

Weather centre secures remote access with HID Global's strong authentication

Challenges:

- Enable users from meteorological offices across Europe to access ECMWF's supercomputers to obtain medium range weather forecasts
- Replace older generation, singlefunction solution which had become costly to maintain
- Integrate with ECMWF's proprietary management portal

Solutions

HID Global's strong authentication solution including:

- HID Global's 4TRESS™ AAA Server for Remote Access
- HID Global's Keychain Tokens

Benefits

- Preventing unauthorised network access
- Easy integration with corporate directory for user account management
- Web-based user self-help portal to reduce help desk costs
- Open standards authentication technology (OATH)
- Reduced total costs of operations

The European Centre for Medium Range Weather Forecasts (ECMWF), based in Reading, Berkshire, United Kingdom, provides 10-day weather forecasts for European meteorological offices. Funded by 28 member states at a cost of approximately £30m per year, it supplies forecasts to all of these countries as well as other nations, the World Meteorological Organisation and the European Space Agency.

Forecasts are produced by gathering data from satellites, buoys, ships and aircraft, which is then processed by ECMWF's High Performance Computing Facility (HPCF), comprising two identical but independent IBM Cluster 1600 supercomputer systems with a POWER5+ microprocessor. The two 68-server clusters are highly resilient, always available and provide the ECMWF team with the flexibility to upgrade applications without needing to shut down the network. The supercomputers not only process the data, but also act as a data repository for archived forecasts and reports.

Challenges

This advanced computing facility needed to be accessible to all of the member states as well as those that had cooperative agreements with the ECMWF to assist research and forecasting work. A robust identity assurance solution is therefore vital to ensure the identity of the user; otherwise sensitive data could be leaked to unauthorised users.

The ECMWF had been using a single-function proprietary token solution since 1995, which ensured secure remote access, but this solution had become too expensive to maintain. Didier Garçon, network analyst at the ECMWF, summarises the challenge: "Our old tokens expired in just three years, which means there was an almost constant need to replace and distribute them to new users. Because our users are based in nearly 40 different locations worldwide, the administrative cost involved in setting up new user profiles along with the token price was becoming prohibitively expensive."

Users were also finding the older generation tokens difficult to use which resulted in weekly complaints and increased the amount of administrative time required to manage the authentication framework.

Solutions

Garçon and his team conducted a comprehensive competitive evaluation of secure remote access solutions from HID Global and other providers.

One of the key considerations was that the solution had to interoperate with ECMWF's proprietary entity management system (EMS). This is accessed by the IT administrator in each of the organisations that require access to the ECMWF network, and allows them to issue and cancel user profiles as required.

The solution offered by systems integrator, Sysec, was based on HID Global's 4TRESS™ AAA Server for Remote Access solution using HID Global's Keychain Tokens, which generate a random one-time password for strong authentication to IT systems. The tokens are expected to last around six years, and come with a lifetime replacement warranty. Since HID Global is based on open standards, the integration with EMS was smooth, such that new users were automatically issued tokens with the appropriate permissions as soon as their new profile was created.

“The solution from HID Global and Sysec has already proved itself to be extremely reliable and easy for users. Because it is based on open standards technology, it integrates with our existing infrastructure and we also have the comfort in knowing that the technology is future-proof which will protect the investment that we’ve made.”

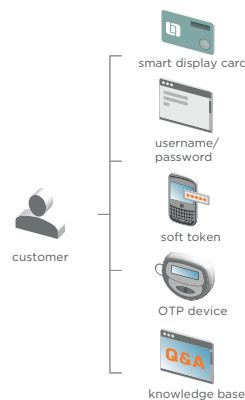
“HID Global was also the only company that could offer us an out-of-the-box tool: HID Global’s 4TRESS AAA Authentication Server for Remote Access which could be used as a web-based helpdesk for all of the administrators.”

Didier Garçon

Network Analyst

European Centre for Medium Range Weather Forecasts

HID Global’s Strong Authentication Solution: How it Works



- HID Global's OTP Tokens (Mini Token, Pocket Token, Token One, Desktop Token)
- HID Global's Display Card
- 3rd party tokens compliant with the Oath OTP standards (HOTP/TOTP/OCRA)
- Vasco Digipass tokens
- HID Global's Mobile Token
- HID Global's PC Token
- HID Global's Web Token
- DeviceID (Transparent Web Token)
- Strong passwords (full and partial)
- Security questions & answers (full and partial)
- x509 Certificate / PKI based authentication (OCSP / CRLs)
- Smartcards running the ActivIdentity OTP applet
- Out of band SMS (password or verification code)
- Out of band Email (password or verification code)
- Temporary activation codes
- LDAP
- RADIUS authentication

Total of 15 two factor authentication methods compliant with PCI-DSS and FFIEC guidelines

Solutions (Continued)

“HID Global was also the only company that could offer us an out-of-the-box tool: HID Global’s 4TRESS AAA Authentication Server for Remote Access which could also be used as a web-based helpdesk for all of the administrators.” Garçon adds. The ECMWF has already rolled out the solution to around 1000 members and users report that HID Global’s tokens are easier to use than the previous system.

HID Global’s strong authentication solution suite will be rolled out to an additional 2000 users over the coming months, with the older generation solution being gradually phased out. As a result, the need for regular replacement of tokens will be eliminated.

Garçon sums up the situation: “The solution from HID Global and Sysec has already proved itself to be extremely reliable and easy for users. Because it is based on open standards technology, it integrates with our existing infrastructure and we also have the comfort in knowing that the technology is future-proof which will protect the investment that we’ve made.”

Benefits

Preventing unauthorised access

The solution has already been rolled out to 1000 users to allow secure remote access to ECMWF’s supercomputer facility, with an additional 2000 members in the pipeline.

Open standards

HID Global’s solution integrates seamlessly with the ECMWF’s entity management system because it is based on open standards technology.

Cheaper to maintain

- HID Global’s tokens are predicted to last six years, compared to the older generation competitor tokens which had a three-year life, thereby significantly reduce administrative costs.
- Longer life OTP tokens reduce administrative costs of token replacement.
- The web-based self help portal reduced help desk costs.
- Integration with the corporate directory reduces administration costs by utilizing existing systems.

© 2013 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID Blue Brick logo, the Chain Design, and 4TRESS are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

2013-03-25-cc-iams-weather-centers-cs-en