CyberPlat
Russia, 123610, Moscow, WTC-2,
Krasnopresnenskaya nab., 12, Entrance 7
Phone: +7 (495) 967-02-20 Fax: +7 (495) 967-02-08
Website: http://www.cyberplat.com Email: info@cyberplat.com

CyberFT Network Terminal

Admin manual

2017

Note

This document is an admin manual for “CyberFT Network Terminal” hardware and software solution developed by CyberPlat LLC.

Document versions

Software version	Date	Changes	Performed by
2.2.1	Jan 5, 2015	Started document version count.	Kosarev
2.2.1.7	Feb 10, 2015	Added a security section. Highlighted the “Configuring keys prior to work” section. Outlined export settings and the “Participants” menu.	Kosarev
2.3.1	Mar 26, 2015	Added and updated sections in line with the new functions.	Kosarev
2.4.0	Apr 22, 2015	Added and updated sections in line with the new functions.	Kosarev
2.5.2	Jun 5, 2015	Document updated in line with the new functions: Remote Banking Services, FileAct.	Kosarev
3.0.1	Aug 1, 2015	Document updated in line with the new functions and switch to the new software version.	Kosarev
3.1.2	Dec 24, 2015	Document revised for the new software version.	Aseyeva
3.1.4	Feb 10, 2016	Updated sections: 3.2.3 Internet access requirements, 15.1 Creating a user, 17.1 Controller. Added sections: 6.7 Editing keys, 10.7 SWIFT codes catalogue, and 15.7 Verifying user function.	Aseyeva
3.1.5	Sep 21, 2016	Document revised in line with the new interface. Added sections: 12.2 Creating a payment order register, 12.3 Working with a payment order register, 13.2.1 General settings, 13.2.4 Document code types catalogue, 15.3 User commands, 17.5 XML export settings, 17.8 CryptoPro keys, 17.13 Terminals, 18 Register of CyberFT participants.	Aseyeva
3.1.6	Feb 20, 2017	Added sections: 11.5 Catalogue of organizations, 11.6 Catalogue of recipients, 11.8 Banking services section settings, 16.1	Aseyeva

		General settings. Revised sections: 11 Banking services. Updated sections: 9.3.2 Export of incoming documents, 12.2.1 General settings, 12.2.3 CryptoPro settings, 13 Working with FileAct documents, 14.1 Creating a user, 16.9 CryptoPro keys, 16.12 Event notification preferences,18 Event log.	
3.3.1.8	Mar 14, 2017	Supplemented sections: 14.1 Creating a user (specified signing level structure) 14.2 Viewing and editing user data.	Aseyeva
3.3.2	May 2, 2017	Added section 8 Home page and interface services.	Aseyeva
3.3.2	May 15, 2017	Added section 4.2 Setting up document signing service.	Aseyeva

Table of contents

1. References....6
  1.1. Terms and abbreviations....6
  1.2. Documentation....8
2. Introduction....9
  2.1. Field of use....9
  2.2. Features....9
  2.3. User proficiency level....9
3. Purpose and conditions of the terminal application....9
  3.1. Terminal’s purpose....9
  3.2. Requirements to the types of the Terminal software....10
    3.2.1. Software requirements....10
    3.2.2. Hardware requirements....10
    3.2.3. Internet access requirements....10
4. Setting up OS and document signing service....11
  4.1. Installing Debian/Linux OS....11
  4.2. Setting up document signing service....11
5. Terminal web-interface access....13
  5.1. Logging in using password....13
  5.2. Logging in using key....14
6. Configuring keys prior to work....14
  6.1. Controller’s key generation....14
  6.2. Controller’s key import....15
  6.3. Sending public key certificate....16
  6.4. Registering public key certificate for CyberFT Processing....16
  6.5. Certificate exchange between associated Participants....16
  6.6. Starting exchange between Terminal and CyberFT Network....17
  6.7. Editing Controller’s key, manual control....17
  6.8. Deleting Controller’s key....17
7. Certificate management....18
  7.1. Adding a certificate....18
  7.2. Example of identifying the outgoing document signature owner....19
8. Home page and interface services....19
  8.1. Home page of the interface....19
  8.2. Interface services: documentation, search, and settings....20
9. SwiftFin section, exchanging Swift documents....21
  9.1. Section menu....21
  9.2. SwiftFin document log....21
  9.3. SwiftFin settings....21
    9.3.1. Routing outgoing documents....21
    9.3.2. Exporting incoming documents....22
    9.3.3. Document printing....22
    9.3.4. Document verification....22
    9.3.5. User access....23
    9.3.6. Exceptions to the general routing rule....23
  9.4. Catalogue of SWIFT codes....23
10. FinZip, exchange of archived data....24
11. Banking services....24
  11.1. Log of payment orders....25
  11.2. Working with payment order registers....25

11.3. Bank statements 25
11.4. Catalogue of banks 26
11.5. Catalogue of organizations 26
11.6. Catalogue of recipients 27
11.7. Accounts of organizations 27
11.8. Banking services section settings 29
12. ISO20022, exchange with external system 29
12.1. Log of ISO20022 documents 29
12.2. ISO20022 section settings 30
12.2.1. General settings 30
12.2.2. SFTP settings 30
12.2.3. CryptoPro settings 31
12.2.4. Document code types catalogue 32
13. Working with FileAct documents 32
13.1. Log of FileAct documents 32
13.2. FileAct section settings 33
14. User management 34
14.1. Creating a user 34
14.2. Viewing and editing user data 35
14.3. Additional user settings 35
14.4. User commands 36
14.5. Account management 36
14.6. User’s key certificate 36
14.7. User activation 37
14.7.1. User activation by the terminal administrator 37
14.7.2. User activation by security officers 37
14.8. Verifying user function 38
15. Reporting 38
16. Settings 38
16.1. General settings 39
16.2. Controller 39
16.3. Automatic signing settings 39
16.4. Exchange with CyberFT Network 40
16.5. Signing settings 40
16.6. XML export settings 41
16.7. Security 41
16.8. Verifying incoming documents 42
16.9. CryptoPro keys 42
16.10. Setting up mail notifications 44
16.11. Notification mailing list 44
16.12. Event notification preferences 44
16.13. Terminals 44
17. Register of CyberFT participants 45
18. Event log 45

1. References

1.1. Terms and abbreviations

Administration is a legal entity, a privileged Participant of CyberFT Network in charge of the Single Network catalogue. The administration has its own CyberFT Network address.

BICFT (Business Identification Code CyberFT) is a Participant's code or an address in the CyberFT Network. If a Participant already has a BIC code (SWIFT address) then he shall keep using that BIC; if he doesn't have a code, then such a Participant is attributed a BICFT code.

CA stands for Certification Authority.

Certificate is a self-signed certificate of the Participant's bank issued through a private key; or a certificate issued by a Certification Authority.

Chief Administrator is a Keys Owner vested with the role of the Chief Administrator in conformity with the "Rules of electronic document flow in CyberFT Network".

Connection of the Participant to the CyberFT Network means series of technical, organizational and legal steps performed by Provider to let the Participant exchange Electronic Documents with other Participants of the CyberFT Network. Prior to Connecting the Participant shall undergo registration in the CyberFT Network.

Controller is an automatic signatory.

Cryptographic Information Protection Facilities (CIPF) are an aggregate of software and hardware means ensuring application of Digital signature and encryption when setting up an Electronic Document Flow. CIPF can be utilized as both separate software modules and built-in tools of applicable software.

Cryptographic Keys is a joint name for both Public and Private Keys.

CyberFT Network is an electronic document flow system that represents an aggregate of software and hardware means designed for exchanging legally-valid Electronic Documents and ensuring informational and technological interaction between Participants.

