HCL Domino

# Certificates Key Rollover

Ein detaillierter Leitfaden für Domino Administratoren

Autor
Manfred Dillmann

# Inhaltsverzeichnis

# 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



**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 (O)**
  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.

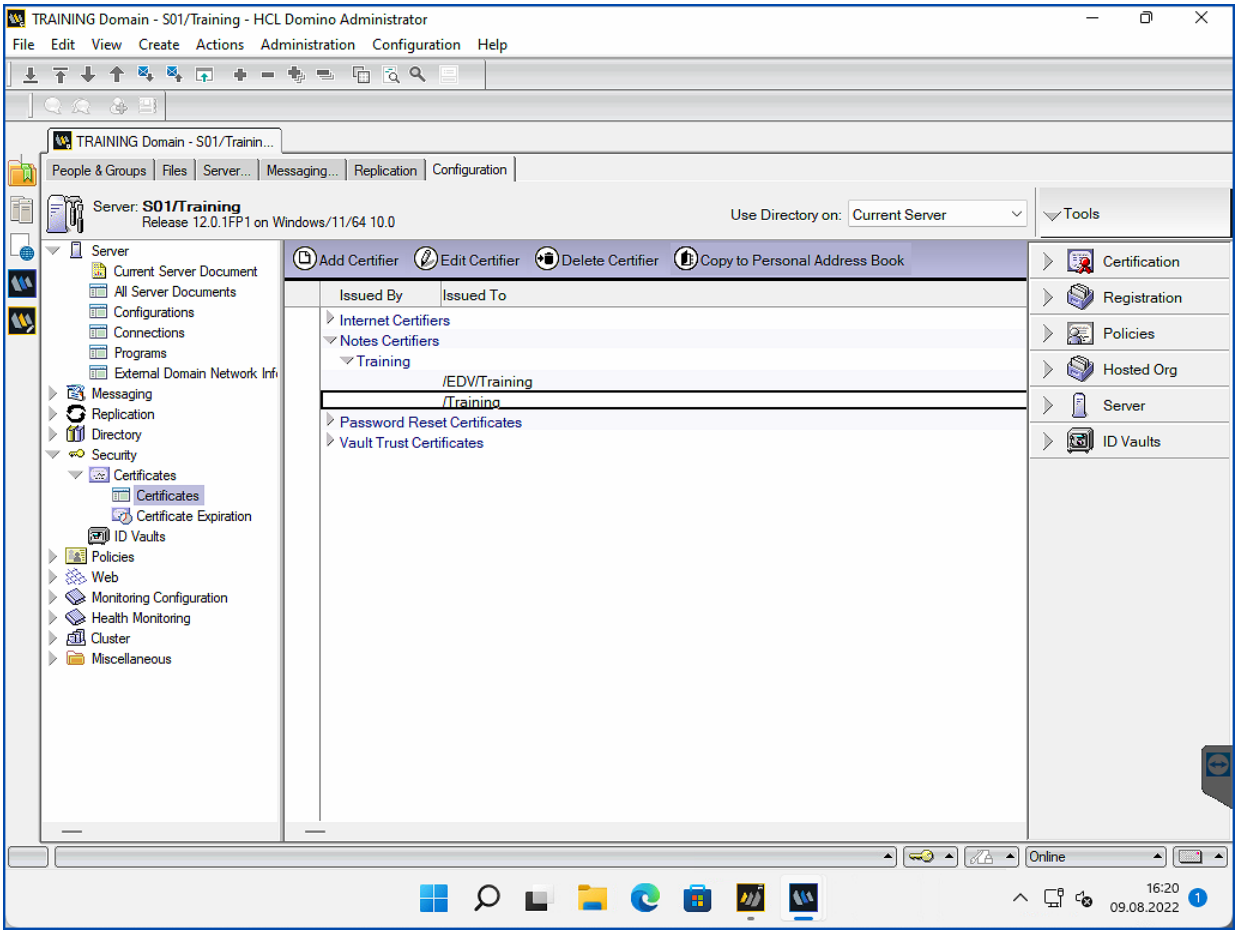
- **Recertify**
  Die Verlängerung der ID eines Anwenders, um zu verhindern, dass sie abläuft.

- **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.

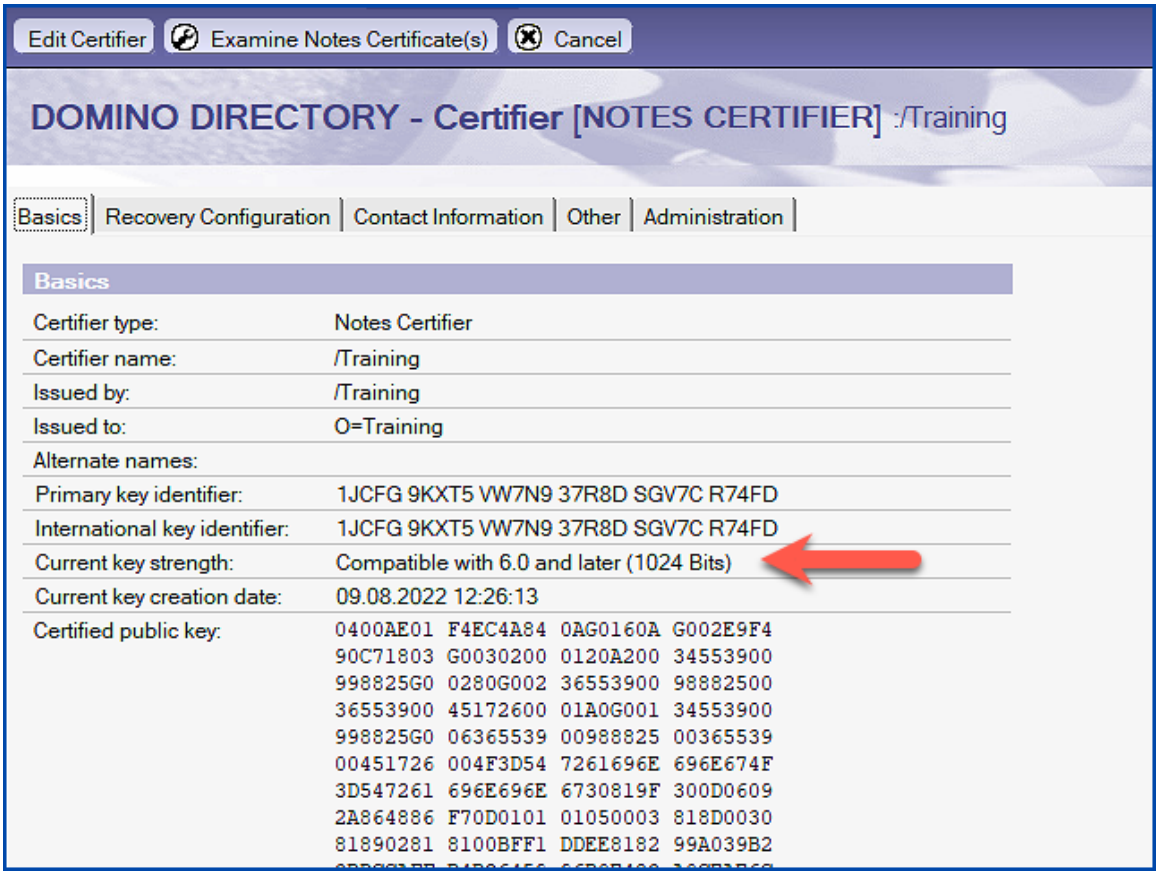
## 2.2. Überprüfung der Zertifikate auf der Ebene: Organisation

