

HCL Domino

Certificates Key Rollover

A detailed guide for Domino Administrators

Author Manfred Dillmann

Table of contents

1. Introduction	4
1.1. Motivation	5
1.2. Legal hints	
2. Terms and the status quo	7
2.1. Terms and abbreviations	
2.2. Verification of certificates at the level: Organization	9
2.2.1. In Domino Directory	9
2.2.2. By Certifier ID	
2.3. Verification of certificates at the level: Organizational Unit	13
2.3.1. In Domino Directory	
2.3.2. By Certifier ID	
2.4. Verification of Domino Server certificates	
2.4.1. In Domino Directory	
2.4.2. By Server ID	
2.5. Verification of Notes user certificates	
2.5.1. In Domino Directory	
2.5.2. By User ID	
3. Key Rollover Introduction	21
3.1. Requirements	
3.2. What is there to consider after a key rollover?	23
3.2.1. Agents	23
3.2.2. Execution Contro Lists (ECL's)	23
3.2.3. Cross certificates	23
3.2.4. Policies	
3.2.5. Templates	
4. Organization key rollover (O)	25
4.1. Execution of the key rollover	
4.2. Verification of changed key lengths	
4.2.1. Certificate document in Domino Directory	
4.2.2. Certifier ID	
5. Organizational Units key rollover (OUs)	
5.1. Execution of the key rollover	
5.2. Verification of the changed key lengths	
5.2.1. Certificate document in Domino Directory	
5.2.2. Certifier ID	
6. Domino Server key rollover	
6.1. Execution of the key rollover	
6.2. Verification of the changed key lengths	
6.2.1. Server document in Domino Directory	
6.2.2. Server ID	
6.3. Alternative: Recertification of a Domino Server	

7. Notes User key rollover	
7.1. Disable public key verification in server document!	
7.2. ID Vault - why is it important?	
7.3. No ID Vault in use? Change immediately!	
7.4. notes.ini parameter for the ID Vault	65
7.5. Execution of the key rollover	
7.6. Verification of the changed key lengths	
7.6.1. Person document in Domino Directory	
7.6.2. User ID	
7.7. Alternative: Recertification of a Notes user	
8. ID Vault	
8.1. Possible problems	
8.1.1. Password reset	77
8.1.2. User registration	
8.1.3. Automatic upload of user IDs	
8.2. Capture current state of ID Vaults	
8.3. Replacement of the Vault Trust and Password Reset certificates	
8.3.1. Delete existing certificate documents	
8.3.2. Create new certificate documents	
9. Optional: Create a new ID Vault	
9.1. Motivation	
9.2. Create a new ID Vault	
9.2.1. Step 1	
9.2.2. Step 2	100
9.2.3. Step 3	
9.2.4. Step 4	102
9.2.5. Step 5	103
9.2.6. Step 6	104
9.2.7. Step 7	106
9.2.8. Step 8	107
9.2.9. Step 9	108
9.2.10. Step 10	
9.3. Review of activities carried out	110
9.4. Review of the policies	
9.5. Customizing the settings documents	
9.6. What else is happening now?	114

1. Introduction

1.1. Motivation

Anyone who has been operating a Notes/Domino environment for a long time started »back then« with small key lengths in the certifiers as well as server and user IDs (630 bits), which are now considered insecure and should be replaced as soon as possible. Secure keys have a length of 2048 - 4096 bits.

The »Domino Certificate Authority Key Rollover« process allows an organization to assign new private and public keys to its Domino organization and its organizational units, servers, and users. The process of provisioning new private and public keys is commonly known as »key rollover« and is referred to as such throughout the remainder of this documentation.

The primary objective of this book is to provide you with a practical guide for performing a key rollover in your own Domino environment. In addition, you will also find some background information about the certifiers as well as server and user IDs, which are not available or difficult to find in the official documentation from HCL on this topic.

✓ This book is very detailed and includes many screenshots. This should also enable administrators who are not so familiar with certificate management to implement a key rollover in their Domino environment without errors.