CyberFT Network Segment is a situation where provider with their own Processing and pool of Participants forms a segment in the CyberFT Network.

CyberFT Processing is a software and hardware solution implementing legally valid electronic document flow in the CyberFT Network. Processing forms a separate CyberFT Network segment with its own Participants. Each Processing in the CyberFT Network has its own address depending on the Provider's address, e.g. CYBERUM@XXX.

CyberFT Provider is a Legal Entity, privileged CyberFT Participant managing the Processing. Each Provider as a Participant has his own address in the CyberFT Network, e.g. CYBERUM@XXX.

CyberFT Terminal is a software and hardware solution installed at the site of the Participant that serves the purpose of connecting the Participant to the CyberFT Network.

Delivery Notification is an XML CyberFT auxiliary ED Type used for notifying the sender about the delivery.

Digital Signature (DS) is electronic information attached to other electronic information (signed information) or otherwise tied to such information and is user for identifying the signatory of such information. DS used in the CyberFT Network is an enhanced non-certified digital signature as defined in the Federal Law dated April 6, 2011 No. 63-FZ “On Digital Signature”.

Document Flow System is a sub-system of the CyberFT Network responsible for the flow of a certain Type of Electronic Documents.

Electronic Document (ED) is an electronic document.

Electronic Document Delivery Time is time indicated in an electronic document before which this document must be delivered to the Recipient. If the electronic document is not delivered before that time it shall be deemed undelivered and all further attempts of its delivery shall be terminated.

Electronic Document Flow (EDF) is an electronic document flow.

Electronic Document Group is Electronic Document types put together, e.g. MT1 group**, MT2 group**.

Electronic Document Type (ED Type) is an acceptable format of electronic documents in the CyberFT Network, e.g. MT***, ISO20022.

Establishing Connection with the Network Participant means establishing the Mutual Trust Mode between Participants (RMA – Relationship Management Application). Without Establishing Connection only certain document types are allowed to be sent to the other Participant.

Key Compromise is announcement by the person owning a Private Key of circumstances where unauthorized use of that key is possible.

Keys Owner is a private individual who acts as an authorized representative of a Participant or Provider for sending electronic documents on behalf of the Participant through the CyberFT Network and who has created Cryptographic keys. Administration assigns to the Keys Owner a corresponding Public key certificate in the CyberFT Network, which allows the Keys Owner create digital signatures in electronic documents and access Electronic Document Flow in the CyberFT Network.

Mutual Trust Mode is a mode of interaction for Participants whereby Participants have exchanged their public key certificates and acknowledge each other’s Digital signature.

OS stands for an Operating System installed on a computer.

Participant is a legal entity (which includes a financial institution) or a private entrepreneur that is registered in the CyberFT Network and participates in the electronic document flow.

Participant Registration in the CyberFT Network means designation by Administration of a Unique ID to the Participant in the CyberFT Network.

Private Key is a unique sequence of symbols intended for creation of Digital signature and for decrypting data using Cryptographic information protection facilities and known only by the Keys Owner.

Public Key is a unique sequence of symbols corresponding to the Private Key that is in public domain and intended for verifying digital signature and encrypting information using Cryptographic information protection facilities.

RBS stands for Remote Banking Services.

Rules are rules of the electronic document flow within the CyberFT Network set out in the Agreement on informational and technical servicing.

Signatory is an Employee of the Participant who is authorized to sign documents on behalf of the Participant. The Participant may activate a double signature mode for certain types of Electronic Documents, in which case the role of the Signatory is divided into two sub-roles:

- 1st signature is a Signatory entitled to the 1st signature
- 2nd signature is a Signatory entitled to the 2nd signature

Unified CyberFT Network Catalogue is a Catalogue of Participants (Providers and other Participants) under control of CyberFT Network Administration.

Unique Participant ID is a unique sequence of symbols that definitively defines the CyberFT Network Participant. Unique ID is used as a Participant’s address when exchanging Electronic Documents in the CyberFT Network.

User is an employee of the Participant who has access to the CyberFT Terminal.

XML CyberFT is an electronic document format or an XML envelope format that is accepted and supported in the CyberFT Network. XML CyberFT can be a stand-alone document or can contain other Types of EDs.

1.2. Documentation

A set of CyberFT Network Terminal documents is as follows:

1. CyberFT Network Terminal. Admin manual. CYBERPLAT LLC, 2017.

2. CyberFT Network Terminal. User manual. CYBERPLAT LLC, 2017.
3. CyberFT Network Terminal. Installation manual. CYBERPLAT LLC, 2015.

2. Introduction

2.1. Field of use

CyberFT was designed to ensure legally-valid exchange of financial messages and electronic documents between the system’s Participants. Any organization participating in the exchange of electronic documents can join the system. In order to become a Participant it is necessary to register in the CyberFT system.

Each Network Participant has their ID (network address). Participant’s BIC (SWIFT address), if any, is used as their address, or else a Participant is attributed a BICFT.

2.2. Features

The system ensures legally-valid exchange of electronic documents between Participants.

Terminal’s main features are:

- Registration of documents in the system;
- Signing documents by the Participant’s DS;
- Delivery of outgoing documents to the Processing;
- Download of incoming documents from the Processing;
- Verifying DS in incoming documents.

Processing’s main features are:

- Ensuring documents are in line with the MT, ISO, CBR formats;
- Verifying DS in the documents;
- Documents routing;
- Tracking document statuses.

2.3. User proficiency level

Terminal’s administrator needs to have basic Linux administration knowledge.

Terminal’s users should have basic PC skills.

3. Purpose and conditions of the terminal application

3.1. Terminal’s purpose

CyberFT Network’s Terminal is server software installed on the end of the CyberFT Participant and intended for signing, sending and receiving electronic documents during the exchange with other Participants. Terminal is shipped as a docker container/docker image and is managed through a web interface. CyberFT Network Terminal Installation manual is laid out in the document [3].

Terminal’s file system is a directory tree containing, among other things, folders for outgoing and incoming documents – **Import** and **Export**. (Terminal’s file system is described in the document [3]).

From time to time Terminal scans the **Import** folder to detect new files. In case there are new files, Terminal transfers those for the signing with a Participant’s private key.

Once signed, the documents are transferred to the CyberFT Processing via the transport protocol. Interaction between Terminal and Processing is carried out through the Internet with a cryptographic protocol TLSv1.

Should there be such an option, Terminal additionally transfers incoming documents to the **Export** folder (for Automated Banking System, hereinafter - ABS) and/or sends them to the printer (for manual handling).

Aside from the documents, receipts about current status of sent documents are also sent (**statusreport**). They are also signed by the sending party. Document delivery status info is available at the Terminal Log. Besides, receipts can be programmed to be automatically exported to the corresponding folder (for ABS).

The bulk of the document processing – receipt, control and delivery of electronic documents – is carried out in the Processing.

3.2. Requirements to the types of the Terminal software

3.2.1. Software requirements

Computer intended for Terminal installation should meet the following software requirements:

- Debian GNU/Linux 7.8 (wheezy), Release: 7.8;
- Ext4 file system.

3.2.2. Hardware requirements

Computer intended for Terminal installation should meet the following hardware requirements:

- Processor architecture x86-64;
- 2GB RAM or more;
- Multi-core central processor Intel Core 2 Duo 3.0 Ghz or higher;
- No less than 20GB of hard drive space.

3.2.3. Internet access requirements

Computer intended for Terminal installation should have internet access as well as access to Debian repository and access to the Docker project:

- https://get.docker.com/ ;
- Repositories used by Debian OS (HTTP, FTP).

Also, the computer with installed Terminal shall have access to the Processing at tcp://service.cyberft.ru:

- For test use tcp://service.cyberft.ru:50090,
- For commercial use tcp://service.cyberft.ru:50091.