### 2.2.1. Im Domino Directory

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



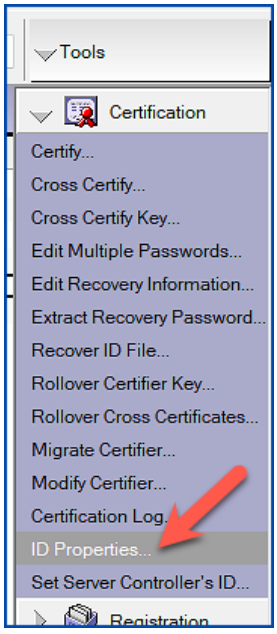

Wählen Sie das Dokument des Zertifizierers auf der obersten Ebene (im Beispiel: /Training) in der Kategorie »Notes Certifiers« und öffnen Sie das Dokument mit einem Doppelklick.



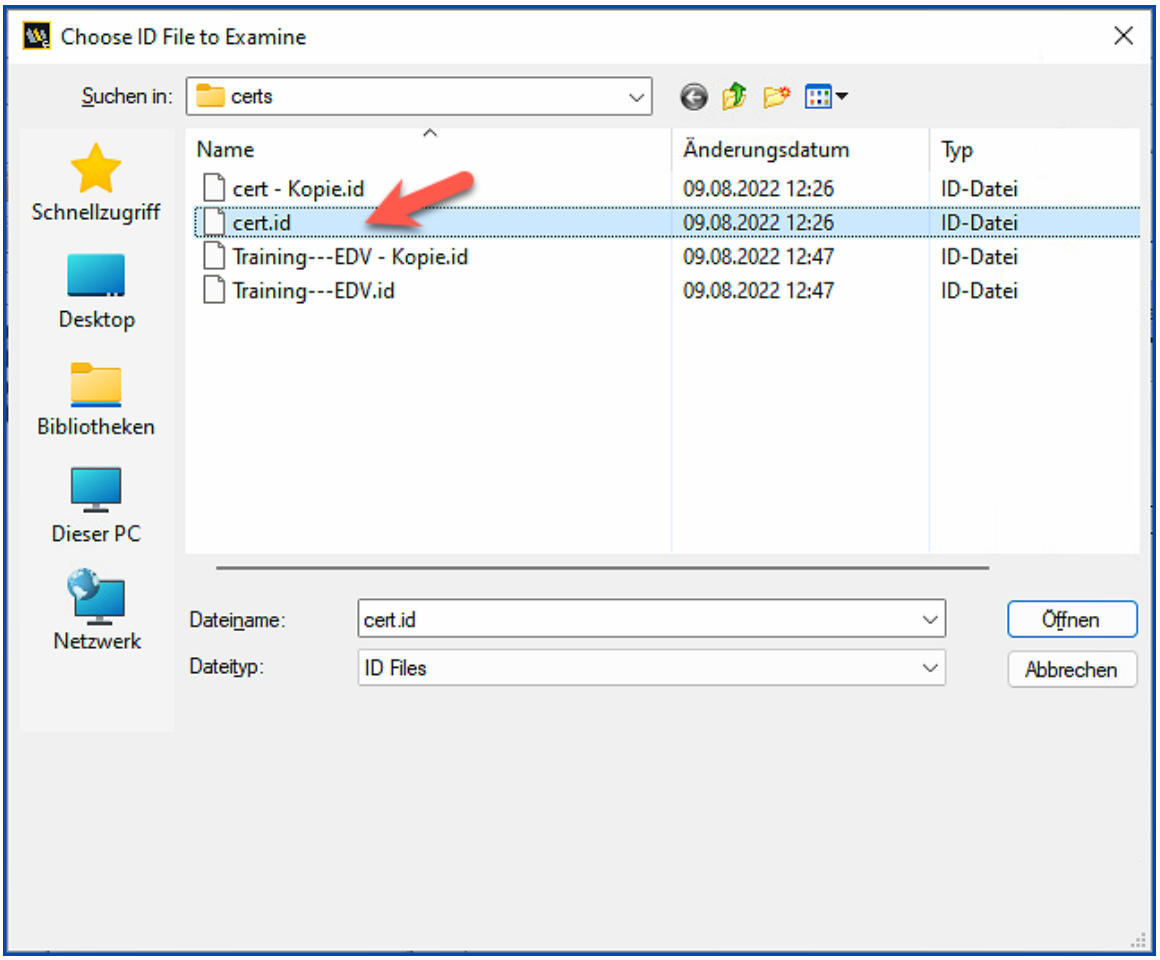

Im Feld »Current key strength« wird die aktuelle Länge des Schlüssels angezeigt.

