### Amendment n° 14

<table>
<thead>
<tr>
<th>Section</th>
<th>Issue Date</th>
<th>Amended Section</th>
<th>Amended Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. INTRODUCTION</td>
<td>16-Feb-2009</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. TERMINOLOGY</td>
<td>16-Feb-2009</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. CONTACT DETAILS</td>
<td>06-May-2009</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. CONNECTION TO NM SYSTEMS</td>
<td>06-May-2009</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. TECHNICAL REQUIREMENTS</td>
<td>16-Feb-2009</td>
<td>Browser support for NOP Portal</td>
<td>02-May-2018</td>
</tr>
<tr>
<td>6. INSTALLATION PROCEDURE FOR THE RSA SecurID SOFTWARE TOKEN</td>
<td>16-Feb-2009</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. MAINTAINING ACCURATE SYSTEM TIME SETTINGS</td>
<td>01-Dec-2008</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. REMOVAL OF THE SOFTWARE TOKEN</td>
<td>01-Dec-2008</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. HOW TO USE THE RSA SecurID SOFTWARE TOKEN</td>
<td>06-May-2009</td>
<td>Removed NMIR from list of NM Protected Applications, as new NMIR does not use a token to authenticate.</td>
<td>02-May-2018</td>
</tr>
<tr>
<td>10. MULTIPLE WINDOWS- USERS SHARING A SINGLE DESKTOP</td>
<td>07-Mar-2012</td>
<td>Updated URL to document that explains how to install the software token for multiple users</td>
<td>02-May-2018</td>
</tr>
<tr>
<td>11. SOFTWARE TOKEN EXPIRATION</td>
<td>07-Mar-2012</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Amendment No. 14 of the Network Management Connection Guide**
# Table of Contents

1. **INTRODUCTION** ........................................................................................................ 1-1  
   1.1. Purpose .................................................................................................................. 1-1  
   1.2. Intended Audience .............................................................................................. 1-1  
   1.3. Scope and Applicability ...................................................................................... 1-2  
2. **TERMINOLOGY** ..................................................................................................... 2-1  
   2.1. Note on CFMU/NM renaming ............................................................................. 2-1  
   2.2. Acronyms and Abbreviations .......................................................................... 2-1  
3. **CONTACT DETAILS** ............................................................................................... 3-3  
   3.1. Requesting access to a NM Service or Application ........................................ 3-3  
   3.2. Technical Support .............................................................................................. 3-3  
   3.3. Support from the Network Supplier .................................................................. 3-3  
   3.4. Designating the Customer Contacts ................................................................ 3-4  
4. **CONNECTION TO NM SYSTEMS** ...................................................................... 4-1  
   4.1. Connection Options ........................................................................................... 4-1  
   4.1.1. Extranet ............................................................................................................ 4-1  
   4.1.2. Internet ............................................................................................................. 4-2  
   4.2. Security ............................................................................................................... 4-2  
   4.2.1. Client Authentication ...................................................................................... 4-2  
   4.2.2. Firewalls .......................................................................................................... 4-3  
5. **TECHNICAL REQUIREMENTS** .......................................................................... 5-1  
   5.1. NOP Portal and Central Claim Management System (CCMS-Web) ............. 5-1  
   5.1.1. Browser support for NOP Portal ..................................................................... 5-1  
   5.1.2. Technical prerequisites .................................................................................. 5-3  
   5.2. Network Manager Interactive Reporting (NMIR) ........................................... 5-3  
   5.3. Collaboration Human Machine Interface (CHMI) ........................................... 5-4  
   5.4. Performance ....................................................................................................... 5-4  
6. **INSTALLATION PROCEDURE FOR THE RSA SECURID SOFTWARE TOKEN** .... 6-1  
   6.1. Installation of the RSA Software Token Application ......................................... 6-1  
   6.1.1. Multiple versions of the RSA SecurID Software Token .................................. 6-1  
   6.1.2. Installing RSA SecurID Software Token version 5.0.2 .................................. 6-2  
   6.2. Available Shortcuts .............................................................................................. 6-7  
   6.3. Advanced Setting ................................................................................................. 6-8  
   6.4. Installation of the Token Record ........................................................................ 6-8  