As an example, a Notes/Domino environment is used, which was created with 1024 bit key length for private and public keys. The keys of organizations and departments are to be extended to 4096 bits and the keys of server and user IDs to 2048 bits (maximum for Domino 12).

Hint

If you want to start yourself in a test environment with 1024 bit key length, you can force this by the following notes.ini entry of the Domino Server:

SETUP_FIRST_SERVER_PUBLIC_KEY_WIDTH=1024

This entry must be set **after** installation and **before** configuring the 1st Domino Server of the test environment.

This documentation was created using Notes/Domino version 12.0.1 FP1 and with this version the single steps were implemented and also the screenshots were created. For older versions back to version 8.5 the steps should be similar - but this was not explicitly verified.

Important

All documentation refers exclusively to the use of certifier, server and user ID **files**.

Key rollover when using the **Domino CA process** is **not** discussed.

1.2. Legal hints

Author

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

Edition

Edition 1 from 2022-08-22

Copyright

All contents of this documentation, in particular texts, photographs and graphics, are protected by copyright. The copyright is held by Manfred Dillmann, unless explicitly stated otherwise.

Please ask me if you wish to use the contents of this documentation.

© Manfred Dillmann. All rights reserved.

Hints

The author of this documentation is not responsible for the function or errors of the software described in this documentation.

The greatest care has been taken in the preparation of texts and illustrations - nevertheless, errors cannot be completely ruled out.

The author cannot accept any legal responsibility or any liability for incorrect information and its consequences. The author is grateful for suggestions for improvement and hints to errors.

In this documentation, product names are used without the guarantee of free usability and without special identification. However, it must be assumed that many of the product names are also registered trademarks or are to be regarded as such.

2. Terms and the status quo

2.1. Terms and abbreviations

The following terms and possible abbreviations are used in this documentation.

• Domino Directory

The official title of the names.nsf database in your Notes/Domino environment.

• Domino Certificate Trust Hierarchy

Trust at the certificate level ranges from the organization's certificate authority to an individual user's certificate. Trustworthiness can be determined by examining the ID properties of each file in the hierarchy and comparing the public key identifiers.

• Organization Certifier (0)

The first certifier that is created when the first Domino Server of a new Notes/Domino environment is installed and from which all further certificates are generated.

• Organizational Unit (OU)

Certifiers that can be created in Domino to group servers and users into logical subdivisions, such as by unit or geographic area, mimicking the hierarchy of an organization.

Key Rollover

The process of assigning new public and private keys to a certifier, often done to increase the key strength of a certifier. Key rollover is usually performed from top to bottom (as also shown in this documentation), but a company may also choose to implement it for its users only, for example.

• Rollover Certificate

Certificate created during a rollover to establish a link between the old and new public key sets for a certificate.

Recertify

The time extension of a user's ID to prevent it from expiring.

• Certify

The process of »stamping« a physical ID file, usually belonging to an OU or server, to prevent the ID from expiring, or in some cases to add a different language, an alternate name, or to restore the certificate's trust hierarchy.

2.2. Verification of certificates at the level: Organization

2.2.1. In Domino Directory

In the Domino Administrator, open the »Configuration« tab and select the »Security« \rightarrow »Certificates« \rightarrow »Certificates« item in the navigation on the left.



Select the certifier's document at the top level (in the example: /Training) in the »Notes Certifiers« category and open the document with a double-click.

Edit Certifier 🖉 Examine Notes Certificate(s) 🛞 Cancel						
DOMINO DIRECT	ORY - Certifier [NOTES CERTIFIER] :/Training					
Basics Recovery Configuratio	on Contact Information Other Administration					
Basics						
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					
	99002060 000000009 00900020 00000009 00451726 004F3D54 7261696F 696F674F					
	3D547261 696E696E 6730819E 300D0609					
	2A864886 F70D0101 01050003 818D0030					
	81890281 8100BFF1 DDEE8182 99A039B2					

The »Current key strength« field displays the current length of the key.

2.2.2. By Certifier ID

In Domino Administrator, open the »Configuration« tab and select the »Certification« tool on the right.