## 2.2.2. Durch die Zertifizierer-ID

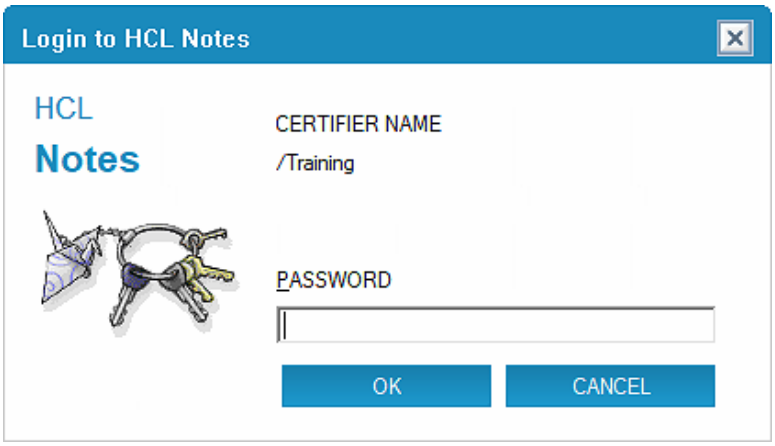
Öffnen Sie im Domino Administrator den Tab »Configuration« und selektieren Sie rechts das Tool »Certification«.



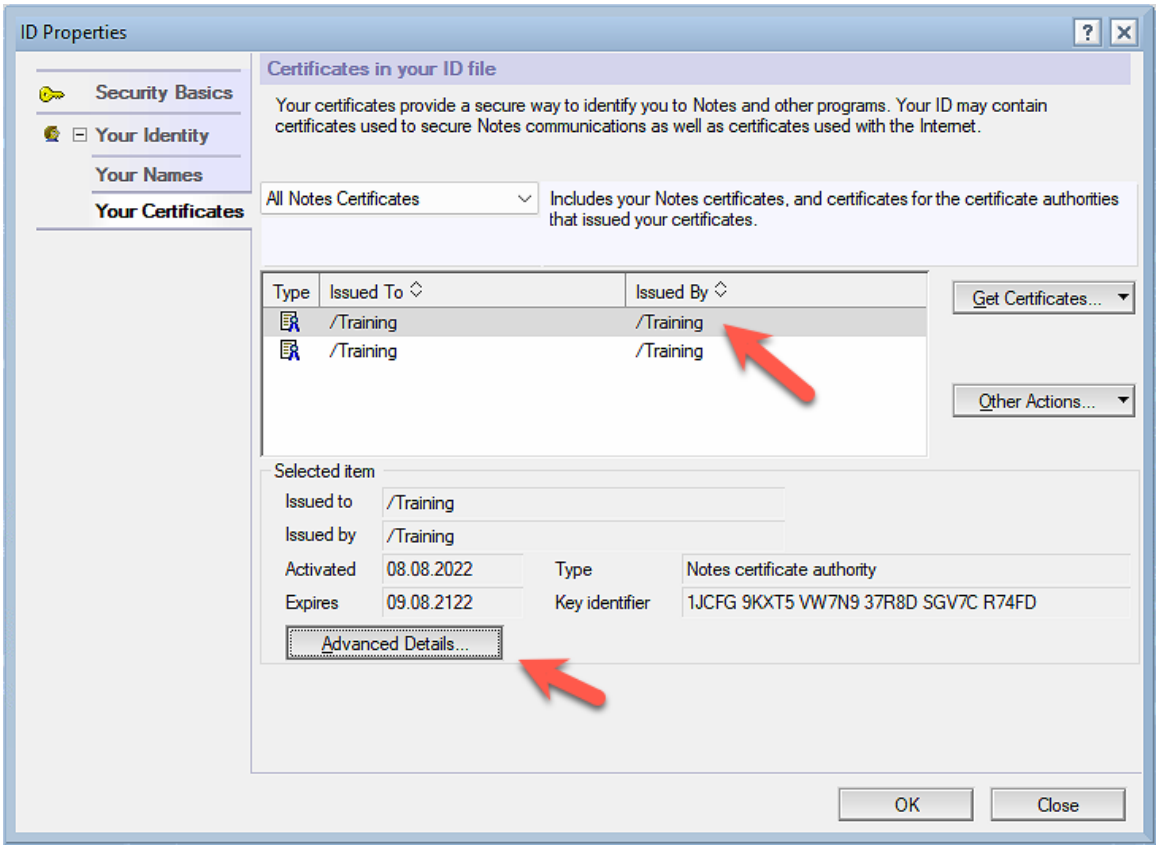
Klicken Sie auf »ID Properties…«.