Amendment date: 02 May 2018  
Edition & produced by the Network Manager  
©1995 The European Organisation for the Safety of Air Navigation (EUROCONTROL)
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4.1.</td>
<td>Principles</td>
<td>6-8</td>
</tr>
<tr>
<td>6.4.2.</td>
<td>Token Record File</td>
<td>6-8</td>
</tr>
<tr>
<td>6.4.3.</td>
<td>Installation of Token Records on a PC</td>
<td>6-9</td>
</tr>
<tr>
<td>6.4.3.1.</td>
<td>Installation of Token Record for RSA SecurID version 5.0.2</td>
<td>6-9</td>
</tr>
<tr>
<td>6.4.4.</td>
<td>Enable Token</td>
<td>6-10</td>
</tr>
<tr>
<td>6.4.5.</td>
<td>Create PIN code</td>
<td>6-10</td>
</tr>
<tr>
<td>7.</td>
<td>MAINTAINING ACCURATE SYSTEM TIME SETTINGS</td>
<td>7-1</td>
</tr>
<tr>
<td>8.</td>
<td>REMOVAL OF THE SOFTWARE TOKEN</td>
<td>8-1</td>
</tr>
<tr>
<td>8.1.</td>
<td>Removal of a Token</td>
<td>8-1</td>
</tr>
<tr>
<td>8.2.</td>
<td>Removal of RSA SecurID Program</td>
<td>8-3</td>
</tr>
<tr>
<td>9.</td>
<td>HOW TO USE THE RSA SECURID SOFTWARE TOKEN</td>
<td>9-1</td>
</tr>
<tr>
<td>9.1.</td>
<td>Starting the NM Protected Application</td>
<td>9-1</td>
</tr>
<tr>
<td>9.1.1.</td>
<td>NOP Portal and CCMS-Web</td>
<td>9-1</td>
</tr>
<tr>
<td>9.1.2.</td>
<td>CHMI Application</td>
<td>9-1</td>
</tr>
<tr>
<td>9.1.3.</td>
<td>Login Screen</td>
<td>9-1</td>
</tr>
<tr>
<td>9.2.</td>
<td>Starting the RSA SecurID Software Token Program</td>
<td>9-1</td>
</tr>
<tr>
<td>9.3.</td>
<td>Token Terminology</td>
<td>9-2</td>
</tr>
<tr>
<td>9.3.1.</td>
<td>What is the UserName or UserID?</td>
<td>9-2</td>
</tr>
<tr>
<td>9.3.2.</td>
<td>What is the PIN code?</td>
<td>9-2</td>
</tr>
<tr>
<td>9.3.3.</td>
<td>What is the Tokencode?</td>
<td>9-2</td>
</tr>
<tr>
<td>9.3.4.</td>
<td>What is the Passcode?</td>
<td>9-2</td>
</tr>
<tr>
<td>9.4.</td>
<td>How to Generate your Passcode?</td>
<td>9-3</td>
</tr>
<tr>
<td>9.5.</td>
<td>How to log in to the NM Protected Applications?</td>
<td>9-3</td>
</tr>
<tr>
<td>9.6.</td>
<td>Wrong Log in</td>
<td>9-3</td>
</tr>
<tr>
<td>9.7.</td>
<td>Next Tokencode</td>
<td>9-4</td>
</tr>
<tr>
<td>9.8.</td>
<td>Token Reactivation</td>
<td>9-5</td>
</tr>
<tr>
<td>10.</td>
<td>MULTIPLE WINDOWS-USERS SHARING A SINGLE DESKTOP</td>
<td>10-1</td>
</tr>
<tr>
<td>11.</td>
<td>SOFTWARE TOKEN EXPIRATION</td>
<td>11-2</td>
</tr>
</tbody>
</table>
1. INTRODUCTION

1.1. Purpose

The purpose of this document is to consolidate in a brief and simple guide all technical and practical information at the attention of the end users of the Network Manager Applications.

The Network Manager Applications are customised applications - such as NOP Portal, the CHMI applications, NMIR or CCMS-Web - which allow external users to connect to the Network Operations Systems. For more information on these applications, consult the Service Catalogue or the corresponding leaflets in the Network Operations Library on the EUROCONTROL Public Web Site:

http://www.eurocontrol.int/network-operations/library

The main topics covered by this guide are:

- The configuration of the users’ PC.
- The use of the authentication device (called token) which is required to access the Network Manager protected applications.
- The network aspects (extranet or internet).

It answers questions such as:

- What are the technical requirements to use the Network Manager Applications?
- How to install the RSA SecurID Software Token?
- How to use the RSA SecurID Software Token to access the Network Manager Applications?

1.2. Intended Audience

This guide is targeted towards:

- New users of the Network Manager Applications who need practical and basic technical information to prepare the initial connection,
- Existing users looking for assistance when experiencing problems with the token authentication, or during the connection to the service.

Generally ‘external users’ belong to organisations which are actively engaged in the operation of aircraft (and related support services), in Air Traffic Management or in Airport Operations. Most of the information provided in this document is applicable to all categories of users. However, where differences occur, they are explicitly mentioned.

No pre-requisite knowledge of the Network Manager is necessary for the readers of this guide.
1.3. Scope and Applicability

This edition is applicable from the indicated edition issue date, until it is replaced by a next edition.

This document forms part of the User Guides, which latest edition is accessible in the Network Operations Library on the EUROCONTROL Public Web Site at: http://www.eurocontrol.int/network-operations/library

For more information, it is recommended to consult the following complementary documentations in the Network Operations Library:

- the Service Catalogue, for an overview of the available services
- the various User Guides of the Network Manager Applications
- the corresponding leaflets
2. TERMINOLOGY

2.1. Note on CFMU/NM renaming

The name of the Central Flow Management Unit (CFMU) is progressively being replaced in EUROCONTROL’s publications by the Network Manager (NM). This results from EUROCONTROL’s nomination on 1st of September 2011 as the European “Network Manager”, as defined in the Single European Sky II (SES) legislation. This does not impact the former CFMU’s activities which continue and form now part of the wider scope of the Network Manager’s activities.

We apologise for the possible inconsistencies that may occur in our documentation updates during the transition period. For more information on EUROCONTROL’s organisation and on the mission of the Network Manager, consult the EUROCONTROL website.

2.2. Acronyms and Abbreviations

**ACE/SERVER** The RSA Security server software provides authentication, administration, and audit-trail services. All users of the NM protected applications are authenticated by this server located at NM.

**AO** Aircraft Operator.

**ANSP** Air Navigation Service Provider.

**CCMS-Web** Central Claim Management System via the Web. It is a Network Manager Application.

**CFMU** Central Flow Management Unit.

**CHMI** Collaboration Human Machine Interface. CHMI is a thin client (a single common user interface) based on Java technology. It is a Network Manager Application.