🚾 Choose ID Fi	ile to Examine			×
<u>S</u> uchen in:	certs	~	G 🦻 📂 🛄 -	
Schnellzugriff Desktop Bibliotheken	Name Cert - Kopie.i Cert.id TrainingEl TrainingEl	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
Netzwerk	Datei <u>n</u> ame: Datei <u>t</u> yp:	Cert.id ID Files		✓ <u>Offnen</u> ✓ Abbrechen

Click on »ID Properties ... «.

Select the desired certifier and confirm the dialog with »Open« (Öffnen).

Login to HCL Notes		×	
HCL Notes	CERTIFIER NAME		
A Charles	<u>P</u> ASSWORD		
	ОК	CANCEL	

Enter the password and confirm the dialog by clicking »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	sed to secure Note	es communications a	s well as certificates used w	<i>i</i> th the Internet.		
Your Names							
Your Certificates	All Notes Certi	ficates	Includes your N that issued you	Notes certificates, and certifi ir certificates.	icates for the certificate authorities		
	Type Issue	d To 🗘	Issu	ued By ≎	Get Certificates 🔻		
	🛐 /Trair	ning	/Tr	aining			
	🛛 🕅 🕅 🕅 🕅	ning	/Tr	aining			
					Other Actions		
	Selected iten	ı ———					
	Issued to	/Training					
	Issued by	/Training					
	Activated	08.08.2022	Туре	Notes certificate authorit	ty		
	Expires	09.08.2122	Key identifier	1JCFG 9KXT5 VW7N9	37R8D SGV7C R74FD		
	Advan	ced Details					
	<u></u>						
					OK Close		

Select »Your Identity« \rightarrow »Your Certificates« in the navigation on the left. Select one of the two entries and click on the »Advanced Details...« button.

Notes Certific	ate Advance	ed Details		? ×
This Notes	certificate	contains the	e following information.	
Certificate	issued to			
/Trainin	p			
Certificate	issued to (alte	emate names)		
Certificate	issued by			
/Trainin	lg			
lssuer ke	ey identifier i	1JCFG 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

The current key length is displayed in the »Key strength« field.

2.3. Verification of certificates at the level: Organizational Unit

2.3.1. In Domino Directory

Verification of a certifier at the »Organizational Unit« level is no different from verification of a certifier at the »Organization« level.

You can find all the information in the chapter: 2.2.1. In Domino Directory on page 9.

2.3.2. By Certifier ID

Verification of a certifier at the »Organizational Unit« level is no different from verification of a certifier at the »Organization« level.

You can find all the information in the chapter: By certifier ID on page 10.

2.4. Verification of Domino Server certificates

2.4.1. In Domino Directory

Open the »Configuration« tab in the Domino Administrator and select the view »Server« \rightarrow »All Server Documents« in the navigation on the left.

Peopl	People & Groups Files Server Messaging Replication Configuration							
ĒĄ	Server: S01/Training Release 12.0.1FP1 on Windows/11/64 10.0							
▼ 🛛	Server	۵	Add Server	DEdit Server	Add to Cluster	Delete Server		
	All Server Documents		Domain	Server Name	 Title 			
21	Configurations		✓ Training					
	Connections			S01/Training	1. D	omino Server		
	Programs External Domain Network Infe		2					
) 🗟	Messaging		-					
	Replication							

Open the desired server document with a double click.

Edit Server 🛞 Create Web (Examine Notes Certificate(s) TOTP Configuration Check ③ Find Server Config 🔇 Cancel
Server: S01/Training	s01.training.de
Basics Security Ports Server Task	s Internet Protocols Miscellaneous Transactional Logging DAOS Notes Traveler Administration
Administration	
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

On the »Administration« tab you will see the current key length.

2.4.2. By Server ID

In the Domino Administrator, open the »Configuration« tab and select »Tools« \rightarrow »Certification« on the right.



Click on »ID Properties...«.

