Recommendations on settings of SP of the AWS of a BoR Customer-FMS

The installation and configuration of the software product (hereinafter, the SP) of the AWS of a BoR Customer-FMS are performed in accordance with the following documents: 'Automated Workstation of a Bank of Russia Customer Using the Financial Messaging System. Installation and Configuration Guide' ('AWS of a BoR Customer-FMS. Installation and configuration guide') and 'Automated Workstation of a Bank of Russia Customer Using the Financial Messaging System. Administrator's guide' ('AWS of a BoR Customer-FMS. Administrator's guide').

The Payment System Operation Centre (hereinafter, the PSOC) informs exchange participants (hereinafter, EPs) that all incoming electronic messages (EMs)/ packets of EMs dispatched by the customer to the Message Exchange Centre (hereinafter, the MEC) of the Financial Messaging System (hereinafter, FMS) shall contain authentication codes (protection variant 1).

In order to enable the exchange of EMs with the MEC within the FMS using AWS of a BoR Customer-FMS, EPs shall use a separate applied user account in the production transport system of the Bank of Russia with the assigned number AWS 53 to exchange EMs with the production MEC, and a separate applied user account in the test transport system of the Bank of Russia with the assigned number AWS 63 to exchange EMs with the test MEC.

The document 'Automated Workstation of a Bank of Russia Customer Using the Financial Messaging System. Administrator's guide CBRF.61299-01 92 01' contains information about the purpose, conditions of use, general description, as well as information on installation, configuration and administration of the SP of the AWS of a BoR Customer-FMS.

1. General parameters

Software complex parameters

'Operation mode': we recommend to employ a combined or automatic mode 'NRD and control' (normative reference data):

Recommend settings:

- 'Automatic import of ED574'
- 'Control for duplicates'

- Universal Time option set to ‘Convert’.

Recipient UIC (MEC) – 7777777000

Other parameters shall be set by the user as appropriate.

Service envelope details:

– for test purposes

Recipient address (MEC): uic:777777700011 – AWS sender address – uic:XXXXXXXXXXNA, where XXXXXXXXXX is the UIC of a BoR customer, which shall be equal to the UIC of the ‘Organisation details’ tab (for example, 4525225000, therefore this field shall contain 4525225000NA, *where NA is AWS number, 63*)

– **for production purposes**

Recipient address (MEC):

uic:777777700000

AWS sender address AWS – uic:XXXXXXXXXXNA, where XXXXXXXXXX is the UIC of a BoR customer, which shall be equal to the UIC in the ‘Organisation details’ tab

(for example, 4525225000, therefore this field shall contain 4525225000NHA, *where NA is AWS number, 53*).

Please note that the sender’s and the recipient’s addresses shall start with ‘uic’:

– the ‘Request receipts’ option shall be set to work with the transport adapter (transmission confirmation is generated).

Setting the ‘Transfer file name’ option is recommended.

Settings related to CDAS Signatura

For group of settings **‘Warn about expiry’** of the certificate and the key the recommended setting is **15 days**.

1. Set of special cryptographic keys

AC (authentication code) generation

CN=<NAME>

Key usage area: Digital signature, Encryption.

Lists of OID of keys used:

Generation of AC 1.3.6.1.4.1.10244.7.20.1

SC (security code) verification

1.3.6.1.4.1.3670.5.10.27 – MEC

SC verification

1.3.6.1.4.1.3670.5.10.28 – MEC

If the OID lists of used keys are empty, OID compliance check is not performed.

Recipient's key OID 1.3.6.1.4.1.3670.5.10.28

When loading the key and verifying ACs in EMs received from the customer, in addition to the OID of the extended key application area the OID of the rules for certificate usage (1.3.6.1.4.1.3670.4.20.20) is verified by lists of ACs allowed for generation.

2. A set of special cryptographic keys used for protection variant 1, if the SP of the AWS of a BoR Customer-FMS is used only for encryption/decryption:

SC* generation

CN=<*NAME*_ABS>

OID:1.3.6.1.4.1.10244.7.20.1

Key application area: Digital signature.

* Used in the customer's ABS for the generation of EM in the AC envelope format

Encryption

CN=<NAME>

OID:1.3.6.1.4.1.10244.7.20.1

Key application area: Key encryption, data encryption.

OID lists of keys used:

Formation of AC 1.3.6.1.4.1.10244.7.20.1

SC check

1.3.6.1.4.1.3670.5.10.27 – MEC

AC check

1.3.6.1.4.1.3670.5.10.28 – MEC

If OID lists of used keys are empty, OID compliance check is not performed.

Recipient's key OID 1.3.6.1.4.1.3670.5.10.28

Settings related to message processing

The 'UFEBM processing', 'SWIFT MT processing', 'SWIFT MX processing', and 'Proprietary format processing' setting blocks can be filled as appropriate.

In order to use the 'UFEBM processing' block, the input folder shall contain a file named as follows: these can include unsigned messages ED501-ED599 or messages with ACs in the SigEnvelope format.

In order to use the ‘SWIFT MT processing’ block, the input folder shall contain a file in the SWIFT format, based on which an ed503 will be generated.

In order to use the ‘SWIFT MX processing’ block, the input folder shall contain a file in the SWIFT format, based on which an ed514 will be generated.

In order to use the ‘Proprietary format processing’ block, the input folder shall contain a file named according to the requirements for the file name as set forth in ‘Automated workstation of a Bank of Russia customer using the Financial Messaging System. Programmer’s guide.CBRF.61299-01 33 01’.

Attributes ed501 ActualReceiver and Edno are generated as follows:

ActualReceiver is taken from file name <Recipient’s UIC[10]>. Therefore the file name shall contain a correct UIC of the recipient, otherwise the generated ed501 object will fail logic verification.

