CyberPlat®

CyberFT

Universal system for financial data exchange and electronic documents workflow

Contents

About CyberPlat

- CyberPlat was established in 1997 and it created Russia's first and by far largest electronic payment system of the same name (CyberPlat®).
- CyberPlat is widely represented in Russia and Kazakhstan, and also operates in India, Austria, Germany and Switzerland.
- As of today, CyberPlat® outlet network consists of over 1,480,000 points of sale.
- Over 8,000 providers use CyberPlat® to process payments, including providers such as MTS, Beeline, MegaFon, Tele2, Rostelecom, and NTV Plus.
- Over 250 banks have joined CyberPlat®, including Alfa-Bank, VTB, Russian Agricultural Bank (Rosselkhozbank), and many others.
- In 2017 CyberPlat® processed over 1 billion transactions.
- Throughout 20 years of operation not a single data breach was detected.

Glossary

CyberFT Platform is a software and hardware solution for organization of a secure information highway for interchange of all generally accepted message types of financial and electronic document flow. CyberFT is developed by CyberPlat, the leader of electronic payments in Russia and CIS.

CyberFT Provider is a legal entity, an entitled member of CyberFT that handles the Processing.

CyberFT Processing is a software and hardware solution for organization of an electronic document flow in CyberFT Network.

CyberFT Customer is a legal entity or individual using CyberFT for data exchange.

Customer Software is software installed at CyberFT Member site for interaction with CyberFT Network.

CyberFT Network is an aggregate of CyberFT Providers and Customers that joined CyberFT.

What is CyberFT designed for?

CyberFT Platform is a convenient and fully secure solution enabling banks and their customers to:

- Operate in total conformity with local legislation
- Fully protect transactions from external threats
- Ensure integrity of the customer information containing trade secrets
- Organize electronic document workflow of legally valid documents between banks, corporate customers, government authorities, etc.
- Optimize financial transaction costs
- Set up a direct data exchange between customers and banks (host-to-host) using uniform channel and standardized message formats

CyberFT as an element of national security

Domestic interbank networks must be autonomous, otherwise state sovereignty might be jeopardized and might become dependable on hostile actions on behalf of the US or other forces.

Before the testimony of Edward Snowden regarding mass surveillance during the PACE on April 8, 2014[1] bank community was almost unaware of the threat posed by the data exchange containing bank secrets through SWIFT that is carried out through hubs and servers situated in the US, the Netherlands and Switzerland. However, from the stability viewpoint data of different hubs is supposed to be stored on the main server to restore data in case a system failure occurs.

1. http://leaksource.info/2014/04/09/edward-snowden-testimony-parliamentary-assembly-of-the-council-of-europe-pace-04-08-2014/

All that in spite of the fact that security experts have been pointing out vulnerability of such a system for years, and they also emphasized that in all developed countries local (domestic) bank information is not allowed to cross borders of its country. Domestic interbank networks must be autonomous; otherwise state sovereignty might be jeopardized and might become dependable on hostile actions on behalf of the US or other forces.

Due to the fact that unlike many other systems operating on the global market all software was developed by Russian experts (license and patent independence), and all CyberFT Platform servers will be situated in the local territory of the platform purchaser's country, possibility of commercially vital data leak of electronic document flow significantly decreases.

CyberFT — conformity with local legislation

In accordance with requirements of local legislation a country usually imposes ban or strict limits when it comes to exit of information related to local (domestic) bank transactions. For instance, personal information of European countries (financial transaction nearly always contains personal information) cannot be processed in a country outside the EU unless the latter ensures provides an adequate level of protection[2].

In early 2011 People's Bank of China issued a Notification for bank financial institutions requiring security of financial information. Among other things, this Notification prohibits banks from storing, processing or analyzing any personal financial information collected in China beyond its borders.

CyberFT Platform is fully compliant with national payment law of any country, including Russia.

2. Directive 95/46/EU also known as Data Protection Directive

CyberFT ensures integrity of business information

One of the key goals of CyberFT is to ensure security of information containing bank or trade secret. According to Zecurion in 2013 losses of both companies and banks from confidential information leaks exceeded USD 25 bn.

Vital commercial information processed by payment systems and transferred through communication channels is vulnerable to many threats, among which are:

1. Security threat of interbank communications, since currently most of the SWIFT transactions (with minor exception) are processed through the servers situated in the territory of the US and Western Europe. Placement of servers in the US, the Netherlands and Switzerland compromises SWIFT customers from other countries, because at any point in time (e.g. due to the change in political situation) servers may be shut down, which in turn will cease data exchange not only with foreign banks-counterparties, but also domestic financial information exchange via the SWIFT system.

2. Threat of theft directly from the system processing and effecting payments. The information may be both accessed at the request of the intelligence agency of a foreign country and intercepted by swindlers or other perpetrators at any section of communication line which can be as long as 20 000 km. Such information, typically related to the bank secret, may be exploited by thieves themselves or by persons that intercepted that information from thieves (as happened time and again in big recent international scandals).

3. Threat of the leak of the previously stolen information. Big recent scandals (e.g. Snowden testimony or appearance of WikiLeaks) indicate that commercial information accessible to intelligence agencies can often become publicly available.

4. Threat of handover of information to competitors. One of the examples of such a leak is a scandal that broke out in the US in the 90s, when because of the interception of talks by the National Security Agency, Airbus lost a USD 6 bn contract with a national airline company of Saudi Arabia. In the end, this contract was signed by McDonnell Douglas, subdivision of Boeing (main rival of Airbus).

5. Threat of sale of stolen information. Today information is a valuable product – the more important it is the more valuable it is. That is why information containing trade and bank secret became a “honey pie” for cyber perpetrators.

As was stated above, protection against these threats is regulated by legislation of an array of countries that prohibit transfer of financial information across their borders or granting of access to such information in the territory of a foreign country.

Usage of CyberFT significantly reduces all risks of theft, loss or sale of vital information of banks and that of their customers. Since hardware will be located in the data center of the CyberFT Provider, the risk of commercial information theft from communication hub servers plummets, and since communication channels will be much shorter, the risk of theft of commercial information from communication lines will be much lower as well.

The message text sent by CyberFT Participant (sender) to another Participant (receiver) and that is not addressed to CyberFT Provider is accessible only to the message recipient, i.e. the customer.