👯 Choose ID Fi	ile to Examine			×
Suchen in:	🛅 Data	~	G 🦻 📂 🛄 -	
-	Name	^	Änderungsdatum	Тур
—	🚞 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.id	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
S			1	_
Netzwerk	Datei <u>n</u> ame:	server.id		 ✓ Öffnen
	Dateityp:	ID Files		~ Abbrechen

Select the desired server ID and confirm the dialog by clicking »Open« (Öffnen).

ID Properties					? ×		
	Certificates	Certificates in your ID file					
Cost 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	sed to secure Notes of	communications as	well as certificates used with the	Internet.		
Your Names							
Your Certificates	All Notes Certi	ficates ~	Includes your N	otes certificates, and certificates f	for the certificate authorities		
	Type Issued SO1/ SO1/ Train	d To ≎ Training Training ning	Issu /Tra /Tra /Tra	ed By 🗘 ining ining ining	<u>G</u> et Certificates ▼ <u>O</u> ther Actions ▼		
	Selected item	S01/Training					
	Issued to	SUT/ training					
	Activated	7 training	Turne	Nataa multi numaaa			
	Evoiree	11 11 2111	Kev identifier	18RAW DG89X LILI8RK 27XY			
	<u>A</u> dvan	ced Details					
				OF	Close		

Server IDs often do not have a password - therefore there may be no password prompt.

Select the item »Your Identity« \rightarrow »Your Certificates« in the navigation on the left. Select one of the two entries for the Domino Server and click the »Advanced Details...« button.

Notes Certific	ate Advance	ed Details		? ×	
This Notes	certificate	contains the	e following information.		
Certificate	issued to				
S01/Tra	aining				
Certificate	issued to (alto	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 484FB					
Key streng	th Compatib	le with 6.0 and	later (1024 Bits)	Close	

The current key length is displayed in the »Key strength« field.

2.5. Verification of Notes user certificates

2.5.1. In Domino Directory

Open the »People & Groups« tab in the Domino Administrator and select the »Domino Directories« \rightarrow »Training's Directory« \rightarrow »People« view in the navigation on the left.

People & Groups Files Server Messaging Replication Configuration							
Release 12.0.1FP1 on Windows/11/64 10.0							
 Domino Directories Training's Directory 	0	Add Person	Dedit Person	Delete Per	son DCopy to F		
E A People			Name	^	Telephone		
A Groups			Admin				
P 229 Mail-In Databases and R	I		Tester, Hans				
V III Dynamic Policies							

Open the desired person document with a double click.

🖉 Ed	it Person	© Examine Notes Certific	cate(s) TOTP Configuration	on Check	× Cancel	🖄 Open Mail File	QI
Ha Ha	ans T	ester/Training er@training.de)				
	Basics	Work/Home Other Mis	scellaneous Certificate	s Roam	ing Admin	istration	
	Notes Co	ertificates Internet Certifi	cates Flat Name Key				
	Notes C	ertificate(s)					
	Notes of	certificate:	Present				
	Primar	y key identifier:	11BQN K5	BBB P4R7	7Z E24ZY ES	9J5 V84AA	
	Interna	tional key identifier:	11BQN K5	BBB P4R7	7Z E24ZY ES	9J5 V84AA	
	Curren	t key strength:	Compatibl	e with 6.0	and later (10	24 Bits)	
	Curren	t key creation date:	17.08.202	2 10:58:48			
	Notes	certified public key:	04003903	3F1C56F	4 0AG01619	G00237CB	

On the »Administration« tab you will see the current key length.

2.5.2. By User ID

In the Domino Administrator, open the »Configuration« tab and select »Tools« \rightarrow »Certification« on the right.



Click on »ID Properties...«.

Choose ID F	ile to Examine			×
Suchen in:	: 🛅 Data		🕑 🧿 🥬 📴 🗸	
_	Name	^	Änderungsdatum	Тур
Schnellzugriff	Help		16.08.2022 21:32	Dateiordner
	BM_IECH	NICAL_SUPPORT	17.08.2022 13:01	Dateiordner
	nroperties		16.08.2022 21:32	Dateiordner
Desktop	theme		16.08.2022 21:32	Dateiordner
	W 32		16.08.2022 21:32	Dateiordner
	aworkspace 🔁		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	e.id	09.08.2022 12:55	ID-Datei
Dieser PC	user.id		17.08.2022 07:33	ID-Datei
3				_
Netzwerk	Datei <u>n</u> ame:	user.id		✓ Öffnen
	Datei <u>ty</u> p:	ID Files		 ✓ Abbrechen

Select the desired user ID and confirm the dialog by clicking »Open« (Öffnen).

