	ed Details		? ×
This Notes	certificate	contains the	e following information.	
Certificate	issued to			
/Trainin	g			
Certificate	issued to (alte	ernate names)		
Certificate	issued by			
/Trainin	g			
	-			
lssuer ke	ey identifier i	IJCFG 9KXT5	VW7N9 37R8D SGV7C R74FD	
Activated	08.08.2022	Туре	Notes certificate authority	
Expires	09.08.2122	Key identifier	1JCFG 9KXT5 VW7N9 37R8D SGV7C	R74FD
Key streng	th Compatib	le with 6.0 and	later (1024 Bits)	Close

Im Feld »Key strength« wird die aktuelle Schlüssellänge angezeigt.

2.3. Überprüfung der Zertifikate auf der Ebene: Abteilung

2.3.1. Im Domino Directory

Die Überprüfung eines Zertifizierers auf der Ebene »Abteilung« unterscheidet sich nicht von Überprüfung eines Zertifizierers auf der Ebene »Organisation«.

Sie finden alle Informationen im Kapitel: 2.2.1. Im Domino Directory auf Seite 9.

2.3.2. Durch die Zertifizierer-ID

Die Überprüfung eines Zertifizierers auf der Ebene »Abteilung« unterscheidet sich nicht von Überprüfung eines Zertifizierers auf der Ebene »Organisation«.

Sie finden alle Informationen im Kapitel: 2.2.2. Durch die Zertifizierer-ID auf Seite 10.

2.4. Überprüfung der Zertifikate eines Domino Servers

2.4.1. Im Domino Directory

Öffnen Sie im Domino Administrator den Tab »Configuration« und selektieren Sie links in der Navigation die Ansicht »Server« → »All Server Documents«.



Öffnen Sie das gewünschte Serverdokument mit einem Doppelklick.

Dedit Server 🛞 Create Web	Examine Notes Certificate(s) TOTP Configuration Check OFind Server Config 🗙 Cancel
Server: S01/Training	01.training.de
Basics Security Ports Server Task	s Internet Protocols Miscellaneous Transactional Logging DAOS Notes Traveler Administration
Administration	1
Owner:	
Administrators:	
Public Key Requirements	
Minimum allowable key strength:	No Minimum 💌
Maximum allowable key strength:	Compatible with Release 7 and later (2048 bits)
Preferred key strength:	Compatible with Release 7 and later (2048 bits)
Maximum allowable age for key:	36500 days
Earliest allowable key creation date:	01.08.77
Don't automatically generate a new key before:	09.08.2122
Maximum number of days the old key should remain valid after the new key has been created:	365 days
Notes Certificate(s)	
Notes certificate:	Present
Primary key identifier:	1ZJT3 UJP3D FW529 7VAQS 4JKR3 484FB
International key identifier:	1ZJT3 UJP3D FW529 7VAQS 4JKR3 484FB
Current key strength:	Compatible with 6.0 and later (1024 Bits)
Current key creation date:	09.08.2022 12:26:14

Auf dem Tab »Administration« wird Ihnen die aktuelle Schlüssellänge angezeigt.

2.4.2. Durch die Server-ID

Öffnen Sie im Domino Administrator den Tab »Configuration« und selektieren Sie rechts »Tools« \rightarrow »Certification«.

	⊸Tools
I	🥪 👿 Certification
Ī	Certify
	Cross Certify
	Cross Certify Key
	Edit Multiple Passwords
İ	Edit Recovery Information
	Extract Recovery Password
	Recover ID File
	Rollover Certifier Key
	Rollover Cross Certificates
	Migrate Certifier
	Modify Certifier
	Certification Log.
	ID Properties
	Set Server Controller's ID
	Begistration

Klicken Sie auf »ID Properties...«.

