



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	6
2. Terms and the status quo	7
2.1. Terms and abbreviations	8
2.2. Verification of certificates at the level: Organization	9
2.2.1. In Domino Directory	9
2.2.2. By Certifier ID	10
2.3. Verification of certificates at the level: Organizational Unit	13
2.3.1. In Domino Directory	13
2.3.2. By Certifier ID	13
2.4. Verification of Domino Server certificates	14
2.4.1. In Domino Directory	14
2.4.2. By Server ID	15
2.5. Verification of Notes user certificates	17
2.5.1. In Domino Directory	17
2.5.2. By User ID	18
3. Key Rollover Introduction	21
3.1. Requirements	22
3.2. What is there to consider after a key rollover?	23
3.2.1. Agents	23
3.2.2. Execution Control Lists (ECL's)	23
3.2.3. Cross certificates	23
3.2.4. Policies	24
3.2.5. Templates	24
4. Organization key rollover (O)	25
4.1. Execution of the key rollover	26
4.2. Verification of changed key lengths	32
4.2.1. Certificate document in Domino Directory	32
4.2.2. Certifier ID	33
5. Organizational Units key rollover (OUs)	37
5.1. Execution of the key rollover	38
5.2. Verification of the changed key lengths	45
5.2.1. Certificate document in Domino Directory	45
5.2.2. Certifier ID	45
6. Domino Server key rollover	49
6.1. Execution of the key rollover	50
6.2. Verification of the changed key lengths	55
6.2.1. Server document in Domino Directory	55
6.2.2. Server ID	55
6.3. Alternative: Recertification of a Domino Server	57

7. Notes User key rollover	60
7.1. Disable public key verification in server document!	61
7.2. ID Vault - why is it important?	63
7.3. No ID Vault in use? Change immediately!	64
7.4. notes.ini parameter for the ID Vault	65
7.5. Execution of the key rollover	66
7.6. Verification of the changed key lengths	72
7.6.1. Person document in Domino Directory	72
7.6.2. User ID	72
7.7. Alternative: Recertification of a Notes user	74
8. ID Vault	76
8.1. Possible problems	77
8.1.1. Password reset	77
8.1.2. User registration	78
8.1.3. Automatic upload of user IDs	78
8.2. Capture current state of ID Vaults	80
8.3. Replacement of the Vault Trust and Password Reset certificates	81
8.3.1. Delete existing certificate documents	81
8.3.2. Create new certificate documents	89
9. Optional: Create a new ID Vault	96
9.1. Motivation	97
9.2. Create a new ID Vault	98
9.2.1. Step 1	99
9.2.2. Step 2	100
9.2.3. Step 3	101
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	109
9.3. Review of activities carried out	110
9.4. Review of the policies	111
9.5. Customizing the settings documents	113
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

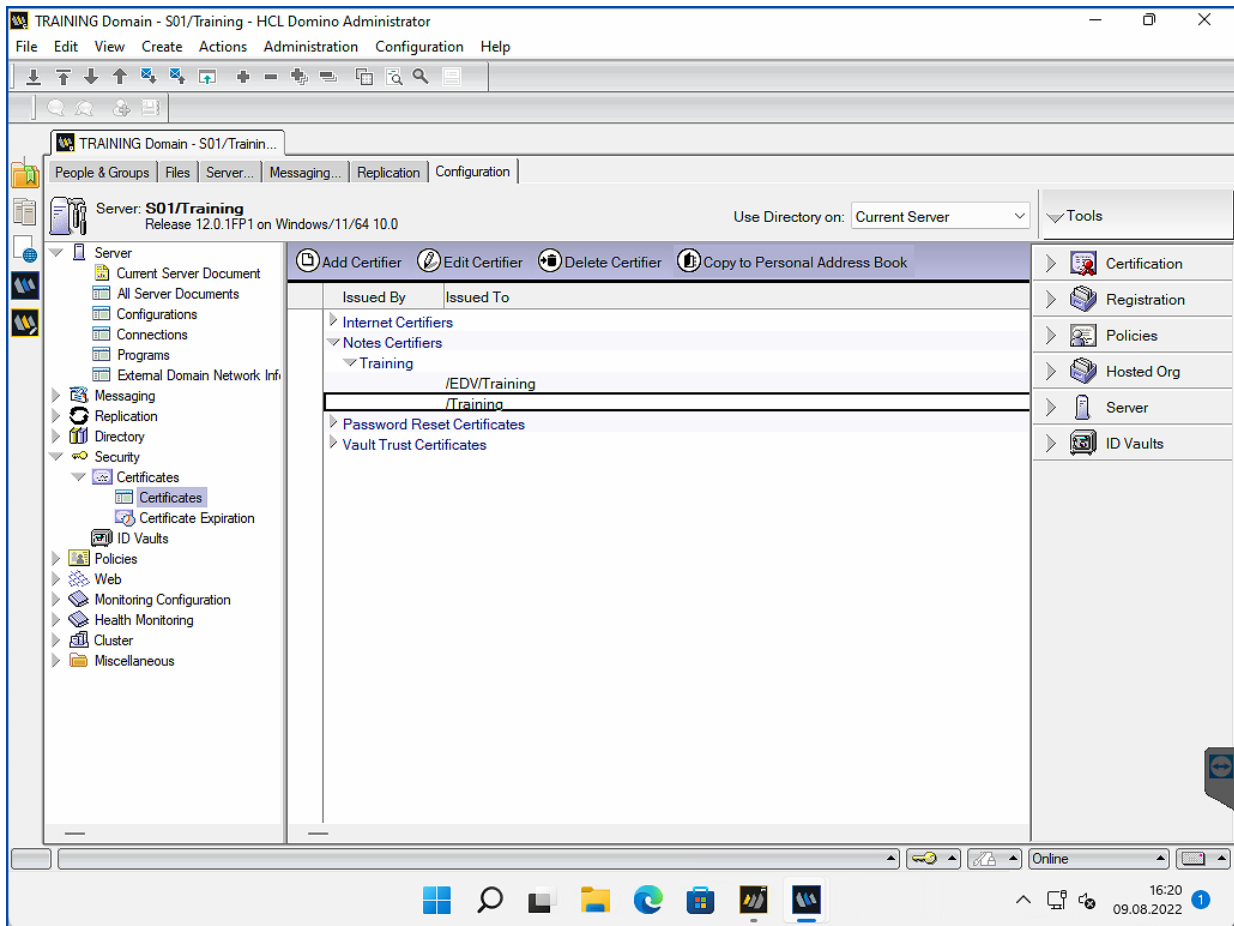
The following terms and possible abbreviations are used in this documentation.