Login to HCL Notes	1	×
HCL Notes	USER NAME Admin/Training	
2R	Password	
	LOG <u>I</u> N	EXIT

Enter the password and confirm the dialog by clicking on the »LOG IN« button.

		Certificates	in your ID file						
🕞 Securi	ity Basics	Your certificates provide a secure way to identify you to Notes and other programs. Your ID may contain							
🔮 🗉 Your 🖡	dentity	certificates u	sed to secure Notes of	communications as	well as certifica	ates used with the Ir	nternet.		
Your	Names								
Your C	Certificates	All Notes Certificates V Includes your Notes certificates, and certificate that issued your certificates					r the certificate authoritie		
				indi locaca your	oontinoutoo.				
		Type Issue	d To 🗘	Issue	ed Bv ≎		Cat Catificates		
		Admir	n/Training	/Tra	ining		Get Certificates		
		🖪 Admir	🚯 Admin/Training /Training						
		🛐 /Training		/Training			Other Actions		
							Other Actions		
		Selected item							
		Selected item	Admin/Training						
		Selected item Issued to Issued by	Admin/Training /Training						
		Selected item Issued to Issued by Activated	Admin/Training /Training 08.08.2022	Туре	Notes multi-p	upose			
		Selected item Issued to Issued by Activated Expires	Admin/Training /Training 08.08.2022 09.08.2024	Type Key identifier	Notes multi-p 1B5ED W8R	urpose IDC YKV36 8DSSY	QEVWR 24488		
		Selected item Issued to Issued by Activated Expires	Admin/Training /Training 08.08.2022 09.08.2024 ced Details	Type Key identifier	Notes multi-p 1B5ED W8R	urpose IDC YKV36 8DSSY	QEVWR 24488		
		Selected item Issued to Issued by Activated Expires <u>A</u> dvan	Admin/Training /Training 08.08.2022 09.08.2024 ced Details	Type Key identifier	Notes multi-p 1B5ED W8R	urpose IDC YKV36 8DSSY	QEVWR 24488		
		Selected item Issued to Issued by Activated Expires	Admin/Training /Training 08.08.2022 09.08.2024 ced Details	Type Key identifier	Notes multi-p 1B5ED W8R	urpose IDC YKV36 8DSSY	QEVWR 24488		
		Selected item Issued to Issued by Activated Expires	Admin/Training /Training 08.08.2022 09.08.2024 ced Details	Type Key identifier	Notes multi-p 1B5ED W8R	urpose IDC YKV36 8DSSY	QEVWR 24488		
		Selected item Issued to Issued by Activated Expires	Admin/Training /Training 08.08.2022 09.08.2024 ced Details	Type Key identifier	Notes multi-p 1B5ED W8R	urpose IDC YKV36 8DSSY	QEVWR 24488		

Select »Your Identity« \rightarrow »Your Certificates« in the navigation on the left.

Select one of the two entries for the user and click on the »Advanced Details...« button.

Notes Certific	ate Advanco	ed Details		? ×			
This Notes	certificate	contains the	e following information.				
Certificate	issued to						
Admin/	Training						
Certificate	Certificate issued to (alternate names)						
Certificate	Certificate issued by						
/Trainin	g			_			
lssuer ke	ey identifier	IJCFG 9KXT5	VW7N9 37R8D SGV7C R74FD				
Activated	08.08.2022	Туре	Notes multi-purpose				
Expires	09.08.2024	Key identifier	1B5ED W8RDC YKV36 8DSSY QEVWF	R 24488			
Key strength Compatible with 6.0 and later (1024 Bits)							

The current key length is displayed in the »Key strength« field.