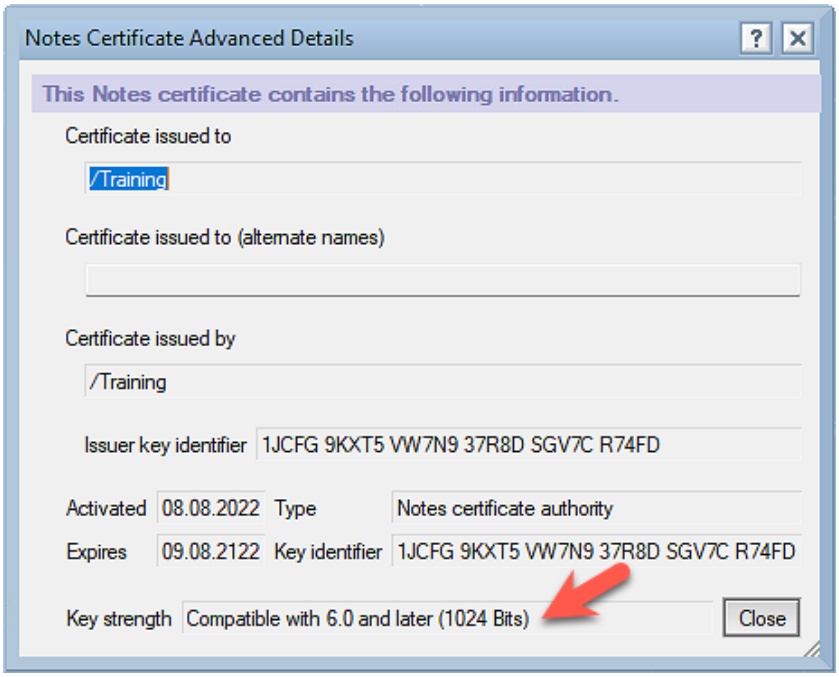

Selektieren Sie den gewünschten Zertifizierer und bestätigen Sie den Dialog mit »Öffnen«.




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




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…«.




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

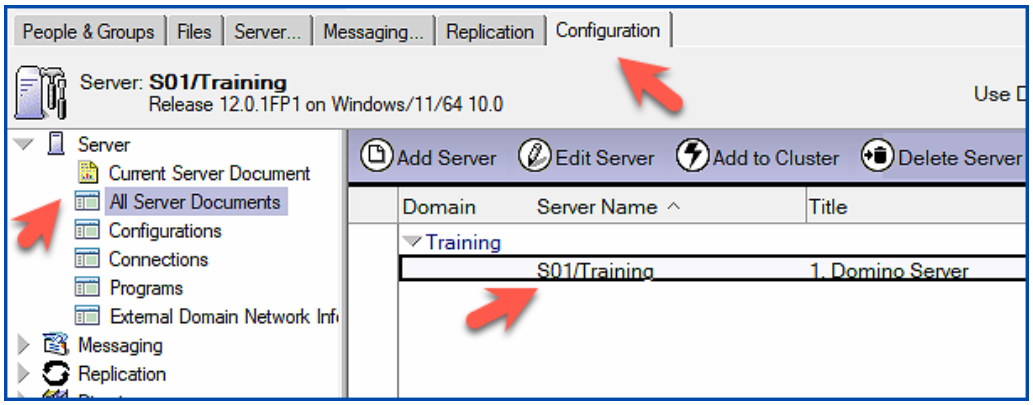
Die Überprüfung eines Zertifizierers auf der Ebene »Abteilung« unterscheidet sich nicht von Überprüfung eines Zertifizierers auf der Ebene »Organisation«.

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

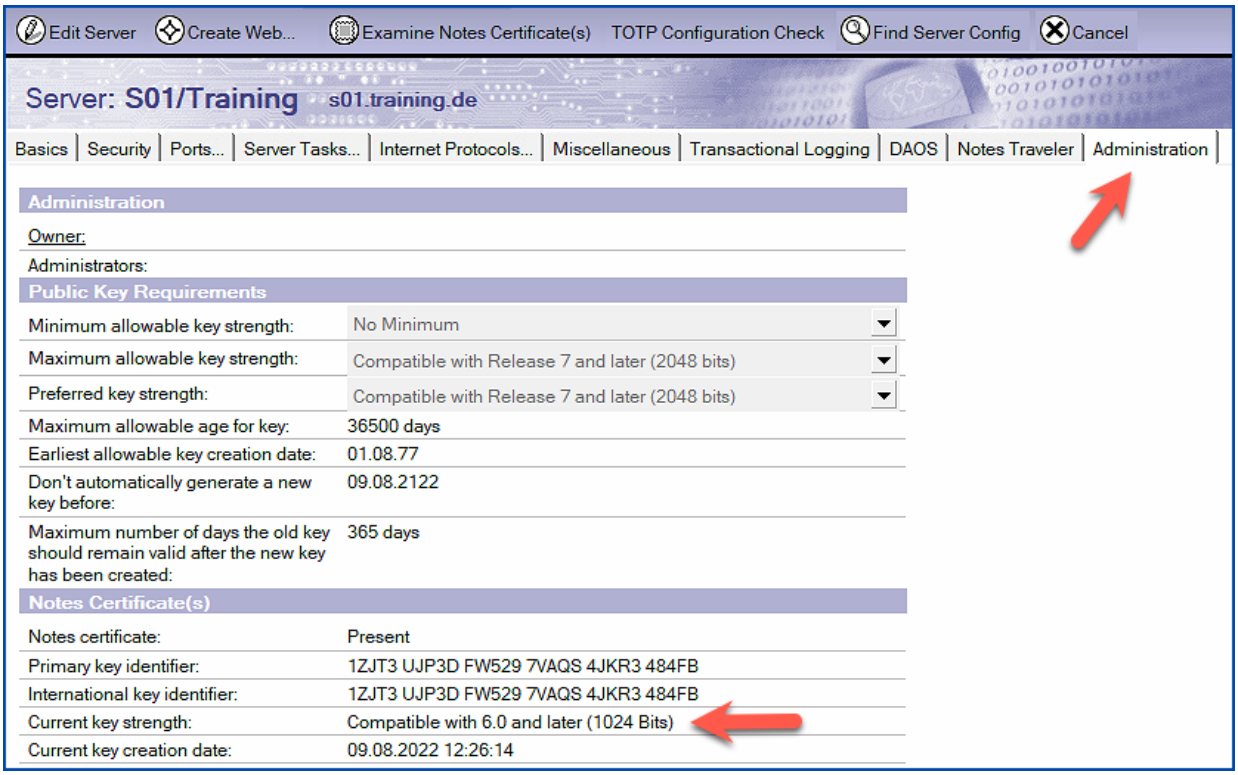
## 2.4. Überprüfung der Zertifikate eines Domino Servers

### 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«.



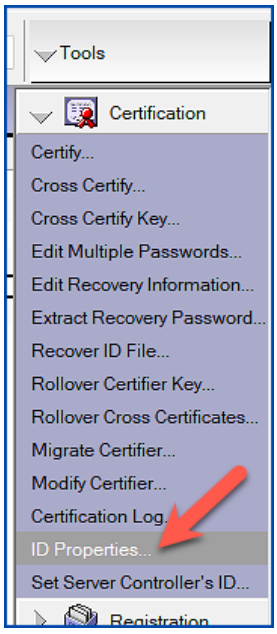

Öffnen Sie das gewünschte Serverdokument mit einem Doppelklick.