4. Setting up OS and document signing service

4.1. Installing Debian/Linux OS

Recommendations for installing Debian GNU/Linux 7.8 (wheezy), Release: 7.8.

Recommended for use OS image consistently compatible with CyberFT is available at http://download.cyberft.ru/OS/.

If you plan on downloading OS independently from the official repository, use the following parameters during installation:

- When selecting image choose amd64;
- In the installation dialog it is recommended to choose option “64 bit install”;
- In the update download mirror selection dialog choose country “Russian Federation” and mirror “ftp.ru.debian.org”;
- In the software installation selection dialog you should uncheck all options except for the SSH server and standard set of system utilities.

4.2. Setting up document signing service

CyberFTSignService software is a local service operating as a service on the signatory’s computer. The service acts as a link between CyberFT Terminal and Windows cryptography services.

CyberFTSignService is available at http://download.cyberft.ru/CyberSignService/.

To install the software on your computer save locally the most recent archive, unzip it and run the installer **as administrator**.

During installation the service will be automatically added to the Windows automatic start.

It is expected that private key and certificate files had been previously received through generating with the **GenKey** software (http://www.cyberplat.ru/download/genkey.pdf).

Setting keys for signing

Upon installation it is necessary to set keys for signing. Follow the procedure below.

Open the automatic start folder and activate the *CyberFTSignService* symbol.

[image]

The following window will pop up.

[image]

Carefully read the instruction with description of options and **choose an option that suits you best**.

Option 1. Signing with drive-stored keys.

If your certificate and private key are stored on the local disk or on the flash drive, choose the first tab called *Drive-stored key*.

This setting is beneficial for those planning to sign using **several signatory keys on one computer**, since it allows you to choose the required certificate during signing.

Select *Add* and in the pop up window (*Add drive-stored key*) choose path to the certificate and private key files. Press *OK*.

[image]

That way you can add several signatory keys, whereafter the keys will become available on the selection list at the signing.

[image]

Option 2. Signing with eToken-stored keys.

If your keys are stored on the eToken device, choose a tab called *Keystore-stored key*.

Insert your eToken device I the USB port and choose the needed certificate from the eToken device.

[image]

In the screenshot above you can see that keystore-stored keys and eToken stored keys have different icons.

From here on, upon signing the key you have selected will be addressed.

Please note that in this case during signing the user will need to enter the password of the associated electronic key.

To sign a document with a different key you will need to once again open the settings and choose a different certificate.

Option 3. Signing with a Windows Keystore-stored key.

This option will be suitable for those signing documents in CyberFT with only one key and those who cannot import their key to an eToken device.

When generating a set of keys with GenKey it creates a keystore file certificate.pfx

This PFX keystore's certificate and a private key can be imported to the Windows keystore and be used later on when signing documents.

In order to add a certificate and a private key to the Windows keystore proceed as follows.

Open the certificate file (PFX extension) from the set of keys created by the GenKey.

[image]

In the *Password* field enter the password indicated during the key generation.

Check options as indicated in the screenshot below and press *Next*.

[image]

In the next step when selecting a certificate keystore click *Browse*.

[image]

Choose "Personal" certificate keystore from the list and click *Done*.

If any security window pops up, click *OK*.

5. Terminal web-interface access

5.1. Logging in using password

Access to the web interface for managing Terminal is provided via IP of the server on which the Terminal operates. Authorization requires login/password of the administrator.

When logging in administrator and user enter into the *Document* section.

For authorizing using login/password you need to press *Log in using password*.

[image]

The following authorization form will appear on the screen. You need to enter your login (email indicated during registration) and your password, after that press *Log in*:

[image]

The first user password is the same as their email; however, upon first authorization the user password is required to be changed.

Upon initial creation of a user they need to be activated by entering the system with the rights of administrator or security officer.

5.2. *Logging in using key*

Log in using key button is for authorizing the user using their key. **Please note** – this feature can be used only when working with the “Slim CyberFT Client” software.

To set up key-based system log-in you need to create a user’s public key certificate as described in User’s key certificate.

When clicking *Log in using key* the following window will pop up.

[image]

When switching to the OpenSSL tab you will need to manually indicate path to the files of the private key and certificate of the public key. When switching to the Windows tab and clicking *Select* you will need to choose a certificate for authorization from the Windows keystore using the list below or from the eToken electronic key.

The certificate list looks as follows.

[image]

6. Configuring keys prior to work

6.1. *Controller’s key generation*

After installing your terminal you will need to set up keys, namely:

1. Create controller’s keys;
2. Send controller’s public key certificate to Cyberplat LLC for registering in the CyberFT Processing at support@cyberft.ru;
3. Register Processing’s public key certificate;
4. Exchange public key certificates with associated participants;
5. Start exchange between Terminal and CyberFT Network.

Further down in this section keys procedures are described in more detail.

To generate Controller’s keys enter *Settings/Controller* and on the next page press *Create a key*.

[image]

In the next window type key’s details.

[image]

Please note – the following fields will be present in the public key certificate and they need to be filled using the Latin alphabet:

- Country;

- Region;
- City;
- Company name;
- Owner's name.

In line with the **private key password** requirements you password must be at least 8 symbols long, it must contain digits, upper and lower case letters and special symbols.

You need to enter your password in both text fields and press *Create a key*.

Choosing the *View* icon will open the next window.

[image]

By selecting *Change key* (or by selecting an *Edit* icon on the list of keys) you can change the key as described in Editing controller's key.

Please note that if you change previously created and registered controller's key, any further file exchange with the previous key becomes impossible. To continue work you will need to register a new controller's public key certificate in CyberFT Processing and pass it on to all associated partners through the CyberFT Network for further installation in the Terminals.

By selecting the *Delete* icon you can delete your key.

Before deleting Controller's keys the following warning will pop up.

[image]

6.2. *Controller's key import*

If you already have active keys you can import them to the terminal to serve as controller's key.

Please note – to register a participant in CyberFT you need to provide your controller's private key certificate.

In order to import you need to press *Import key* on the *Controllers' keys* page.

You need to fill out the following fields:

- Key's name that will be displayed to the recipient of your messages;
- Initial/additional key – choose from the list;
- Private key/company key – choose from the list;
- Path to the private key;
- Path to the public key;
- Path to the key certificate;
- Password to your private key.

Press *Import key* one more time.

If you press the *View* icon in the certificate line you will see information about the key and will be able to download the key certificate by pressing *File download*.

[image]

6.3. Sending public key certificate

Pressing the *File download* link will form an associated participant public key certificate file that will look as follows:

[participant's terminal ID]-[certificate fingerprint].[crt extension], for example:

TESTZZZ@Z001-85E9A9BE7A9335CE16D2C990EDFD7EF703A50B61.crt.

You will need to send this file to support@cyberft.ru to register in the CyberFT Processing. You will need to be sending out this same file to other Participants when exchanging certificates.

6.4. Registering public key certificate for CyberFT Processing

After that you need to register the Processing's public key certificate.

Public key for joining the test processing is available at http://download.cyberft.ru/Testcert/, where you need to save the file locally (*Save as* in your browser or other likewise option):

CYBERUM@TEST-900924C49EC6EC8488180F92A0E35EC7A0AB59AD.pem

After that the certificate is downloaded via the "Certificates" menu in the same fashion as certificates of other Participants (screenshots of the process are shown in the next section).

Test processing Terminal ID is **CYBERUM@TEST**

Public key for connecting to the **production** processing will be sent to you by the CyberFT Network implementation manager. Production processing Terminal ID is **CYBERUM@AFTX**.

6.5. Certificate exchange between associated Participants

When establishing connection, CyberFT participants must exchange their controller's public keys and employees' private keys (once generated by the user). Key certificate files are as follows.