Overview of CyberFT's distinctive features

	SWIFT	CyberFT
Clients	About 10 000 banks and a small number of corporate clients	✓ Capability to encompass all banks and corporate clients without any limitations.
Coverage	✓ Whole world	✓ Whole world
Conformity with legislation	Doesn't conform to the federal law 112 dated May 5, 2014 'On amending the federal law 'On the Natonal Payment System'.	✓ In full conformity with requirements of Russian legislation
Operating hours	✓ 24*7	✓ 24*7
Implementation costs	No less than USD 53 000 including mandatory cabling from a specific communciation service provider up to USD 200 000 for each new client	✓ Free of charge
Transaction costs	SWIFT FIN: Domestic transaction EUR 0.02 – 0.05, cross-border transaction EUR 0.03 – 0.18	✓ No more than 50% from the SWIFT fee for the same transaction
Maintenance costs	No less than EUR 10 000 per year	✓ Free of charge.
Implementation time	No less than 8 weeks in case of shared connection and at least 16 weeks in case of direct connection	✓ Connection to CyberFT processing including integration with automated banking system takes from 1 to 3 weeks, and no more than 2 weeks in case of customer's own CyberFT platform implementation
Data transfer speed	✓ A few seconds	✓ 1.5 seconds
Data exchange formats	✓ SWIFT Fin (MTXXX messages), InterAct (MX messages), FileAct (unstructured messages)	✓ SWIFT Fin (MTXXX messages), InterAct (MX messages in accordance with ISO 20022), FileAct (unstructured messages with attachments), EDI documents (contracts, invoices) and more.
Maximum message size	No more than 10 Mb	✓ Standard maximum message size limit is 100 Mb. It can be easily increased according to customers' needs
User interface	✓ Several versions of SWIFT Alliance software for full-fledged working	✓ User friendly web-interface for full-fledged working
Additional services for corporate customers	Special conditions for corporate customers comparing to conditions for banks.	✓ Special conditions for corporate customers. Designated 1S-module. Service for electronic documents workflow
Archive availability	Data is normally stored for only 4 months	✓ Special conditions for corporate customers, specialized 1C payment module, EDI service of legally valid documents.
Types of interaction	Processing only	✓ Processing and clearing.
Cryptography	SWIFT cryptographic means. No capability to change cryptographic means	✓ Various cryptographic means (including OpenSSL, PGP and GOST algorithms based on CryproPro, Signal-COM, etc.) Support of any means of cryptographic protection. E-signature for electronic messages
Transactions security	Data is available to SWIFT	✓ Data is not available to the CyberFT provider.
Servers location	USA, Switzerland and Netherlands	✓ Russia and any part pf the world by the CyberFT Provider choice
Reliability	Specialized data exchange protocol and 'hot backup' of each network element. A total of 4 datacenters.total of 4 datacenters	✓ Advanced and effective software and hardware measures (both technical and organizational) to provide high system reliability. Number of service providers is unlimited
Network topology	Star (all participants are connected to the single center)	✓ Fully connected (there can be unlimited number of centers connected between each other where network participants are connected to these centers)

Supports multiple providers

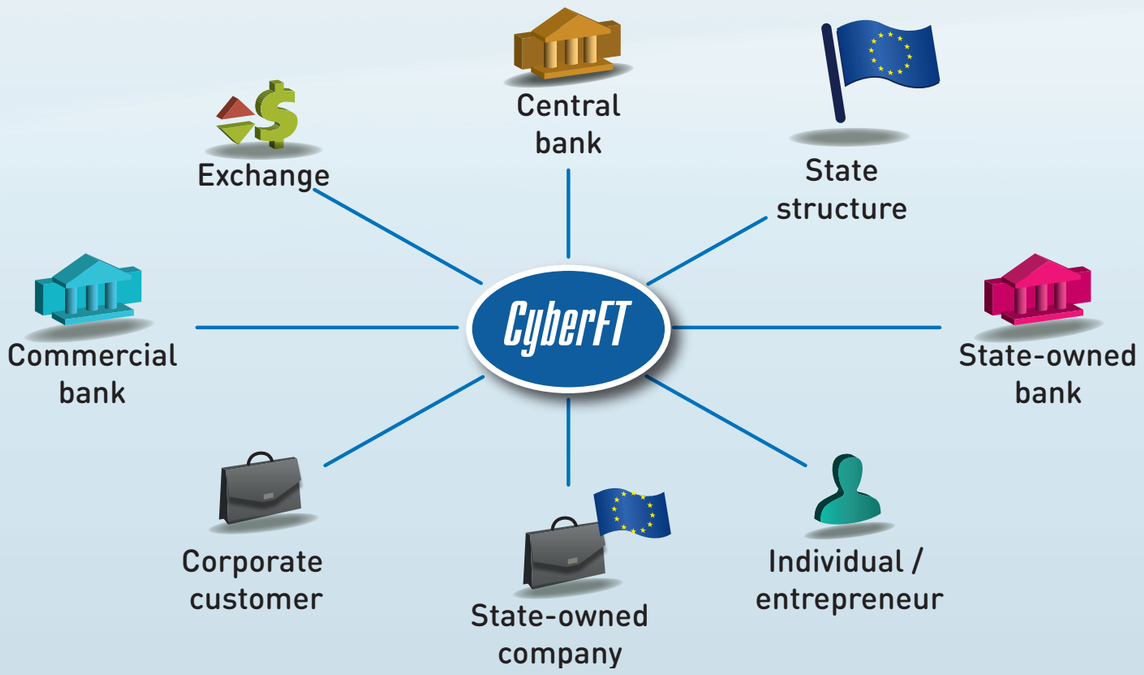
CyberFT Network consists of unlimited number of Providers and Participants which use CyberFT Platform for organization of financial data exchange and electronic documents workflow.

CyberFT Network consists of unlimited number of CyberFT Participants that are using CyberFT Platforms for their electronic document flow. CyberFT Platform is set up at the purchaser's area and is independent from CyberPlat. CyberFT Provider can serve banks and their customers both in the regions of their presence and within a specific bank or corporate group.

