Chapter 1

Strong Customer Authentication and Common and Secure Methods of Communication

Article 22 General requirements

(1) Payment service providers shall ensure the confidentiality and integrity of the personalised security credentials of the payment service user, including authentication codes, during all phases of the authentication.

(2) For the purpose of paragraph 1, payment service providers shall ensure that each of the following requirements is met:

(a) personalised security credentials are masked when displayed and are not readable in their full extent when input by the payment service user during the authentication;

(b) personalised security credentials in data format, as well as cryptographic materials related to the encryption of the personalised security credentials are not stored in plain text;

(c) secret cryptographic material is protected from unauthorised disclosure.

(3) Payment service providers shall fully document the process related to the management of cryptographic material used to encrypt or otherwise render unreadable the personalised security credentials.

(4) Payment service providers shall ensure that the processing and routing of personalised security credentials and of the authentication codes generated in accordance with Chapter 2 take place in secure environments in accordance with strong and widely recognised industry standards.