REPORT

DANMARKS NATIONALBANK

30 APRIL 2018 — NO. 4

Oversight of the financial infrastructure

- Denmark has an up-to-date and efficient payments infrastructure. The core systems and solutions extensively comply with international security and efficiency standards. The infrastructure requirements are regularly tightened.
- Danmarks Nationalbank monitors the efforts of key actors to comply with international cyber security guidelines. Not all have made the same headway in these efforts. Part of the work regarding cyber resilience takes place at sector level.
- At the recommendation of Danmarks Nationalbank, collaboration was established to identify and address risks related to interdependencies between Kronos, the VP settlement system and the retail payment systems. A final model is expected to be in place by mid-2018.

CONTENT

Room for improvement

Cyber risks

Cyber risks have been a focus area of Danmarks Nationalbank's oversight in 2017

Read more

Important infrastructure

Kr. 502 billion

Payments averaging kr. 502 billion are settled each banking day

Read more

Secure and efficient infrastructure in Denmark

Denmark is one of the most digitised countries in the world, and payments and financial transactions are widely settled by electronic means. It is important to society and to individual consumers and firms that this exchange is effected in a secure and efficient manner. The Danish payments infrastructure is described in Box 1.

By international comparison, Denmark has an up-to-date and efficient payments infrastructure. As demonstrated by Danmarks Nationalbank's oversight, the core infrastructure systems and solutions extensively comply with international standards for secure and efficient systems and solutions[1].

Instant payments can be made within seconds, and securities are settled in accordance with best practice. The performance of infrastructure systems and solutions is stable, and significant breakdowns or delays are rare. Liquidity can be distributed smoothly among the various payment and settlement systems, and generally there is ample liquidity to settle payments between banks. All the same, there is room for improvement.

Room for improvement

Danmarks Nationalbank has previously made recommendations that have not yet been fully complied with. At the same time, the world and the potential infrastructure threats are constantly changing, so what was sufficient yesterday may not necessarily be adequate tomorrow. Best practice is evolving, thereby enhancing requirements for infrastructure systems and solutions.

Danmarks Nationalbank keeps up an ongoing dialogue with those responsible for the core systems and solutions subject to oversight about the work regarding open recommendations and other areas with potential for improvement. Efforts are made on a current basis to improve the security and efficiency of the core infrastructure systems and solutions.

Danmarks Nationalbank's oversight

Danmarks Nationalbank oversees that payments and financial transactions in Denmark can be effected in a safe and efficient manner. Oversight comprises the core systems and solutions in the Danish payments infrastructure:

- Kronos (interbank payments)
- the Sumclearing, Intradagclearing and Straksclearing (retail payments)
- the VP settlement system (securities transactions)
- Dankort, Betalingsservice and credit transfers (the most important payment solutions)
- International systems of relevance to Denmark.

This report presents the conclusions of Danmarks Nationalbank's oversight of the Danish payments infrastructure in 2017.

Again in 2017, Danmarks Nationalbank's oversight had particular focus on the management of cyber risks and risks arising from interdependencies between the infrastructure systems. An important part of this work takes place at sector level, i.e. in collaboration between financial sector participants.

Focus on cyber resilience

Recent years have seen several serious cyberattacks. Two clear examples are the attacks on the Bangladeshi central bank two years ago and on Maersk last year. Accordingly, both public authorities and private actors across the financial sector have had strong focus on establishing the best possible defence against cyberattacks.

1 For a description of Danmarks Nationalbank's oversight, see Danmarks Nationalbank, *Oversight Policy,* 2015 (*link*).

The Danish payments infrastructure

Box 1

Each banking day[1], payments averaging kr. 502 billion, corresponding to almost one fourth of GDP, are settled via the Danish payments infrastructure.

The payments infrastructure is the network of systems that enables consumers, firms and public authorities to exchange payments and financial transactions.

Danmarks Nationalbank's payment system, Kronos, plays a central role in this infrastructure, both in relation to settlement of large, time-critical payments between banks (interbank payments) and by virtue of Danmarks Nationalbank's role as settlement bank for other payment and settlement systems. Interbank payments amounting to kr. 74 billion are settled in Kronos on a daily basis.