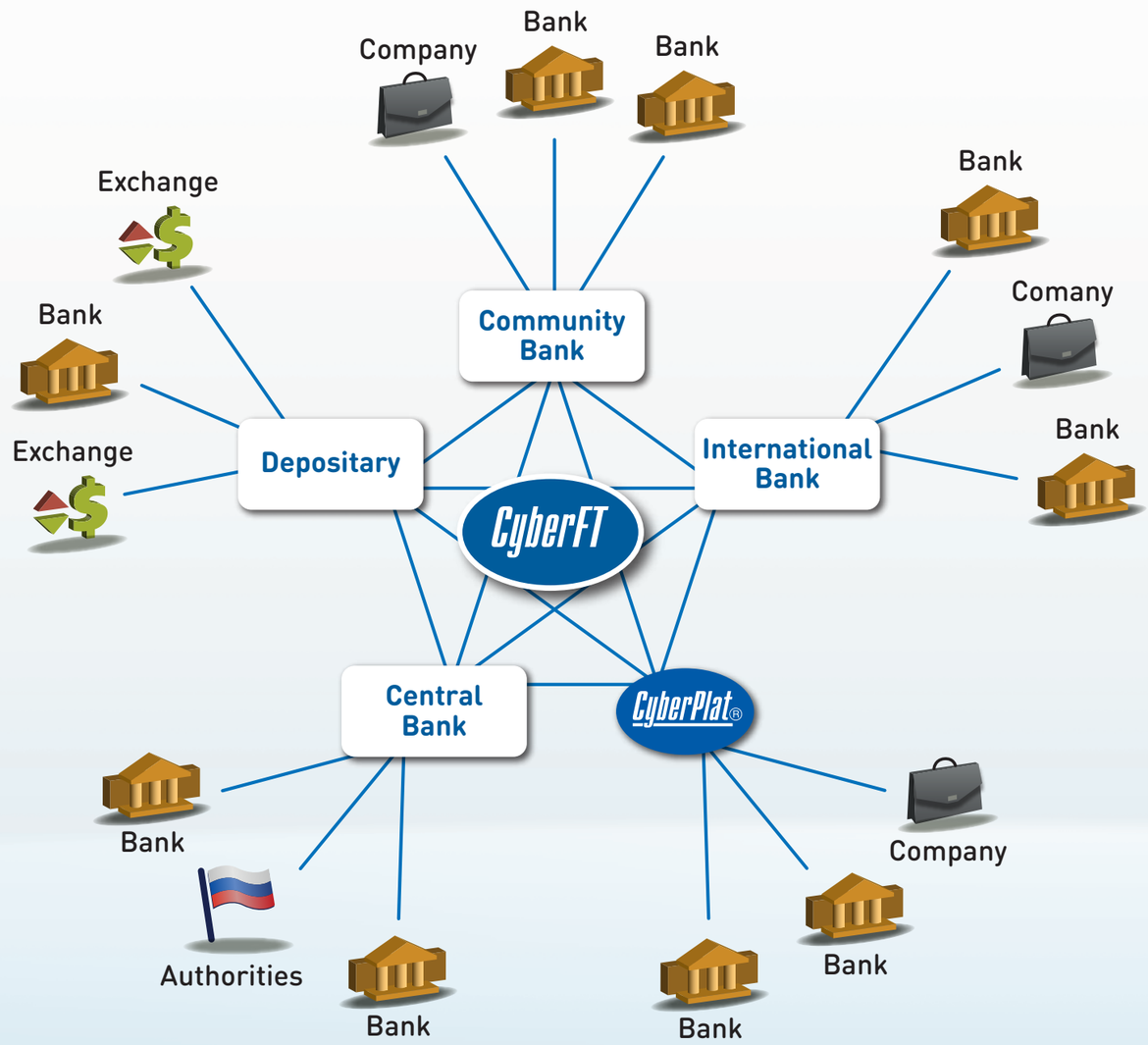
Banks, corporate customers, exchanges, brokers, state structures and other types of organizations can become CyberFT Providers or Participants. Each CyberFT Participant gets his own unique identifier (unless he is a participant of SWIFT) or SWIFT identifier is used.

Catalogue of CyberFT Participants is distributed on regular basis to each Participant and is updated automatically. CyberFT identifier is unique not only in the frame of certain CyberFT Provider but whole CyberFT Network. Thus, Participant with certain identifier can be connected to one Provider only, which ensures CyberFT Network integrity.

CyberFT Providers can be connected with each other by different ways. Some of examples are presented below:



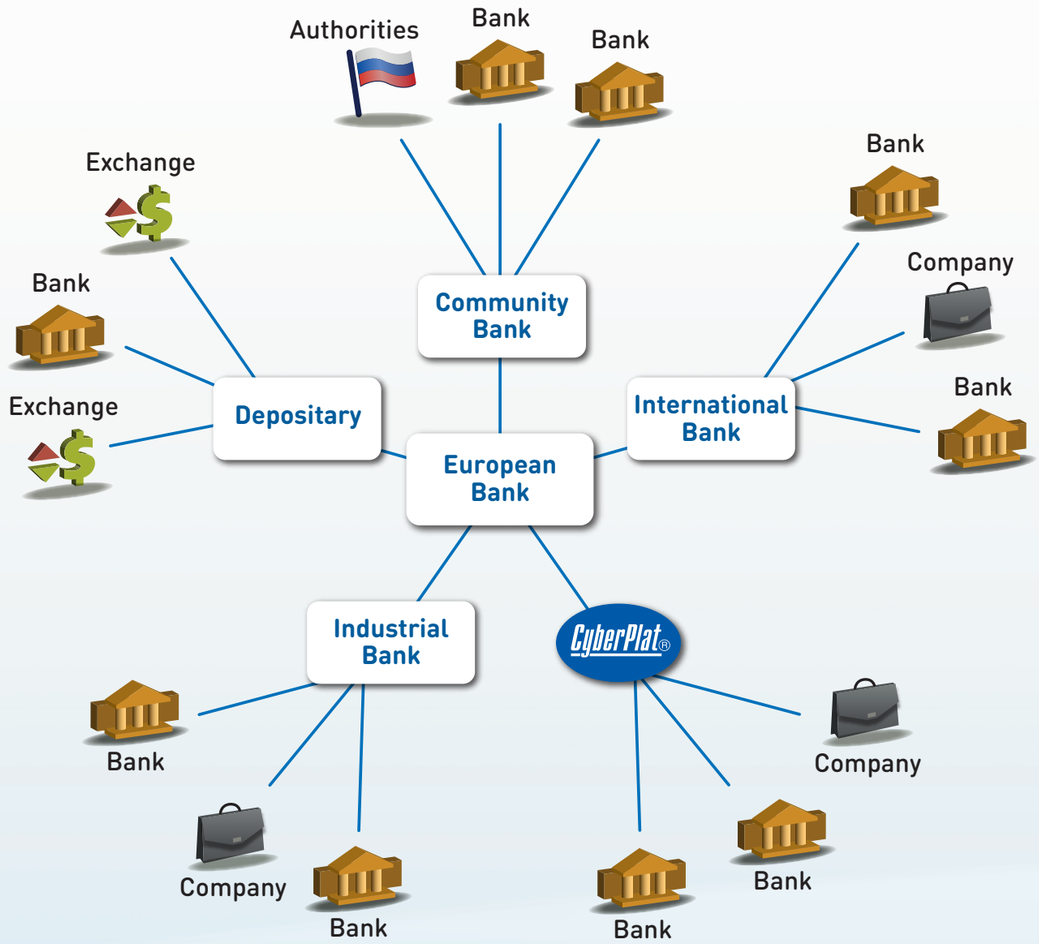
1. With each other*



Route of the document is stored on every CyberFT Provider's end that participated in its delivery. Moreover, all transactions with Sender's electronic signature are stored on the Sender's and Receiver's ends as well as on CyberFT Provider's end in encrypted mode. Thus, each Participant of the information exchange process in CyberFT has comprehensive legally valid electronic documents.