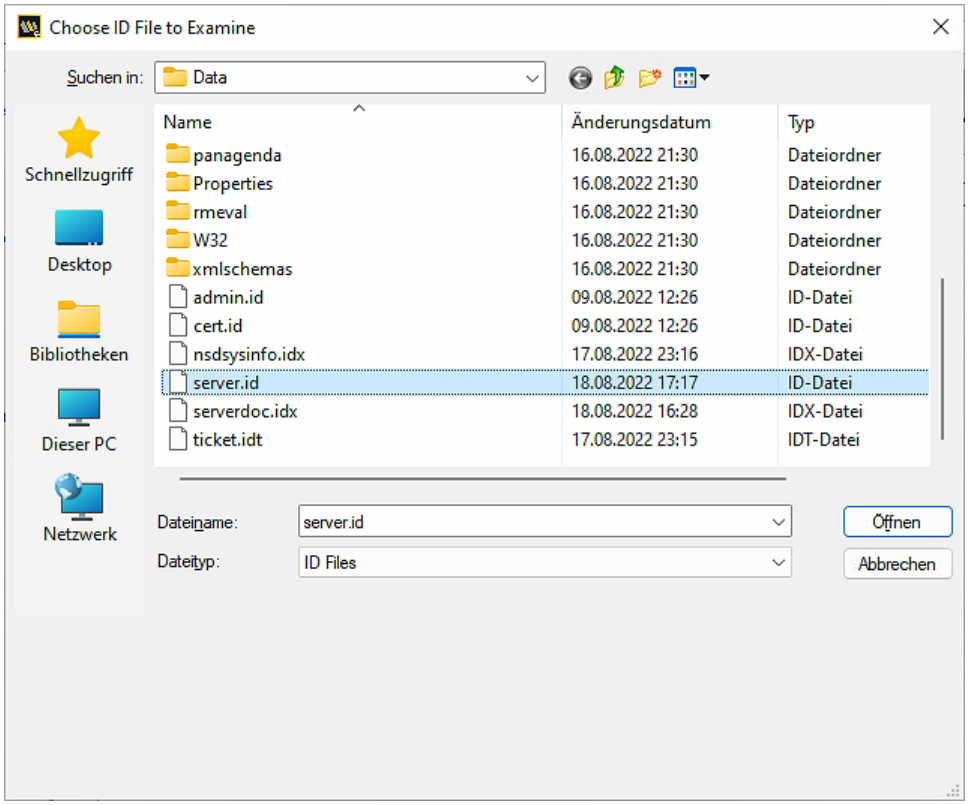

Auf dem Tab »Administration« wird Ihnen die aktuelle Schlüssellänge angezeigt.