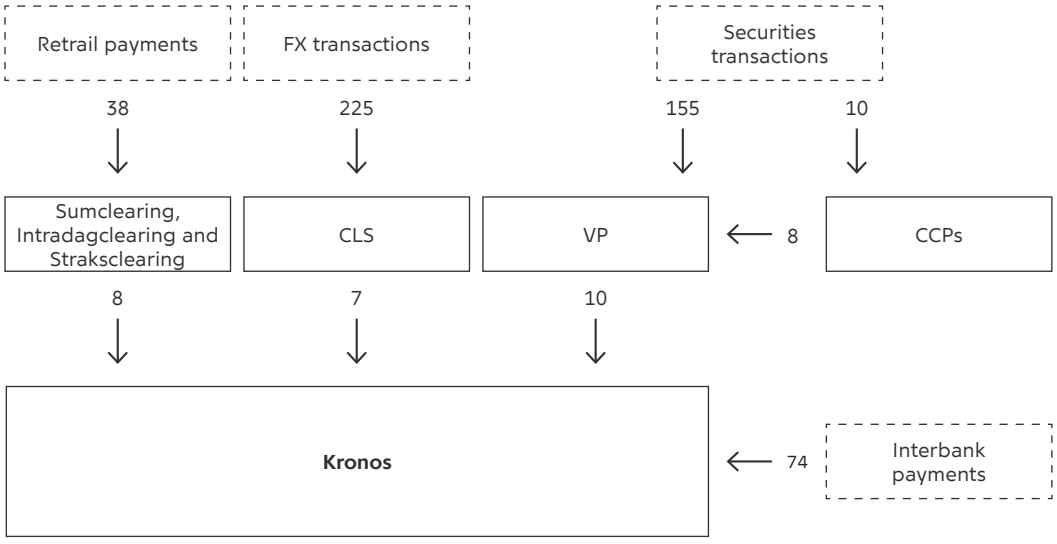
Retail payments are payments between consumers, firms and public authorities, e.g. by Dankort or as credit transfers. Depending on their type, retail payments are settled through the Sumclearing, the Intradagclearing or the Straksclearing.

Foreign exchange transactions in CLS comprise e.g. FX spot, FX forward and FX swap transactions.

Securities transactions in VP comprise trading in bonds, equities and investment fund shares. Some securities transactions, such as equities transactions, are cleared via a central counterparty, CCP. However, this applies to only a limited share of the total turnover.

The payment and settlement systems in the infrastructure, i.e. CLS, VP and the three retail payment systems (the Sumclearing, the Intradagclearing and the Straksclearing), settle their participants' net positions in Kronos. Net positions are calculated by offsetting participants' claims and obligations in the respective systems. Netting reduces the participants' liquidity requirement for settlement considerably compared with a situation in which all payments are settled individually. For instance, netting reduces the daily liquidity requirement for the settlement of retail payments from kr. 38 billion to kr. 8 billion, equivalent to a reduction of 79 per cent. In CLS and VP, netting reduces the liquidity requirement by 97 per cent and 94 per cent, respectively.

Payment flows, billion kroner, averages per banking day in 2017



1. Some types of payment can be made 24/7/365, others only during bank opening hours. However, for all payments, final settlement and exchange of amounts between banks take place on banking days, i.e. when banks are open for business.

In 2016, CPMI-IOSCO issued guidance on cyber security in payment and settlement systems.[2] The guidance specifies the more general CPMI-IOSCO principles[3] of 2012 in view of increasing cyber risk. Danmarks Nationalbank regularly monitors the efforts to comply with the guidance. Not all have made the same headway in these efforts as described in more detail in the section below on oversight of individual payment and settlement systems.

Sectoral collaboration

Cyber risk is also addressed at sector level, including the cyber resilience work of the Financial Sector forum for Operational Resilience, FSOR, cf. Box 2.

Comprehensive mapping of the most critical business activities, processes, systems and financial sector participants has been carried out under the auspices of the FSOR. On this basis, a detailed analysis of potential risks across infrastructure systems and solutions has been initiated, cf. below on the work concerning risks related to interdependencies.