For the controller:

[participant's terminal ID]-[certificate fingerprint].[crt extension], for instance:

TESTZZZ@Z001-85E9A9BE7A9335CE16D2C990EDFD7EF703A50B61.crt.

Key certificate files are available to the controller from the *Setting/Controller* menu in the viewing mode by pressing the *File download* link.

In order to add a certificate of other associated participant you need to go to *Certificates* and press *Add a certificate*. The procedure of adding certificates is described in the Certificate management section.

In the Terminal certificates of the participants are stored in the MySQL database.

6.6. Starting exchange between Terminal and CyberFT Network

Automatic information exchange between Terminal and CyberFT Network is launched from *Settings/Exchange with CyberFT Network*.

6.7. Editing Controller's key, manual control

Editing controller's key is carried out after pressing the *Edit* icon in the right-hand column of the list of keys. In that case you will see the form depicted in the image below.

That form allows you to edit the following key parameters:

- *Terminal ID* – ID of your terminal;
- *Key name* - any name; it will be displayed to the recipient of your messages;
- *Initial/additional key* – choose from the list;
- *Controller* – name of the employee who accepts sending documents to the CyberFT Network but does not sign the documents.

If *Manual control* is checked then prior to sending outgoing document must be accepted by the **verifying employee**. Otherwise the documents are not going to be sent. To have a verification option in place the system must have a registered user with the respective verification role.

[image]

Please note that controller's key can be edited only when terminal's automated processes are turned off.

Please note that if you change previously created and registered controller's key, any further file exchange with the previous key becomes impossible. To continue work you will need to register a new controller's public key certificate in CyberFT Processing and pass it on to all associated partners through the CyberFT Network for further installation in the Terminals.

Please note the verifying employee can accept outgoing documents only as described in section 15.8 Verifying user function only when *Manual control* is checked.

6.8. Deleting Controller's key

To delete a Controller's key use the *Settings/Controller* menu and select the *Delete* icon in the corresponding line on the list of keys. The key will be deleted after approval of the administrator.

7. Certificate management

7.1. Adding a certificate

The *Certificates* section is for handling system certificates.

Certificates registered in the terminal's certificate register are used for two purposes:

- **Certificates of associated participants** are used for verifying incoming documents;
- **Certificates of the terminal user** are used for identifying user who signed an outgoing document.

By going into the *Certificates* menu you get access to the certificates registered in the system.

[image]

To add a new certificate to the register click *Add a certificate*. Fill out certificate and certificate owner's details as follows.

[image]

Adding a certificate:

Certificate – certificate download file is indicated by the *Select…* button;

Type – key format that is selected from the list: Undefined, Open SSL, CryptoPro;

Terminal ID – Participant's Terminal ID who is a key owner (key of a Participant or an associated Participant);

Role:

Signatory – for all user keys, Participant keys and associated Participant keys;
Controller – for all controller keys, Participant keys and associated Participant keys.

Owner's name, Position, Email, Phone – values of the fields will be displayed in incoming messages and upon signing outgoing messages.

A certificate is added to the system by clicking the *Add* button.

Certificate editing form is prompted by the *Edit* icon in the right-hand column on the list of certificates. Changes are saved after clicking the *Refresh* button.

[image]

7.2. Example of identifying the outgoing document signature owner

In this example we are going to show you how to identify the owner of the keys of the outgoing document.

To find a document with ID=16873 in the *Documents/Document log* menu enter the Document log and set up a filter by ID. As a result one entry is found.

[image]

By clicking the *View* icon in the right-hand column of the document entry you can view its contents.

[image]

In the *Signatories* tab you can see information about the document signatories.

In this example a payment order is signed by the controller key “Test terminal Platina CB”. To have information about the keys displayed in the document you need to add a private key certificate of a user and key certificate of a controller to the certificate register.

8. Home page and interface services

8.1. Home page of the interface

Main menu of the CyberFT Network Terminal looks as follows.

[image]

Documentation structure is presented in the Interface services section.

On entering the interface you will see the main page of the interface that looks as follows. (**Return to the home page** from any interface page by clicking the CyberFT logo above the main menu)

[image]

The first section on the home page - *Accounts information* – is for receiving information on accounts of a participant, which is detailed in the “Accounts of organizations” section in documentation [2]. Clicking the account number link will bring you to the account details.

In the *Statements* you can manage bank statements. By clicking *Request a statement* you can get an account statement.

In the second section of the home page is information about documents generated in various sub-systems during the day. Each link will lead you to the document log containing documents of the selected category. Document log is detailed in the corresponding sections of this manual and in documentation [2].

In the *Document templates* you can view current templates of bank documents and create new template-based documents. Details of the bank document templates can be found in the section of the same name in documentation [2].

8.2. Interface services: documentation, search, and settings

When selecting the *Documentation* in the main menu you will see the following page.

[image]

Download documentation enables you to download full manuals about the CyberFT Network Terminal web interface.

Info contains a list of documentation sections that you can use online. When clicking *Info* you will see a page with a list of sub-categories. When clicking a sub-category menu item you can read that sub-category's text.

The following services are provided to the user for handling document logs: document **search**, log column display **settings**, **Info**.

As an example of a log in the next picture you can see a bank statements log. In the upper right corner of the screen you can see regular service icons.

[image]

Data search

By clicking the *Search* icon the following window will appear where you can insert a range of document dates that you want to be displayed in the log. The selection starts when you click *Search*.

[image]

You can also filter out documents using fields that have space for entering criteria below them.

You can **set up log column display** by clicking the *Settings* icon. In the windows that pops up you can check log columns you want to be displayed on the screen. You can change order in which columns appear by selecting a column on the list and moving it with your mouse to the desired place.

[image]

The *?* (info) icon prompts the *Info* sub-category tied to this screen.

9. SwiftFin section, exchanging Swift documents

9.1. Section menu

SwiftFin section is intended for organizing document exchange in the SWIFT format. This section allows you to view all incoming/outgoing/erroneous documents in the SWIFT format and set up a SWIFT module on your terminal. Choose *SwiftFin* from the main menu to start working. If you are an administrator, use the following menu.

[image]

9.2. SwiftFin document log

Layout of the *Document log* of the SwiftFin module is illustrated below.

[image]

Structure of the *Document log* is detailed in the document [2] in the “Log of SWIFT documents”.

Clicking the *Settings* icon will display a list of columns, you can organize contents of the displayed columns.

Download XLS allows you to download an XLS file of the document log information.

Delete selected allows you to delete documents selected in the right-hand column. You can only check documents that have one of the final statuses missing.

Document log enables you to view all SWIFT documents.

Incoming documents shows a log of incoming SWIFT documents.

Outgoing documents allows you to manage outgoing documents.

Erroneous documents shows a log of erroneous SWIFT documents.

9.3. SwiftFin settings

SwiftFin/Settings will open settings for the module.

Settings includes several tabs.

[image]

9.3.1. Routing outgoing documents

In the CyberFT Terminal settings you can optionally define a working folder for **importing** documents from the automated banking system (ABS) to the terminal.

To activate automated document routing you need to go to *SwiftFin/Settings/General* and check *Activate SWIFT document routing*, select a new folder for redirected documents and save these settings.

The folder shall be within the docker folder described in the Terminal installation manual. Name of the folder is arbitrary.

You need to set up rights for the folder 0777.

Linux command: sudo chmod 777 /folder.

Please note that if ID of the Recipient is indicated in *SwiftFin/Settings/Routing* then even when automatic of SWIFT document routing is enabled, the Recipient will continue to receive them via the CyberFT Network.

