Annex to the Authentication Data Transfer Services Agreement of [date]

SPECIFICATIONS FOR THE TRANSFER OF AUTHENTICATION DATA

1. Technical Requirements for the Realisation of Authentication

1.1. Integration of authentication data required by the Bank on the Service Recipient’s website (hereinafter referred to as the Website).

The Bank’s authentication system must be registered on the Website with the following parameters:

1. Web address of the authentication home page (URL). This address will be used to provide an initialisation command for the authentication procedure with a link to the source, i.e. the Website. Following the successful authentication in the Bank’s system, automatic redirection could be realised and authentication package could be returned to the Website;
2. The Bank's public key.

The following parameters of the Service Recipient must be registered and used in the Bank’s authentication system:

1. Web address of the Website page (URL) to which the User is directed after successfully completing the authentication procedure and to which an authentication package is sent;

Server clocks of the Bank’s Website (hereinafter referred to as the Bank’s Website) must be synchronised with the internet’s atomic clocks, because accurate authentication time is one of the parameters of the authentication package. The same requirement also applies to the servers of the website of the Service Provider.

Measures used to generate the authentication packages and redirect them to the Website must be realised on the Bank’s Website in accordance with the technical requirements set out below.

During a normal operating mode, the pages of the Bank’s Website must include links, menus or other controls that can be used by the user who was successfully authenticated in the Bank’s system to interactively access the Website without the need to perform repeated authentication.

1.2. Integrated authentication process

Authentication data are transferred on the basis of the Server-Client-Server principle, where the redirection between the Websites and the authentication packages is physically realised using the internet browser on the User's device even though the initiated and transported data are generated on the servers of the Website and the Bank’s Websites.
.

1.3. Authentication scenarios

Integrated authentication is performed in two ways:

1. The User initiates a session on the Website;
2. The User initiates a session on the Bank’s Website.

Detailed descriptions of both scenarios are provided below.

1.3.1.The user initiates a session on the Website (*Fig. 1 Initiating a Session on the Website*):

1. the User visits the Website, chooses the desired bank from the list of pre-registered banks and clicks on the authentication button;
2. The User is redirected to the authentication page of the Bank’s Website using the HTTPS GET parameter, which identifies the system to which the connection is requested.
3. The User is authenticated on the Bank’s Website following a standard (usual) procedure;

4. Upon successful identification of the User, an authentication package is formed on the Bank’s Website and redirection to the Website is initiated by forwarding the authentication data using the HTTPS POST method (dataset BANK-01).

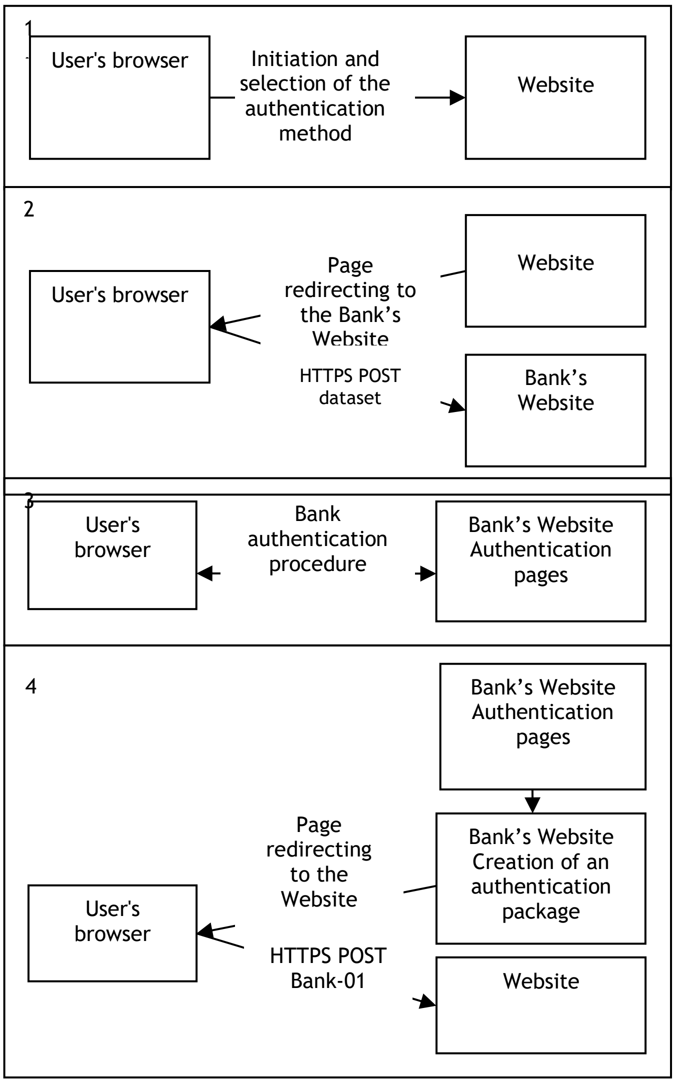
1
User's browser
Initiation and selection of the authentication method
Website
2
User's browser
Page redirecting to the Bank’s Website
Website
HTTPS POST dataset
Bank’s Website
3
User's browser
Bank authentication procedure
Bank’s Website Authentication pages
4
Bank’s Website Authentication pages
Page redirecting to the Website
Bank’s Website Creation of an authentication package
User's browser
HTTPS POST Bank-01
Website

Fig. 1 Initiating a Session on the Website

1.3.2. The User initiates a session on the internet bank (*Fig. 2 Initiating a Session on the Internet Bank*):

1. The user initiates an internet bank session immediately and completes the usual authentication procedure;
2. The User performs the desired functions on the internet bank;
3. In the specific section of the internet bank, the user chooses to access the Website and clicks on the respective button. The internet bank then generates an authentication package and automatically initiates the redirection to the Website by forwarding the authentication data using the HTTPS POST method (dataset BANK-01).