- **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 (O)**
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.

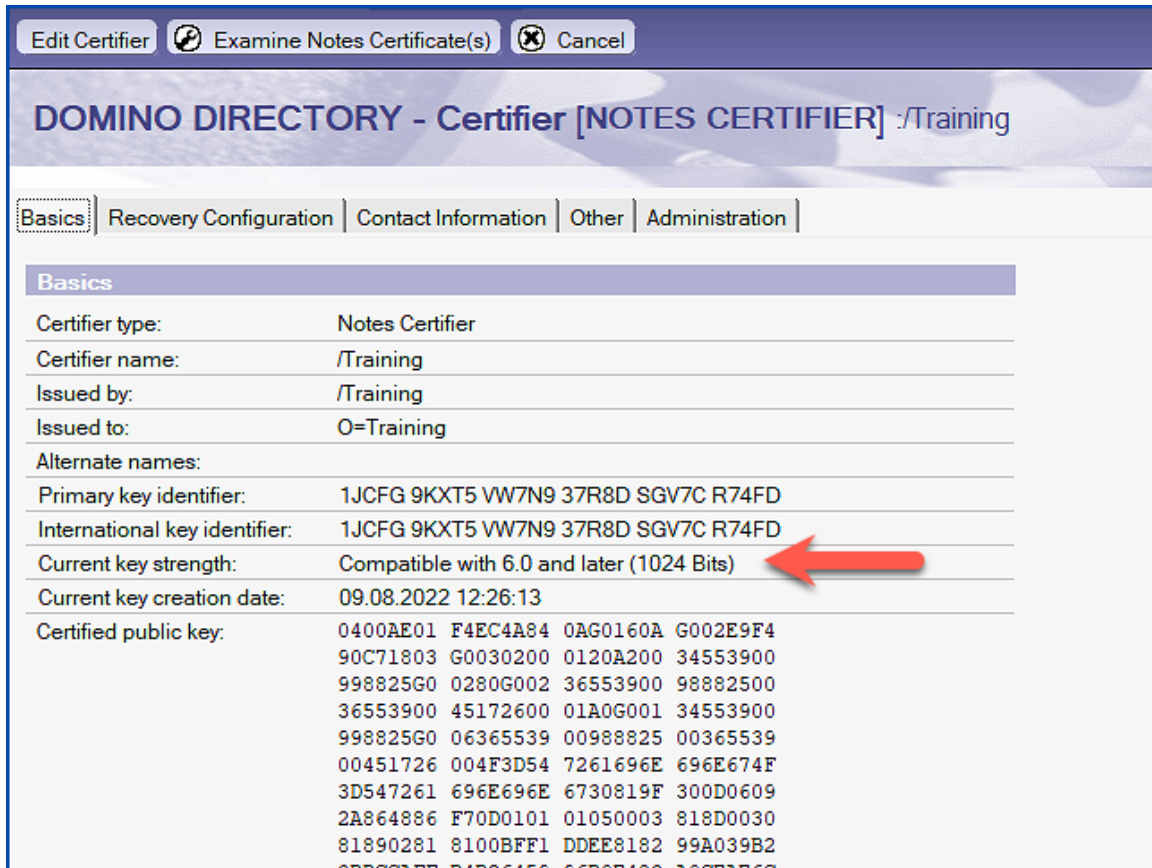
2.2. Verification of certificates at the level: Organization

2.2.1. In Domino Directory

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



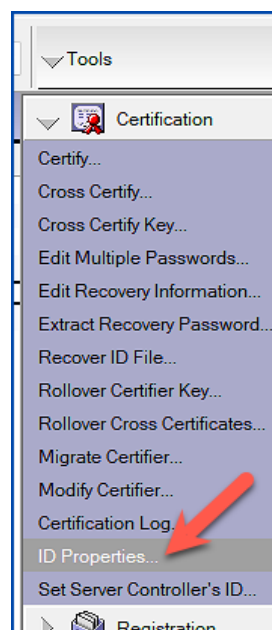
Select the certifier's document at the top level (in the example: /Training) in the »Notes Certifiers« category and open the document with a double-click.



