1.6.2007

Security guide of the Posti's electronic services

1. General Information

This document describes how Posti Group Corporation (later Posti) safeguards its customers´ electronic services that require identity verification. For more detailed information, please refer to "Instruction" section on the service menu after login.

2. User Registration

When you register as a user of electronic consumer services, your identity will be verified via an online banking authentication service, by means of an ID card with a chip or at the post office. After that, you will have an access to the service via the username and password given by the Posti, your online bank user ID or your ID card with a chip.
With respect to extranet services for business customers, a company will conclude a customer agreement with Posti for the use of the services. After that, Posti will provide the verified corporate representative with extranet access codes. This person is authorised to administer these codes for his/her company.

3. Username and Password

Your username and password together will give you an access to the services and your personal data recorded in these services. Therefore, you should store them as carefully as you store your bankcard's PIN code. Please keep your username and password separate from each other.

4. User's Personal Data and Equipment

The information required for providing the services will be recorded in the customer register. This information may be used for purposes specified in the File Description and will not be given to the third parties for marketing purposes. Posti will compile user statistics for the service, including, for example, the session time and frequency, and the computer's IP address, which it will use for the development of the service and for other maintenance purposes. This information will not be linked with the user's name and address information.
The service will use cookies, as prescribed by Section 9 of the Privacy Protection Act (516/2004), only when:

- Doing so is necessary for the implementation of the service, or
- The only purpose of using them is to implement or facilitate communication in networks

The customer shall ensure that:

- The computer hardware and other equipments, software and data communications (s)he uses meet the standards of which (s)he has been notified by Posti
- (S)he provides the information required for the service and that this information is accurate and up to date
- (S)he does not forward or otherwise process material that violates copyrights, good practices, the law or official regulations, or that contains computer viruses or other detrimental features

5. Secure Online Sessions

During login, the browser will establish a secure connection between the service and the PC. Consequently, the transfer of username and password is encrypted, making it impossible for anyone else to know, change or copy them.
The locked padlock icon at the bottom of the browser window ensures a secure online session. Posti will guarantee the security of the online connection between the service and PC only concerning its own
pages.

After logging out of Postis service or entering to the sites of third parties, Posti will no longer be responsible for the level of information security.

6. Session Encryption

For the purpose of securing message transfer within online connections between Postis electronic Consumer services and the customer, SSL (Secure Sockets Layer) encryption technology supported by browser programs is used. The browser program will create a session key that will be transmitted in encrypted form to Posti. The session key is used to encrypt the contents of the message and to calculate the checksum that guarantees the immutability of the message.
The certificate used by Postis servers, can be checked that PC is connected to Posti. The certificate information can be verified by double-clicking Internet Explorer of Firefox browser's padlock icon at the bottom of the screen and verifying the information in the 'details´ section

7. Logging Off

Log out from the online session as soon as you do not need it. For security reasons, the online session will be terminated automatically if the service is not used for 60 minutes. If the online connection is disconnected in any other way, the system will automatically terminate the session.
In order to accelerate their operation, browser programs make use of the so-called cache memory. We recommend that the cache will always be cleared after an online session so that nobody else using the same computer can view your used pages. Instructions for clearing the cache are available on the service menu.

8. Additional Information

Our Call Centre will be pleased to help you if you have any questions or problems related to the information security of our ectronic services. Please see contact information on the service menu.