9.3.2. Exporting incoming documents

In the CyberFT Terminal settings you can define **export** rules for incoming terminal documents intended for ABS. To activate that feature you need to check *Activate export of SWIFTFIN documents*, indicate document file extension in line with the ABS settings and save these settings. In this case after check correct incoming documents will be renamed and directed to /cyberft/export/swiftfin/swift.

When checking *Add checksum to MT documents when exporting* checksum is transferred along with the MT document. On receiving the document checksum is reconciled with a newly calculated sum in the recipient's system. If these sums are equal than the document is considered to have had no alterations.

Checking *Use XML export* is going to send a container with encrypted XML file of the document on top of the document.

Export MT011 document should be checked for delivery when you need to from an MT011 document for an undelivered incoming document. Incoming document is considered undelivered if it was not delivered within the time period stated in the *Lifetime in minutes for undelivered documents*.

9.3.3. Document printing

In the *Print* tab of the *SwiftFin/Settings* interface you can set automatic printing of incoming SWIFT documents.

For automatic printing of undefined types of incoming SWIFT documents check necessary document types and press *Save* in the form as depicted below.

[image]

9.3.4. Document verification

In the *Document verification* tab of the *SwiftFin/Settings* menu you can set verification of outgoing SWIFT documents. In the following table it is necessary to check the types of documents that need to be verified by user.

[image]

The procedure of document verification by user is detailed in the document [2] in “Documents to be verified by user”.

9.3.5. User access

SwiftFin/Settings/User access menu allows you to define SWIFT roles for users. Find more in Additional user settings.

9.3.6. Exceptions to the general routing rule

In case you have automatic routing of SWIFT documents activated, you can add exceptions to the general routing rule. If a Participant needs to send a document via the CyberFT Network, this address must be present in the table of participants – menu *SwiftFin/Settings/Routing*.

[image]

After pressing *Create* you will see the following input form.

[image]

In the *Address* field specify the terminal address and when necessary add a comment in the *Information* field. For Participants added to that list messages will be transmitted through the CyberFT Network.

9.4. Catalogue of SWIFT codes

Catalogue of SWIFT codes is handled by administrator at *SwiftFin/Catalogue of SWIFT codes*.

The catalogue of SWIFT codes can be loaded in the **SWIFT format** or in the **Central Bank of Russia (CBR)** format.

The catalogue of SWIFT codes looks as follows.

[image]

To load the catalogue in the **SWIFT format** the terminal’s administrator should go to *SWIFT/Catalogue of SWIFT codes*. On the screen you will see information about the last catalogue session. After clicking *Select* administrator should choose a catalogue file in the **SWIFT format** and by clicking *Save* saves it to the terminal’s database. Now in the *CBR SWIFT catalogue* you will see the entire list of SWIFT codes with a search option.

Similarly, to load the catalogue in the **CBR format** by clicking *Browse* administrator should choose the catalogue file in the CBR format (dbf format) and by clicking *Download* saves the file to the terminal’s database.

As a result, in the *Catalogue of SWIFT codes* you will see the full list of SWIFT codes with a search option; however, the unfilled codes are not displayed.

In the upper left corner of the form you will find automatically displayed download information:

- Last load date,
- File name,
- File type,
- File size,
- Name of the downloading administrator.

The catalogue that is used is the last downloaded catalogue or the only downloaded catalogue.

You can view the catalogue entry by clicking the *View* icon in the entry line.

[image]

10. FinZip, exchange of archived data

FinZip section is for exchanging archived data. *FinZip's* document log has the following format.

[image]

The log operations are described in more detail in the document [2] in “FinZip, exchange of archived data”.

Clicking the *View* icon allows you to view the log document in the following window.

[image]

In the tabs of the form you can view the following information:

- Outgoing/incoming archive;
- Information about signatories of incoming/outgoing messages;
- Events, i.e. technical information about sending/receiving messages;
- Associated documents, including technical status reports;
- Document container, i.e. an encrypted XML file.

11. Banking services

Banking services section allows you to view all incoming/outgoing/erroneous bank documents and adjust the *Banking services* module of your Terminal (catalogues of banks, senders and recipients). *Banking services* has the following menu.

[image]

11.1. Log of payment orders

To work with your payment order log you will need to go to *Banking services/Payment orders*.

Administrator's functions when working with the payment order log:

1. Sorting and filtering payment orders;
2. Deleting a payment order;
3. Viewing a payment order.

Payment order log procedures are laid out in the document [2] in "Creating a payment order" and "Payment order log".

In the administrator's interface payment order log looks as follows.

[image]

Unlike users, administrators cannot create payment orders or generate register of payment orders.

11.2. Working with payment order registers

Banking services/Registers of payment orders section is for handling registers of payment orders.

When working with registers of payment orders, the following features are available to the administrator:

1. Register deletion;
2. Data sorting and filtering;
3. Register viewing;
4. Register signing and sending;

Payment order register log is prompted from *Banking services/Payment order register*. An example of a register is illustrated in the image below.

[image]

Procedures of the payment order registers is detailed in the document [2] in "Creating payment order registers" and "Payment order registers".

Please note that unlike users, administrators cannot create payment orders or create payment order registers.

11.3. Bank statements

Bank statements/Statements menu is for handling bank statements. *Statement log* structure is illustrated below.

[image]

Administrator can only view bank statements.

Statements are created by users; user interaction with bank statements is detailed in the document [2] in “Bank statements”.

11.4. Catalogue of banks

Catalogue of banks is for handling database of the banks of Russia.

By default the database is empty. It is assumed that a Participant will fill the catalogue by themselves.

To update the bank catalogue you need to:

1. Download the catalogue from the CBR website at http://www.cbr.ru/mcirabis/?PrtId=bic. File type bik_db_09112015.zip;
2. Specify path to the file by clicking *Browse*;
3. Upload the downloaded archive to the terminal by clicking *Upload*.

Once successfully added, the database will be updated and the terminal will have a table with the list of all banks.

[image]

When clicking the *View* icon (or double-clicking the line) you will see the next form for viewing the bank info. Platina CB has its own Terminal ID – **PLATRUMMBXXX**.

[image]

Clicking the *Edit* icon brings you to the next editing screen. Click *Save* to save the changes.

[image]

11.5. Catalogue of organizations

Catalogue of organizations is for handling catalogue of sender organizations. The catalogue’s structure is as follows.

[image]

Creating a new organization

Clicking *Add organization* will trigger the following form for specifying details of the new organization.

[image]

Organization details:

Terminal ID – code of the CyberFT terminal; choose ID from the list of terminals;
Organization name – organization name;
Type – type of organization; selected from the list: legal entity, private individual;
INN – tax reference number;
KPP – tax registration reason code.

After entering the data click *Create*.

Viewing the organization details

Clicking *View* (or double-clicking the catalogue line) on the list of organizations will bring you to the next form of viewing the catalogue entry.

[image]

Deleting the catalogue entry

Clicking *Delete* button or icon will delete details of an organization from the catalogue.

Editing the organization details

Clicking *Edit* in the viewing form (or similar icon in the catalogue) will bring you to the next from of editing the organization details.

[image]

Save the changes by clicking *Save*.

11.6. Catalogue of recipients

Banking services/Catalogue of recipients enables administrator to do the following:

1. Recipient search;
2. Viewing recipient details;
3. Editing recipient details;
4. Deleting recipient.

Only users can create new recipients.

The catalogue procedures are detailed in document [2].

Administrator interacts with the *Catalogue of recipients* on the following page.

[image]

11.7. Accounts of organizations

Banking services/Accounts of organizations menu is for handling bank accounts of payer organizations. The image below illustrates the catalogue structure.

[image]

In the catalogue you can sort data by columns: *Account name* and *Settlement account*. **Catalogue search** works in the fields under which you can see the input field with an example.

