EESTI PANK
GOVERNOR'S DECREE No. 9

Tallinn, 9 December 2011

Requirements for submission of reports
formatted as XML documents

The Decree is established on the basis of subsection 91 (1) of the Credit Institutions Act.

Chapter 1
GENERAL PROVISIONS

§ 1. Scope of the Decree
The Decree establishes technical requirements for the submission of reports formatted as XML documents to Eesti Pank and the Financial Supervision Authority.

§ 2. Application of the Decree
The Decree is applied to credit institutions and branches of foreign credit institutions operating in Estonia that are obliged to submit reports formatted as XML documents.

§ 3. Definitions used in the Decree
Definitions having the following meaning are used in this Decree:

1) **"Report"** is a data set with information value established by the legislation the content of which is true and integral to the extent required by legislation;

2) **"Report message"** is a formally correct XML document containing the report (*Extensible Markup Language*, defined in the recommendation of the World Wide Web Consortium http://www.w3.org/TR/REC-xml);

3) **"Reporting entity"** is a legal person obligated to submit reports;

4) **"Addressee of reporting"** is Eesti Pank and/or Financial Supervision Authority;

5) **"Transmission of message"** is making the report message electronically available to the addressee of reporting;

6) **"Submission of report"** is the transmission of a formally correct report complying with the Decree establishing the report to an addressee of reporting.

Chapter 2
Format of reports and XML schemas

§ 4. Format of reports
(1) Report messages are formatted as XML documents.
(2) The structure and contents of report messages are determined on the basis of XML schemas (http://www.w3.org/standards/xml/Schema) referred to through the web page http://www.fi.ee/schemas.
(3) An example how to format report messages is located on the webpage of Eesti Pank in the subheading "For reporters" under heading "Statistical indicators".

§ 5. XML schemas
(1) The contents of report messages are determined by the XML schema describing the general structure and by the XML schema connected to the specific report. The XML schema of a report is the formalised presentation of contents of corresponding report which has been established by the legislation.

(2) The XML schema 'x_headers.xsd' describing the general structure of report message is located at the web address http://www.fi.ee/schemas.
(3) The XML schema describing the report has a version number which shows the changes in the report (or also in the schema) over time. The web address of the XML schema searched for is located at http://www.fi.ee/schemas/[versioon]/[fail] where the text in square brackets marks the value of respective element. The values for elements "version" and "file" are found on the basis of the report code and the validity of report from the file 'skeemid.xml' at the web address http://www.fi.ee/schemas.
(4) XML schema is the basis for establishing the formal correctness of the report message. A report message is formally correct if it complies with the valid XML schema.

Chapter 3
Securing data transfer

§ 6. Securing report messages
(1) Report messages are secured by encryption and/or digital signature.
(2) Public-key algorithms are used for securing the report messages which are realized by applications (for example, PGP, GnuPG, DigiDoc Client) supporting platforms OpenPGP (http://www.ietf.org/rfc/rfc4880.txt) or DigiDoc (http://www.sk.ee/digidoc/).
(3) If a public channel is used for the transmission of a report message (e.g. Internet), the report message has to be encrypted and digitally signed.
(4) If a secure channel is used for the transmission of a report message (e.g. HTTPS), the report message may be just digitally signed.

§ 7. Securing with OpenPGP
(1) The following requirements have to be complied with upon using OpenPGP:
1) The type of the encryption and signing key has to be RSA;
2) The minimum length of the public side of the key pair has to be 1024 bits;
3) Encryption algorithm may be 3DES or CAST5. The use of IDEA encryption algorithm is allowed but not recommended;
4) Hash function may be SHA1. The use of MD5 hash function is allowed but not recommended.

(2) The public key of the application receiving the reports is located at the web address referred to in § 5 (2) of this Decree.

§ 8. Securing with DigiDoc
(1) If DigiDoc is used, the DigiDoc platform will determine the keys and the terms for using digital signature and encryption.
(2) The identification of the public key to be used in the application receiving the reports is located at the web address referred to in § 5 (2) of this Decree.

Chapter 4
Key Management

§ 9. Key management upon using OpenPGP
(1) The following requirements shall be applied to key management:
1) The key identification has to contain the code of the reporting entity, the word "ARUANDLUS", the name of the person using the key pair and the final date of validity of the key pair;
2) Key pairs have to be renewed on a regular basis, at least once every two years;
3) Used key pairs have to be preserved in order to ensure the availability of exchanged data;
4) Invalid key pairs have to be removed from further use.