* Names of the organizations are for demonstration purposes only

2. Through the jointly chosen central CyberFT Provider*

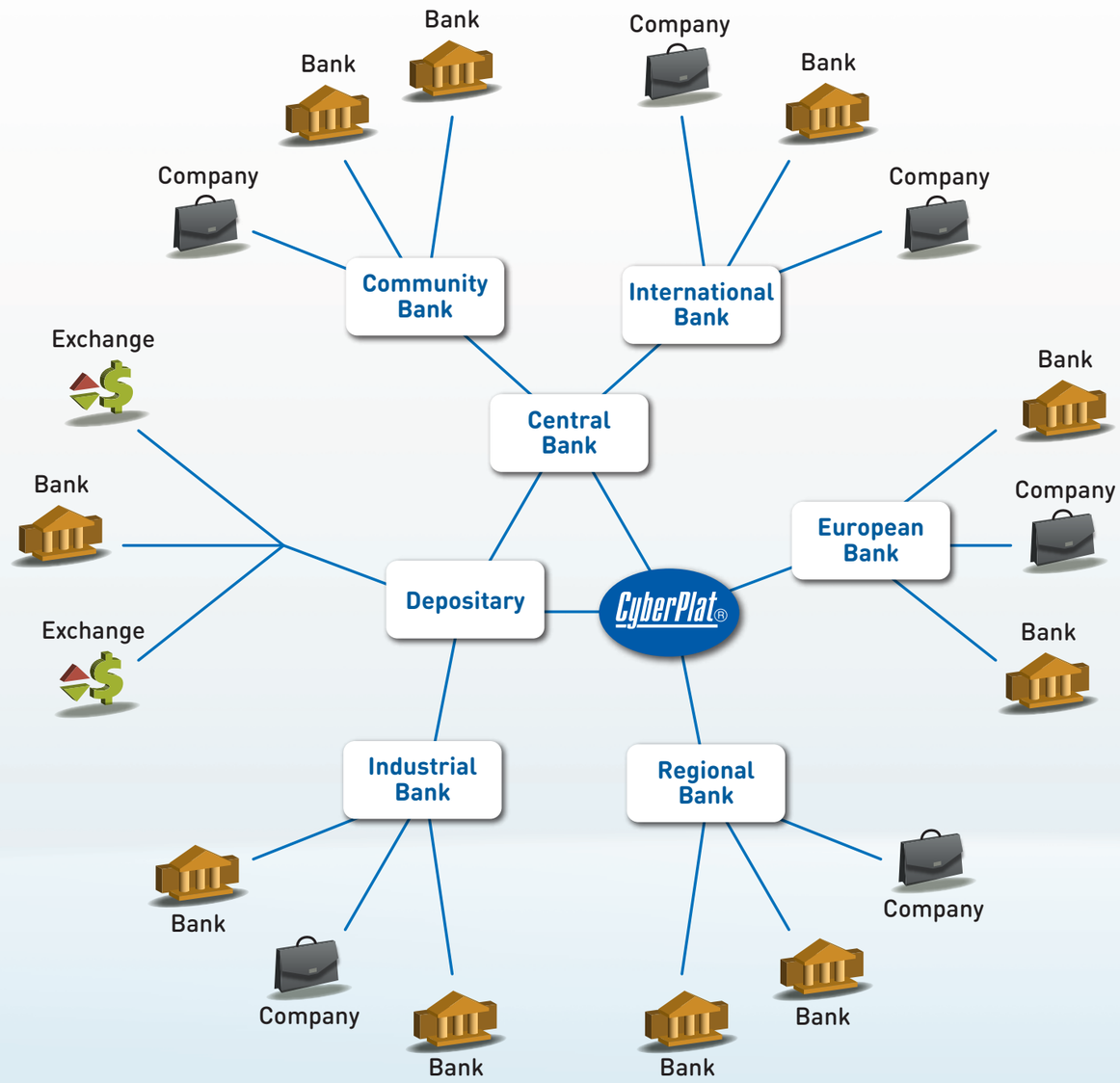


For instance, any major bank group can become a CyberFT Provider and combine its subsidiary organizations, correspondent banks and customers. At the same time, to exchange data between Participants of different bank groups all Providers sign an agreement with a common Provider (e.g. European Central Bank) who will be responsible for message routing between CyberFT Providers.

On one hand, such network topology significantly simplifies organization issues related to establishment of relationship between the Providers and allows the Providers to interact through the uniform organization (central Provider) which all of them trust. On the other hand in case of technical issues at the end of the main provider, interaction between the network participants will be interrupted.

* Names of the organizations are for demonstration purposes only

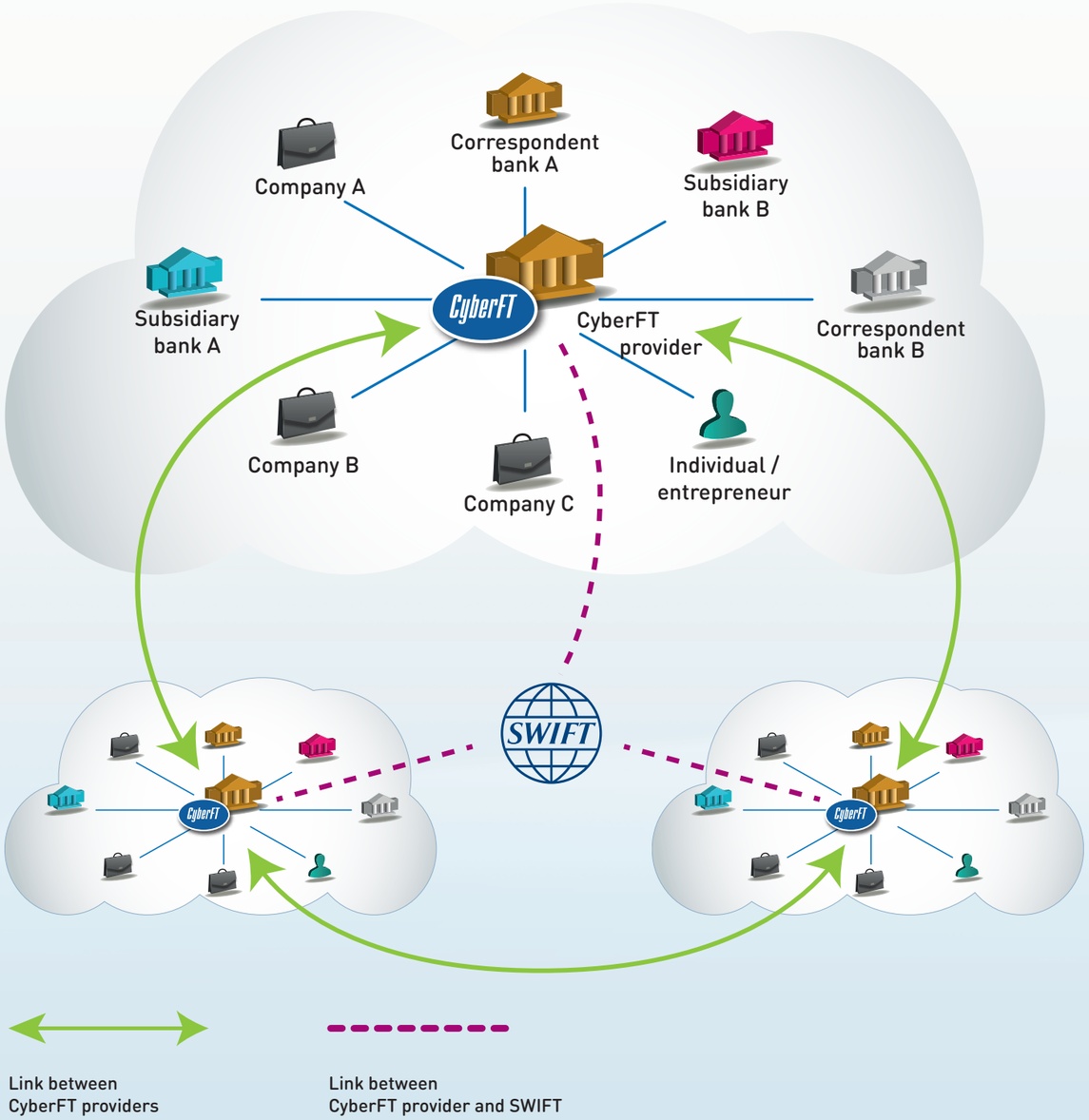
3. Through the group of interconnected CyberFT Providers*



This option of network organization has an improved resilience in spite of complicated organization processes related to relationship development and contract signing between CyberFT Providers. In case of any technical issues at the end of one or several Providers, interaction between other CyberFT Providers will remain intact.