**CSO** Customer technical Service desk & Operations.

**HTTP** Hypertext Transfer Protocol.

**HTTPS** Secure HTTP.

**Kbps** Kilobits per second.

**NM** Network Manager

**NM Applications** Network Manager Applications (former CFMU Applications)

**NMIR** Network Manager Interactive Reporting. It is a Network Manager Application.
<table>
<thead>
<tr>
<th><strong>NM Terminal</strong></th>
<th>Network Manager Terminal (former CFMU Terminal)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NOP Portal</strong></td>
<td>Network Operations Portal.</td>
</tr>
<tr>
<td><strong>PASSCODE</strong></td>
<td>The passcode is the combination of your personal PIN code and of the Tokencode. It is generated by the RSA SecurID Software Token after entering your PIN code. This is the only valid code to connect to the Network Manager protected applications.</td>
</tr>
<tr>
<td><strong>PIN</strong></td>
<td>Personal Identification Number. The PIN code is your personal code, chosen by yourself the first time your token was activated. This is a number between 4 and 8 digits long. Your PIN is one of the two components that make up a PASSCODE.</td>
</tr>
<tr>
<td><strong>RSA</strong></td>
<td>The full name is RSA Security Incorporation: the company that provides the authentication solution based on the token technology.</td>
</tr>
<tr>
<td><strong>SITA</strong></td>
<td>Société Internationale de Télécommunications Aéronautiques</td>
</tr>
<tr>
<td><strong>RSA SecurID SOFTWARE TOKEN</strong></td>
<td>A software-based one-time password authentication method of protecting network resources, typically used for remote access. It is a small independent program that runs on the PC and that generates every minute a random number called the token code. The SecurID software licenses are bought from RSA Security Corp, therefore the installation guide refers mainly to the RSA SecurID (and not the Network Manager SecurID).</td>
</tr>
<tr>
<td><strong>TOKEN RECORD</strong></td>
<td>An encrypted file imported into the Software Token application. The SecurID Software Token application uses this file to generate a PASSCODE that the ACE/Server can recognise as yours.</td>
</tr>
<tr>
<td><strong>TOKEN CODE</strong></td>
<td>The pseudo-random code generated and displayed by your SecurID Software Token application. Every minute a new Token code is generated, making the previous one invalid. The combination of the token code and of your PIN makes up the PASSCODE.</td>
</tr>
</tbody>
</table>
3. CONTACT DETAILS

3.1. Requesting access to a NM Service or Application

All requests for service shall be addressed via the quick link ‘Requesting access to services’ available on the Network Operations home page: [http://www.eurocontrol.int/network-operations](http://www.eurocontrol.int/network-operations), or via the corresponding web form accessible from the Network Operations Library.

It shall be noted that the NM Services are only provided to eligible organisations and are subject to the signing of an agreement, through which the organisation commits to comply with the Data Policy, IT Security policy, and Acceptable Behaviour rules.

All details on the process for requesting access to a Service and for the signing of the Agreements are described in the ‘Access conditions’ of the related service. The Service Catalogue provides an overview of the available Services and describes the applicable policies and rules: [http://www.eurocontrol.int/network-operations/nm-operational-services-and-products](http://www.eurocontrol.int/network-operations/nm-operational-services-and-products)

3.2. Technical Support

To report any technical problem or if you have questions related to the installation or the use of the RSA Software Token, please contact Customer technical Service desk & Operations (CSO) - available 24 hours/day, 365 days/year:

- By phone: +32 2 745 19 97
- By email at: nm.cso.help-desk@eurocontrol.int

3.3. Support from the Network Supplier

For connecting to the Network Manager Applications, you can choose to use Internet or the Network Manager Extranet which is provided by SITA.

In case of network problems, please report to:

- The maintenance service of your Internet Service Provider, if you have chosen Internet.
- Your local SITA service provider, if you have chosen the Network Manager Extranet.

**Specific case: NM Terminals for ANSPs:**

Users of ANSPs’ operational positions which have an NM Terminal supported by the Network Manager must report any technical problem with the Network or the NM Application to Customer technical Service desk & Operations (CSO).

Technical problems with the hardware (desktop, monitor, printer, …) shall be reported to your local technical department.
3.4. Designating the Customer Contacts

When signing the Agreement for access to the Services, the Customer is responsible for providing to the Network Manager the contact details of a Single Point of Contact (SPOC) who is responsible for interacting with the Network Manager for any matter related to:

- The management of the service (subscription, modification, cancellation of services or of user accounts).
- The dissemination within his/her organisation of the Network Manager information related to the evolutions of the Services, such as system upgrades and software releases.

Optionally, the Customer may also designate a technical Point of Contact (POC) specifically dedicated to the NM Applications.

The SPOC (and the POC when available) will receive through e-mail the information related to the evolution of the services and the relevant user guides.
4. CONNECTION TO NM SYSTEMS

4.1. Connection Options

Users have two ways to connect to the NM Systems as indicated in the diagram below: either via the Internet or via the Network Manager dedicated network (Extranet).

**Figure 4-1 Connection Options**

**Specific case: NM Terminals for ANSPs:**

ANSPs’ NM terminals use the Extranet to connect to the CHMI. The Network Manager is responsible for setting up the connection and for installing the software. Any technical problem with the Network or the NM Application should be reported to CSO (see § 3.2). Next chapters are therefore not relevant for ANSP users of NM terminals, who can go directly to the chapter ‘How to use the RSA SecurID Software Token’ (See Section 9).

4.1.1. Extranet

SITA was chosen as the supplier of the Network Manager TCP/IP network (Extranet).

The users are responsible for the installation of the connection between their local site and the Extranet network. There may be several different methods of technically achieving this connection, either directly with SITA or via another intermediate service provider.

If you want an access to the Network Manager Extranet, send your request to the appropriate SITA e-mail address as indicated here after:

- **For the countries:**
  - UK, Ireland, Benelux, Germany, Denmark, Scandinavia, Finland, Switzerland, Austria, Israel.
  - Customer Service: SC.NE.Service.Centre@sita.aero
  - Sales: SC.NE.Sales@sita.aero
b) For the countries:
Portugal, Spain, France, Italy, Malta, Serbia, Kosovo, Croatia, Bosnia-Herzegovina, the FYROM, Montenegro, Greece, Albania, Poland, Romania, Bulgaria, Hungary, Czech Republic, Slovakia, Slovenia, Moldavia, Russian Federation, Azerbaijan, Turkmenistan, Uzbekistan, Tajikistan, Kyrgyzstan.