## 2.4.2. Durch die Server-ID

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

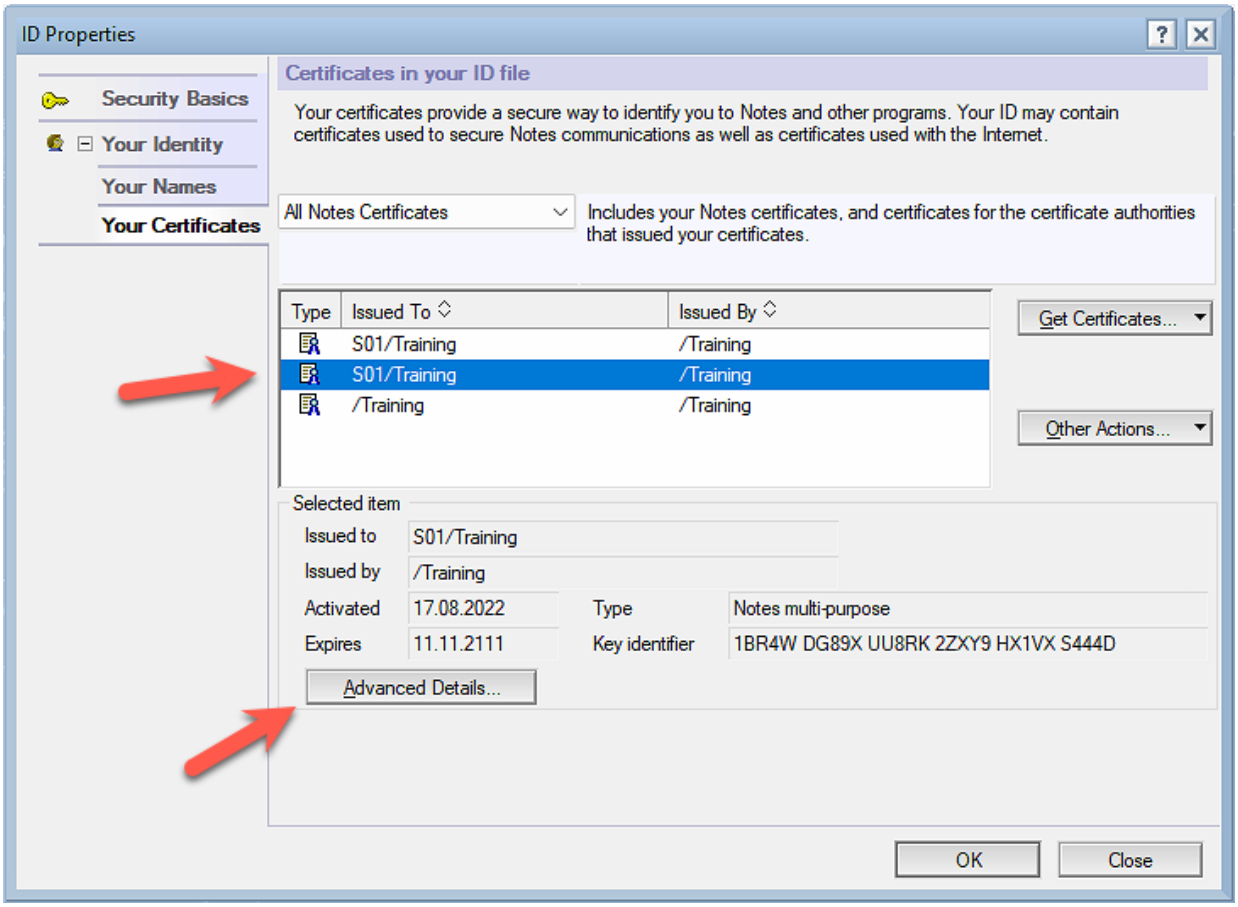



Klicken Sie auf »ID Properties…«.

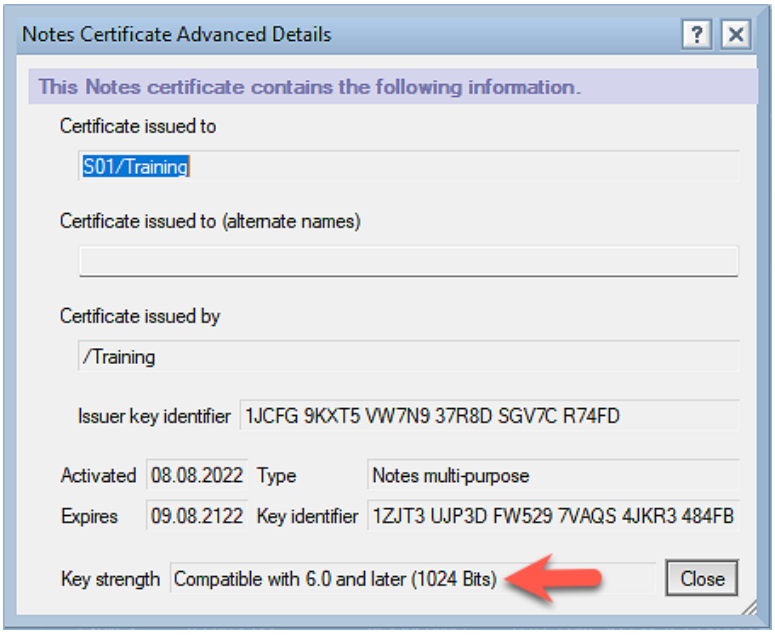



Selektieren Sie die gewünschte Server-ID und bestätigen Sie den Dialog durch »Öffnen«.

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…«.

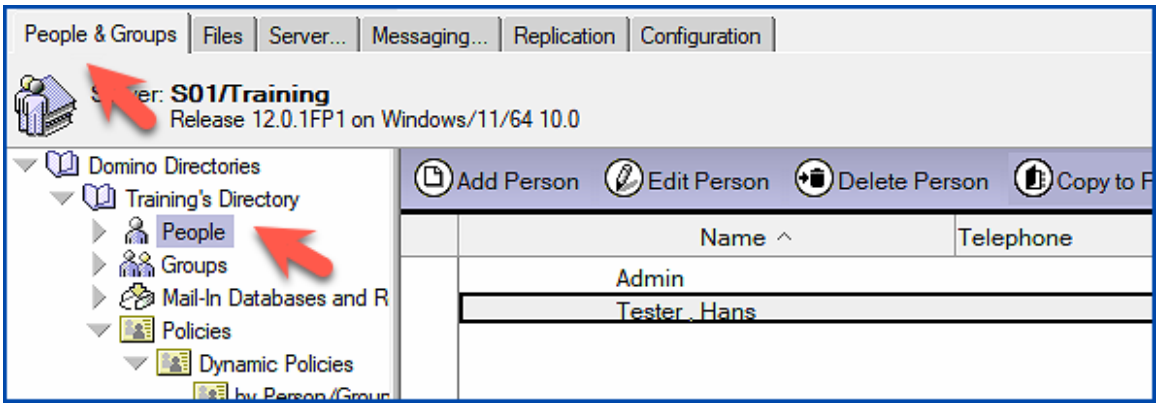



Im Feld »Key strength« wird die aktuelle Schlüssellänge angezeigt.