🚾 Choose ID Fi	ile to Examine			×
Suchen in:	📒 Data	~	③ 🌶 📂 ▼	
-	Name	^	Änderungsdatum	Тур
X	🚞 panagenda		16.08.2022 21:30	Dateiordner
Schnellzugriff	🚞 Properties		16.08.2022 21:30	Dateiordner
	🚞 rmeval		16.08.2022 21:30	Dateiordner
	🚞 W32		16.08.2022 21:30	Dateiordner
Desktop	= xmlschemas		16.08.2022 21:30	Dateiordner
	🗋 admin.id		09.08.2022 12:26	ID-Datei
	🗋 cert.id		09.08.2022 12:26	ID-Datei
Bibliotheken	🗋 nsdsysinfo.io	łx	17.08.2022 23:16	IDX-Datei
	server.id		18.08.2022 17:17	ID-Datei
	serverdoc.id	ĸ	18.08.2022 16:28	IDX-Datei
Dieser PC	🗋 ticket.idt		17.08.2022 23:15	IDT-Datei
A			1	-
Netzwerk	Datei <u>n</u> ame:	server.id		✓ Öffnen
	Dateityp:	ID Files		 Abbrechen

Selektieren Sie die gewünschte Server-ID und bestätigen Sie den Dialog durch »Öffnen«.

ID Properties					? 🗙			
	Certificates	Certificates in your ID file						
Security Basics	Your certifica	Your certificates provide a secure way to identify you to Notes and other programs. Your ID may contain						
🔮 🖻 Your Identity	certificates u	certificates used to secure Notes communications as well as certificates used with the Internet.						
Your Names								
Your Certificates	All Notes Certi	ficates	Includes your N that issued your	otes certificates, and certific certificates	cates for the certificate authorities			
	Type Issued Solotion Solotion Solotion br>Solotion Solotion	d To ≎ Training Training ing	Issu /Tra /Tra /Tra	ed By \$ ining ining ining	<u>G</u> et Certificates ▼ <u>O</u> ther Actions ▼			
	Issued to	S01/Training						
	Issued by	/Training						
	Activated	17.08.2022	Туре	Notes multi-purpose				
	Expires	11.11.2111	Key identifier	1BR4W DG89X UU8RK	2ZXY9 HX1VX S444D			
	<u>A</u> dvan	ced Details						
					OK Close			

Server-IDs haben oft kein Passwort - daher erfolgt ggf. keine Passwortabfrage.

Wählen Sie links in der Navigation den Punkt »Your Identity« → »Your Certificates«. Wählen Sie einen der beiden Einträge für den Domino Server und klicken Sie auf die Schaltfläche »Advanced Details…«.

Notes Certific	ate Advance	ed Details		? ×
This Notes	certificate	contains the	following information.	
Certificate	issued to			
S01/Tra	aining			
Certificate	issued to (alte	emate names)		
Certificate	issued by			
/Trainin	g			
lssuer ke	ey identifier	IJCFG 9KXT5	VW7N9 37R8D SGV7C R74FD	
Activated	08.08.2022	Туре	Notes multi-purpose	
Expires	09.08.2122	Key identifier	1ZJT3 UJP3D FW529 7VAQS 4JKR3	3 484FB
Key streng	th Compatib	le with 6.0 and	later (1024 Bits)	Close

Im Feld »Key strength« wird die aktuelle Schlüssellänge angezeigt.

2.5. Überprüfung der Zertifikate eines Notes Anwenders

2.5.1. Im Domino Directory

Öffnen Sie im Domino Administrator den Tab »People & Groups« und selektieren Sie links in der Navigation die Ansicht »Domino Directories« \rightarrow »Training's Directory« \rightarrow »People«.

People & Groups Files Server Messaging Replication Configuration									
Release 12.0.1FP1 on Windows/11/64 10.0									
 Domino Directories Training's Directory 	۵	Add Person	C Edit Perso	on 🤆	Delete Pers	on (Copy to F		
> 🔏 People			Nam	ne ^	٢	Felep	hone		
Admin Admin Admin Admin Admin Admin Admin									
								V III Dynamic Policies	Vicies
by Person/Group									

Öffnen Sie das gewünschte Personendokument mit einem Doppelklick.