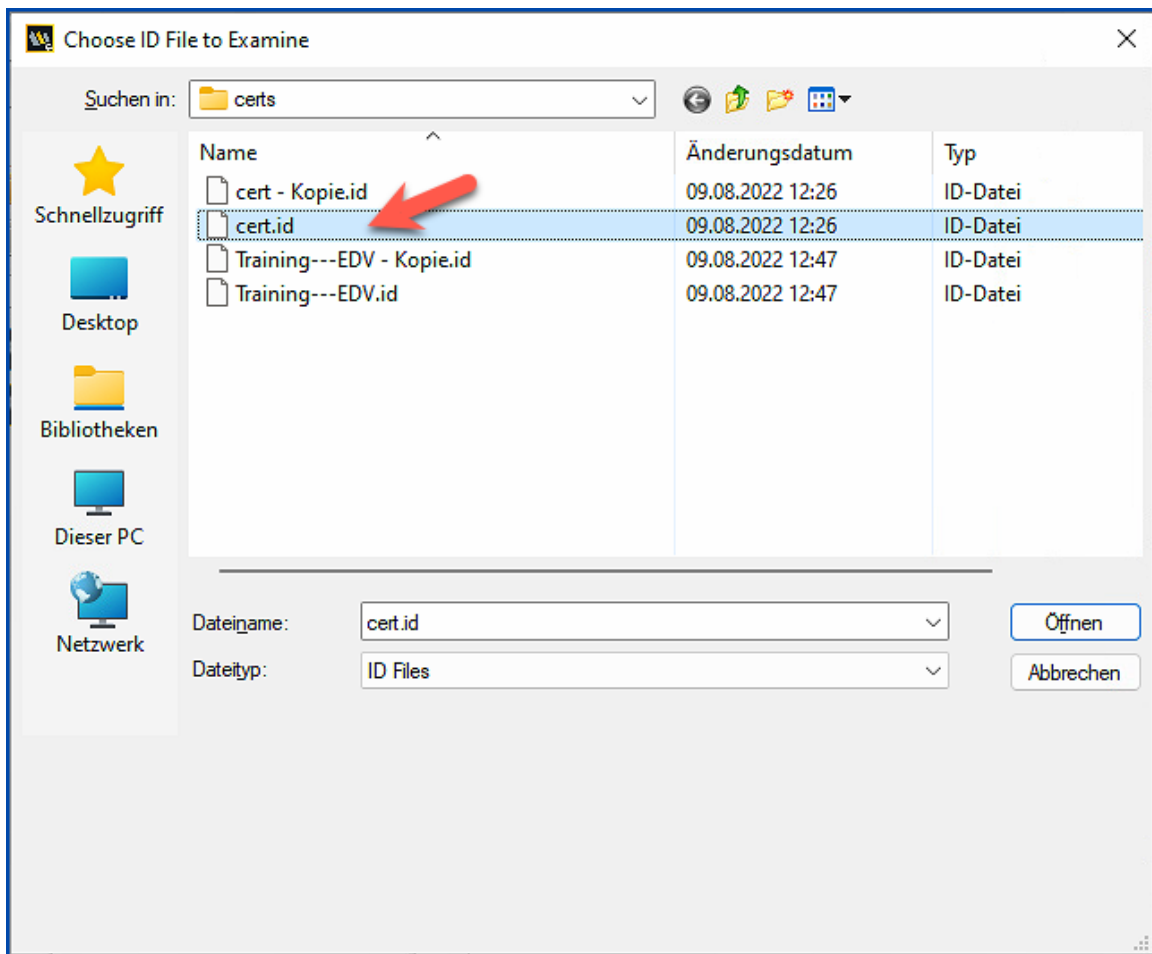
The »Current key strength« field displays the current length of the key.

2.2.2. By Certifier ID

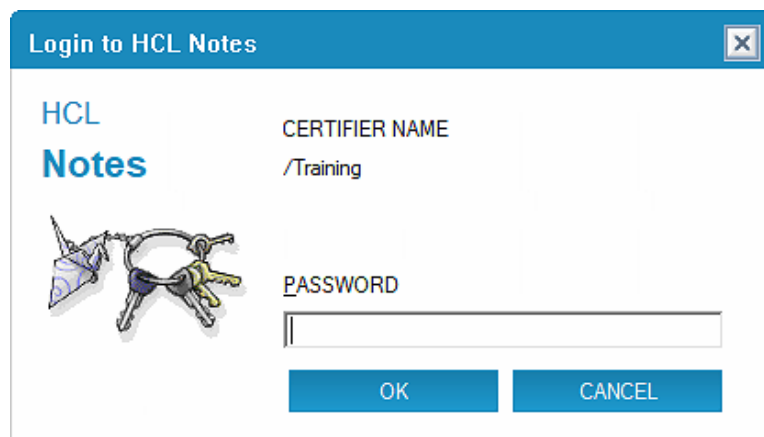
In Domino Administrator, open the »Configuration« tab and select the »Certification« tool on the right.



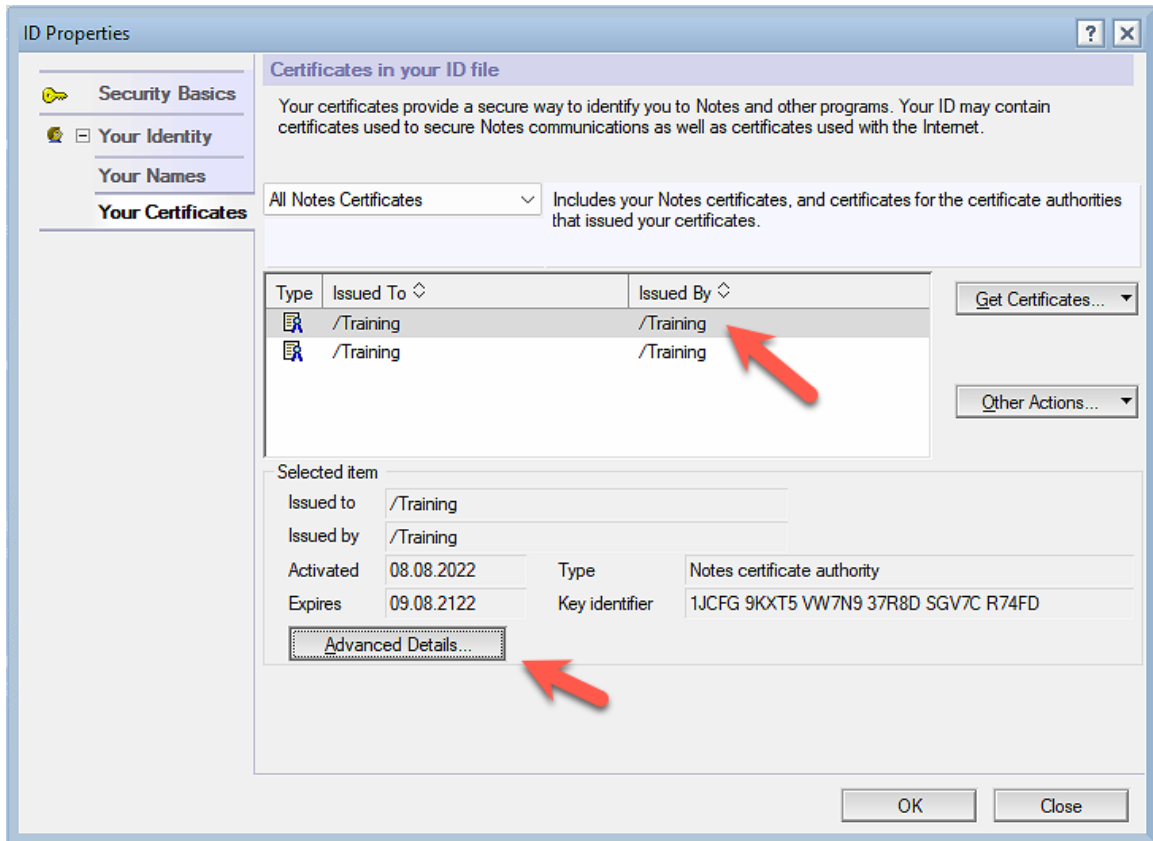
Click on »ID Properties...«.



