ETS LIMITED

EUROPEAN COMMISSION

DIRECTORATE-GENERAL
CLIMATE ACTION

EU Registry

Security Plan

Contact:
VELGHE Ronald, Telephone:84052, ronald.velghe@ec.europa.eu

1. ROLES AND RESPONSABILITIES

Please refer to **[Roles and Responsibilities]**.

2. SERVER SECURITY

The Weblogic servers and Oracle Database servers are protected by login and password. Remote access requires a VPN connection whose authentication scheme relies on the use of personal tokens. The servers are also confined within a logic network domain which is firewalled and protected against viruses.

The EU Registry has been classified as "EU CONFIDENTIAL". Therefore the physical machines hosting the EU Registry servers are stored in a class II security area accordingly with the provisions presented in section 18.3 of **[Internal Rules of Procedure]**. The access to the machines is reserved to officials who have undergone the screening procedure presented in section 20 of **[Internal Rules of Procedure]**. Other persons can access the machines when necessary but only if they are accompanied by trusted personel who have undergone the screening procedure.

3. USER AUTHENTICATION

The EU Registry being a system of the European Commission, the authentication of its users is handled by the ECAS (European Commission Authentication Service). The basic authentication under ECAS relies on username/password, the password must be at least 10 characters long and the chose characters must belong to at least 3 of the following character groups:

- Upper Case: A to Z
- Lower Case: a to z
- Numeric: 0 to 9
- Special Characters: !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~

Examples: qlpDhXaGh2, IOphEZAqL8, EQ9HwOEtnv

The passwords expire 180 days after their creation or update. A notice is sent by e-mail to the user 5 days before the expiration. If a user enters five consecutive times a wrong password then this user is blocked for 15 minutes during which he cannot try to log in.

For sensible applications such as the EU Registry, ECAS also implements a second level of authentication which relies on the use of a non-encrypted SMS containing a one-use and short-lived (5minutes) code sent to the mobile phone of the user. Finally please note that there is an under work project named Stork. The aim of this project is to enable ECAS to use electronic identity card as a second level of authentication. Assuming that this project is a success and is widely adopted by member states then the EU Registry might use in the future electronic identity card as a second level of authentication. It is foreseen that the support of electronic identity card should be effective within 5 years.

This authentication mechanism applies to all users including the member state administrators.

4. USER AUTHORISATION

As the user authentication is handled by ECAS, an external agent, and as the registry administrators want to control who can access the non-public Web pages of the EU Registry dedicated to their member state; an ECAS login is not sufficient for getting access to the non-public pages of the EU Registry such as the Account List, the Transaction List, etc.

A user who wants to be granted access to a member state's registry hosted by the EU Registry must first fill an online form for providing personal information along with scans from its identity

papers. Upon review, the registry administrator decides whether or not the access request is granted. Please note that a registry administrator granting access to his registry to a specific user does not affect the access rights of the same user for the other registries. Therefore a user who wants access to several registries hosted by the EU Registry must repeat the procedure for each registry. Once the user request has been accepted and that he becomes representative of at least one account in the registry, he receives offline (conventional mail, phone, etc.) an enrolment key that he must enter online in order to be given access to the registry.

For administrators, the processus is the same except that the enrolment key is directly sent to them upon approval of their registration request. They do not need to be nominated representative of an account.

5. TRADING PLATFORMS AUTHENTICATION

The trading platform systems send requests to the EU Registry for initating transaction on behalf on their clients, querying the balance of a managed account, etc. The authentication of the trading platform will be performed by verifying that their requests are digitally signed and that the used digital certificate is valid.

6. SESSION SECURITY

The EU Registry communicates over the Internet with the following systems and persons:

- Users and administrators;
- ITL;
- Trading platforms systems.

Please note that the EUTL is not listed above because it is hosted alongside the EU Registry in the EC Luxembourg primary site. Therefore communications between the two systems are confined within the secured network of the EC and do not require encryption.

The communication between the EU Registry and the ITL are encrypted accordingly with the provisions presented in section 3.3 of [**DES**]. The communications between the EU Registry and the users, administrator, and trading platforms use TLS (Transport Layer Security) connections in order to ensure the encryption of communication. The TLS protocol is an evolution of the SSL protocol which is more secure. The used version of TLS is 1.0 or above.

7. AUDITING

The log files generated by the Weblogic servers, Oracle Database servers, operating systems are stored and backed up. No cleanup of those files is currently foreseen. An automated monitoring of those log files has been set in order to detect intrusion attempts and othe suspect activities.

The EU Registry also generates application logs fore each member state which contain an entry each time a user executes an action in the EU Registry Web interface or when a trading platform sends a request. An action can be the initation of a transfer, the consultation of an account, etc. The log entry will provide the unique identifier of the person or system at the origin of the action, the IP address used, and details of the action (e.g. for the creation of account it would be the account identifier, its type, etc.). Finally, the EU Registry for each incoming or outgoing Web service message, the EU Registry generates a disctinct log file containing a copy of the message and writes an entry in a database table for recording general details of the message (sender, receiver, WS operation, etc) and the name of the generated log file.

8. DEPRECATED AND REVOKED USERS

A user who is no longer associated to any account or a user suspected or convinced of having broken European or national rules related to the use of the EU Registry will be un-enrolled by an administrator meaning that the EU Registry will refuse subsequent login requests from this user. No user accounts will ever be deleted. A user who has been un-enrolled can be re-enrolled but with a different user account which will be linked to the same ECAS account. The same ECAS account cannot be related to more than one open user account at any time.

9. NON-REPUDIATION

The EU Registry requires the user to sign important operation such as the initiation of transaction, the modification to administrators, and the modifications to the unit block holdings. This signature is handled by ECAS and it consists in sending to the user a non-encrypted SMS containing a summary of the operation along with a short-lived (5minutes) one-off code. The user reviews the SMS and if the content matches the expected details, then the user enters the code hereby signing the operation.

10. PRIVATE KEY PROTECTION POLICY

The private keys are stored in password-protected JKS keystores which are stored in the file system of the EU Registry server and therefore replicated in the DRP site and backed up. Only the Central Administrator knows the passwords of the keystores and of the contained keys (each private key has its own password).