🖉 Ed	it Person 🤇	Examine Notes Certificat	e(s) TOTP Config	juration Check	× Cancel	🖄 Open Mail File	QI	
Ha Ha	ans Te	ster/Training @training.de						
	Basics Work/Home Other Miscellaneous Certificates Roaming Adminis					istration		
	Notes Certificates Internet Certificates Flat Name Key							
	Notes Certificate(s)							
	Notes certificate: Primary key identifier: International key identifier:			Present 11BQN K5BBB P4R7Z E24ZY ES9J5 V84AA				
				11BQN K5BBB P4R7Z E24ZY ES9J5 V84AA				
	Current key strength: Current key creation date:		Com	Compatible with 6.0 and later (1024 Bits)				
				17.08.2022 10:58:48				
	Ourient	ey creation date:	17.08	8.2022 10:58:4	18			

Auf dem Tab »Administration« wird Ihnen die aktuelle Schlüssellänge angezeigt.

2.5.2. Durch die User-ID

Öffnen Sie im Domino Administrator den Tab »Configuration« und selektieren Sie rechts »Tools« \rightarrow »Certification«.

)	', Tools
	🥪 🧱 Certification
Ī	Certify
	Cross Certify
	Cross Certify Key
	Edit Multiple Passwords
	Edit Recovery Information
	Extract Recovery Password
	Recover ID File
	Rollover Certifier Key
	Rollover Cross Certificates
	Migrate Certifier
	Modify Certifier
	Certification Log.
	ID Properties
	Set Server Controller's ID
	Begistration

Klicken Sie auf »ID Properties...«.

🔣 Choose ID Fi	ile to Examine			×	
Suchen in:	🚞 Data	~	G 🦻 📂 🛄 -		
-	Name	^	Änderungsdatum	Тур	
Calan allan aniff	📒 Help		16.08.2022 21:32	Dateiordner	
Schneilzügnin	BM_TECHN	ICAL_SUPPORT	17.08.2022 13:01	Dateiordner	
	ids		16.08.2022 21:32	Dateiordner	
	properties 🔁		16.08.2022 21:32	Dateiordner	
Desktop	theme		16.08.2022 21:32	Dateiordner	
	W 32		16.08.2022 21:32	Dateiordner	
	workspace		17.08.2022 13:01	Dateiordner	
Bibliotheken	= xsl		16.08.2022 21:32	Dateiordner	
	ticket.idt		17.08.2022 11:45	IDT-Datei	
	user - Kopie.id		09.08.2022 12:55	ID-Datei	
Dieser PC	user.id		17.08.2022 07:33	ID-Datei	
S			1	_	
Netzwerk	Datei <u>n</u> ame:	user.id		✓ Öffnen	
	Dateityp:	ID Files		 Abbrechen 	
19					

Selektieren Sie die gewünschte User-ID und bestätigen Sie den Dialog durch »Öffnen«.

Login to HCL Notes	:	×
HCL Notes	USER NAME Admin/Training	
2R	PASSWORD	
	LOG <u>I</u> N	EXIT

Geben Sie das Passwort ein und bestätigen Sie den Dialog durch die Schaltfläche »LOG IN«.

D Properties					? 🗙	
	Certificates in your ID file					
Security Basics	Your certificates provide a secure way to identify you to Notes and other programs. Your ID may cont				ms. Your ID may contain	
Your Identity	certificates used to secure Notes communications as well as certificates used with the Internet.					
Your Names						
Your Certificates	All Notes Certif	ficates	Includes your Not that issued your	Includes your Notes certificates, and certificates for the certificate authorities that issued your certificates		
	Type Issued To <> Ist Admin/Training Ist Admin/Training Ist Admin/Training Ist Admin/Training Ist Admin/Training		Issue /Tra /Tra /Tra	ed By 🗘 ining ining ining	<u>G</u> et Certificates ▼ <u>O</u> ther Actions ▼	
	Issued to	Admin/Training				
	Issued by	/Training				
	Activated	08.08.2022	Туре	Notes multi-purpose		
	Expires	09.08.2024	Key identifier	1B5ED W8RDC YKV36	8DSSY QEVWR 24488	
	Advanced Details					
	-				OK Close	

Wählen Sie links in der Navigation den Punkt »Your Identity« → »Your Certificates«.