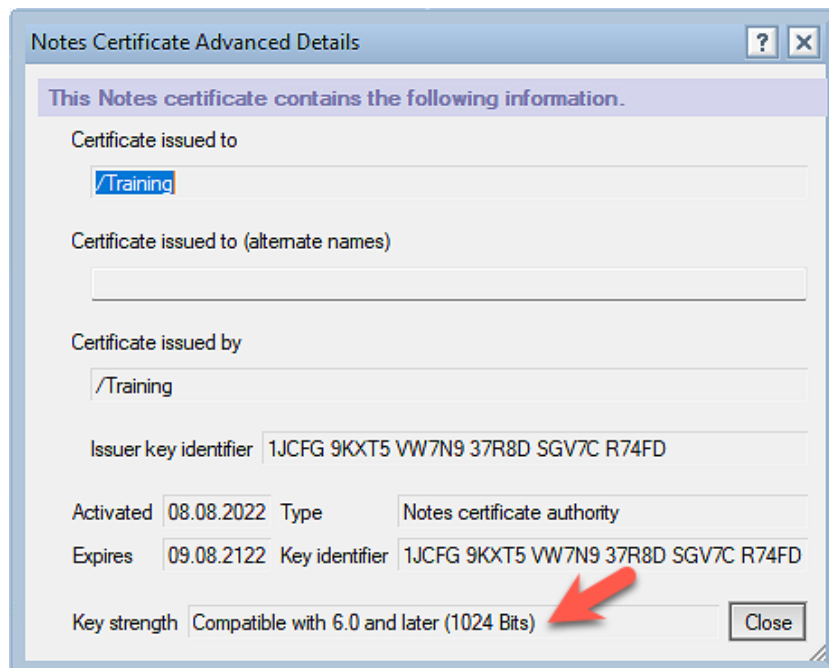
Select the desired certifier and confirm the dialog with »Open« (Öffnen).



Enter the password and confirm the dialog by clicking »OK«.



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



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

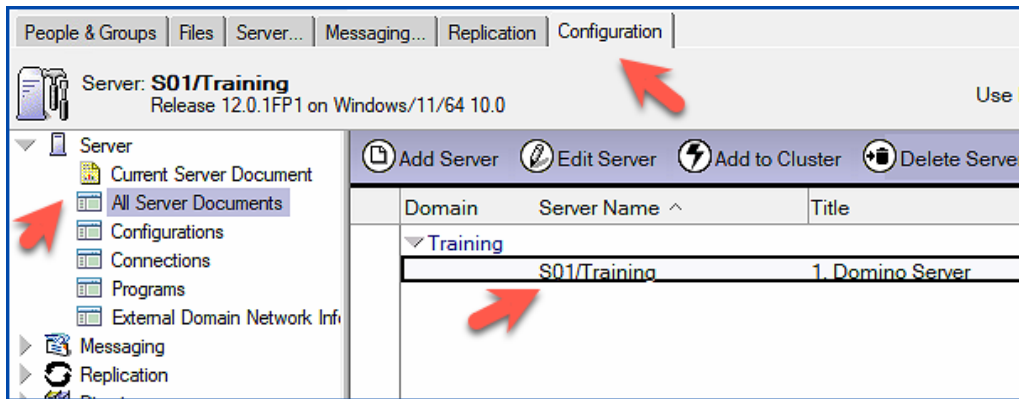
Verification of a certifier at the »Organizational Unit« level is no different from verification of a certifier at the »Organization« level.

You can find all the information in the chapter: [By certifier ID](#) on page 10.

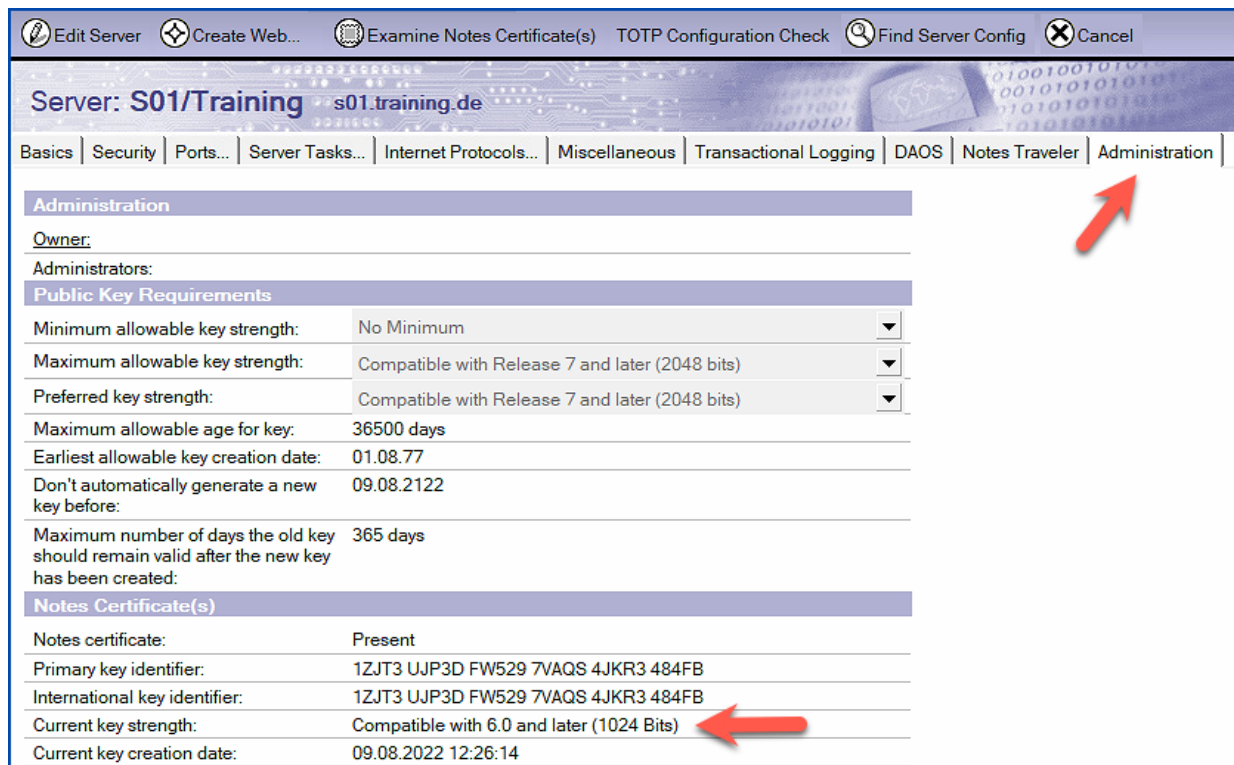
2.4. Verification of Domino Server certificates