EnNo is taken from file name <unique number for the UIC over an operating day [0-9][9]>.

If folders used for EM exchange differ from the standard ones generated upon AWS installation, then user access rights for these folders shall be set as equal to the access rights of standard EM exchange folders.

Please note that the requirements for the structure of file names are specified in the document ‘Automated workstation of a Bank of Russia customer using the Financial Messaging System. Programmer’s guide.CBRF.61299-01 33 01’.

Operation mode ‘Configuration of BoR Customer TG’ – ‘Configuration of communication with BoR Customer TG’

Connection parameters

Protocol – ‘HTTP’

Format marker – ‘XMLEPD’

Transmission attempts – 1-2

Operation timeout (s) – 60 sec

When using **SW Cisco AnyConnect,** designed to establish a VPN connection, the ‘HTTP’ group contains the following parameters:

The following settings shall be used to operate in a test mode using the HTTP protocol:

Source address – http://172.16.19.211:7777/in

Target address – http://172.16.19.211:7777/get

The following settings shall be used to operate in a test mode using the IBM MQ protocol:

WMQ / Server: 172.16.19.221

WMQ / Port: 1414

WMQ / Channel: KBR.SVRCONN

WMQ / Manager: FRONTGATE

Transmission / Sequence: FROM.KBR

Transmission / Manager of responses: FRONTGATE

Transmission / Sequence of responses: INBOX.xxxxxx (to be verified via the Unified User Support Service when starting the operation according to MQ)

The Transmission / Request for Delivering/Receiving Receipts option is installed additionally if necessary

Acceptance / Sequence: INBOX.xxxxxx (to be verified via the Unified User Support Service when starting the operation according to MQ)

The following settings shall be used to operate in a production mode using the HTTP protocol:

For the operation in the production mode –

Source address – http://172.16.18.211:7777/in

Target address – http://172.16.18.211:7777/get

The following settings shall be used to operate in a production using the IBM MQ protocol:

WMQ / Server: 172.16.18.211

WMQ / Port: 1414

WMQ / Channel: KBR.SVRCONN

WMQ / Manager: FRONTGATE

Transmission / Sequence: FROM.KBR

Transmission / Manager of responses: FRONTGATE

Transmission / Sequence of responses: INBOX.xxxxxx (to be verified via the Unified User Support Service when starting the operation according to MQ)

The Transmission / Request for Delivering/Receiving Receipts option is installed additionally if necessary

Acceptance / Sequence: INBOX.xxxxxx (to be verified via the Unified User Support Service when starting the operation according to MQ)

When using data encryption tools for DiSec-W channels the HTTP group contains the following parameters:

The following settings shall be used to operate in a test mode using the HTTP protocol:

Source address: http://172.21.5.57:7777/in

Target address: http://172.21.5.57:7777/get

Also, it is necessary to specify the backup values of the server IP-addresses:

172.21.5.58:7777

172.21.5.59:7777

172.21.5.60:7777

Backup servers – a click on the button opens a window where the user needs to set a list of IP addresses of BoR Customer TG, to which the connection will be redirected if there is no connection to the main server.

The following settings shall be used to operate in a test mode using the IBM MQ protocol:

WMQ / Server: 172.21.5.57

WMQ / Port: 1414

WMQ / Channel: KBR.SVRCONN

WMQ / Manager: FRONTGATE

Transmission / Sequence: FROM.KBR

Transmission / Manager of responses: FRONTGATE

Transmission / Sequence of responses: INBOX.xxxxxx (to be verified via the Unified User Support Service when starting the operation according to MQ)

The Transmission / Request for Delivering Receipts option is installed additionally if necessary

Acceptance / Sequence: INBOX.xxxxxx (to be verified via the Unified User Support Service when starting the operation according to MQ)

Also, it is necessary to specify the backup values of the server IP-addresses:

172.21.5.58:7777

172.21.5.59:7777

172.21.5.60:7777

The following settings shall be used to operate in a production mode using the HTTP protocol:

Source address: http://172.21.1.57:7777/in

Target address: http://172.21.1.57:7777/get

Also, it is necessary to specify the backup IP-addresses of the server:

172.21.1.58:7777

172.21.1.59:7777

172.21.1.60:7777

The following settings shall be used to operate in a production mode using the IBM MQ protocol:

WMQ / Server: 172.21.1.57

WMQ / Port: 1414

WMQ / Channel: KBR.SVRCONN

WMQ / Manager: FRONTGATE

Transmission / Sequence: FROM.KBR

Transmission / Manager of responses: FRONTGATE

Transmission / Sequence of responses: INBOX.xxxxxx (to be verified via the Unified User Support Service when starting the operation according to MQ)

The Transmission / Request for Delivering Receipts option is installed additionally if necessary

Acceptance / Sequence: INBOX.xxxxxx (to be verified via the Unified User Support Service when starting the operation according to MQ)

Also, it is necessary to specify the backup IP-addresses of the server:

172.21.1.58:7777

172.21.1.59:7777

172.21.1.60:7777

'Authentication' – 'Applied authentication'

User name*

Password*

* The Administrator shall fill in these values in accordance with received user accounts.

'Transport' mode

In order to use the HTTP/MQ protocols, it is necessary to select 'HTTP' or 'IBM MQ' from the list after activating the 'Transmission to transport. Protocol' and 'Receipt from transport. Protocol' parameters.

The BoR Customer TG User's Manual and the Procedure for Connecting to BoR Customer TG Using Encryption Tools for DiSec-W Channels are available on the Bank of Russia website at: http://cbr.ru/development/mcirabis/Involve_EM/.