Selektieren Sie einen der beiden Einträge für den Anwender und klicken Sie auf die Schaltfläche »Advanced Details...«.

Notes Certificate Advanced Details							
This Notes certificate contains the following information.							
Certificate	Certificate issued to						
Admin/	Admin/Training						
Certificate issued to (alternate names)							
Certificate issued by							
/Training							
lssuer ke	Issuer key identifier 1JCFG 9KXT5 VW7N9 37R8D SGV7C R74FD						
Activated	08.08.2022	Туре	Notes multi-purpose				
Expires	09.08.2024	Key identifier	1B5ED W8RDC YKV36 8DSSY QEVW	R 24488			
Key strength Compatible with 6.0 and later (1024 Bits)							

Im Feld »Key strength« wird die aktuelle Schlüssellänge angezeigt.

3. Key Rollover Einführung

3.1. Voraussetzungen

Damit Sie auf keine unvorhergesehenen Probleme stossen, sollten Sie die folgenden Punkte überprüfen und beachten.

• In nächster Zeit ablaufende O-, OU, User- oder Server-IDs

Falls bei Ihnen in den nächsten Tagen irgendwelche IDs ablaufen, sollten Sie diese zunächst mit den noch nicht geänderten Zertifizieren verlängern. Ich persönlich empfehle eine Haltbarkeit von mindestens 60 Tagen.

• Alle Anwender Umbenennungen müssen abgeschlossen sein

Während ein Key Rollover ausgeführt wird, darf keine Umbenennung (das betrifft den Vor- und Nachname als auch ein Wechsel zu einem anderen Zertifizierer) ausgeführt oder gestartet werden.

Stellen Sie sicher, dass diese Vorgänge abgeschlossen sind, bevor Sie einen Key Rollover starten.

• ID Vault

Ein einwandfrei funktionierender ID Vault ist zumindest im Bezug auf den Key Rollover von User-IDs als Voraussetzung zu benennen.

Wenn Sie keinen ID Vault nutzen oder dieser nicht alle aktiven User IDs gespeichert hat (also nicht richtig funktioniert), werden die Anwender am Notes Client diverse Dialoge sehen, welche sie möglicherweise nicht verstehen und sich dann beim IT-Support melden (siehe Kapitel 7.3. Keinen ID Vault im Einsatz? Sofort ändern! auf Seite 64).

Ein Anwender kann in diesen Dialogen den Key Rollover auch ablehnen!

• Zeitnahe und fehlerfreie Replikation

Zusätzlich zu den Änderungen an den ID-Dateien selbst, werden auch die Zertifikatsinformationen in den Zertifikats-, Server- und Anwenderdokumenten geändert.

Diese geänderten Dokumente müssen zeitnah zwischen allen Domino Servern repliziert werden!

• Einwandfreie Funktion der Domino Server

Wenn Sie an den Konsolen Ihrer Domino Server kritische Fehlermeldungen (warning low, warning high, failure oder fatal) sehen oder Ihre Domino Server »nicht richtig funktionieren«, sollten Sie diese Probleme zwingend **vor** der Durchführung eines Key Rollover beheben.

Backup Ihrer Notes/Domino Umgebung

Nachdem Sie ihren Administrationsserver heruntergefahren haben, erstellen Sie über das Dateisystem Sicherungskopien der folgenden Dateien:

- Domino Directory (names.nsf)
- Certification Log Datenbank (certlog.nsf)
- Alle ID-Dateien (Organisation, Abteilungen, Server)
- Alle Anwender ID-Dateien (vor allem die ID-Datei des Administrators)

• Nutzung des Administrationsserver für alle Aufgaben des Key Rollovers

Da alle Aktivitäten im Zusammenhang mit einem Key Rollover Änderungen im Domino Directory (names.nsf) auslösen und diese vom Administrationsserver durchgeführt werden, sollten **immer** der Administrationsserver als der **aktuelle Domino Server im Domino Administrator** ausgewählt sein.

Alle anstehenden Aufgaben können so schneller umgesetzt werden, als wenn diese von einem anderen Domino Server erst zum Administrationsserver repliziert werden müssen.