“Accounts of organizations” in the document [2] describes actions that can be performed by the terminal **user** with regard to the accounts of an organization:

1. Search for organization’s account;
2. View account details;
3. Request bank statement.

Terminal **Administrator** can perform the following actions with the organization’s account:

1. Search for organization’s account;
2. View account details;
3. Edit account details;
4. Request bank statement;
5. Add new organization’s account;
6. Delete account.

Please note that on the list of banks you will only see banks that have been assigned a *Terminal ID* in *Banking services/Catalogue of banks*.

Adding an account

Clicking *Add a payer account* will bring you to the next window for adding a new account. Save the entered data by clicking *Create*.

[image]

Viewing account details

Click the View icon on the list of accounts to go to the next account details viewing form.

[image]

Editing account details

Click *Edit* in the viewing form (or the *Edit* icon from the line on the list of accounts) to go to the bank account editing form. Save the changes by clicking *Save*.

[image]

Bank statement request

By clicking the *Statement request* button in the viewing form administrator will prompt the following window. To create a statement you need to set starting date and ending date and then click *Submit*.

[image]

The type of the bank statement is detailed in the document [2] in “Bank statements”.

You can **delete a paying organization’s account** by clicking *Delete* in the account viewing form and by clicking the *Delete* icon on the list of accounts. The account will be deleted after you confirm that the operation is correct.

11.8. Banking services section settings

*Banking services/Setting*s menu allows you to do the following.

[image]

Checking *Turn on automatic export of incoming statements into 1C format* will automatically export incoming bank statements into 1C file format. The files will be put into the folder as follows /home/cyberft/app/export/edm/1c.

12. ISO20022, exchange with external system

ISO20022 menu allows you to set up exchange of ISO20022 messages by way of connecting through SFTP and also view ISO20022 messages.

[image]

12.1. Log of ISO20022 documents

ISO20022/Document log menu allows you to view ISO20022 documents.

[image]

Procedures with ISO20022 documents are detailed in the document [2] in “Log of ISO20022 documents”.

In the example, log entries are **sorted** in descending order of the ID field. The up arrow next to the field name will sort entries in the ascending order, whereas the down arrow will sort entries in the descending order.

Log entries are **filtered** by the condition “Status = Delivered”.

The *Delete selected* button will delete documents selected in the first column. You can only select documents that do not have a final status.

Clicking the *View* icon will bring you to the next document viewing form.

[image]

In the *Signatories* tab you can view information about the document’s signatories.

[image]

In the *Events* tab you can view events related to the document.

[image]

In the *Associated documents* tab you can view documents associated with the viewed document.

[image]

In the *Container* tab you can download document container files and encrypted document container files.

[image]

12.2. ISO20022 section settings

12.2.1. General settings

The *ISO20022/Settings* section allows you to set up your terminal for receiving/sending ISO20022 documents. The settings page looks as follows.

[image]

In the *General settings* tab you will see the following options:

- *Terminal code for transforming BIC into a terminal address* – specify the recipient’s terminal code, which is the 9th symbol in the full recipient’s terminal address.
- *Search sender and recipient in the document during import* – check when the terminal loader detects sender’s and recipient’s names in the document. When left unchecked, the loader determines the recipient’s address using the folder name where the outgoing document is located.
- *Save the original document name during export* – when checked, the original document name is preserved during export.
- *Ensure that the attached file has a unique name* – a unique code is added to the attached file so that it is more convenient to process attached files in the recipient’s system.
- *Validate documents in line with XSD during import* – checking XML documents against the existing XSD scheme.

12.2.2. SFTP settings

SFTP serves for exchange of ISO20022 documents.

The *ISO20022/Settings/SFTP settings* menu allows you to set up your terminal for receiving/sending ISO20022 documents.

[image]

In the *SFTP settings* tab you will find the following options:

- *Enable SFTP access* – check when it is necessary to export and import documents from a remote SFTP server;
- *Server address* – address of the server, which ISO20022 document exchange is going with;
- *Hostport* – port of the server, which ISO20022 document exchange is going with;
- *Login* – user's login on the server;
- *Password* – user's password on the server;
- *Folder's server address* – specify the server address of the folder containing ISO20022 documents.

12.2.3. CryptoPro settings

The *ISO20022/Settings/CryptoPro settings* menu is for setting up document signature with CryptoPro keys in the web interface.

Please note that to operate CryptoPro you need CryptoPro CSP v3.9 software installed on the terminal's server.

You will also need the following libraries:

libc6-i386,
lib32z1,
libnss3-1d,
libnspr4-0d,
lsb-security,
lsb-core.

[image]

In the *CryptoPro settings* tab you will see the following options:

- *Activate CryptoPro signing* – check when you need to activate signing of documents with CryptoPro keys;
- *Use certificate's serial number instead of the fingerprint* – check if indicated in the signature you want to have serial number instead of the fingerprint.

In the *Available keys* section you can do the following:

- By clicking the *Download* icon you can download the key certificate file;
- By clicking the *Settings* icon you can edit key parameters using the window depicted below.

On the list of available keys there are sorting and search options in place.

Key description is depicted below.

[image]

On this page you can change the following details.

If a participant owns several terminals then by clicking *Add* you can add terminals associated with this key.

Clicking the *Delete* icon will delete the terminal associated with the key.

In the *User* field you can change the key user. The new user will need to activate the key.

Save the changes by clicking *Save*.

12.2.4. Document code types catalogue

In the *Document code types catalogue* tab:

- Add new code by clicking *Add new code*;
- Edit data by clicking the *Edit* icon;
- Delete an entry by clicking the *Delete* icon.

[image]

13. Working with FileAct documents

13.1. Log of FileAct documents

FileAct menu section is designed for exchanging free-format documents.

Procedures with free-format documents are described in more detail in the document [2] in the section of the same name.

FileAct/Log menu allows you to view log of incoming/outgoing/erroneous FileAct documents.

The log has sorting and filtering options for a range of fields.

[image]

Log entries can be **sorted** by the field value. The arrow next to the field name changes the sorting direction. The up arrow sorts in ascending order, the down arrow sorts in descending order.

The log allows you to filter entries by the fields below which there is a search window. To filter by the document registration date you need to click *Search* in the first line of the window and in the pop-up line set the range of dates for search and click *Search* on your right.

The *Delete selected* button will delete documents selected in the first column. The document status must allow you to do so.

Clicking the *View* icon in the log's right-hand column or double-clicking the line will allow you to view the log entry.

[image]

On the screen you will see:

- Document details;
- In the *View* tab you can download RCU and BIN files.

In the *Signatories* tab you will see information about the signatories of the incoming/outgoing document.

In the *Events* tab you will see events related to the document.

[image]

In the *Associated documents* tab you will see information about the documents associated with this document as follows.

[image]

13.2. FileAct section settings

The *FileAct/Settings* menu allows you to activate automatic signing with CryptoPro keys.

[image]

You will see the same options as the ones for the ISO20022 documents:

- *Activate CryptoPro signing* – check when you need to activate signing of documents with CryptoPro keys;
- *Use certificate's serial number instead of the fingerprint* – check if indicated in the signature you want to have certificate's serial number and not its fingerprint.

In the *Available keys* section you can do the following:

- By clicking the *Download* icon you can download the key certificate file;
- By clicking the *Settings* icon you can edit key parameters as described in CryptoPro settings.

In *Verification of incoming documents – Available certificates* you can view the certificate on the page as follows.

[image]

Download allows you to download the certificate file.

Deactivate allows you to deactivate the certificate.

14. User management

14.1. Creating a user

Clicking *User* in the main menu brings you to the user log.

[image]

To create a new user account click *Create*.