* Names of the organizations are for demonstration purposes only

CyberFT Participants are also able to interact with other counterparties that are using SWIFT. One of the examples of such interaction is illustrated below.



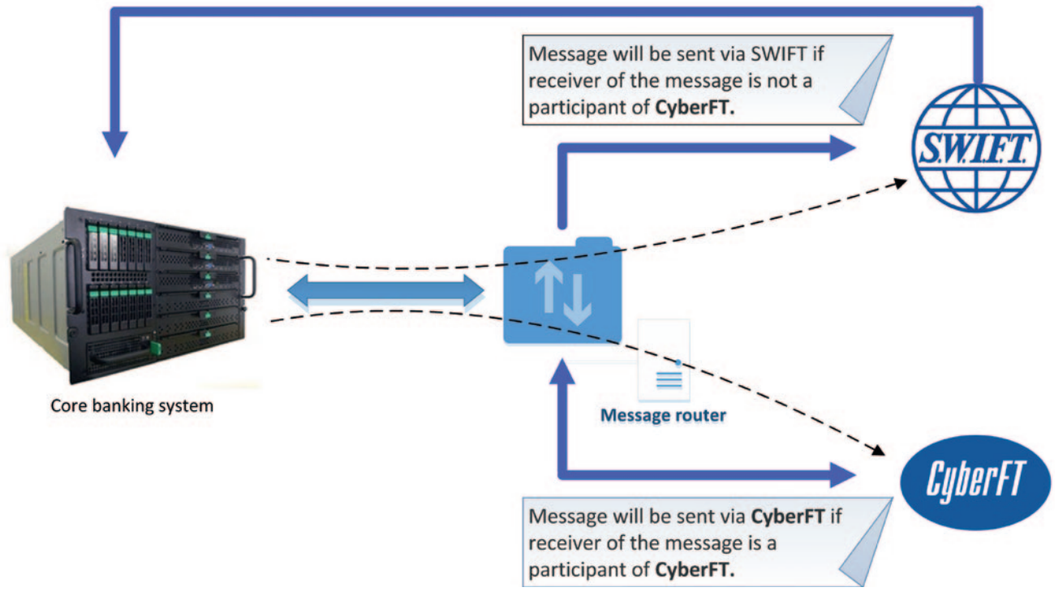
Thus, CyberFT allows its participants to interact via SWIFT if receiver of the message has not joined CyberFT Network yet or type of the transmitted message is not yet supported by CyberFT.

Compatibility

When connecting to CyberFT, Customer software can operate in parallel with SWIFT. The chart below illustrates interaction between SWIFT and CyberFT at the end of the Customer.

Before CyberFT implementation

After CyberFT implementation

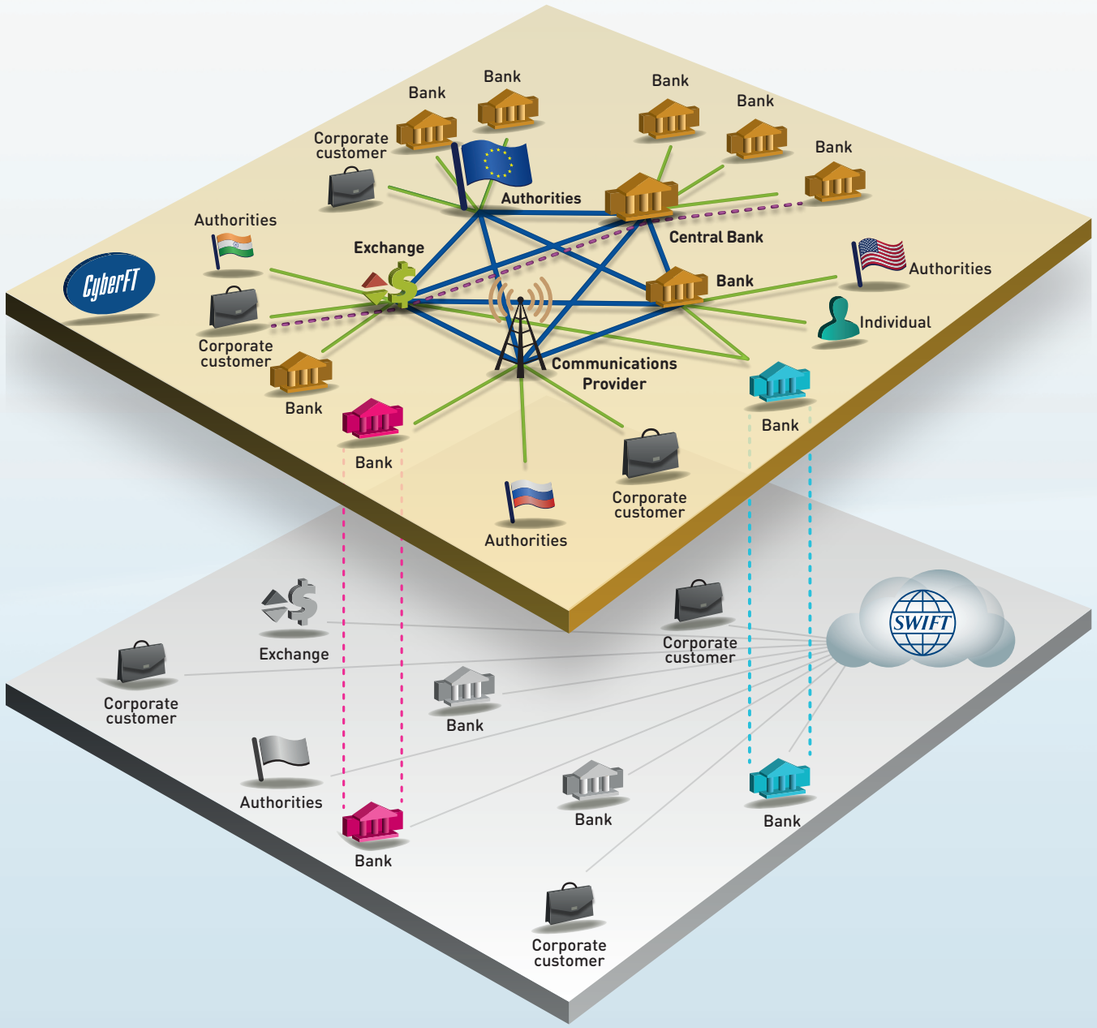


If a recipient is in the CyberFT Network then the Message Router will redirect that transaction through CyberFT.