3. Key Rollover Introduction

3.1. Requirements

To ensure that you do not encounter any unforeseen problems, you should check and observe the following points.

• 0, 0U, User-, or Server-IDs expiring in the near future.

If you have any IDs expiring in the next few days, you should first renew them with the certifications that have not yet changed. I personally recommend a expiration of at least 60 days.

• All user renaming must be completed

While a key rollover is being performed, no renaming (this applies to the first and last name as well as a change to another certifier) may be performed or started. Make sure that these operations are completed before starting a key rollover.

• ID Vault

A properly functioning ID Vault is a prerequisite, at least with regard to the key rollover of user IDs.

If you do not use ID Vault or it does not store all active user IDs (i.e. it does not work properly), users will see various dialogs on the Notes Client, which they may not understand and then report to IT support (see chapter 7.3. No ID Vault in use? Change immediately! on page 64).

A user can also reject the key rollover in these dialogs!

• Timely and error-free replication

In addition to the changes to the ID files themselves, the certificate information in the certificate, server and user documents is also changed.

These changed documents must be replicated between all Domino Servers in a timely manner!

• Flawless functioning of the Domino Servers

If you see critical error messages (warning low, warning high, failure or fatal) on your Domino Server consoles or your Domino Servers are »not working properly«, it is imperative that you fix these issues **before** performing a Key Rollover.

Backup of your Notes/Domino environment

After you shut down your Administration Server, use the file system to create backup copies of the following files:

- Domino Directory (names.nsf)
- Certification Log Database (certlog.nsf)
- All ID files (Organization, Organization Units, Server)
- All user ID files (especially the administrator's ID file)

• Use of the Administration Server for all key rollover tasks

Since all activities related to a key rollover trigger changes in the Domino Directory (names.nsf) and these are performed by the Administration Server, the Administration Server should always be selected as the **current Domino Server in Domino Administrator**. All pending tasks can thus be implemented more quickly than if they first have to be replicated from another Domino Server to the Administration Server.

3.2. What is there to consider after a key rollover?

When planning a key rollover, you need to be clear about how to handle your policies, agents, execution control list, and cross certificates, if any.

By default, these items are signed by a certifier, a user, or in some cases, a server ID. When key rolling over the signing entities, Domino does not automatically perform a key rollover with the new key in these items, but the administrator must perform this action manually.

3.2.1. Agents

Agents must be edited and thus re-signed once the original signer completes their key rollover.

As with all other entities, you have time until the rollover certificate expires to perform these actions.

3.2.2. Execution Contro Lists (ECL's)

Execution control lists (ECL's) must be edited and thus re-signed as soon as the original signer completes their key rollover.

As with all other entities, you have time until the rollover certificate expires to perform these actions.

3.2.3. Cross certificates

If you have granted another organization access to your domain, you should provide it with a new secure copy of the appropriate certifier or server ID for which the key rollover is complete.

That organization should then delete its current cross certificate for your organization and create a new cross certificate from the secure copy you provided to it.

If the organization's users have copies of the cross certificate stored in their local address book, they must be replaced with the new counterpart certificate.

If you access another organization, you should ask them to send you a new secure copy of the ID file you are cross-certified with. Once you receive it, you must delete the current cross certificate and create a new cross certificate with the appropriate, extended ID.

If any of your users have a copy of the cross certificate in their local address book, the existing copy should be removed and replaced with a new cross certificate.

As with all other entities, you have time until the rollover certificate expires to perform these actions.

3.2.4. Policies

For policies, the policy and associated settings document(s) must be re-signed once the original signer completes their key rollover.

This is a simple process of getting the document into edit mode by the signer and then saving it. However, some customers have reported that they had to make a small change to the document and then remove the change in order for the document to be signed correctly.

As with all other entities, you have time until the rollover certificate expires to take these actions.

3.2.5. Templates

Templates for Domino applications must be re-signed once the signer has completed their key rollover.

As with all other entities, you have time until the rollover certificate expires to perform these actions.

4. Organization key rollover (O)