EUMETSAT

EPS Key Dissemination System - User Guide

Doc.No. : EUM/TSD/MAN/04/0341
Issue : v2A
Date : 17 August 2006

EUMETSAT
Am Kavalleriesand 31, D-64295 Darmstadt, Germany
Tel: +49 6151 807-7
Fax: +49 6151 807 555 Telex: 419 320 metsat d
http://www.eumetsat.int

Intentionally blank

Document Signature Table

Removed for Internet Publication

Intentionally blank

Document Change Record

Issue / Revision	*Date*	*DCN. No*	*Changed Pages / Paragraphs*
Issue 1	6 June 2005	N/A	First issue
v2	2 August 2006	N/A	General – Updated description text. Section 3 – Deleted.
v2A	17 August 2006	N/A	General – Small text updates. Section 2.2.1 – Replaced reference to time-out by a recommendation to download keys as soon as possible. Updated description of downloaded files. Section 2.2.2 – Updated description of downloaded files.

Distribution List

Removed for Internet Publication

Table of Contents

1 INTRODUCTION

1.1 Purpose

The purpose of this document is to describe the use of the EUMETSAT Polar System (EPS) Key Dissemination System (KDS), for the METOP Direct Readout Service.

1.2 Scope

The scope of this document is limited to providing instructions to users and operators of the EPS KDS.

1.3 Applicable Documents

N/A

1.4 Reference Documents

N/A

1.5 Document Structure

This document contains two main sections.

Section 1 - General introduction
Section 2 - How to download new keys using the KDS

1.6 Definitions, Acronyms, and Abbreviations

EPS	EUMETSAT Polar System
KDS	Key Dissemination System
C-KMC	Common-Key Management Centre
HRPT	High Resolution Picture Transmission
LRPT	Low Resolution Picture Transmission
SKU	Station Key Unit
MSK	Master Station Key
PBK	Public Key
XML	Extensible Mark-up Language
DTD	Document Type Definition
URL	Uniform Resource Locator

2 EPS KEY DISSEMINATION SYSTEM

The EPS KDS is available to all registered METOP Direct Readout users issued with one or more EPS Station Key Unit/s (SKU). The KDS allows users to download the public keys associated with their SKU. These public keys are required to decrypt the encrypted instrument data from the METOP satellites during periods of Data Denial.

2.1 Background

During periods of Data Denial, data from the NOAA instruments (AVHRR, AMSU and HIRS) on-board the METOP satellites will be encrypted. Users who are never to be denied access to these data (priority users), may continue to receive the data if their reception station (A/HRPT/LRPT) is equipped with an SKU programmed for the reception of these data. To receive and decrypt these data, the SKU must be configured with a set of valid Public Keys (PBKs).

The PBKs are subject to change, so SKU holder's must download the new keys in order to be able to decrypt the disseminated A/HRPT/ LRPT data. When the PBKs change the new keys are delivered to the user via KDS. An email notification is sent to the user stating that new keys have been generated and are available for download.

2.2 Downloading New Keys

The notification is the starting point of the downloading process. Each user receives a notification that includes a URL from where the keys can be retrieved.

In addition to the URL included in the notification, users can also download the PBKs directly from the Web Site. To do this the KDS has a set of web pages where it is possible to see and download the PBKs. These pages are protected by username/ password, so users only see, or download their own PBKs.

The following paragraphs describe how to download the PBKs using both mechanisms.

2.2.1 Download PBKs from the URL included in the notification

When new PBKs are generated, each user receives a notification that includes:

- the URL from where it is possible to download the keys.

To avoid any loss of data, it is recommended to download the new PBKs and load them into your reception station as soon as possible.

The URL included in the notification is unique per user and can only be used for that particular set of keys. When new keys are generated, new URLs are assigned to the user.

After receiving the notification, follow the steps below to download the keys:

1. Click on the URL included in the notification. The Web Browser should open automatically in the "Public Keys" page. If not, open the Web Browser, then copy the URL from the notification and paste it into the address bar in the Web Browser. The "downloading" page should now be displayed.

2. Select "Download" from the Key Dissemination System menu to display the download page. The following should be displayed:

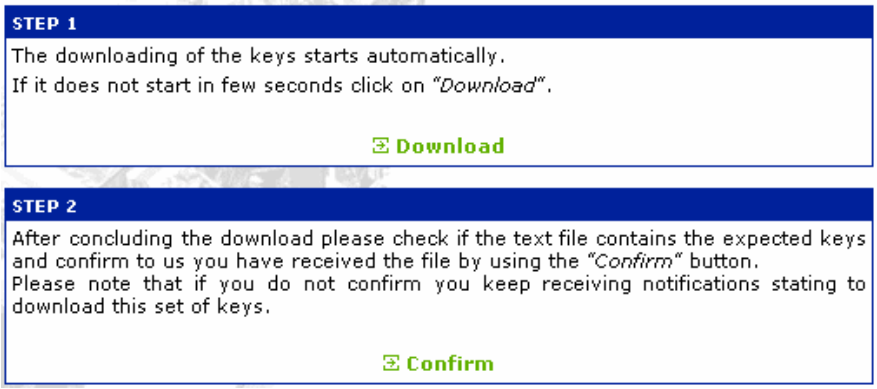

Figure 1 – "Downloading" page

3. The file downloading should start automatically after 5 seconds. If not, click on the "Download" button to begin. Most of the browsers display a dialog box with two options: open the file or save the file. It is recommended to save the file for later use. The downloaded file is compressed ZIP file and can be opened with any ZIP tool. It contains a plain text file and an XML file with the new key sets. It also contains the DTD file with the definition of the XML file. The files contain the new key sets distributed according to the Channel (A/HRPT/ LRPT) and the SKU hexadecimal number.