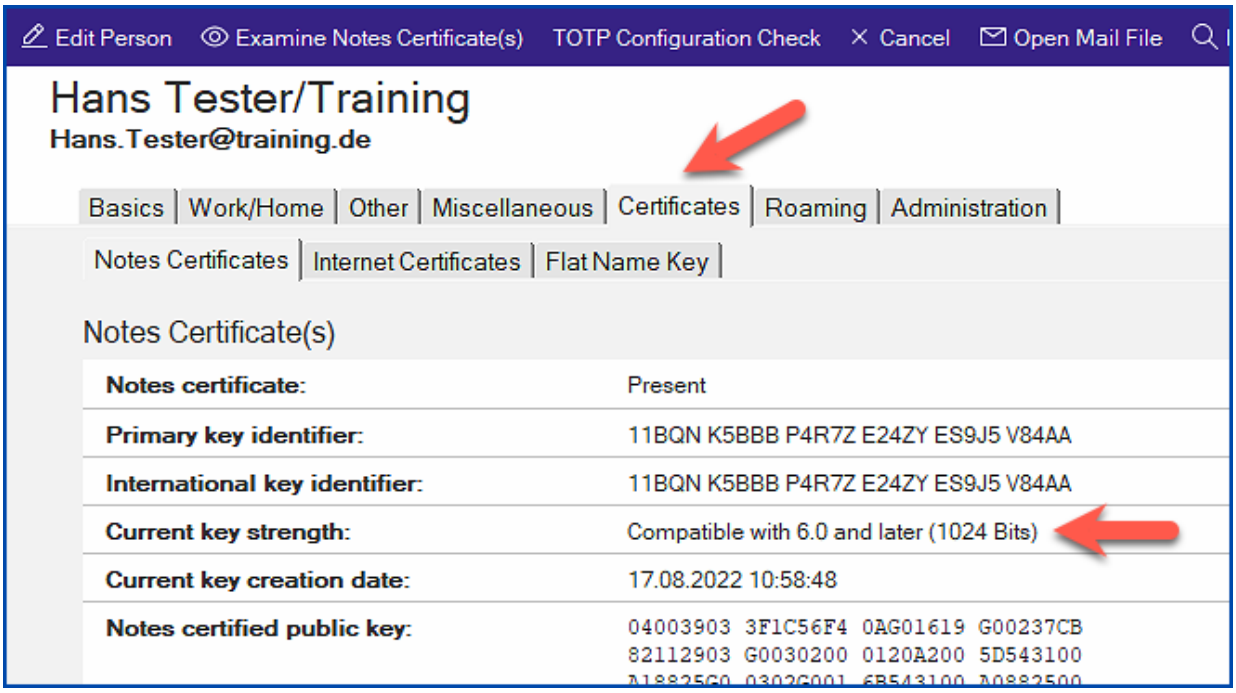
## 2.5. Überprüfung der Zertifikate eines Notes Anwenders

### 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« ➜ »Training's Directory« ➜ »People«.



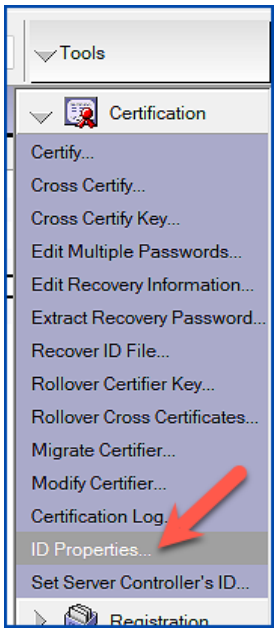

Öffnen Sie das gewünschte Personendokument mit einem Doppelklick.



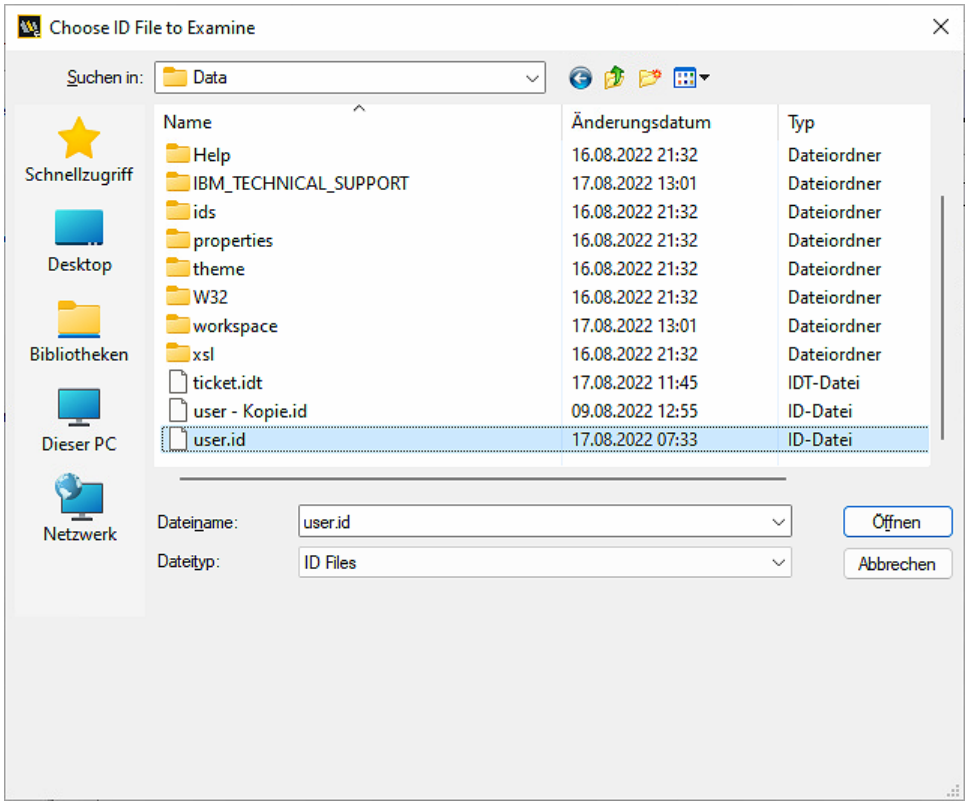

Auf dem Tab »Administration« wird Ihnen die aktuelle Schlüssellänge angezeigt.

## 2.5.2. Durch die User-ID

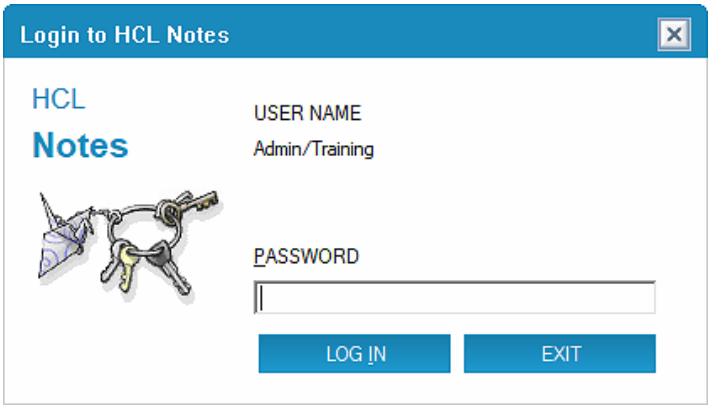
Öffnen Sie im Domino Administrator den Tab »Configuration« und selektieren Sie rechts »Tools« ➜ »Certification«.



