



HCL Domino

# Certificates Key Rollover

A detailed guide for Domino Administrators

Author  
Manfred Dillmann

# Table of contents

<b>1. Introduction</b>	4
1.1. Motivation	5
1.2. Legal hints	6
<b>2. Terms and the status quo</b>	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
<b>3. Key Rollover Introduction</b>	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
<b>4. Organization key rollover (O)</b>	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
<b>5. Organizational Units key rollover (OUs)</b>	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
<b>6. Domino Server key rollover</b>	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

<b>7. Notes User key rollover</b>	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
<b>8. ID Vault</b>	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
<b>9. Optional: Create a new ID Vault</b>	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