The FSOR has established financial sector crisis response plans to ensure coordination across the sector in the event of e.g. an extensive cyberattack. Danmarks Nationalbank chairs FSOR and provides secretariat services. The crisis response plans were tested in both 2016 and 2017. Participation in this work serves to ensure, for the systems subject to oversight, compliance with the CPMI-IOSCO principles which recommend participation in sector tests.

Furthermore, it has been decided at sector level to establish a Danish intelligence-led red team test programme setting out common requirements for the testing process that participants must complete (*link*). The purpose of the framework is to ensure that all participants will be subject to a uniform minimum level of cyber testing requirements. A team to support the participants during the testing process will be established in Danmarks Nationalbank. Red team tests are conducted as a simulated cyberattack on systems in production, i.e. live testing.

As system owners, Danmarks Nationalbank, VP and Finance Denmark have all committed themselves to participating in the upcoming Danish red team test programme. Red team testing is an import tool to verify and strengthen cyber security and is part of the CPMI-IOSCO cyber security guidance.

Financial Sector forum for Operational Resilience Box 2

The Financial Sector forum for Operational Resilience (FSOR) was set up in 2016 with the purpose of increasing operational resilience in the Danish financial sector, including cyber resilience. Participants in the FSOR include payment and settlement systems, data processing centres, the largest Danish banks and mortgage banks, financial industry associations and authorities.
The tasks of the FSOR are to:

- ensure a shared overview of operational risks that may have an impact across the sector and could potentially pose a threat to financial stability in Denmark
- decide on and ensure implementation of joint measures to ensure financial sector resilience to major operational incidents, including cyberattacks
- create a framework for collaboration and knowledge sharing – within the sector, between different sectors and internationally.

Danmarks Nationalbank chairs the FSOR and provides secretariat services.

2 CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures (*link*) was published by the Bank for International Settlement, BIS, and International Organization of Securities Commissions, IOSCO. The Committee on Payment and Market Infrastructures, CPMI, is the BIS committee that contributed to formulating the guidance. Members of the CPMI include representatives of a large number of central banks such as the ECB, the Federal Reserve Bank and the Bank of England.

3 The Principles for financial market infrastructures (*link*) were published by BIS/IOSCO. The BIS committee, CPMI, was called the Committee on Payment and Settlement Systems, CPSS, when the principles were formulated. Accordingly, they are also referred to as the CPSS-IOSCO principles.

Finally, a joint CERT[4], Nordic Financial CERT, NFCERT, has been established at sector level. The objective is to collect, share and use information on cyberthreats and cyberattacks across the Nordic countries. NFCERT also provides expert assistance to address any cyberattacks. The CPMI-IOSCO cyber security guidance emphasises knowledge sharing as an important aspect of being cyber resilient.

Risks arising from interdependencies

Danmarks Nationalbank has previously recommended a strengthening of the collaboration to identify and address risks related to interdependencies between Kronos, the VP settlement system and the retail payment systems.

This collaboration has now been formalised as a working group with the participation of Danmarks Nationalbank, VP and Finance Denmark and with the objective of identifying and assessing risks related to interdependencies and ensuring that robust measures are in place for addressing and countering the risks identified.

Risks may arise e.g. as a result of:

- the interaction between infrastructure systems which entails that operational problems in one system may affect settlement in other systems, or that external risks, for instance a cyberattack, may spread by contagion between the systems

- the dependence on joint critical communications networks and joint use of key IT service providers.

The working group on interdependencies is developing a joint method for managing risks arising from interdependencies[5]. The joint method is to be anchored in the risk management policies of the individual participants.

Throughout 2017, the working group also mapped existing infrastructure and business processes and identified a number of risks related to interdependencies. Those risks will be assessed, and if a risk is deemed to exceed the jointly agreed risk appetite, initiatives to counter this will be launched.

Risk management and monitoring of risks related to interdependencies is an ongoing process to be jointly undertaken by VP, Finance Denmark and Danmarks Nationalbank. The final collaboration model is expected to be in place by mid-2018.