- Customer Service: SC.SEE.Service.Centre@sita.aero
- Sales: SC.SEE.Sales@sita.aero

4.1.2. Internet
Internet allows access to all NM Applications: NOP Portal, NMIR, the CHMI Applications and CCMS-Web. Internet access requires a conventional connection to Internet and the use of a web browser recognised by NM as appropriate for the connection.

Note: The use of CHMI requires the installation of client software (as described in the CHMI ATFCM SYSTEM REFERENCE User Guide) which can be downloaded from our website: http://www.eurocontrol.int/network-operations/library

See 5. TECHNICAL REQUIREMENTS for further details on hardware/software requirements.

4.2. Security
4.2.1. Client Authentication
It is very important that access to the NM Systems is restricted to authorised users. To ensure this level of security the Network Manager uses a one-time password mechanism based on Secure ID software tokens.

The software token is a program on the user's PC. Each copy of the program has a unique identification and generates every minute a new pseudo-random number (8 digits) referred to as token code. No other token generates the same token code. Each token code is valid for only one minute.

**Important notice on the policy for the use of the NM Applications:**
- Each PC using the NM Applications requires an individual user account and therefore the installation of an individual token. A token can only be installed on one PC. Duplication of a token is strictly forbidden.
- More on the policy for the use of the NM Applications can be found in the Service Catalogue and Agreements.

Each user is accountable for the interactions with the NM Systems performed with his user account (username). To avoid abuse of your account, protect it by keeping your PIN secret and controlling access to the computer on which your token is installed.

If an unauthorised person learns your PIN and has access to your computer, this person can wrongly take your identity. Any action taken by this intruder will be attributed to you in the NM security log.
Therefore for your own protection and that of the system:

a) Lock your computer when you leave your office.

b) Never reveal your PIN or password to anyone. Do not write them down.

c) When entering your PIN, shield it from view so that no one can see the keystrokes.

d) If you think someone knows your PIN, ask CSO (see § 3.2) to reset your PIN. At next log in, you will have to create a new PIN.

e) If your computer has been stolen, notify the theft to CSO so that they can disable your token. It is impossible to abuse your account with a disabled token. The Helpdesk operator can give you a temporary password that you can use while waiting for reception of a new token.

f) Avoid that others log in to your computer under your identity.

4.2.2. Firewalls

The NM Applications are Web applications accessed from a Web browser on the users’ PC. Users having installed a firewall system between their Local Area Network and the Internet, should be able to let the NOP Portal, NMIR or CHMI communications pass through without any problem since these communications are based on the standard Web protocols HTTP (Hypertext Transfer Protocol) and HTTPS (Secure HTTP) supported by practically all commercial firewall products.

Transfer of some restricted pages is encrypted by use of the HTTPS protocol. Clients do not need to have a X.509 client certificate installed in their Web browser in order to access these restricted pages. When in doubt, clients can consult with their firewall system vendor for configuring the firewall filters or proxy servers for HTTP and HTTPS.

CHMI requires a dedicated application to be installed on the PC itself. More information can be found in the CHMI Installation Guide, which is sent to you via e-mail after your request for access to the CHMI is approved.
5. TECHNICAL REQUIREMENTS

The following Section provides information concerning the hardware, software and configuration required to use the NM Applications (NOP Portal, NMIR, CCMS-Web or the CHMI Applications). It should be noted that the configurations indicated here are the ones that have been tested and validated by NM and are therefore the recommended configurations. They are not the minimum configuration and they are also not the only configuration possible.

5.1. NOP Portal and Central Claim Management System (CCMS-Web)

5.1.1. Browser support for NOP Portal

Policy:

For each NM release, NM will provide a list of at least two browser brands and versions for use with the NOP Portal.

This list will be communicated as part of the NM Release notification process.

A recommended browser brand/version is a browser on which NOP Portal services have been tested and are suitable for operations. This does not mean that these browsers support the NOP Portal in an identical way; one browser might be slightly better than another, maybe depending on the exact service, but the differences do not provide an impediment to using the NOP Portal.

A supported browser brand/version is a browser on which regression testing has been performed for previously existing NOP Portal services and they remain suitable for operations; new services/features may not work (in particular if they use new browser features).

Note, it is the responsibility of users to apply the latest security updates.

When a browser is no longer recommended for Release N it will be supported for at least that release (and its associated increments).

Recommended browsers for NM 22.0:

- Internet Explorer 11
- Edge
- FireFox
- Chrome

The NM web-based HMIs will have been fully tested on Internet Explorer 11, Edge and FireFox. For these recommended browser brands, NM undertakes to investigate and attempt to resolve problems that can be reproduced on the latest stable version of that brand. Any other browser or version is on a “best efforts” basis.

- Using a browser zoom level different to 100% might lead to degradations in rendering the GUI.
- Flash player plug-in is required.
Change default browser settings:

- **Firefox:**
  By default and as a safety feature, Firefox forbids scripts to raise windows and, subsequently, the Portal feature of bringing windows to the front cannot work. To overwrite this safety measure one has to open the options dialogue by selecting the menu entry Tools -> Options, select the Content tab, click on the Advanced button next to "Enable JavaScript" and ensure that the check box "Raise or lower windows" is selected.