When creating a new user fill in the following fields:

Email – user's email address;

Full name – user's first name and last name;

Role is selected from the list:

- User – terminal user who can send any message type;
- Administrator – CyberFT terminal administrator;
- Verifier – user that accepts sending of documents to the CyberFT Network, but that does not sign documents. Functions of the verifier are detailed in Verifying user function.

List of available terminals – select terminal available to the user or select the "All terminals" option. Add the selected terminal by clicking *Add*. Delete the terminal from the list by clicking the *Delete* icon, whereafter it will appear in the Add field above the list. On the list you can also choose the "All terminals" line.

Turn off visual division of interfaces by organizations – when checked, in the catalogue user can see data of all terminals available to him.

Signing level is selected from the list (Not a signatory/Level 1/Level 2/…/Level 7). **Please note** that documents should be signed by users in **ascending order** of the signing level.

Authorization type of a user is selected from the list (by password/by key).

Upon checking the entered data click *Create*.

[image]

The first user password is the same as their email; however, upon first authorization the user password is required to be changed. The new user password is displayed on the screen and later on it can be changed only by the chief administrator.

Upon initial creation of a user they need to be activated by entering the system with the rights of administrator or security officer.

14.2. Viewing and editing user data

In the *Users* catalogue clicking the *View* icon in the right-hand column will bring you to the next user data viewing form.

[image]

Delete a user by clicking *Delete*.

To edit user data click *Edit* (or the *Edit* icon in the user log). You will see the form as follows.

In the first section of the form you can edit values of the filled in fields.

[image]

List of available terminals enumerates terminals available to the user. Remove a terminal from the list by clicking the *Remove* icon. After that it will appear in the field above the list from where you can add it. The list has an “All terminals” line that you can choose. Add the selected terminal by clicking *Add*. (The list is empty in the example).

Turn off visual division of interfaces by organizations – when checked, in the catalogue user can see data of all terminals available to him.

In the second section of the *Services* form you can edit user access to system services.

[image]

Checking a particular **service** will allow a user to use that service. After checking *On* and clicking *Save* in the *Additional settings* field you will see a settings icon and a *More* link that allows you to set additional settings for interaction of user with a particular document type.

Checking *Manage documentation widgets* will allow a user to add links to the documentation sections, which can be used by clicking the <?> icon.

14.3. Additional user settings

In the previous image in the *Additional settings* field you will see links for creating additional service settings.

[image]

In the *Role* tab assign one of the two **SWIFT roles**:

- Preliminary authorizer – checks **all** SWIFT documents with **any** amount range;
- Authorizer – checks SWIFT documents with a particular amount range.

Please note that the “Preliminary authorizer” role can be attributed to a certain user only if another user is attributed the “Authorizer” role. A preliminary authorizer role is not mandatory. You can assign several authorizers for documents with different amount ranges.

In the next image you can see *Role settings*. Here you can choose *Document type* that user can work with, document *Currency*, and document *Amount range*. An authorizer can approve only those documents that comply with the conditions above.

Add document type by clicking *Add*. The list may contain several types.

[image]

Check an option in the *Rights* tab to grant a user the right to delete documents.

[image]

To change the user password check *Password reset*.

14.4. User commands

In the *Commands* tab on the user viewing page you can view the following information.

[image]

14.5. Account management

In the *Account management* tab on the user viewing page you can view an activity log of a user’s account.

[image]

14.6. User’s key certificate

In the *Certificates* tab on the user viewing page you can view user status and user’s public key certificate fingerprint.

[image]

Clicking the *Edit* icon in the previous form will bring you to the following certificate editing form.

[image]

To edit or create a new public key certificate you need to:

- Obtain a public key certificate file;
- Open the certificate file using a text editor;
- Copy the certificate;

- Put the certificate in the *Certificate* field in the previous image;
- Click *Edit*.

Changing the certificate will also change the certificate fingerprint, which means the user will receive a new key.

14.7. User activation

To enable a user to work with the CyberFT terminal the user needs to be activated. Users are activated by the terminal administrator or by security officers.

14.7.1. User activation by the terminal administrator

If you check a “do not use security officers” option during terminal installation in the *User/Information* section you will see an *Activate* button. When pressed by administrator it activates the user and they receive an “activated” status.

[image]

14.7.2. User activation by security officers

If you check a “use security officers” option during the terminal installation follow the instruction below.

A user with administrator rights should enter the interface in the *Users* section, open *View* of the to-be-activated user and click *Activate* as depicted below.

[image]

After that a user with the rights of the left security officer should enter the interface and click *Approve*. The form should display an activation key for the left officer. In the example it is represented by “bV” letters.

[image]

Now you need approval of the right security officer.

[image]

A user with the rights of the right security officer should enter the interface in the *Users* section, open *View* of the to-be-activated user and click *Approve*.

[image]

In the next image you can see a key for the right security officer. In the example it is represented by “6M” letters. The user is then given the keys.

[image]

The first time user should enter the interface using their login and password, enter the key's value consisting of the left part ("bV") and the right part ("6M") in the *Activation key* field and click *Activate*. Now the user is activated.

[image]

14.8. Verifying user function

As detailed in the Creating a user section, **verifier** is a user who accepts sending documents to the CyberFT Network, but does not sign documents.

The image below shows an example of parameters for a user who is assigned a role of the verifier.

This user accepts terminal's outgoing documents. He either approves or denies sending of the terminal's outgoing documents.

[image]

As illustrated below, clicking *Send* allows the document to be sent, whereas by clicking *Do not send* verifier prohibits the document from being sent.

[image]

Please note that a verifying user can perform a **document accepting function** only if you check the *Manual control* option for controller's keys as described in Editing controller's key.

After the verifying user completes the *Send* command, the document is automatically signed by the key of the automatic controller.

15. Reporting

Main menu's *Reporting* contains information about the participants' signatories. The *Automatic signing* tab in the *Signatories* sections shows information about the certificates of the keys used for automatic document signing by Participants.

[image]

In the *Manual signing* tab you will see a report about users that have been attributed particular manual document signing levels depending on the module they work with.

[image]

16. Settings

The *Settings* menu in the main menu has subsections as illustrated below.

[image]

16.1. General settings

The *Settings/General settings* menu has the following settings.

In the *Terminal* field when selecting “All terminals” the same settings will be applied across all terminals of the sending organization. When selecting isolated terminals you can set different settings for each terminal.

Check *Use old template for signing outgoing documents* if you need to send documents from the new version terminal to the old version terminal. (Different versions use different signature formats.)

Check *Apply ZIP archiving for outgoing documents* if you need to ZIP archive outgoing documents.

Click *Save* to save the changes.

[image]

16.2. Controller

The *Settings/Controller* interface menu is meant for creating the controller’s key. This menu is described in Controller’s key generation. The controller’s key import procedure is detailed there also.

All terminal’s outgoing documents are automatically signed by the controller’s key.

Please note that if you checked the manual control option, the terminal’s outgoing document sending needs first to be accepted by the verifying employee and then signed by the controller’s key.

16.3. Automatic signing settings

Settings/Automatic signing settings allows you to set automatic document signing for a **specific recipient**.

To do so you need to choose a recipient’s address and choose an **additional key** used with a particular terminal for signing documents in the automatic mode. When these settings are in place messages will be automatically signed with the controller’s key and with the additional user key.

[image]

Choose *Sender’s terminal ID* and *Receiving participant’s address*, click *Next*.

In the next window check the additional key used for automatic terminal message signing and click *Save*.

(In the illustrated example the receiving participant is SABRUMMXXX, the sending terminal is PHPTEST@001, the controller key name is phptest, and the name of the additional user key for automatic signing is User 2.)

[image]

16.4. Exchange with CyberFT Network

Automatic exchange between the Terminal and the CyberFT Network is started from *Settings/Exchange with the CyberFT Network*.