2.4.1. In Domino Directory

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



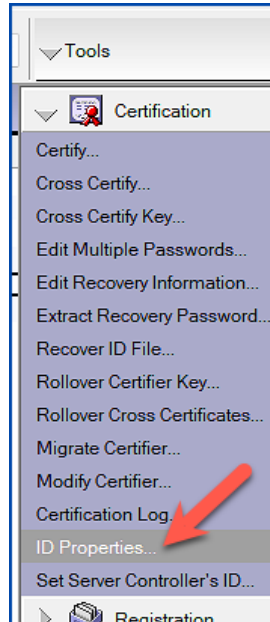
Open the desired server document with a double click.



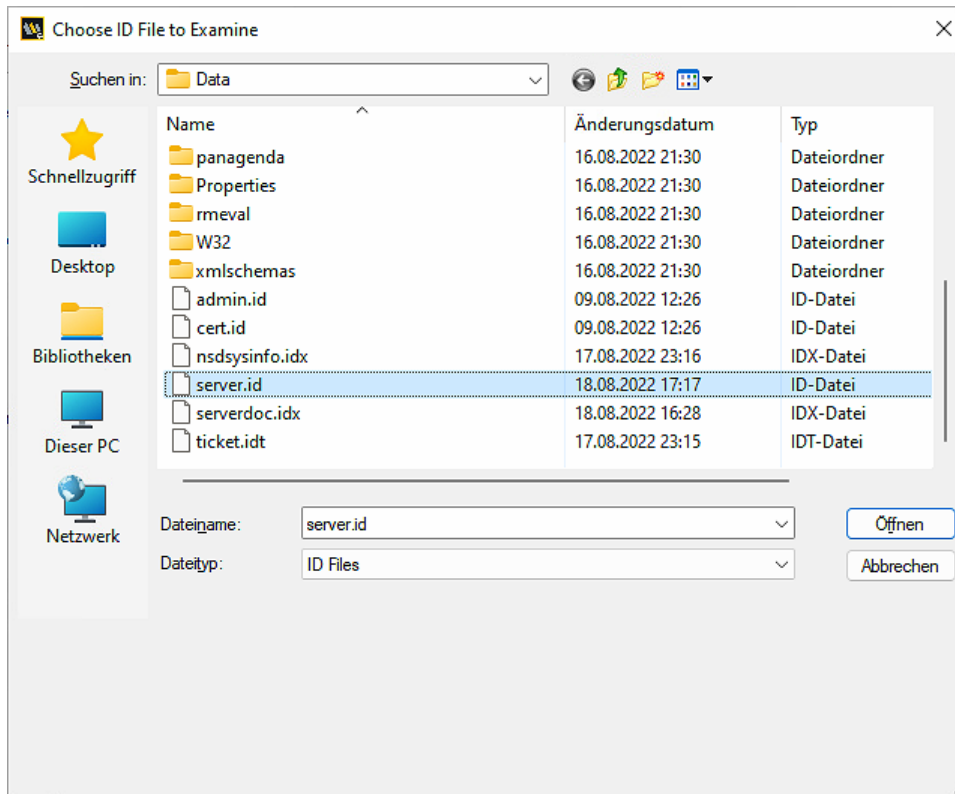
On the »Administration« tab you will see the current key length.

