

REGISTRATION OF A CTBTO USER AT ECMWF

(Please **read** the accompanying notes **before** completing this form. Please write **clearly**)

A)

This section is to be completed by the User

Full name of user: _____

Nationality of user: _____

Organisation: _____

Address: _____

Telephone / Extension: _____

E-mail address¹: _____

I **agree** to the conditions under which access to ECMWF's computer system is permitted² (see note overleaf)

User's signature²: _____

B)

This section is to be completed by the Computing Representative:

User identifier (3 characters)³:

In addition to ECGATE and ECFS services⁴, access to the services selected below is requested

HPCF: YES NO⁵

Project account(s)⁶: ECCTBTO _____

Group(s)⁷: CTBTO _____

MARS⁸ - access to current forecast data allowed YES NO

I confirm on behalf of the _____ (Institution) that usage will be **in accordance with the agreement between the ECMWF and the above Institution and for no other purpose**. I also confirm that, where applicable, the "Rules governing the distribution and dissemination of ECMWF real-time Products" as given in the "Guide to the Catalogue of ECMWF Products" will be adhered to.

Date: _____ Place: _____

Signed: _____ Title: _____

This section is for ECMWF use only

Checked by User Support, signed: _____ Date: _____

Authorised on behalf of ECMWF, signed: _____ Date: _____

Conditions of access to the ECMWF computer systems

In signing at A), the user **agrees** that:

- he/she will use the user identifier and the SecurID smart card for his/her own personal use and will not make it available to another person **under any circumstances**;
- he/she will use it solely **in accordance with Article 2 (f) of the ECMWF Convention**, which states

"The objectives of the Centre shall be:

(f) to make available to the meteorological offices of the Member States for their research, priority being given to the field of numerical weather forecasting, a sufficient proportion of its computing capacity, such proportion being determined by the Council;"

- he/she will use it in accordance with Annex A.3 of the Centre's Computer Security Policy, as laid down in ECMWF Computer Bulletin B0.2/3 which, in particular, states

"Annex 3 Passwords and smart cards

- *Passwords and smart cards protect the Centre's computer systems against unauthorised access. Smart cards are personal access tokens and, like user identifiers, are issued to users for their sole use. The underlying authentication process is based on the physical possession of these cards; hence smart cards must be kept securely.*
- *Login passwords and the PIN numbers of smart cards must be kept confidential and must not be disclosed to other persons*
- *All users shall:*
 - *employ non-trivial passwords and PINs;*
(...)
 - *safeguard smart cards issued to them against physical access by other persons;*
 - *change passwords or PIN numbers whenever there is any indication that the passwords or PIN numbers have been compromised;*
 - *report lost or stolen smart cards without delay. Member State users should report lost or stolen cards to (...) the Call Desk at ECMWF."*

The cards are property of the Centre and of some value until expiry. When no longer needed they should be returned to the Computing Representative.

NOTES

These notes should be **detached for reference** when completing the form and **retained** by the **user**. They should **NOT** be returned with the form.

Complete **part A** of the form.

Ensure that your Computing Representative has completed part B. See note 8 for situations where Member State Computing Representatives **must** countersign the form. Then post or fax the form to:

User Support
ECMWF
Shinfield Park
Reading RG2 9AX
UK

Fax: +44 118 986 9450

¹ Electronic Mail

Any email generated at ECMWF will be automatically forwarded to your email address. If you prefer a different arrangement, please specify.

² In signing, the user **agrees** that:

- he/she will use the user identifier and the SecurID smart card for his/her own personal use and will not make it available to another person **under any circumstances**;
- he/she will use it solely be **in accordance with the agreement between the ECMWF and the above Institution and for no other purpose**
- he/she will use it in accordance with Annex A.3 of the Centre's Computer Security Policy, as laid down in ECMWF Computer Bulletin B0.2/3 which, in particular, states

"Annex 3 Passwords and smart cards

- *Passwords and smart cards protect the Centre's computer systems against unauthorised access. Smart cards are personal access tokens and, like user identifiers, are issued to users for their sole use. The underlying authentication process is based on the physical possession of these cards; hence smart cards must be kept securely.*
- *Login passwords and the PIN numbers of smart cards must be kept confidential and must not be disclosed to other persons*
- *All users shall:*
 - *employ non-trivial passwords and PINs;*
(...)
 - *safeguard smart cards issued to them against physical access by other persons;*
 - *change passwords or PIN numbers whenever there is any indication that the passwords or PIN numbers have been compromised;*
 - *report lost or stolen smart cards without delay. Member State users should report lost or stolen cards to (...) the Call Desk at ECMWF."*

The cards are property of the Centre and of some value until expiry. When no longer needed they should be returned to the Computing Representative or ECMWF.

³ The Computing Representative should assign the 3 character user identifier. If the first **two** characters of the identifier are new, then a **Section Identifier Registration** form needs to be completed. These forms are available from User Support.

- 4 All users will automatically be registered for the SecurID card protected computing services on ECGATE, and for use of the Data Handling System (ECFS).
- 5 The underlined choice (e.g. NO for HPCF) indicates the default if no specific choice is made.
- 6 Project account: this will normally be assigned by the Computing Representative.
- 7 Group(s): by default users from one Institution/Organisation will be assigned to their Institution/Organisation group e.g. group “eumetsat” for EUMETSAT users.
Please **specify** any changes required to the above default assignments.
- 8 If no specific request is made, the default will be **no access** to currently valid forecast or analysis data.