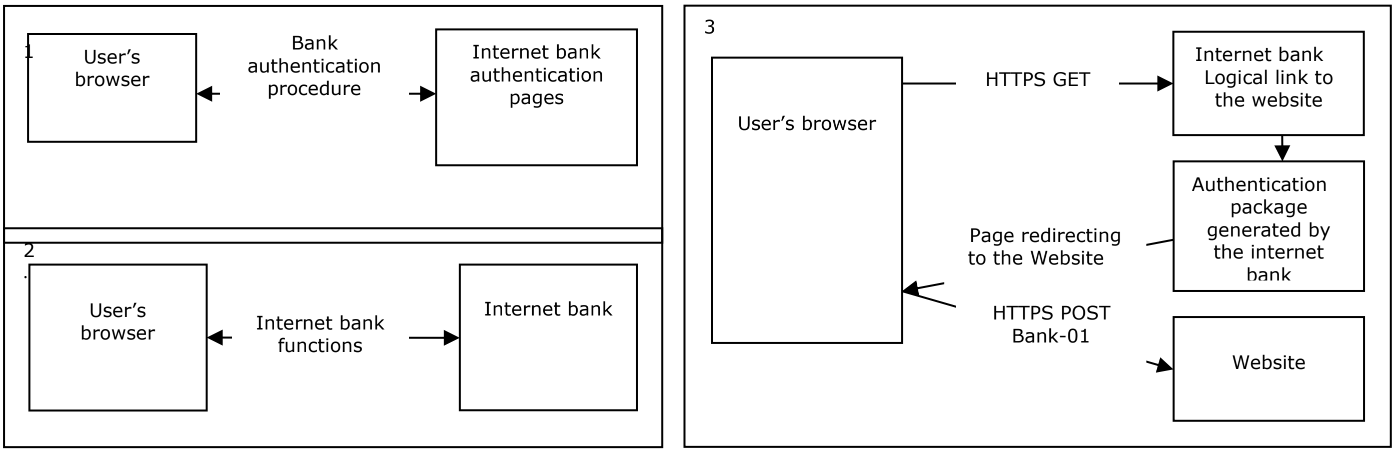
1
User’s browser
Bank authentication procedure
Internet bank authentication pages
2
User’s browser
Internet bank functions
Internet bank
3
User’s browser
HTTPS GET
Internet bank Logical link to the website
Authentication package generated by the internet bank
Page redirecting to the Website
HTTPS POST Bank-01
Website

Fig. 2 Initiating a session on the internet bank

2. Authentication Data

2.1 Natural persons

The following User authentication data must be identified in the Bank’s system and transferred to the Website:

1. Current time of authentication in the Bank’s system (on a per-second basis).
2. National identification number of the person;
3. Name of the natural person;
4. Surname of the natural person.

Text data from the package are delivered using the standard UTF-8 encryption.
Authentication data are transferred to the Website as different parameters of the BANK-01 package.

3. Security

3.1. Security of data transfers

Security of data transfers is ensured by the HTTPS protocol used for data exchange, when redirecting the user between the Website and the Bank’s Websites, as well as within the Websites.

3.2. Signing the authentication data

Authentication data must be digitally signed using the Bank’s private key and the **RSASSA-PKCS1-v1_5** with a **SHA-1** HASH-function.

The Bank’s public key certificate used for signature control must be handed over to the Service Recipient and registered at the moment of conclusion of the final agreement on the Website.

The digital signature must be calculated for a text string comprising all authentication data parameters.

Natural persons: *SRC || TIME || PERSON_CODE || PERSON_FNAME || PERSON_LNAME*

Legal persons: *SRC || TIME || PERSON_CODE || PERSON_FNAME || PERSON_LNAME || COMPANY_CODE || COMPANY_NAME*

Where || is the operation for combining the text strings, rather than a divider. Parameter names are presented in accordance with the BANK-01 package.
The calculated digital signature must be sent to the Website in a separate parameter of the BANK-01 package.

Natural Persons

From the Website, the authentication page of the Bank's Website is accessed using the HTTPS GET method and the address
https://e.sb.lt/authorization/login?system=

BANK-01

This parameter dataset is sent from the Bank's Website to the authentication page of the Website using the HTTPS POST method and the following address:

Structure of the parameter dataset:

Parameter	**Maximum Length**	**Purpose**
SRC	20	Inquiry source code – **Bank code**
TIME	20	Date and time of redirection of the user from the Website to the Bank's Website (on a per-second basis). Date is transferred in a text format ***YYYY.MM.DD hh:mm:ss***
PERSON_CODE	20	National identification number
PERSON_FNAME	100	First name of the person
PERSON_LNAME	100	Last name of the person
SIGNATURE	300	Digital signature of the Bank for the authentication data converted into the BASE64 format. The signature is calculated using the algorithm described in Section 3.2. *Signing the authentication data*
TYPE	10	Type of inquiry. Fixed value: *BANK-01*

SIGNATURES OF THE PARTIES

On behalf of the Service Recipient	**On behalf of the Bank**
[Position, name, surname]	[Position, name, surname]
Position, name, surname, signature of the Service Recipient's representative	Position, name, surname, signature of the Bank representative
Seal	Seal