ANNEX XV

Security standards

Communication link between the Community independent transaction log and each registry

1. **[**[F1]When the communication link between the Community independent transaction log and the UNFCCC independent transaction log is not established, all processes concerning allowances, automatic national allocation plan table changes, verified emissions and accounts shall be completed using a communication link with the following properties:**]**

Textual Amendments

F1 Substituted by Commission Regulation (EC) No 916/2007 of 31 July 2007 amending Regulation (EC) No 2216/2004 for a standardised and secured system of registries pursuant to Directive 2003/87/EC of the European Parliament and of the Council and Decision No 280/2004/EC of the European Parliament and of the Council (Text with EEA relevance).

(a) Secure transmission shall be achieved through the use of secure socket layer (SSL) technology with a minimum of 128 bit encryption.

(b) The identity of each registry shall be authenticated using digital certificates for the requests originating from the Community independent transaction log. The identity of the Community independent transaction log shall be authenticated using digital certificates for each request originating from a registry. The identity of each registry shall be authenticated using a user name and password for each request originating from a registry. The identity of the Community independent transaction log shall be authenticated using a user name and password for each request originating from the Community independent transaction log. Digital certificates shall be registered as valid by the certification authority. Secure systems shall be used to store the digital certificates and usernames and passwords, and access shall be limited. Usernames and passwords shall have a minimum length of 10 characters and shall comply with the hypertext transfer protocol (HTTP) basic authentication scheme (http://www.ietf.org/rfc/rfc2617.txt).

[[F1]2. When the communication link between the Community independent transaction log and the UNFCCC independent transaction log is established, all processes concerning allowances, automatic national allocation plan table changes, verified emissions, accounts and Kyoto units shall be completed using a communication link with the properties set out in the functional and technical specifications for data exchange standards for registry systems under the Kyoto Protocol, elaborated pursuant to Decision 24/CP.8 of the Conference of the Parties to the UNFCCC.**]**

Communication link between the Community independent transaction log and its authorised representatives, and each registry and all authorised representatives in that registry

3. The communication link between the Community independent transaction log and its authorised representatives, and between a registry and the authorised representatives of account holders, verifiers and the registry administrator, when the authorised representatives are obtaining access from a network different from the one serving the Community independent transaction log or that registry, shall have the following properties:

(a) Secure transmission shall be achieved through the use of secure socket layer (SSL) technology with a minimum of 128 bit encryption.

(b) The identity of each authorised representative shall be authenticated through the use of usernames and passwords, which are registered as valid by the registry.

4. The system for issuing usernames and passwords pursuant to paragraph 3(b) to authorised representatives shall have the following properties:

(a) At any time, each authorised representative shall have a unique username and a unique password.

(b) The registry administrator shall maintain a list of all authorised representatives who have been granted access to the registry and their access rights within that registry.

(c) The number of authorised representatives of the Central Administrator and registry administrator shall be kept to a minimum and access rights shall be allocated solely on the basis of enabling administrative tasks to be performed.

(d) Any default vendor passwords with Central Administrator or registry administrator access rights shall be changed immediately after installation of the software and hardware for the Community independent transaction log or registry.

(e) Authorised representatives shall be required to change any temporary passwords they have been given upon accessing the secure area of the Community independent transaction log or registry for the first time, and thereafter shall be required to change their passwords every two months at a minimum.

(f) The password management system shall maintain a record of previous passwords for an authorised representative and prevent re-use of the previous ten passwords for that authorised representative. Passwords shall have a minimum length of 8 characters and be a mix of numeric and alphabetical characters.

(g) Passwords shall not be displayed on a computer screen when being entered by an authorised representative, and password files shall not be directly visible to an authorised representative of the Central Administrator or registry administrator.

Communication link between the Community independent transaction log and the general public, and each registry and the general public

5. The public area of the website of the Community independent transaction log and the public website of a registry shall not require authentication of its users representing the general public.

6. The public area of the Community independent transaction log website and the public area of a registry website shall not permit its users representing the general public to directly access data from the database of the Community independent transaction log or the database of that registry. Data which is publicly accessible in accordance with Annex XVI shall be accessed via a separate database.

General security requirements for the Community independent transaction log and each registry

7. The following general security requirements shall apply to the Community independent transaction log and each registry:

(a) A firewall shall protect the Community independent transaction log and each registry from the Internet, and shall be configured as strictly as is possible to limit traffic to and from the Internet.

(b) The Community independent transaction log and each registry shall run regular virus scans on all nodes, workstations and servers within their networks. Anti-virus software shall be updated regularly.

(c) The Community independent transaction log and each registry shall ensure that all node, workstation and server software is correctly configured and routinely patched as security and functional updates are released.

(d) When necessary, the Community independent transaction log and each registry shall apply additional security requirements to ensure that the registry system is able to respond to new security threats.

Status:
Point in time view as at 01/01/2009.

Changes to legislation:
There are currently no known outstanding effects for the Commission Regulation (EC) No 2216/2004 (repealed), ANNEX XV.