2.4.2. By Server ID

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

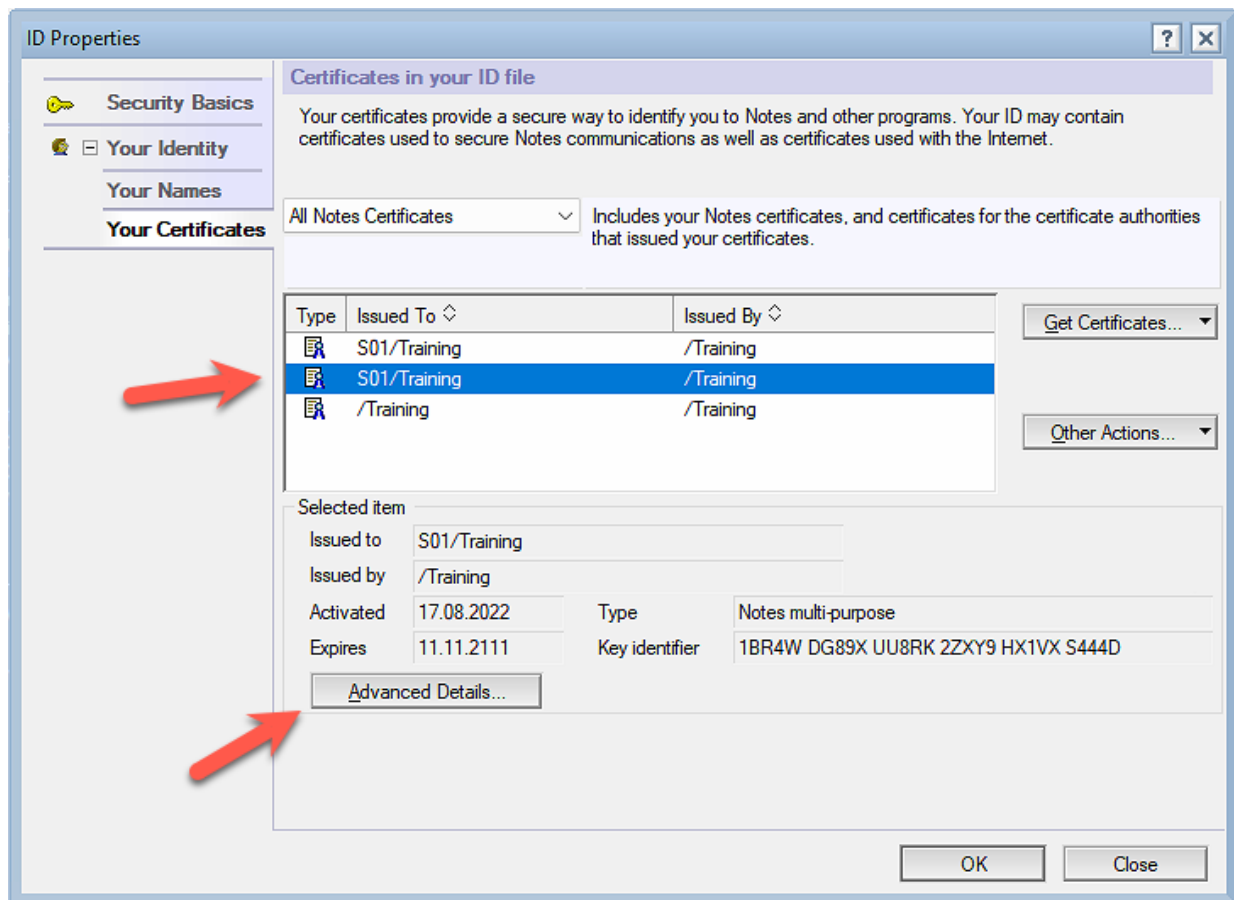


Click on »ID Properties...«.

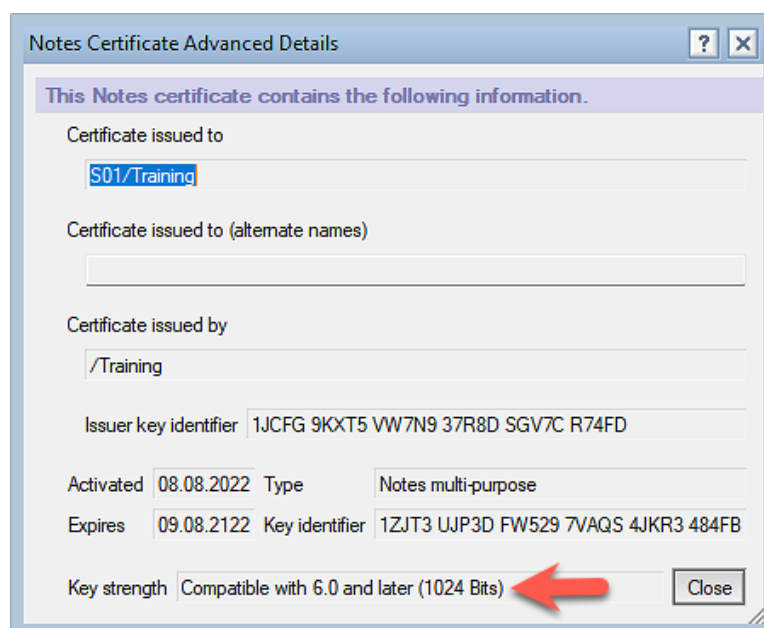


Select the desired server ID and confirm the dialog by clicking »Open« (Öffnen).

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



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

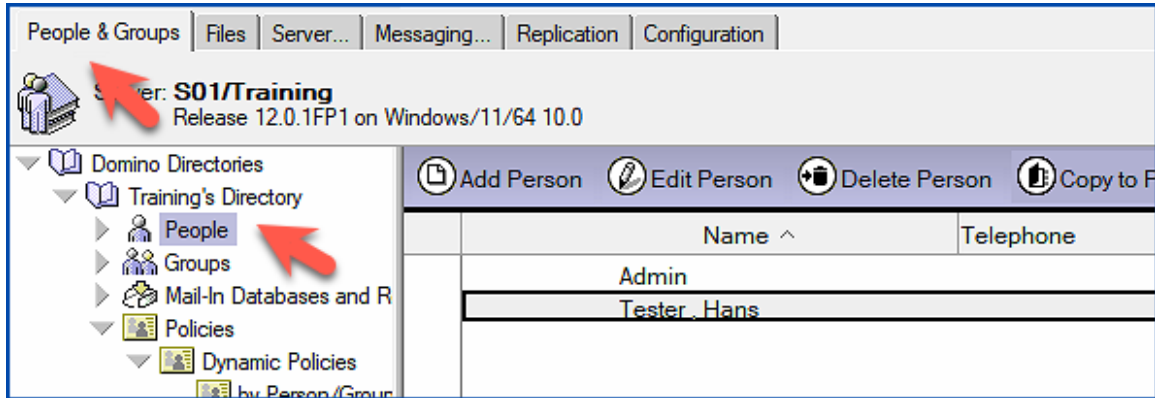


The current key length is displayed in the »Key strength« field.