![Firefox options dialogue](image)

**Figure 5-1 Firefox forbids scripts to raise windows**

- **Internet Explorer:**
  For the NOP Portal to work on Internet Explorer, it is necessary to un-tick the two check boxes "Display intranet sites in Compatibility View" and "Display all websites in Compatibility View". You can find these settings in the "Compatibility View Settings" dialogue, available under Tools -> Compatibility View Settings.
5.1.2. Technical prerequisites

The technical prerequisites for using the NOP Portal can be found in the online Help page of the NOP Portal: [https://www.nm.eurocontrol.int/HELP/webframe.html](https://www.nm.eurocontrol.int/HELP/webframe.html). Select “The Network Operations Portal” in the Table of Contents of this online help page and then “Technical Prerequisites”.

In addition: a token Software Package (to be provided by NM). The Token Software program requires a PC equipped with at least:

- 32 Mb of physical memory
- 20 Mb of free disk space

5.2. Network Manager Interactive Reporting (NMIR)

NMIR technical requirements are described in a specific document called ‘NMIR Technical Requirements’, downloadable from the Network Operations Library:

[http://www.eurocontrol.int/network-operations/library](http://www.eurocontrol.int/network-operations/library)
5.3. **Collaboration Human Machine Interface (CHMI)**

A PC with:
- Dual Screen (to enlarge horizontal desktop)
- CD-ROM drive
- Windows 7 or Windows 10
- Processor speed 2.8 GHz
- 1 Gb RAM
- Ethernet Port

In addition: the CHMI Software and Token Software Package (to be provided by NM).

The Safety Assessment for the CHMI system was conducted using the Microsoft Windows 7 operating system. NM cannot ensure safe usage of the CHMI system with any other operating system. **The recommended operating system is Windows 10, Windows 7 is also supported.**

5.4. **Performance**

The overall performance, as observed by the end-user, is dependent upon many aspects e.g. the line speed, the quality of the local service provider, the network load, the remote web or network server(s), the PC performance (PC load, stand-alone, networked) etc.

Some of these aspects are variable (network loads) and many are outside our direct control (e.g. internet web servers). Overall performance is therefore almost impossible to quantify.

The line speeds that are required to enable an acceptable level of performance are as follows:
- Internet connection from any commercial provider.
- AOs using CHMI via Extranet are recommended to request minimum a 128 Kbps connection.
6. INSTALLATION PROCEDURE FOR THE RSA SECURID SOFTWARE TOKEN

Preliminary Steps

- You - or your organisation’s Single Point of Contact (SPOC) - have filled in a ‘Request for Service’ Web Form on the NM Public Web Site.
- After validation of the request, you or your SPOC have received in return an e-mail from NM with the Software Token Package which contains:
  - The link to the Web page where the RSA Token software can be downloaded together with this Network Manager Connection guide.
  - Your unique Token record file (*.sdtid file), indicating your User account.
  - The installation procedure and/or User Guide of the NM Application you requested (NOP Portal, CHMI, CCMS-Web)
- You have prepared a PC with the appropriate hardware and software configuration.

You are now ready to proceed with the installation, which consists of 2 steps:

- First, download and install the Software token application, which is common to all users (as explained in § 6.1).
- Second, call CSO to:
  - Retrieve your installation password. The password shall indeed be provided through a different channel for security reasons. You will be requested to provide over the phone your identity details and your UserID.
  - Import your individual Token Record (as explained in § 6.4).

If you encounter any problem during the installation, do not hesitate to contact CSO (see § 3.2).

6.1. Installation of the RSA Software Token Application

6.1.1. Multiple versions of the RSA SecurID Software Token

NM supports 2 versions of the RSA Software Token:

- version 5.0.2-32bit: for Windows 32 Bits (Windows 7, 8 & 10)
- version 5.0.2-64bit: for Windows 64 Bits (Windows 7, 8 & 10)

Go to: [http://www.eurocontrol.int/network-operations/nm-software-download](http://www.eurocontrol.int/network-operations/nm-software-download) and download the version of the Software token you need on your system. Then follow the corresponding installation procedure.

The downloaded file is a compressed version of the software (ZIP file) so that it is considerably smaller and faster to download. You need to unzip the file before you can install the software. To unzip a file, right-click the file and then click “Extract” on the shortcut menu. Save the unzipped file onto your desktop or in a temporary folder on your computer.
If you don’t have a ZIP utility installed on your computer, check with your system administrator or download it from the internet. Most programs offer a 30-day limited trial period where you can download and try the utility for free.

It is assumed that the software has never been installed before on the PC. If not refer first to Section 8. in order to remove the previous software.

To install the software, you need Administrator rights on your PC.

6.1.2. Installing RSA SecurID Software Token version 5.0.2
Once you have downloaded and unzipped the Token software, start the installation by double clicking on the file:
- ‘RSASecurIDToken502.msi’ (v 5.0.2-32bit)
- ‘RSASecurIDToken502x64.msi’ (v 5.0.2-64bit)
Windows will recognize the file type as a Windows Installer File and will start up the InstallShield Wizard.

On the ‘InstallShield Wizard’ window, click on ‘Next’ to continue.

![Welcome SecurID – V 5.0.2](image)

On the ‘Place of Purchase’ window, choose the appropriate region then click on ‘Next’ to continue.
Read the license agreement and if you accept the terms of the license agreement, select “I accept the terms in the license agreement” and click on ‘Next’ to continue.

You are requested to choose the Setup Type. Select ‘Custom’ then click on ‘Next’ to continue.
By Default the “Browser Plug-Ins” is deselected. Click on the little arrow next to the red cross (X) and select “This feature will be installed on local hard drive”. Do this for all the different web browsers you might use in the future.
The window will then look as follows (no more red cross).

![Figure 6-6 Selected Browser Plug-ins – V 5.0.2](image)

Click on ‘Next’ and then on ‘Install’ to begin the installation of the Software Token.

