BULGARIAN STOCK EXCHANGE - SOFIA

БЪЛГАРСКА ФОНДОВА БОРСА
СОФИЯ

TECHNICAL PROCEDURE CONCERNING THE SECURITY MECHANISMS USED FOR DATA ENCRYPTION, PROTECTION OF CERTIFICATE GENERATION AND STORAGE PROCESSES, AND THE CONDITIONS FOR DISSEMINATION OF CERTIFICATE VALIDITY DATA BY BSE-SOFIA AD

Procedures for generation of electronic certificates by the Exchange

1. To ensure the required protection and security level for trading in COBOS, the subscribers of the Exchange authorise BSE to create and define electronic certificates (keys) for the individual users.
2. The keys issued by the BSE are used for signing electronic certificates (certificates) and serve for identifying the particular user (object). The electronic certificate links the public key to a natural person or to an organization. The link is confirmed by a trusted source.
3. BSE-Sofia, in the capacity of COBOS developer and provider of security services for electronic data exchange, issues certificates only with limited application and sets up its own Certification Agent, which signs the certificates of the objects as well as COBOS server certificate.
4. COBOS is accessible only by users, who possess valid certificates signed by COBOS in the capacity of Certification Agent. Depending on the certificate the subscribers are given different rights for access to the information in COBOS and for performing various types of transactions.
5. Each certificate contains details about the name of the holder, its email address, location, certificate validity. The certificate also contains details about the public key and a unique value (hash), which guarantees that the certificate has not been changed.
6. The unique value is a number obtained by means of a hash-algorithm. Applying the algorithm to the message does not allow the original message to be recovered from the unique value.
7. If the message is changed, the unique value changes too. This guarantees that non-authorised third parties can not modify the message unnoticed.
8. The process of issuing a user certificate using COBOS or other means provided for by Exchanges comprises the following steps:
   - 8.1. The object sends to the Exchange an application for issuance of a certificate. This application generates a CRS file (Certificate Signed Request), which contains the following information as minimum:
     - 8.1.1. Holder name
     - 8.1.2. PIN/BULSTAT
     - 8.1.3. Number of the identity document/tax identification number
     - 8.1.4. City
     - 8.1.5. Country code
     - 8.1.6. Expiry date of the certificate
     - 8.1.7. Email address
   - 8.2. The respective COBOS administrator registers the user and defines the user's rights.
   - 8.3. The administrator of the Certification Agent referred to in paragraph 9 verifies the registration and identification details against the information provided on the paper copy of the application submitted to the Exchange.
   - 8.4. The administrator of the Certification Agent proceeds with the generation of the certificate.
   - 8.5. The certificate, signed by Exchange and converted in a format suitable for installation on the browser, is sent by email to the holder's email address provided at the time of registration.

Procedures concerning protection and storage of certificates and the conditions for dissemination of certificate validity data

9. Generation and storage of keys by the Exchange takes place in a physically secure environment by authorised employees of the Exchange (administrators of the Certification Agent) under dual control as a minimum. Such employees have to be authorized by an order issued by the Executive Director of the Exchange.
10. The details entered by the subscriber are stored on a secure server of the Exchange in case the certificate has to be reinstated.
11. The private keys of all subscribers are generated automatically and stored on a secure server of the Exchange.
12. The private key of COBOS is stored on a secure server of the Exchange.
13. The private key of COBOS and to the private keys of the subscribers are accessible upon entry of passwords by two independent administrators of the Certification Agent.
14. The Exchange maintains a Certificate Revocation List with certificates, the validity of which validity has not expired yet, but are not valid for another reason. This list is stored on a secure server. After each trading session the Exchange publishes the Certificate Revocation List.
15. The secure server is set up as follows:

15.1 Access to the server from any networks is prohibited; only HTTPS connection is allowed for operating in COBOS;

15.2. The private keys and the certificates are kept in an encrypted form, signed by the private key of the Exchange, in a redundant file configuration (in two different directory trees);

15.3. The details the private keys and certificates are saved simultaneously on two hard disc pairs installed on the server.

Procedures for buildings an encrypted connection between the object and the Exchange server

16. Encryption is based on a public/private key pair, which guarantees that the data encrypted with a particular public key can be read only by one specific private key (a pair of asymmetric keys).
17. Using the same key for encryption and decryption is not possible.
18. The process of establishing a connection and exchanging of data between the object and the server comprises the following steps:

18.1. The object's browser sends a request to the secure HTTP server.

18.2. The object sends its public key to the server.

18.3. The server verifies the object’s identity by checking the certificate. The check covers its validity and whether it has been signed by a third trusted party. If the certificate has expired or has been signed by a third non-trusted party, the server sends a warning message and terminates the connection.

18.4. The server sends its own public key and its certificate.

18.5. The browser checks whether the certificate is valid and signed by a third trusted party (root Certificate Authority).

18.6. The browser uses the public key for encrypting a random symmetric key and sends it to the server together with the requested data.
18.7. The server decrypts the data decryption symmetric key.
18.8. The server returns the data requested by the browser encrypting them with the symmetric key.
18.9. The browser decrypts the data using the symmetric key and displays the data.