4. After the file has been downloaded, confirm the download. To confirm the download click in the "Confirm" button. It is very important to confirm this action to indicate to EUMETSAT that you have received the notification and that the new keys are being uploaded to your reception station.

To upload new keys consult your reception station user/installation instructions provided by your station manufacturer.

2.2.2 Download PBKs through the EEIS Web Interface

An alternative way to access and download the keys is through the EUMETSAT Web site. To do this, a user must be a registered user and have a username and password to access the KDS. Follow the steps below to access the public keys through the Web site:

1. Access the KDS link from: Access to Data – METOP/NOAA Direct Readout page

2. On the left menu click on the Key Dissemination System link and then “Login”.

3. In the Login page, insert the username and password in the appropriate fields and click on the “Login” link.

4. If you do not know the password, click on the “Forgotten Password” link and the password will be sent by e-mail to the e-mail address specified during the registration process. If the username is not known, contact the EUMETSAT User Service. It is important that e-mail addresses are kept up to date in order to receive any notifications.

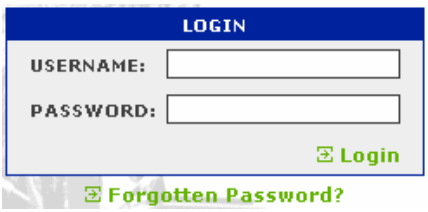

Figure 2 - “Login” Form

5. After logging in, the public keys are displayed. The left menu contains a link to start the downloading of the new keys.

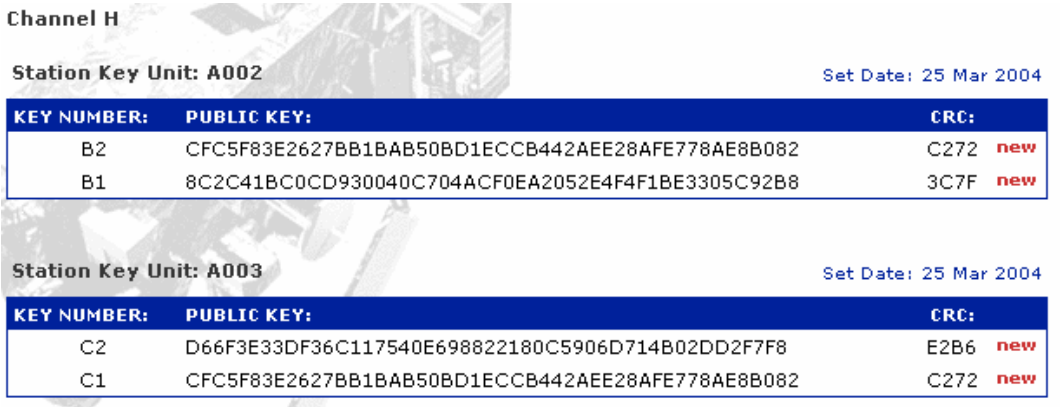

Figure 3 - “Public Keys” Page

6. To download the keys, click on the “Download” button in the left menu to display the downloading page.

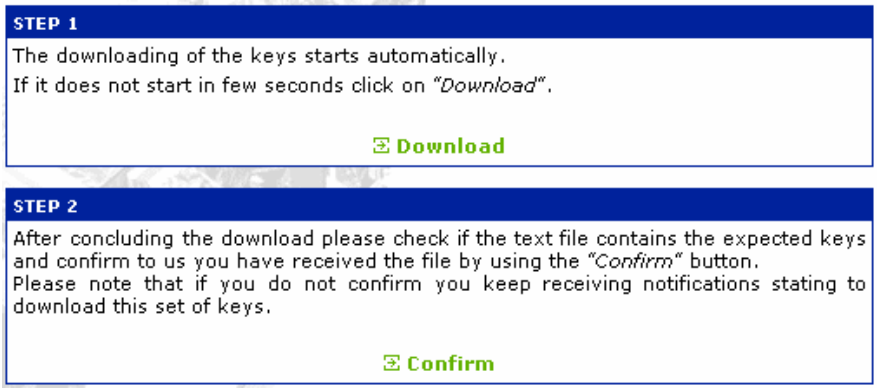

Figure 4 - "Downloading" Page

5. The file downloading should start automatically after 5 seconds. If not, click on the "Download" button to begin. Most of the browsers display a dialog box with two options: open the file or save the file. It is recommended to save the file for later use. The downloaded file is compressed ZIP file and can be opened with any ZIP tool. It contains a plain text file and an XML file with the new key sets. It also contains the DTD file with the definition of the XML file. The files contain the new key sets distributed according to the Channel (A/HRPT/ LRPT) and the SKU hexadecimal number.

6. After the file has been downloaded, confirm the download. To confirm the download click in the "Confirm" button. It is very important to confirm this action to indicate to EUMETSAT that you have received the notification and that the new keys are being uploaded to your reception station.

To upload new keys consult your reception station user/installation instructions provided by your station manufacturer.