To heads of organisations participating in the electronic exchange with the Bank of Russia (4525000829, 4525000821, 4525000833, 4525000831, 4525000832)

On scheduled key replacement

Information notice

The Payment System Operation Centre of the Information Technology Department of the Bank of Russia (hereinafter, the PSOC ITD) informs that on 17 April 2021 (the reserve day is 24 April 2021) keys of the cryptographic document authorisation system 'Signatura' (hereinafter, CDAS Signatura) of the Message Exchange Centre of the Financial Messaging System (hereinafter, MEC FMS) version 12.1 will be exchanged for keys version 13 in production systems used by the PSOC ITD.

Due to the important nature of this operation, we kindly ask you to take part in the test exchange on 17 April 2021 in the production environment.

Operational procedure:

Until 16 April 2021, exchange participants (hereinafter, EPs) will need to update their local certificate directories.

Until 17 April 2021, 10.00 Moscow time, the PSOC ITD will change CDAS Signatura keys version 12.1 for version 13 in production systems used by the PSOC ITD. Keys will be exchanged without interrupting services provided by the MEC FMS systems. The work will be conducted within the '17 April 2021' operating day;

From 17 April 2021, 10.00, the PSOC ITD will allow EPs to conduct a test exchange with the MEC FMS (using ED599 Request-probe). For EPs, a probe exchange is considered successful if the MEC FMS returns a decrypted EM and signature-verified EM ED201 with control result code 2999 'Successful verification of probe authenticity' or 2000 'Incorrect EM date'. Other test exchange results are considered unsuccessful.

If an EP does not have a technical capability to send an ED599, they may send an ED540 'Request for information on EMs transferred/received'

(InquiryDate="17.04.2021", ExchangeTypeCode=2) and control the decryption and signature verification in the received response.

In case of any errors related to the test exchange, EPs should refer to the Unified User Support Service (Information Technology Department by phone +7 495 957 80 01 or email SPFS@cbr.ru.

The PSOC ITD is sending an archive with MEC FMS certificates to EPs. The archive contains:

- *CR_CA_COC_КЦОИ_13.pse* -

an update with certificates of keys of Certification Authorities, Registration Authorities and a Certificate Revocation List.

- *ЦОС_13.pse* -

an update with certificates of MEC keys (processing and control contours).

EPs need to process the received files (Directory of Certificates – Update objects) by 16 April 2021.

This message will be published on the Bank of Russia website at www.cbr.ru/eng/development/mcirabis/involve_spfs/.

Contact details of the Unified User Support Service (Information Technology Department):

multi-line phone: +7 495 957 80 01;

email: SPFS@cbr.ru.

Annex: SPFS_13.rar.

Mikhail Shashlov
Deputy Director
Information Technology Department –
Director
Payment System Operation Centre