If the payment recipient is not connected to the CyberFT Network, further transaction processing will be carried out by SWIFT. That said, a customer has flexible options for routing outgoing messages only via SWIFT, even if the message recipient is a CyberFT Participant; e.g. to certain addressees of a certain type or category, above the threshold amount, etc.

When a new Participant joins CyberFT, a centralized catalogue of Participants is updated automatically remotely. CyberFT software is provided to Customers free of charge.

CyberFT can be easily integrated with different systems used by a Participant and can operate in parallel with SWIFT.

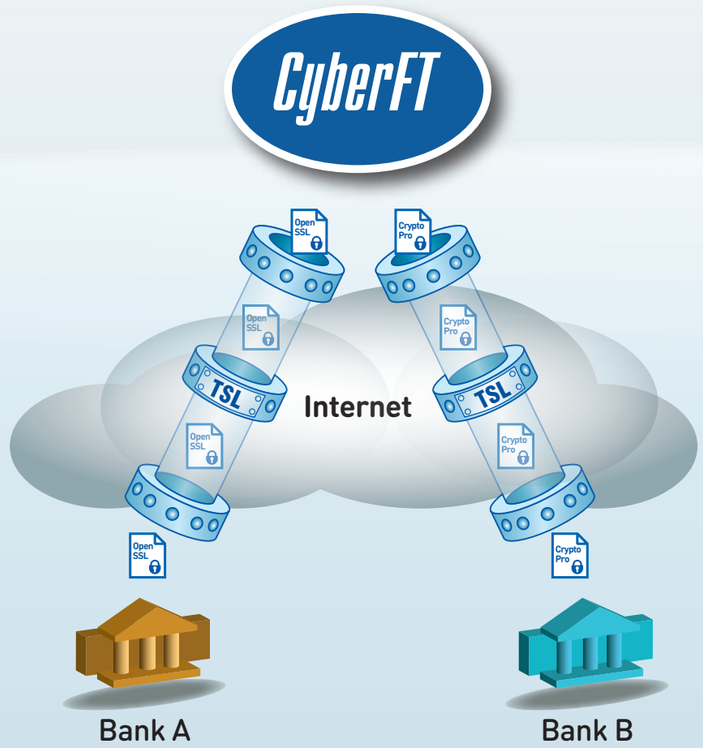


Accessibility

Connection of the customer to the CyberFT Networkr is carried out through the public Internet (i.e. there is no need to use services of a specific network provider, e.g. Orange). Thanks to the used approaches if a connection loss occurs, the internet finds a new channel and a new connection will be established within one minute.

All interaction is secure and flows through the open Internet-channels with application of our own know-how in the field of the financial message processing. In its solutions, CyberPlat uses HTTPS communications protocol as its main transport mechanism. All transmitted messages are signed digitally.

The fundamental difference between CyberFT and the traditional SWIFT system is departyre from the hardware-based encryption. For 18 years GPC Serives AG used only software-based encryption in its products.



Such a mechanism enables CyberFT Platform to connect new customers and other CyberFT counterparties without any fumbling with settings of the network equipment. In particular, such connection enables customers to connect to CyberFT using any proxy-server.

At the counterparty's end, it is not required to have additional network devices and more often than not, the counterparty is not required to change its network security policy either. Therefore, additional work of network administration services is not required. Absence of additional arrangements and engineering works provides a high-speed connection and makes it accessible to anyone.

Over 20 years of exploitation through open channels with software-based encryption more than 12 000 000 000 (twelve billion) messages were transferred without a single break-in. That is why CyberFT Network operates using any Internet channels without resorting to special devices. Application of solely software-based encryption and of any communication channels dramatically lowers the price of connection to CyberFT that is set up in parallel with SWIFT. Cyberplat doesn't charge for connection to CyberFT.

Without doubt dedicated channel can also be used. For instance, they may be used for large payments transferred between prominent customers (e.g. Citi, UniCredit, etc.).

In that respect CyberFT Platform developer recommends:

- If daily payment transaction volume does not exceed USD 1 million, then a dedicated channel is not required.
- If daily payment transaction volume is between USD 1 million and USD 20 millions a dedicated channel may be activated at counterparty's discretion.
- Dedicated channel is recommended if your daily payment transaction volume exceeds USD 20 millions or for very urgent transactions (forex, stock market transactions, etc.). In that case internet connection is reserved as a backup channel.

The system supports replaceable (plug-in) Cryptographic Information Protection Facilities (CIPF), including OpenSSL, CryptoPro, Signal-COM, PGP, etc.

Besides, Cyberplat is willing to connect any other cryptographic security mechanisms to the CyberFT Platform at request of the customer within a couple of days.

Competitiveness

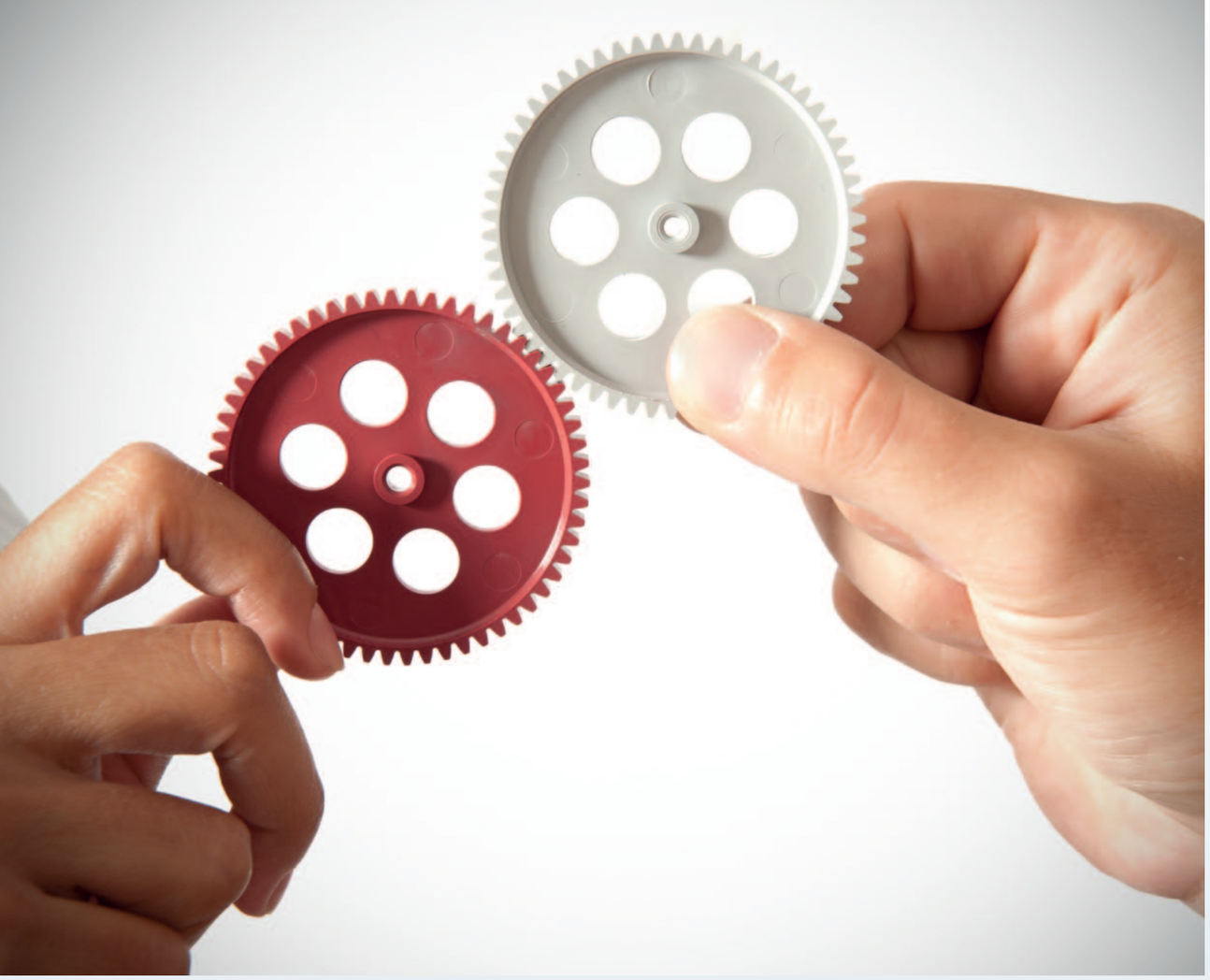
For a customer CyberFT is more efficient and cost-effective, than its foreign analogue (SWIFT). Transaction processing within CyberFT will cost the customers twice as little as compared to similar transactions within the international SWIFT system. And keep in mind that Cyberplat doesn't charge for CyberFT connection.