![Figure 6-7 Ready to Install – V 5.0.2](image)

The installation process will start. Wait until the software is completely installed. This will take a few minutes.
When the software is completely installed, click on 'Finish' to close the InstallShield Wizard.

If you selected "Launch RSA SecurID Software Token" on the previous screen, the following window will appear.
Click on “Cancel” as you can not use the program yet to connect to the NM Applications, you first need to install the unique Token Record (See § 6.4).

The following window will appear. Click on “Close”.

6.2. Available Shortcuts

After the SecurID software application is installed, 2 shortcuts will be created in the Windows Start menu:

- Start/Programs/RSA/RSA SecurID Token/RSA SecurID Token.
- Start/Programs/RSA/RSA SecurID Token/Token Transfer Utility.

The first shortcut will be used to start the application.

The second shortcut is not used by NM and will therefore not further be described in this user guide.
When starting the RSA SecurID Software Token application, the “Import Token” window will be displayed. This is normal as the Token Record still needs to be installed (See § 6.4).

Click on “Cancel” and then close the next window. How to import your token will be explained in § 6.4.

6.3. Advanced Setting

If the user of the PC has no administration rights, ensure that he/she has a ‘write’ access to the following folder: c:\Program Files\RSA Security\RSA SecurID Software Token\n
6.4. Installation of the Token Record

6.4.1. Principles

- **One single User Account (token) per PC**
  
  Each Token Record corresponds to an individual User account (UserID). Therefore, once the SecurID Software Token program is installed on your computer, it is recommended to install only one Token Record on this PC. This means that multiple users using the same computer must share the same SecurID Software Token application, the same token serial number and the same PIN to authenticate to any of the NM protected applications. See also § Section 10.

- **Several NM Applications per User Account (token)**

  The same token can be defined for one or for a combination of the NM Applications (example: NOP Portal+ CCMS-Web, CHMI+CCMS-Web). A Token can only be used for the NM Applications which have been requested in the Web Form ‘Request for Service’. Thus, if a UserID is requested for NOP Portal, it can only be used for NOP Portal.

  Refer to your initial request in the Web Form. If you need to add more NM Applications to an existing User account (UserID), you must send an update request via the same Web Form.

6.4.2. Token Record File
The token record is an encrypted file which needs to be imported in the Software Token application. Each token record file contains one token which is unique and can be identified with its token serial number.

The token record file is sent to you via e-mail with a file attached which has the .sdtid extension. Each token record file is associated to a username, therefore the complete filename is username.sdtid.

All tokens are password protected. Before installing a token, you shall retrieve your installation password by calling CSO (see § 3.2).

6.4.3. Installation of Token Records on a PC

The token can only be installed if the installation procedure of the RSA Software token Application has been correctly followed (See § 6.1).

Verify especially if the end-user has write permissions to the folder C: \ Program Files \ RSA Security \ RSA SecurID Software Token.

Ensure that each PC uses a different Token Record.

Save the token file (*.sdtid file sent to you via e-mail) in a temporary folder or on your desktop. The token record will be automatically removed once it is installed.

6.4.3.1. Installation of Token Record for RSA SecurID version 5.0.2

Important note: With version 5.0.2, the token is installed in the User directory. Therefore the token record must be installed with the end-user account. So after installing the RSA SecurID Software, log out of Windows with the administrator account and log in again with the end-user account.

When a single desktop is used by several users and the same token must be shared by all users, the token must be installed for every end-user account. See § Section 10

Ensure that the Software Token program is not running (closed).

Double click on the token file (*.sdtid file sent to you via e-mail) that you have copied in a temporary folder or on your desktop.

You will be prompted to enter the Installation Password that you have been provided previously by calling CSO (see § 6.4.2).

![Figure 6-13 Installation password – V 5.0.2](image)
When you have entered the correct installation password, the following window will appear. Click on OK to terminate the installation procedure.

![Successful Import - V 5.0.2](image)

The following window will appear.

![Software Token Installed - V 5.0.2](image)

### 6.4.4. Enable Token

A new token which has been installed on your system is by default disabled for security reasons. Contact **CSO** (see § 3.2) to enable your token(s).

### 6.4.5. Create PIN code

The PIN (Personal Identification Number) code is your personal code, which you have to choose the first time you use your token. If you have already used your token in the past, you do not have to re-create your PIN if you re-install the token on your PC.

If you do not remember your PIN code, you can contact **CSO** (see § 3.2) to have it reset.

If you did not create your PIN code yet, follow the procedure below:

- Start the RSA SecurID Software Token Program (see § 9.2)
Go to the NM Protected Applications login page: https://www.nm.eurocontrol.int/PORTAL/gateway/spec/index.html and fill in your User Name.

In the “Passcode” field, copy/paste the code from the RSA SecurID Software Token, without entering a PIN code first:

- Press the little blue arrow (see Figure 9-1) without entering a PIN code first. You will see “Tokencode” in the display of the RSA SecurID Software Token. Copy this code into the Passcode field of the NM application login window.

Press the “Sign In” button on the NM Protected applications login window.

Note: An error message "user pin has expired..." will be displayed. You can ignore this, it is normal as you did not create a PIN code yet.

You are now requested to create your PIN code. This is a number you can choose yourself, which you have to remember as you will have to use it every time you want to connect to the NM Protected Applications. It must be a number between 4 and 8 digits long and cannot start with a zero. Confirm your PIN code in the second field.

If your PIN code has been successfully created, you are redirected again to the NM Protected applications login window. You will have to use the normal login procedure to connect to the NM Protected Application (see Section 9).

In case your token is used by multiple users on a shared working position, do not forget to communicate this new PIN code to your colleagues, as the PIN code is related to the UserID.