Interbank payments in kroner

Interbank payments are payments between financial institutions. Such payments are typically characterised by being time-critical and of high value, and hence they are settled in real-time gross settlement, RTGS, systems that settle payments individually and immediately.

Kronos is Danmarks Nationalbank's RTGS system for interbank payments in Danish kroner. It is also used for the settlement of monetary policy operations and net positions from connected payment and settlement systems.

Use

There are 88 direct Kronos participants, mainly Danish banks, mortgage banks and branches of foreign banks.

In 2017, approximately 5,000 interbank payments were settled via Kronos every day, corresponding to a daily value of kr. 74 billion, cf. Table 1, compared with kr. 83 billion in 2016. The value of monetary policy operations in the form of sale of certificates of deposit increased, but that is primarily attributable to the participants' deposits with Danmarks Nationalbank often exceeding their individual current account limits. Danmarks Nationalbank converts that part of the participants' deposits which exceeds their current account limits into certificates of deposit.

4 CERT stands for Computer Emergency Response Team.

5 The working group has defined interdependencies as: business processes and/or data flows across infrastructures and underlying systems, or networks shared by several parties, where operational failures may interact in such a way that one or more parties are unable to carry on their businesses without collaborating on recovery.

Payments in Kronos Table 1

Kr. billion, averages per banking day	2013	2014	2015	2016	2017
Interbank payments	**96.1**	**92.0**	**99.3**	**83.0**	**76.3**
- Of which customer payments	10.3	11.0	12.8	11.5	11.8
Monetary policy operations	**33.5**	**25.5**	**37.5**	**28.7**	**38.6**
- Of which sale of certificates of deposit	33.4	24.9	37.3	28.6	38.6
- Of which monetary policy lending	0.2	0.6	0.2	0.1	0.0
Transfers to settlement systems	**196.5**	**329.5**	**389.6**	**292.7**	**335.4**
- Of which for the Sumclearing, Intradagclearing and Straksclearing	130.1	272.2	332.3	240.0	284.7
- Of which for VP settlement	44.7	40.9	40.8	37.0	35.9
- Of which for CLS	21.8	16.5	16.5	15.7	14.8
Net positions settled	**21.7**	**25.8**	**27.6**	**25.1**	**24.7**
- Of which the Sumclearing, Intradagclearing and Straksclearing	3.1	7.0	7.6	7.6	7.8
- Of which VP settlement	11.5	12.2	12.7	10.6	10.5
- Of which CLS	7.1	6.5	7.2	6.9	6.4

Operational reliability

Kronos uptime[6] exceeded 99.9 per cent in 2017, which is satisfactory. However, one incident caused the system uptime in one month to be lower than the agreed service level. As a result of network problems, Kronos participants were unable to send and receive payments for a short period on 30 March 2017. Manual procedures were initiated to ensure that CLS settlement could be completed within the time limits set.

In 2017, Kronos was also affected by a number of minor incidents that did not have any impact on its uptime, however. It is assessed that all incidents were satisfactorily followed up.