3.2. Was gibt es nach einem Key Rollover zu beachten?

Wenn Sie einen Key Rollover planen, müssen Sie sich darüber im Klaren sein, wie mit Ihren Richtlinien, Agenten, der Ausführungskontrollliste und - falls vorhanden - mit Gegenzertifikaten umgegangen werden soll.

Standardmäßig werden diese Elemente durch einen Zertifizierer, einen Benutzer oder in einigen Fällen durch eine Server-ID signiert. Beim Key Rollover der signierenden Entitäten führt Domino nicht automatisch einen Key Rollover mit dem neuen Schlüssel in diesen Elementen aus, sondern der Administrator muss diese Aktion manuell ausführen.

3.2.1. Agenten

Agenten müssen editiert und damit erneut signiert werden, sobald der ursprüngliche Unterzeichner seinen Key Rollover abgeschlossen hat.

Wie bei allen anderen Entitäten haben Sie bis zum Ablauf des Rollover-Zertifikat Zeit, diese Maßnahmen durchzuführen.

3.2.2. Execution Contro Lists (ECL's)

Ausführungskontrolllisten (ECL's) müssen editiert und damit erneut signiert werden, sobald der ursprüngliche Unterzeichner seinen Key Rollover abgeschlossen hat.

Wie bei allen anderen Entitäten haben Sie bis zum Ablauf des Rollover-Zertifikat Zeit, diese Maßnahmen durchzuführen.

3.2.3. Gegenzertifikate

Wenn Sie einer anderen Organisation Zugriff auf Ihre Domäne gewährt haben, sollten Sie ihr eine neue sichere Kopie des entsprechenden Zertifizierers oder Server-ID zur Verfügung stellen, für diese der Key Rollover abgeschlossen ist.

Diese Organisation sollte dann ihr aktuelles Gegenzertifikat für Ihre Organisation löschen und ein neues Gegenzertifikat aus der sicheren Kopie erstellen, die Sie ihr zur Verfügung gestellt haben.

Wenn die Endanwender der Organisation Kopien des Gegenzertifikats in ihrem lokalen Adressbuch gespeichert haben, müssen diese durch das neue Gegenzertifikat ersetzt werden.

Wenn Sie auf eine andere Organisation zugreifen, sollten Sie diese bitten, Ihnen eine neue sichere Kopie der ID-Datei zu schicken, mit der Sie gegenzertifiziert sind. Sobald Sie diese erhalten haben, müssen Sie das aktuelle Gegenzertifikat löschen und ein neues Gegenzertifikat mit der entsprechenden, verlängerten ID erstellen.

Wenn einer Ihrer Anwender eine Kopie des Gegenzertifikats in seinem lokalen Adressbuch hat, sollte die bestehende Kopie entfernt und durch ein neues Gegenzertifikat ersetzt werden.

Wie bei allen anderen Entitäten haben Sie bis zum Ablauf des Rollover-Zertifikat Zeit, diese Maßnahmen durchzuführen.

3.2.4. Policies

Bei Richtlinien müssen die Richtlinie und das/die zugehörigen Einstellungsdokument(e) erneut signiert werden, sobald der ursprüngliche Unterzeichner seinen Key Rollover abgeschlossen hat.

Dies ist ein einfacher Prozess, bei dem das Dokument vom Unterzeichner in den Bearbeitungsmodus gebracht und dann gespeichert werden muss. Einige Kunden haben jedoch berichtet, dass sie eine kleine Änderung am Dokument vornehmen und dann die Änderung entfernen mussten, damit das Dokument korrekt signiert wird.

Wie bei allen anderen Entitäten haben Sie bis zum Ablauf des Rollover-Zertifikat Zeit, diese Maßnahmen durchzuführen.

3.2.5. Templates

Templates für Domino Anwendungen müssen erneut signiert werden, sobald der Unterzeichner seinen Key Rollover abgeschlossen hat.

Wie bei allen anderen Entitäten haben Sie bis zum Ablauf des Rollover-Zertifikat Zeit, diese Maßnahmen durchzuführen.