The installation procedure of the RSA SecurID Software token is now completed. You are now ready to use it to access the NM Applications. Refer to Section 9 for details on how to use the Software Token.
INTENTIONALLY LEFT BLANK
7. MAINTAINING ACCURATE SYSTEM TIME SETTINGS

The RSA SecurID Software Token program and the NM servers both rely on standard time settings known as Greenwich Mean Time (GMT) or Co-ordinated Universal Time (UTC).

Your authentication to NM Protected Applications will only be successful if the UTC time of your PC is set correctly. To check the UTC time of your PC, go to the following Web Page: http://www.nm.eurocontrol.int/utc.html

This page does not show the real UTC time, it calculates to what time the UTC time is set on your local PC, based on your PC settings. If the date or time shown does not correspond to real UTC time, change your PC clock or time zone by double clicking the time display on the Windows taskbar.

If the time settings on your computer happen to drift (more than 10 min), your passcode to access the NM applications will be considered as invalid.

You are responsible for maintaining the time settings on your local computer.
8. REMOVAL OF THE SOFTWARE TOKEN

NM recommends to use version 5.0.2 of the RSA SecurID program (see § 6.1.1).

If you have no problem with the current version installed nor with the token itself, there is no need to install the latest version of the RSA SecurID program.

However, if you encounter any technical problem, CSO highly recommends upgrading to the latest version of the SecurID program.

You may either remove a specific token record or remove the whole Software Token Application.

8.1. Removal of a Token

In some cases you might want to uninstall a token record without removing the complete RSA SecurID Software Token software.

Start the RSA SecurID Software Token application by clicking on Start/Programs/RSA/RSA SecurID Token/RSA SecurID Token.

Click on the small arrow next to "Options" and select "Manage Token" and then "Delete token".

![Image of RSA SecurID application with options menu]

Press "Yes" to confirm or "No" to cancel.

![Image of confirmation window]

You will see a confirmation window that the token is removed.
If you open the RSA SecurID Software Token application now, you will be asked to import a token file. See § 6.4.3.1 to import a new token.

If you cancel that request, you will see the following window and the RSA SecurID Software Token application will close if you close this window.

You need to import a token file into the RSA SecurID Software Token application. Otherwise you will not be able to access the NM Protected Applications.
8.2. Removal of RSA SecurID Program

When you want to upgrade to a higher version of the SecurID program, you need to remove first the older version.

Removal of the software can only be done by a user with sufficient administrator rights.

To remove the complete RSA SecurID Software Token program, use the standard Windows tool to Add or Remove Software: click on Start/Control Panel and double click on “Software”. All available software on your computer will be listed.

Select “RSA SecurID Software Token” and click on the “Remove” button.

Wait until the complete program has been deleted from your computer.

“RSA SecurID Software Token” will no longer appear in the list of available software. You can close the window.

To ensure that all traces of the RSA Software token are gone, verify if the folder c:\Program Files\RSA Security\RSA SecurID Software Token is removed. If this folder is not removed, at the next Software token installation, it will use the existing token database.
9. **HOW TO USE THE RSA SECURID SOFTWARE TOKEN**

9.1. Starting the NM Protected Application

9.1.1. NOP Portal and CCMS-Web
Open your Web Browser and go to [http://www.eurocontrol.int/network-operations](http://www.eurocontrol.int/network-operations)
At the right-hand side of the screen, select one of the NM Protected Applications:

a) ‘NOP’ - to access the Network Operations Portal.

b) ‘CCMS Web’ - to access the Central Claim Management System.

9.1.2. CHMI Application
Access to the CHMI application is available from the Windows Start menu of your PC by clicking on Start/Programs/NM Applications.

9.1.3. Login Screen
After starting one of the NM protected applications, you will see a login screen where you have to enter your User Name and Passcode.

9.2. Starting the RSA SecurID Software Token Program
The Software Token program is an independent application that can be started at any time.

The Software Token program can be started in the same way as any other program running under Windows: Click on Start/Programs/RSA/RSA SecurID Token/RSA SecurID Token.

**Figure 9-1 RSA SecurID Software Token**

- **SERIAL NUMBER**
  In case of problems to access the NM Protected Applications, **CSO** might ask you this number.

- **PIN CODE BOX**
  Box to enter your PIN CODE. Use the number keys on your keyboard to enter the PIN code.

- **BLUE ARROW**
  Press the little blue arrow or press the 'Enter' button on your keyboard to generate your Passcode.
9.3. **Token Terminology**

9.3.1. **What is the UserName or UserID?**

Your ‘UserName’ or ‘UserID’ is a login name which has been assigned to your User account by NM. (For example: p0xxx1). The ‘UserName’ is not case sensitive.

9.3.2. **What is the PIN code?**

The PIN (Personal Identification Number) code is your personal code, that you have chosen the first time you have used your token. This is a number between 4 and 8 digits long. If you do not remember your PIN code, you can contact CSO (see § 3.2) to have it reset.

In case your token is used by multiple users, do not forget to communicate this new PIN code to your colleagues, as the PIN code is related to the UserID.

9.3.3. **What is the Tokencode?**

The Tokencode is a random number generated by the RSA SecurID Software Token. Every minute a new Tokencode is generated, making the previous one invalid.

You can only see the Tokencode when you did not yet create a PIN code (see § 6.4.5). Once you have created a PIN code, the tokencode is hidden, as it is not a valid access code.

9.3.4. **What is the Passcode?**

The passcode is the combination of your personal PIN code and of the Tokencode. It is generated by the RSA SecurID Software Token after entering your PIN code. The Passcode is only valid for a short while. You will see the little blue boxes disappear one by one. Once they are all gone, a new Passcode, which is also valid, will be automatically generated. Only when you see the text ‘PASSCODE’ in the display of the software token, you have a valid code to connect to NM. If you do not see the text ‘PASSCODE’, all valid Passcodes have expired and you will have to enter your PIN code again.