Liquidity

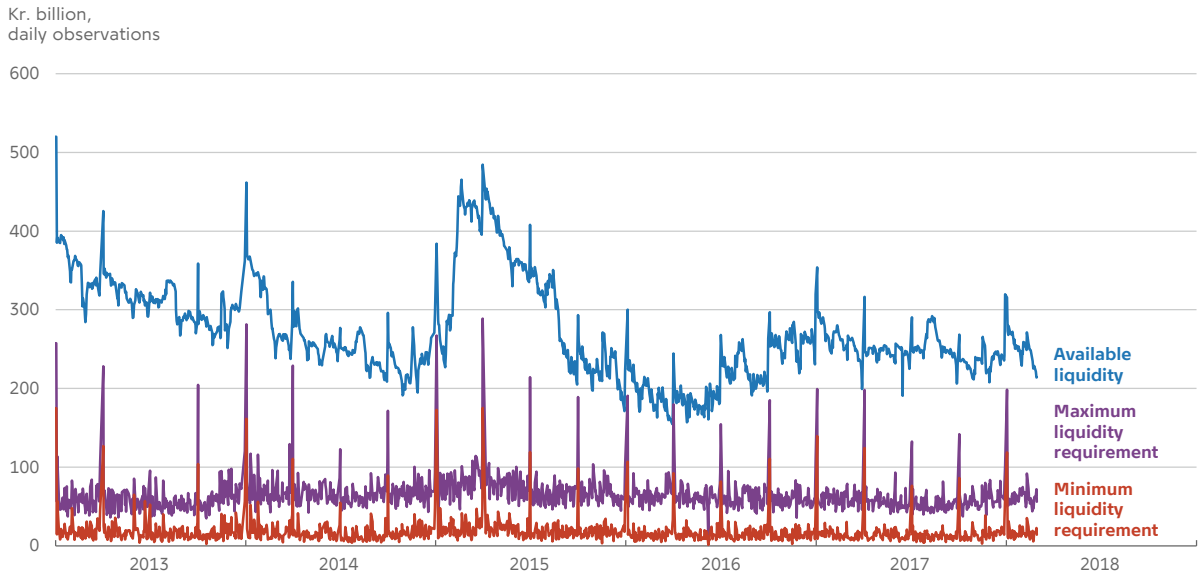
Overall, Kronos participants had ample liquidity for settlement of payments in 2017. Chart 1 shows the participants' excess liquidity cover.

Traditionally, the liquidity requirement is particularly high on days when auctions of fixed rate bullet bonds for financing adjustable rate mortgage loans are settled, i.e. typically at the start of the year and at the end of the quarterly settlement periods. The ample liquidity among Kronos participants contributed to smooth settlement of payments.

6 The uptime is the technical uptime supplied by Kronos's IT service provider. Operational disruptions caused by other circumstances are not included.

Participants' liquidity requirements in Kronos

Chart 1



Note: Available liquidity is the participants' total line plus their current account balances when Kronos opens at 7:00 am, from 24 June 2013 including amounts received in VP settlement cycle 30 at 7:05 am. The maximum liquidity requirement corresponds to the liquidity that the participants need for settlement of all that day's payments without delay. The amount depends on the sequence of the payments within the day. The minimum liquidity requirement is calculated as the liquidity that the participants need for settlement of all the day's payments after maximum netting of incoming and outgoing payments.
Source: Danmarks Nationalbank.

International standards

Kronos observes the vast majority of the requirements in the CPMI-IOSCO principles. In 2017, Danmarks Nationalbank continued its work on the four areas with potential for improvement that were identified in its assessment of Kronos in 2016. This includes the work to manage risks arising from interdependencies, cf. above, and to analyse risks arising from indirect participation, cf. below. The other areas with potential for improvement are expected to be addressed when Kronos2 goes live.

In November 2017, Danmarks Nationalbank published an analysis of indirect participation in Kronos. The majority of indirect participants are foreign banks settling payments in Danish kroner via direct participants. Indirect participation is a good solution for banks without in-depth knowledge of the Danish market or the necessary operational capacity for direct participation. In this way, settlement of kroner is left to participants who have Danish kroner as a major market and who therefore have a strong interest in ensuring that settlement is as smooth as possible.

By performing this analysis, Kronos complies with the CPMI-IOSCO requirement for identifying and managing risks associated with indirect participation.

Stress tests

Danmarks Nationalbank performs annual stress tests of liquidity in Kronos. The purpose of the stress tests is to measure the effect on the settlement of payments and the liquidity of the participants under various forms of stress. A stress scenario may include removing a major participant from the settlement of payments, or limiting the participants' intraday credit. In practice, a payments simulator is used to compare the respective stress scenarios to a benchmark scenario corresponding to the actual settlement of payments in Kronos. In 2017, the test showed that Kronos is resilient to the liquidity shocks inflicted on the system by the stress scenarios. The effect of the settlement of payments is limited and can be mitigated by means of Kronos' contingency procedures to settle critical payments. By performing annual stress tests, Danmarks Nationalbank complies with the CPMI-IOSCO requirement for stress testing liquidity in the system.