Also, unlike SWIFT, CyberFT doesn't charge for additional services such as archived data or assigning ID to a Participant and their inclusion to the centralized catalogue. Customer side of CyberFT can be operated by limitless number of users; that being said, there are no fees for additional automated workplaces. Module for integrating with accounting bank systems is also shipped free of charge as part of the CyberFT customer software package.

It is worth mentioning that system requirements to run CyberFT are also significantly lower than those set forth by SWIFT. Which is why working in CyberFT allows you to cut server and telecom maintenance costs, as well as maintenance personnel costs.

Universality

CyberFT network is needed not only by banks that get more secure, reliable, functional, flexible and cost-effective solution, but also for banks' customers.



Large and medium enterprises working with several banks simultaneously are forced to maintain several Electronic Banking Systems and interact with different data exchange formats and cryptographic libraries. CyberFT will allow such companies to organize a Universal Electronic Banking System. In practice that means that a company should create a financial document (or message) and choose a settlement bank whereafter the document will be sent to that bank via the uniform channel. That same channel will be used for receiving centralized feedback from the settlemnt banks (statuses of the sent documents, statements, etc.) That means the companies can have a direct interaction with banks via their accounting system and also use uniform technologies when exchanging data.

Within the scope of the flexible transport solution there is an opportunity in CyberFT to implement a legally-value electronic document workflow. Using of such an approach enables you to optimize business-processes involving document exchange with government authorities (e.g. submission of tax returns and processing of customs declaration), as well as other inter-corporate communication (signing of contracts, provision of reports, submission of stock exchange inquiries, etc).

Additionally there is a great possibility to build interbank Cash Pooling solutions on the CyberFT platform that is highly required by corporate customers.

Scalability

As of now the SWIFT Fin service is fully implemented in CyberFT including the following message categories:

- **Category 1** – Customer Payments & Cheques
- **Category 2** – Financial Institution Transfers
- **Category 3** – Treasury Markets – Foreign Exchange, Money Markets & Derivatives
- **Category 4** – Collections and Cash Letters
- **Category 5** – Securities Markets
- **Category 6** – Treasury Markets – Precious Metals
- **Category 7** – Documentary Credits & Guarantees
- **Category 8** – Travellers Cheques
- **Category 9** – Cash Management and Customer Status

CyberFT supports SWIFT InterAct services or (SWIFT MX messages in accordance with ISO 20022). CyberFT can be also used as electronic legally valid documents interchange system (e.g. for structured contracts, invoices, certificates, factoring purposes, etc.). FileAct services is also available in CyberFT that allows to Participants to send / receive any unstructured messages with attachments.

Within the scope of the offered CyberFT solution, it may be possible that a new message format will arise out of the existing message categories. For instance, if some MT103 field length is not sufficient enough, experts of Cyberplat will promptly develop a new format at request of the Platform Purchasers, e.g. MT 103E (extended) and implement the necessary field length.

CyberFT Platform may be enhanced on short notice to suit customers' needs. For instance, there is an ability to promptly develop new formats, new document forms, users' rights or to implement new cryptographic system.

Current situation in Russia

When it comes down to timely payments, current Russia's settlement system doesn't meet needs of the economy. To illustrate that, it would suffice to compare existing Russia's payment options with the foreign ones.

Market size

Unofficial sources claim that the Bank of Russia annually processes 600 million payments (made by commercial banks) worth 900 trillion rubles. Payments under 100 thousand rubles account for up to 80% of the total number of payments (400 million), which is less than 1% of the total turnover (6 trillion rubles).

Payment fee for banks

Minimal payment fee for banks is set at 7 rubles, with 12 rubles being the average payment fee. Total costs of banks related to the Bank of Russia services related to small payments make up 4,8 billion rubles and 2,8 billion rubles according to the most moderate estimates. Lowering of that figure will have a favorable effect on the costs structure of banks, and will therefore increase reliability of the banking system on the whole.

Current fee for payments made via the Bank of Russia makes up:

- from 7 to 24 rubles for a discrete-time payment processing; processing of a single payment takes from one up to several hours;
- 25 or 30 rubles for a single online Banking Electronic Speed Payment (is unavailable at night and on weekends).

Admittedly, current fees are exorbitant and could be cut several-fold, which is proven by much lower fees for similar services in neighboring countries. Let's take a look at the fees for similar services charged by the Kazakhstan Center of Interbank Settlements of the National Bank of the Republic of Kazakhstan. That said, all settlements between Kazakhstan banks are real-time settlements and are processed within minutes.

Payment processing time	*Fee amount in local currency (tenge)*	*Fee amount in rubles*
from 4 pm to 9 am	9	2,8
from 9 am to 1 pm	11	3,4
from 1 pm to 4 pm	22	6,8

Table 1. Payment fees in the Kazakhstan Center of Interbank Settlements of the National Bank of the Republic of Kazakhstan.

From that we can see that fee for the speed payment in Russia is 3.6 (!) times as expensive as the most expensive payment fee in Kazakhstan. And keep in mind that processing of any type of payment in Kazakhstan takes just a few minutes, whereas in Russia it can take as long as 9 hours.

Evidently, this is the case due to the fact that as of now Russia has no full-fledged system for online interbank settlements.