![Figure 9-2 Valid Passcode](image)

Up to 4 different Passcodes will be generated, then all valid Passcodes have expired and you have to enter your PIN code again.
9.4. How to Generate your Passcode?

- Start the RSA SecurID Software Token (see § 9.2).
- Enter your PIN code on the Software Token via the number keys on your keyboard.
- Click on the little blue arrow.
- Click on the ‘Copy’ button.
- Return to the NM application login screen (see § 9.1) and paste the passcode into the “Passcode” field. (Click your right mouse button and select “Paste” from the drop-down menu or press CTRL + V simultaneously)

9.5. How to log in to the NM Protected Applications?

A new token which has been installed on your system is by default disabled for security reasons. You have to contact CSO (see § 3.2) to enable your token.

If you are not using your token for the first time, follow the steps below to log in to the NM Protected Applications.

Start the NM application (See § 9.1.)
At the Login screen:

a) Enter your UserID in the “UserName” field.
b) Enter the Passcode in the “Passcode” field. (See § 9.4”)
c) Press the “Sign In” or “Log on” button.

Pay attention to press the ‘Sign In’ / ‘Log on’ button only once, otherwise our system will see it as a security violation and will reject your passcode. A valid UserID and Passcode can only be used once within the same minute. If a second log in is attempted within the same minute i.e. using the same Passcode, both attempts will be seen as a security violation and therefore will be rejected.

9.6. Wrong Log in

- **NOP Portal or CCMS-Web**: if you enter a wrong Username and/or Passcode, the following message will appear on the Login screen: ‘HPDIA0201W The client supplied invalid authentication information’.

- **CHMI**: if you enter a wrong Username and/or Passcode, the CHMI Login window will show the error message ‘Access denied. Credentials rejected. Try again’.

Before trying to log in again, do the following:
- Only when using Internet access: Delete the cookies and temporary Internet files via the Internet options of your Web browser. Close the Web browser and open it again.
- Check the UTC time of your PC. (See Section 7.)
- Start the NM Application you want to use. (See § 9.1.)
- Enter the correct UserID in the “UserName” field.
- Generate a new Passcode and try to log in again. (See § 9.4.)
- If you tried several times to log in, but still fail to connect to the NM Protected Application, contact CSO (See § 3.2) to guide you through the log in procedure.

After 10 unsuccessful attempts to log in to the NM application, your UserID will be disabled. You will keep receiving the same error message ‘HPDIA0201W The client supplied invalid authentication information’ (NOP Portal & CCMS-Web) or ‘Access denied. Credentials rejected. Try again.’ (CHMI), even if you enter the correct passcode. In that case, contact CSO to enable your UserID again.

9.7. Next Tokencode

Occasionally, after you entered your Passcode correctly, the system detects a possible security attack and will ask for a confirmation by entering the next token code. This can happen when someone has tried to login a few times with a wrong Passcode (example wrong PIN used) followed by a correct Passcode. To be sure the Passcode provided was indeed a correct code from your software token, you are requested to provide the Next Tokencode.

To authenticate when your token is in Next Tokencode mode:
- On the RSA Token software, click on “Options” and select “Next Tokencode"

![Figure 9-4 Next Tokencode](image)

- When the "Next Tokencode" appears, click on the ‘Copy’ button.
- Return to the NM application login screen and paste the code into the “Next Tokencode” field on the login page (press CTRL + v).

You should now be logged into the NM Protected Application. If not, close the NM Application and RSA Token software, open them both again and try to login as normal. If you receive the same error “Next token required...“, perform the steps above again.
9.8. Token Reactivation

If your token is not used for more than 2 months, it will be automatically disabled.

If you want to use it again, contact CSO (See § 3.2) to enable your UserID again.

If your token is not enabled, you will keep receiving the error message ‘HPDIA0201W The client supplied invalid authentication information’ (NOP Portal & CCMS-Web) or ‘Access denied. Credentials rejected. Try again.’ (CHMI), even if you enter the correct passcode.
10. MULTIPLE WINDOWS- USERS SHARING A SINGLE DESKTOP

When a single desktop is used by several users (typically for users working in shifts, using roaming profiles), additional configuration might be required in order that all the different Windows users can use the same Software Token.

With version 5.0.x the token is installed in the User directory C:\Documents and settings\USER\Local Settings\Application Data\...and therefore the same Token cannot be shared by different Windows users on the same desktop.

The following document explains how to circumvent this:
http://www.nm.eurocontrol.int/chmi_appsoft/CHMI/Tokens/RSA-SecurID-Software-v5.0.2-Installation-Procedure.pdf
11. SOFTWARE TOKEN EXPIRATION

The RSA SecurID software token is programmed to expire at a fixed time. In this case it requires the provision and installation of a new token. This is a regular activity which is monitored by the NM technical support group.

When your token is about to expire, your site contact person will be informed in due time about the need to install a new token. The notification will include all material, guidelines and support information needed to proceed with this replacement in a smooth way, without any impact to your operations.

The expiration date of the software token can be checked on the RSA SecurID Software token application: Click on "Options/Manage Token/Token Information ..."

If the token is not replaced in due time, the end-user will receive a notification when starting up the RSA SecurID Software as of 30 days before the token expires.

Figure 11-1 Token Expiration notification

The end-user should then take contact with the site contact person (SPOC), who should have received a new token and the installation procedure.
If a new token was recently installed and the above warning still pops up, probably the old token was not removed when the new token was installed.

To delete the old token:
- The name of the old token is mentioned in the Token Expiration notification
- Using the little black arrow next to the token serialnr, select the token to be deleted
- Using the little red arrow next to “Options", select manage token > delete token

Pay attention not to delete the wrong token.