If automatic terminal processes are running, in order to enter and tweak settings you need first to stop automatic terminal processes. To do so you should go to the tab with the terminal's name and click *Stop processes* (when terminal processes are not running you will see a *Start processes* button instead).

In the *Network exchange settings* tab enter the processing URL value: either test processing or production processing.

[image]

Enter the following values in the corresponding terminal tabs.

STOMP settings – processing queue.

Login – participant's terminal ID;

Password – come up with a password for the processing queue that would meet the requirements described in the window.

Password Hash will be formed automatically.

To save the changes click *Save*.

Please note that after creating or changing the password you should communicate the Password Hash value to the CyberFT implementation engineer.

[image]

Then you need to enter the controller's private key password in the *Password* field of the *Automatic processes settings* section. To **start** automatic terminal processes click *Start processes*. Once started, you should see the following message: "Automatic processes for the terminal <ID> have been started on {date time}".

To **stop automatic processes** for the terminal click *Stop processes*. (You may need to do that when replacing your key, for instance). With exchange stopped only the document registration process of the *Document log* remains, meanwhile processing does not receive any requests.

16.5. Signing settings

Settings/Signing settings contains settings for document signing. **Please note** that each document type requires its own settings.

The first column in the image below shows names of the **data load channels**.

[image]

For each document type can specify the number of signatures you need, the same goes for signing sources.

For instance, SWIFT documents can be sent without signing, whereas *Banking services* documents must be signed before sending.

To be signed in the interface – check documents that need private user signature (unchecked by default).

To be automatically signed – check documents that need controller's automatic signature with the additional key.

Required number of private user signatures – choose one of the following: Not required (automatic signatory only) / one signature / two signatures / … / seven signatures.

Please note that when a document has one or more required private signatures, it will not be processed until it has the required number of signatures.

A document can be signed by the private user signature only with the "Slim CyberFT Terminal Network Client" software, installation of which is detailed in the documentation [2].

16.6. XML export settings

Settings/XML export settings is designed for specifying the XML export path of CyberFT documents.

[image]

If you need to export the module documents in the XML format, check the corresponding table line. By default the *Specify the XML files export path* field has /transport, but you can specify a different folder.

Save the changes by clicking *Save*.

16.7. Security

Settings/Security has the following settings:

- *Number of failed login attempts* – after the specified number of failed login attempts the user is blocked;
- *Password life* – you will need to change the password after the specified number of days;
- *Additional encryption certificate* – choose an additional encryption certificate from the list.

[image]

Check *Use SHA 256* if you need to additionally use the SHA 256 encryption algorithm.

Check *Mandatory strong password* if when logging into the web interface you want users first to enter a difficult password that meets the following requirements:

- Is at least 8 characters long;
- Contains both upper and lower case letters;
- Contains a digit and a service character;
- Does not match current terminal ID.

Upon initial interface login user has to change the standard password to a strong one.

16.8. Verifying incoming documents

In *Settings/Verification of incoming documents* you can set up verification of incoming documents depending on the sender, currency and amount range.

In the following window you will need to:

- Choose sender’s terminal;
- Specify currency;
- Click *Next*.

[image]

You will see the window below.

[image]

There you will need to fill in:

- Range of amount values for the chosen currency;
- Signatures necessary for verifying messages. Signatures are added on the “AND” or “OR” basis;
- Click *Save*;
- If you need to add a range, click *Add amount range* and repeat.

If in incoming messages from the TESTRUMM@A001 terminal there are no specified signatures for the indicated amount ranges, documents of that sender with indicated amount ranges will be received with an error.

You can **remove amount range** by clicking the *Remove* icon in the amount range line. You will see a message saying “Condition removed”. You can then enter new amount range values.

16.9. CryptoPro keys

In *Settings/CryptoPro Keys* you can set up signing documents with CryptoPro keys in the web interface.

Please note that to work with CryptoPro the terminal server should have CryptoPro CSP 3.9 installed.

You will also need the following libraries: *libc6-i386, lib32z1, libnss3-1d, libnspr4-0d, lsb-security, lsb-core.*

On the *CryptoPro Keys* page you will see CryptoPro keys available at the terminal. In the first column you will see a key certificate fingerprint, in the second column you will see key owner’s name.

[image]

Clicking the *View* icon will bring you to the next page where you can view the key details.

[image]

After clicking *Save* the following window will pop up:

[image]

You can download the key certificate as a file.

Clicking *Delete* will delete the key certificate. **Please note** that you can only delete inactive keys.

Clicking *Change* (or clicking the *Change* icon form the list of keys) will bring you to the next page for **key editing**.

On this page you can change the following details:

- If a participant owns several terminals, you can add/remove terminals associated with that key;
- In the *User* field you can change the key user; the new user will need to activate the key.

Click *Save* to save the changes.

Key certificate details are displayed automatically and cannot be changed.

[image]

In the example above you can see PLATRUMMAXXX terminal added to the selected key, you can delete it by clicking *Delete*.

In this case on the list of available terminals there is only one PLATRUMMBXXX terminal; you can add it to the list of terminals associated with the key by clicking *Add*.

16.10. Setting up mail notifications

In *Settings/Mail notification settings* you can tweak settings of the mail server used for sending mail messages to the users.

[image]

On this page you can specify the following **mail server parameters**:

STMP host – mail server address;
STMP port – port number;
Login – login of the user on whose behalf the messages are going to be sent;
Password - password of the user on whose behalf the messages are going to be sent;
Encryption – choose from the list: (None / TLS / SSL);
Test address – user's test address. Upon entering the test address you can send a test letter by clicking *Test*.

16.11. Notification mailing list

Settings/Notification mailing list allows you to specify mail addresses of users who are going to receive notifications.

[image]

To add a new user to the mailing list, choose their name from the list. Click *Add*. User's email can be edited.

To remove a user from the list, click the *Remove* icon in the user line.

16.12. Event notification preferences

In *Settings/Event notification preferences* you can set up preferences for events that users from the mailing list are notified about.

[image]

The first column contains notification *event type*s. Check event types that you want to notify users about.

"*Delivery time threshold* = 15 minutes" means that notifications are sent if a particular document was not delivered to the user within 15 minutes.

When checking *Expiration of the certificates* you will see reminder about the certificate's validity time coming to an end. In the *Remind _ days in advance* enter the N number of days and the reminder will start popping up N days in advance to the expiration of the certificate.

16.13. Terminals

In *Settings/Terminals* you can manage the list of terminals operating in the CyberFT.

[image]

By clicking the *View* icon you can view the terminal info as illustrated below.

[image]

Clicking the *Edit* icon on the list of terminals or clicking the *Edit* button in the viewing window will allow you to edit the terminal parameters.

Clicking *Remove* will remove the entry from the list of terminals.

Clicking *Create a terminal* on the list of terminals will bring you to the next page.

There you will need to enter *Terminal address* and *Company name*.

Terminal status is selected from the list: Active / Inactive.

Click *Create* to complete the process of creating a terminal.

[image]

17. Register of CyberFT participants

In *Register of CyberFT participants* you can manage the *CyberFT Network Participants* catalogue.

[image]

Clicking *Request update* will update the *Catalogue of network participants*.

View full column description by hovering the mouse cursor over the column name.

By clicking the *View* icon you will see the following page of the catalogue viewing.

[image]

By clicking the *Edit* icon on the next page you can edit a participant’s parameters and save the changes by clicking *Save*.

[image]

18. Event log

In the *Event log* menu you can view system events. In the example below the log is sorted in the *Event ID* descending order.

[image]

Component is a subsystem in which an event occurred. A list of subsystems is depicted in the image.

[image]

Level is an event level; list of levels is illustrated in the image below.

[image]

EC stands for Event Code;

Initiator is an event initiator from the list below.

[image]