(2) The following requirements shall be applied to the reporting entity's organization of work:
1) The reporting entity has to appoint a ranking representative for organizing data exchange whose duty is to ensure that the reporting entity's key are made (incl. the replacement of key pairs which have become unusable), that the keys are used by the reporting entity's authorised employee(s) and the availability of exchanged data;

2) In order to start the exchange of data the reporting entity's ranking representative has to send the ranking representative of the addressee of reporting (preferably in digital form) a signed public key and the legal instrument for changing the key; the legal instrument for changing the key shall indicate the reporting entity's name, the key identification(s) and authorised employee(s); the reporting entity's signatory shall sign the legal instrument for changing the key;
3) Only authorised employee(s) are allowed to know the password phrase protecting the reporting entity's secret key of the key pair.

(3) If keys are renewed on a regular basis, the reporting entity and the addressee of reporting shall replace new public key by digital signature.

(4) In case of an emergency situation when the secret key has become unusable (e.g. it has become public or it has been damaged) the addressee of reporting/reporting entities are notified thereof promptly, a new key pair is generated and taken into use.

§ 10. Key management upon using DigiDoc
(1) The key pair must have a unique identification which has to include the name of the reporting entity in case of the reporting entity's ID-card. In case of a personal ID-card, the personal identification code is the unique identification.

(2) The following requirements shall be applied to the reporting entity's organization of work:
1) The reporting entity has to appoint a ranking representative for organizing data exchange whose duty is to ensure that the reporting entity's keys (ID-cards) are obtained (incl. the replacement of ID-cards which have become unusable), that the keys are used only by the reporting entity's authorised employee(s) and the availability of exchanged data;
2) In order to start the exchange of data the reporting entity's ranking representative has to send the ranking representative of the addressee of reporting (preferably in digital form) a signed legal instrument. The legal instrument shall indicate the reporting entity's name, the identification(s) of used ID-cards(s) and authorised employee(s). The reporting entity's signatory shall sign the legal instrument;
3) Only authorised employee(s) are allowed to know the password phrases (PIN1, PIN2) protecting the secret keys of the reporting entity's of ID-cards(s).

Chapter 5
Transmission of report messages and deeming the reports to have been submitted

§ 11. Requirements for the transmission of report messages
(1) Upon using E-mails, the signed and encrypted report message(s) has (have) to be sent as attachment(s) to the address xml@fi.ee. Every attachment may contain only one report message.
(2) The transmitted E-mail has to be in MIME encoding. The text part (the body field) of the E-mail is ignored.
(3) The number of E-mail attachments is not limited but it is recommended to follow the good practice of the E-mail total volume (at maximum 10 megabytes).
(4) Reducing the volume of a report message enclosed to the attachment by electronic means, i.e. zipping is not allowed.
(5) Upon using data transmission protocols not referred to in this section (e.g. HTTPS), the specific transmission mode is specified by the operating procedure of applications being used.

§ 12. Primary processing of report messages
(1) Primary processing of report messages will be performed using the application for receiving reports of by the addressee of reporting.
(2) The application for receiving reports shall send the reporting entity a confirmation concerning the arrival of a report message only if the value of the element <comment> was "yes". In this case the reporting entity will be sent a message containing the name of the file name included in the attachment, the codes of the report and the reporting entity and the date of the report. This message is also the confirmation of the addressee of reporting for the reporting entity that the report message has been forwarded.

(3) Messages concerning the errors ascertained in the report message are sent to the addressee appointed by the reporting entity both in text format and as a file in XML format.
(4) Error messages concerning the general format of the report message are sent to the address shown in the header of the report message. Error messages concerning the contents of the report are sent to the address indicated in the header of the report.
(5) If the value of the element <comment> is not empty, the application for receiving reports shall send the information therein to the processor of corresponding report appointed by the addressee of reporting.

§ 13. Transmission of warnings to reporting entities
If a formally correct report has not been transmitted by the prescribed term, a reporting entity is sent a corresponding warning. The warning is sent to the E-mail address determined by the ranking representative of the reporting entity.

§ 14. Deeming the reports to have been submitted
A report is deemed to have been submitted if the content of a report is correct and it has been prepared and forwarded in compliance with the requirements established by this Decree.

Andres Lipstok
Governor