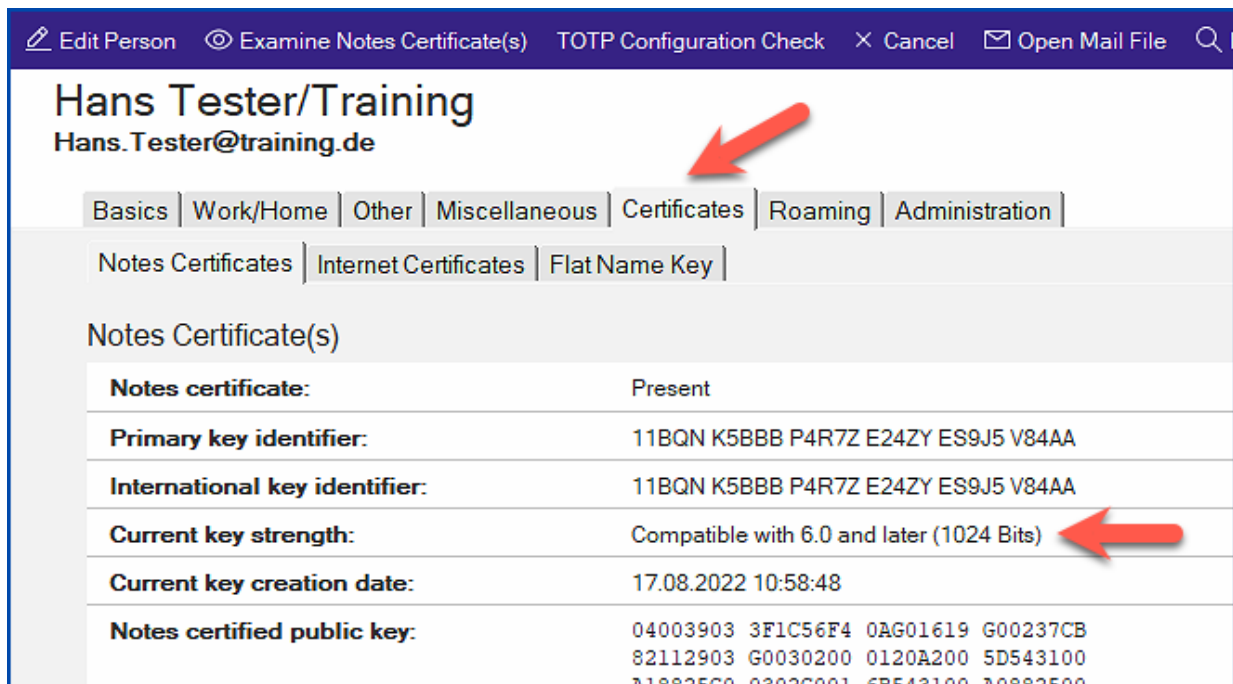
2.5. Verification of Notes user certificates

2.5.1. In Domino Directory

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



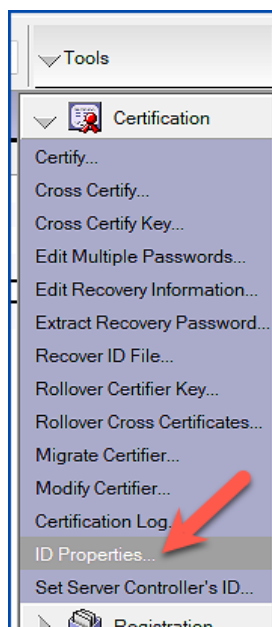
Open the desired person document with a double click.



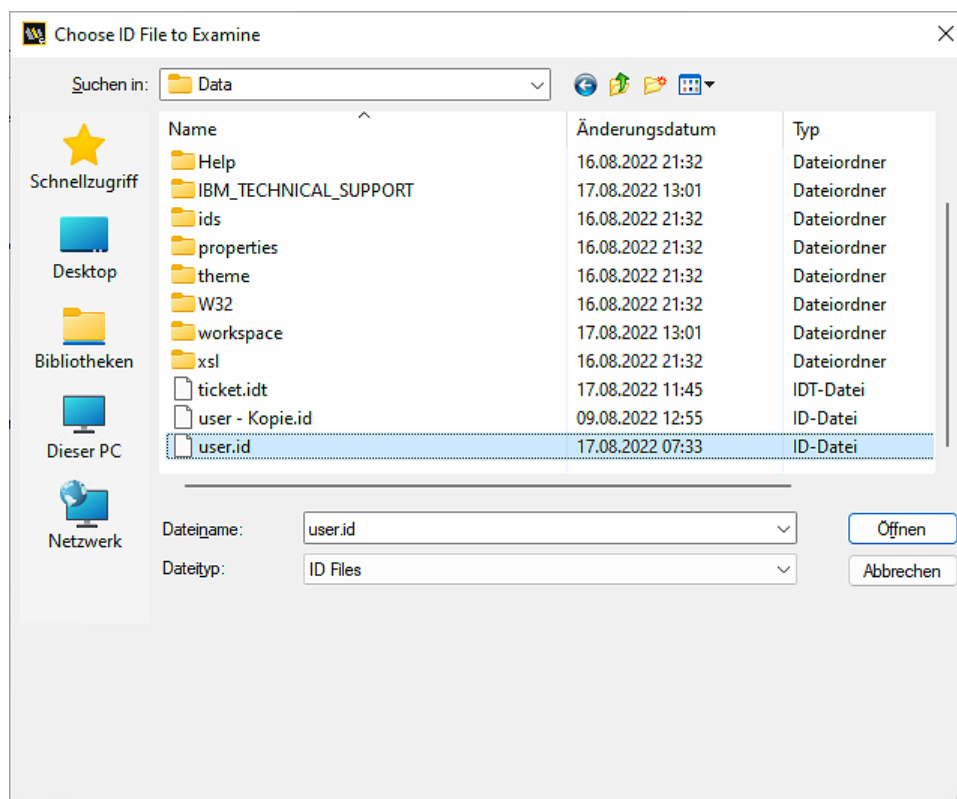
On the »Administration« tab you will see the current key length.

2.5.2. By User ID

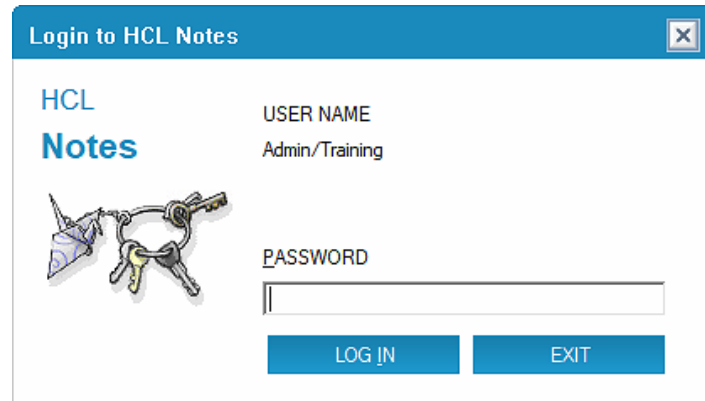
In the Domino Administrator, open the »Configuration« tab and select »Tools« → »Certification« on the right.



Click on »ID Properties...«.