It is worth noting that building a system for processing of small electronic payments became not only necessary, but also quite doable. Technological progress makes it possible to substantially cut the payment processing fees making such payments affordable for every single market player (according to our estimates, payment fee can be as little as 1 ruble per payment). On average, banks will save 4,4 billion rubles 2,4 billion rubles according to the most conservative estimates. That said, one should bear in mind that processing of relatively small payments implies smaller risks, and, therefore doesn't require as much effort from the perspective of security and settlements control. This nuance allows us to put this type of payments into a separate category that on one hand, should be reliable, and on the other hand, should return the investments and be cost-effective for its users.

Benefits of joining CyberFT

The expected benefits of joining CyberFT will, first of all, present themselves in retail banking and SME market. Besides, CyberFT will lay the groundwork for growth of the payment amount and subsequent emergence of an all-new level of settlements.

For retail banking

Retail banking market got to the point where in order to stay competitive a bank has to ensure highest quality of services provided to its customers. For instance, loan borrowers expect that after depositing money in any way convenient for them they will no longer have to worry about its processing. Depositors prefer to work with banks where deposited funds instantly credited to the account. That said, a system meeting the modern requirements of quick money crediting with a reasonable transaction fee will immediately become in demand.

Besides, once the issue of change given to a specific end-user while making interbank settlements is resolved, Bank of Russia will encourage development of this payment system segment.

For SMEs

One of the main problems of the small business development is absence of any counterparty limits whatsoever. That said, level of trust between counterparties during purchase and sale of goods or consumer services is extremely low, even more so in distant regions of Russia. The risk of losing assets and proceeds for a small business is going through the roof, because careless behavior of counterparty can jeopardize the entire business.

For instance, a truck with grain stays on elevator until elevator gets paid for the shipped goods. And even if everything is paid in advance, before the truck arrives, discrete-time processing can take hours, and that is hours of the driver's working time; moreover, untimely grain delivery even if for a couple of hours, can have a negative impact on operation of the entire flour mill or bakery.

One of the problems of retail and small-scale wholesale trade is that it's impossible to make electronic payments during operating hours of points of sale, which would be seven days a week, 24 hours a day. Revenue from sales that builds up during the weekend can be used to pay for new small-scale wholesale shipments of necessary goods.

Without enough trust between wholesale and retail merchants the former expect goods to be paid for prior to the shipment, whereas the latter are oftentimes reluctant to pay substantial amounts prior to shipment. This issue is especially relevant during national holidays, when turnover skyrockets and operating hours of banks are short. To maintain the turnover by storing up enough goods, points of sale are forced to take bank

loans in advance. However loan is not always an option and loans are rather expensive, whereas storing up surplus is unacceptable when it comes to perishable goods.

Trust issue between retailers and individuals was resolved long ago. Payments are done in cash or through credit cards. In practice, settlements between retailers (especially small ones) and providers also tend to be done in cash with cash being delivered by undesignated persons (drivers, freight forwarders). Such state of affairs clearly stifles growth of e-payments, leads to criminal risks and off-the-book cash.

Apart from resolving many pressing tasks, CyberFT is a tool for effective handling of the mentioned problem of retailers, which will allow you to speed up your turnover and increase your retail turnover by 5-7%.

Customer-centered approach

Ability to adjust to the needs of the customers is a cornerstone of any reliable and well-oiled system. CyberFT is not limited by SWIFT functionality. For the movement of financial and commercial information there may be developed as many message categories as may be required by the customers depending on peculiarities of their businesses.

For example, if there is demand on the end of customers, Cyberplat experts may implement a world-renowned Direct Debit. It can be created as an isolated category, as an addition to the SWIFT invoice category, or as a scheduled payment service activated at request. It will all depend on needs of the platform purchasers.

At request of holding companies within the scope of CyberFT our company may develop a solution that would enable customers to optimize internal electronic document workflow, interbank Cash Pooling and a whole lot more.

CyberFT is designed to effectively tackle business tasks of any customer. Cyberplat is open for wishes and suggestions of all interested market participants and constantly maintains and upgrades CyberFT on the basis of incoming information.

Pricing

Basic participation — processing is provided by Cyberplat Company

CyberFT processing on the end of CyberPlat (banks, retailers, corporations, sole proprietors).

A customer joins CyberFT Platform set up by CyberPlat. Interaction with the Network is carried out either via CyberFT web-interface of the client, 1C, or directly via the system of the client (in case of integration between the customer's system and customer's CyberFT software). Once connected, the customer get access to the counterparty network, CyberFT members, and operates in CyberFT network as follows:

- Connection fee: free
- Operating hours: 24/7
- Transaction processing type: online
- Software: free
- Support: free
- Cost of a message: 50% of the cost of the similar SWIFT message

Stand-alone implementation

(For major banks, banks with an extensive network of correspondents, central banks, stock exchanges, and providers)

Any given organization installs CyberPlat-provided platform at its data-centre.

The provider can connect new members to the CyberFT processing on his conditions and determine parameters, such as servicing fee and fee for the transmitted messages, servicing time, supported services and formats, etc.

Complete package

This option implies that CyberPlat has no access to the information, transmitted or stored within the Provider's CyberFT Network segment.

- CyberFT hardware and software are separated into two server groups operating under GRID technology: a lump sum payment worth $10 million. Processing limit: up to 500 thousand messages a day. Messages exceeding the limit are paid for at a negotiated price.
- Software for the clients: free.
- Support fee: $200 thousand per year. In case of negotiated price the support fee is negotiated separately.
- Message cost: CyberPlat doesn't charge for messages this type of implementation.

Economy package

- Processing limit: up to 500 thousand messages a day. Messages exceeding the limit are paid for at a negotiated price.
- CyberFT hardware and software per data processing centre: a lump sum payment makes up $1 million.
- Backup data processing centre is located at CyberPlat.
- Software for the clients: free.
- Support fee: $200 thousand per year. In case of negotiated price the support fee makes up 20% of the lump sum payment.
- Message cost: 50% of the cost of the similar SWIFT message.

Main perks

Optimized costs related to financial transactions and document exchange between counterparties

Advanced high-tech platform that supports latest data exchange formats including SWIFT FIn and ISO 20022

High security standards and ensured integrity of transferred information, including information containing trade secrets

Flexibility and scalability of the system (message formats, cryptographic means, channels, etc.)

Financial transactions are in full conformity with the law

One system for different tasks (from closed banking group up to interaction on international level)

Fast and low-cost system implementation

Great possibility for banks to offer new services for their customers

- Instanteneous processing of transactions
- Extended cut-off time
- Flow of electronic legally-valid documents for bank customers
- Integration with ERP/ accounting system of a customer and building of the universal host-to-host solution.

Various connection types taking into account specifics of a particular company factoring in its wishes and security requirements

24x7 availability

Possibility for corporate customers to shift to a uniform channel for interaction with banks (host-to-host) and abandon the conventional online banking

Possibility to set up interbank cash pooling and much more!

Full independence from external political situation

High fault-tolerance

All transactions are processed online

World Trade Center, entrance 7,
12 Krasnopresnenskaya nab.,
Moscow, 123610, Russia

Tel. +7 (499) 681-11-44
E-mail: cyberft@cyberplat.com

http://cyberft.com
http://cyberplat.com