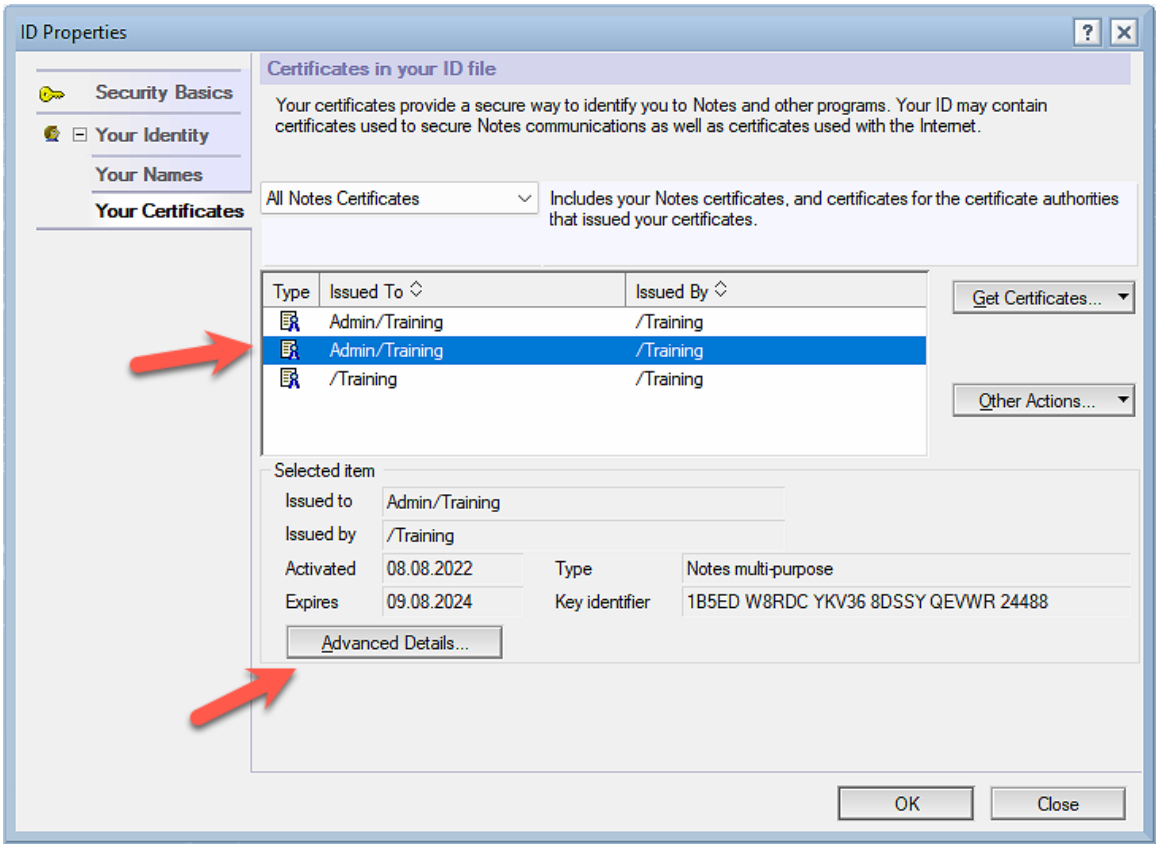

Klicken Sie auf »ID Properties…«.




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

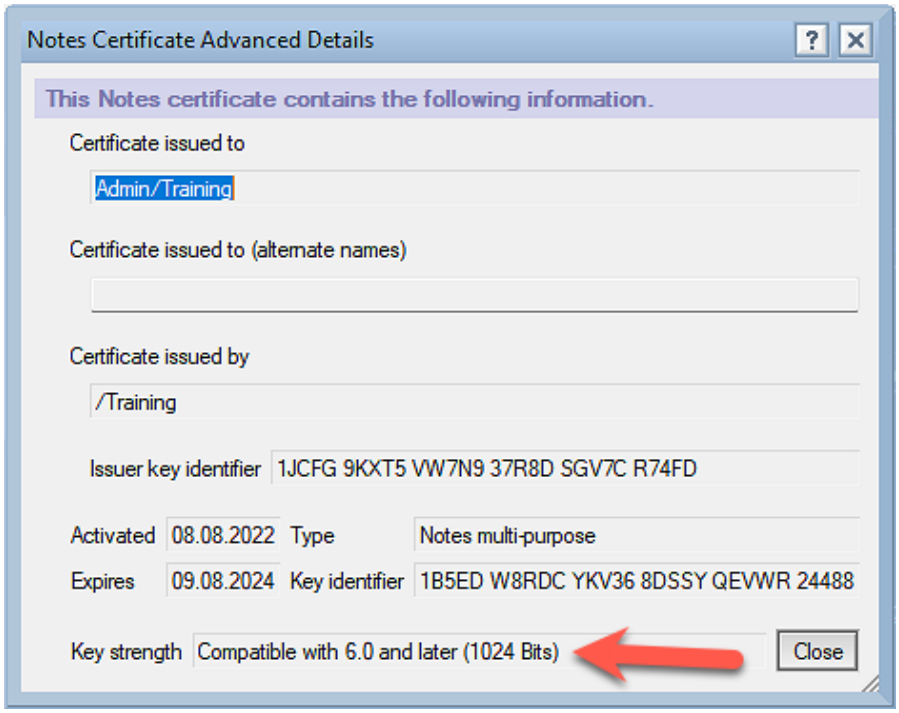



Geben Sie das Passwort ein und bestätigen Sie den Dialog durch die Schaltfläche »LOG IN«.




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…«.




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.