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



Login to HCL Notes

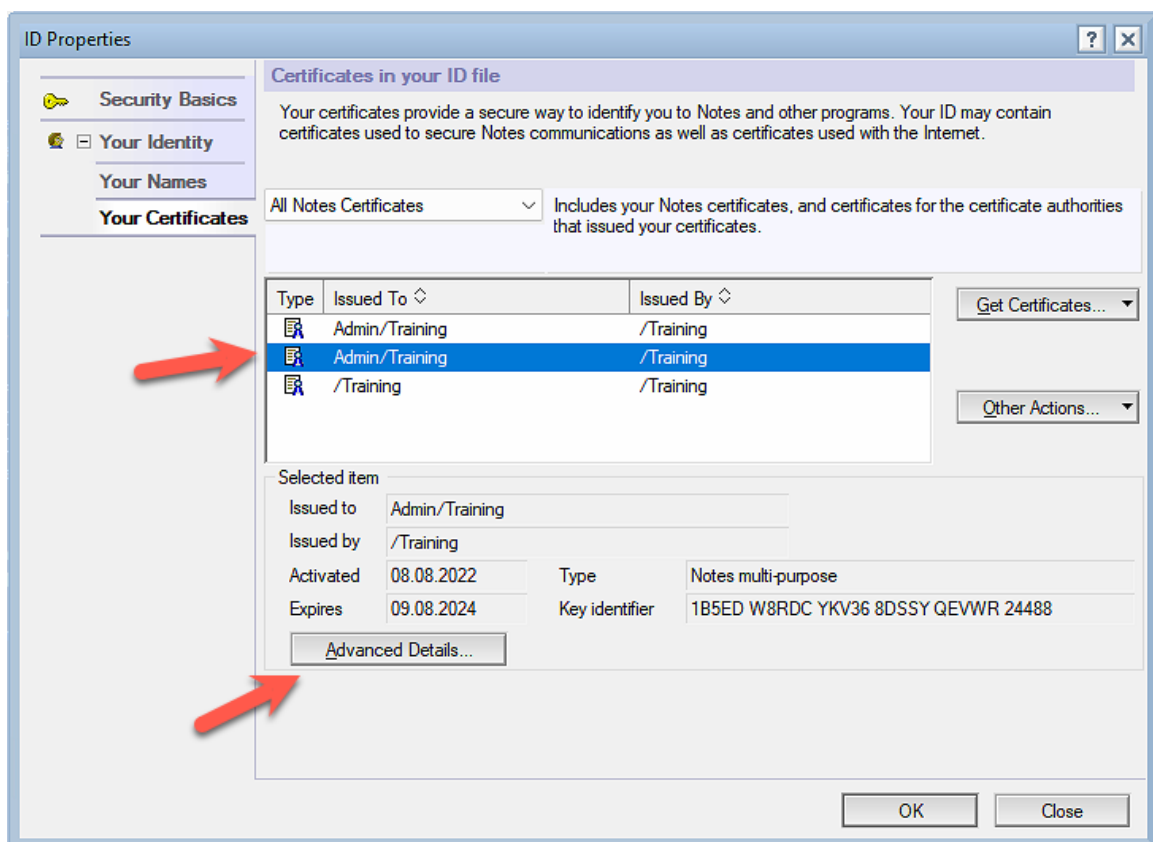
HCL
Notes

USER NAME
Admin/Training

PASSWORD

LOG IN EXIT

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



ID Properties

Security Basics
Your Identity
Your Names
Your Certificates

Certificates in your ID file

Your certificates provide a secure way to identify you to Notes and other programs. Your ID may contain certificates used to secure Notes communications as well as certificates used with the Internet.

All Notes Certificates Includes your Notes certificates, and certificates for the certificate authorities that issued your certificates.

Type	Issued To	Issued By
	Admin/Training	/Training
	Admin/Training	/Training
	/Training	/Training

Get Certificates...
Other Actions...

Selected item

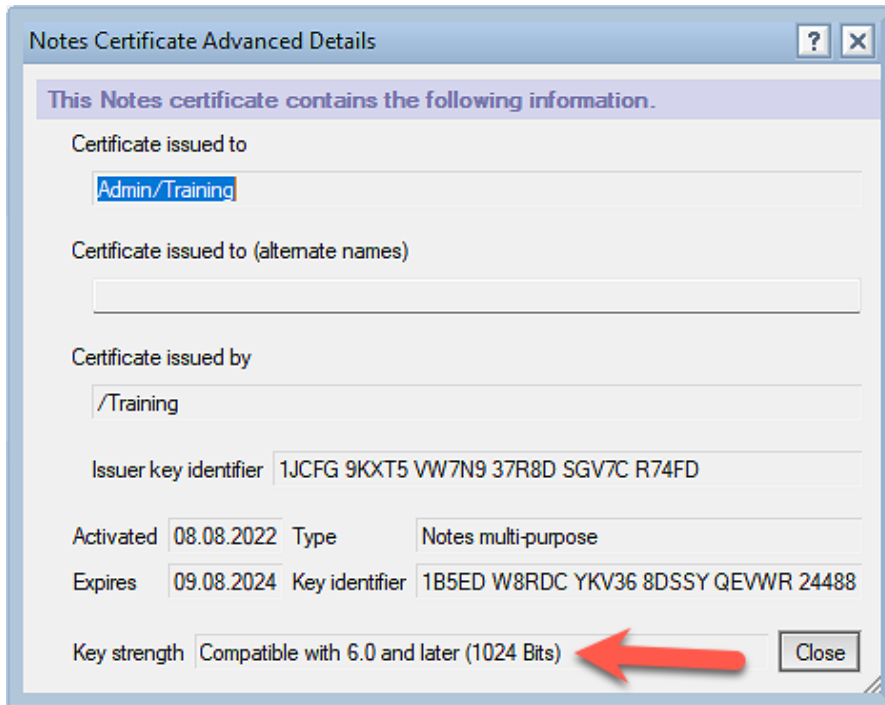
Issued to	Admin/Training	Type	Notes multi-purpose
Issued by	/Training	Key identifier	1B5ED W8RDC YKV36 8DSSY QEVR 24488
Activated	08.08.2022		
Expires	09.08.2024		

Advanced Details...

OK Close

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

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



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.

- **O, OU, 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 Control 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)