Access to ECMWF computing systems. Replacement of ECMWF HID hardware token by TOTP software token

⚠ The HID service will be discontinued in **March 31st 2023**. Please migrate to the TOTP before that date

⚠ Time-based One-Time Passwords are only required for login access to:

- the Atos HPCF and ECS services service using Teleport SSH
- the ECaccess gateways
- ECPDS

Time-based One-Time Passwords are NOT required for logging in to the ECMWF web site, ecCharts, to use the WebAPI to download data from MARS or the CDSAPI to download data from the Copernicus Climate Data Store (CDS).

The ActivIdentity (HID) security token has been used for over a decade at ECMWF, replacing similar RSA tokens which were used before. These tokens provide a second factor for user authentication alongside a user's password, enabling strong authentication for security sensitive services such as login access to ECMWF's Unix systems and services such as ECPDS.

ECMWF is replacing the ActivIdentity tokens with the use of a Time-Based One-Time Password authenticator application, more accurately known as TOTP Client ("time-based one time password"). Typically, the TOTP clients are implemented on a smartphone, but they can also be installed in your laptop or any other computing devices. The Client is synchronised with systems at ECMWF by following the instructions at TOTP: How to activate. Clients usually use PIN codes, or biometric features, for protection.

In the case of a TOTP App installed on a smartphone, after the initial synchronisation, the One-Time Password (OTP) is displayed in the application and automatically changes every 30 seconds.

TOTP Apps have the following beneficial properties:

- Users are free to choose the TOTP App they use, as this is a widely used open standard for second factor authentication. You can find apps for this in the Apple Store, Google Store or Mac Application Store, some of them free, some of them commercial
- Management is self-service for the user through the use of QR Codes (2D barcodes) to establish synchronisation with ECMWF's systems.

What you need to do now

- The current HID tokens (the white small keyboard or phone app) **will stop working at the end of March 2023** so please ensure you are migrated by then
- Do remember that you can use your HID again (until the end of March) if you have any problem with the OTP, so there is no harm in testing the new system. Just delete all your OTP tokens and the HID will be enabled again.
- You may consider installing an TOTP application in your desktop computer in addition to your phone. If you have more than one TOPT you will need to specify which one you are using when logging in.
- ECPDS and ECaccess (boaccess.ecmwf.int) accept only the first TOTP configured. When the system asks for a passcode you should use the first TOTP you have ever configured. This is not indicated in the ECPDS/ECaccess login page.

Main OTP software options

- Google Authenticator
- Microsoft Authenticator
- LastPass Authenticator
- Red Hat FreeOTP

On a laptop

A few users have had good experiences with

- StepTwo (available for Mac and iPhone)
- OTP Manager

Of course, with OTP being a standard, you can find many other apps.

See for more information Using Time-based One-Time Passwords, and in particular TOTP: How to activate and TOTP: How to use