Cyber resilience
In 2017, Danmarks Nationalbank prepared a cyber security strategy to strengthen the cyber resilience of its critical business activities, including Kronos and the forthcoming Kronos2, cf. below.

Kronos2 will strengthen cyber resilience, as the system is implemented on a new IT operating platform designed to meet high security requirements and capable of continuous adjustment to comply with relevant requirements.

Kronos'/Kronos2's compliance with the CPMI-IOSCO cyber guidance has been mapped, and the security of the forthcoming Kronos2 is being reviewed by external experts. Danmarks Nationalbank is continuously working to address any deficiencies identified.

System updates – New system underway
Danmarks Nationalbank is replacing Kronos with Kronos2. The new system consists of an RTGS module for handling critical payments and transfers for settlement of retail payments, securities transactions, etc., a module for handling monetary policy operations and a module for collateral management. The Perago system is used for payments and monetary policy operations and is also used by Sveriges Riksbank and Norges Bank, among others, while the Calypso system is used for collateral management.

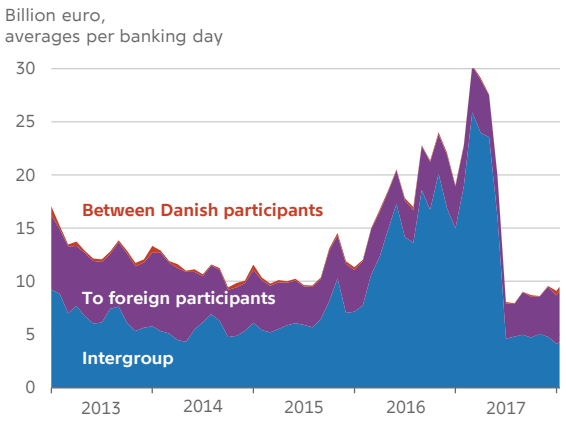
In December 2017, Danmarks Nationalbank decided to postpone the implementation of Kronos2. The IT platform did not yet have the desired stability which is essential due to the central role of Kronos in Danish payment services. Moreover, Danmarks Nationalbank found the system management processes to be insufficiently resilient. The date for implementation of Kronos2 is 20 August this year.

Interbank payments in euro

Denmark is connected to Target2, the trans-European RTGS system for settlement of interbank payments in euro. Payments between financial institutions and transfers for settlement in other euro payment and settlement systems are settled in Target2.

Use
There are 28 Danish participants in Target2. In 2017, Danish participants' daily interbank payments averaged 16.7 billion euro. Exchange of euro mostly takes place with participants in Germany, Finland, France and the Netherlands.

Interbank payments in Target2 Chart 2



Note: The chart shows payments submitted by Danish participants via Target2. Daily averages have been calculated on a monthly basis.
Source: Danmarks Nationalbank.

Danish participants use Target2 mainly for intergroup payments and payments to non-resident participants. According to Chart 2, there has been a decline in intergroup payments in the second half of 2017. This can be attributed to a change in market participants' liquidity management practice.

Operational reliability
The operational reliability of the local Target2 components for which Danmarks Nationalbank is responsible was satisfactory in 2017. There were only a few minor incidents in 2017.

System updates
The European Central Bank, ECB, has been working towards modernising the European payments infrastructure in recent years. The ECB is developing an instant payment system in Target2 called Target Instant Payment Settlement or TIPS. This will allow Danish banks to clear and settle instant payments in euro. TIPS will support multi-currency, meaning that at a later stage it will also be possible to clear and settle instant payments in other currencies than euro through the system. TIPS in euro is expected to be launched in November 2018.

On 6 December 2017, the ECB's Governing Council approved the migration of Target2 to the upgraded T2S platform[7], which will increase security and reduce operational costs. The consolidated platform offers new RTGS services, including improved liquidity management procedures and a multi-currency service. The Target2-T2S platform is expected to be operational from November 2021.

The Governing Council also approved the establishment of a joint system called the Eurosystem Collateral Management System, ECMS, for collateral management in euro, which will replace the existing systems of 19 national central banks. The new system is expected to be launched in November 2022.

Retail payments

Payments between consumers and firms can be made using banknotes and coins or various electronic payment solutions, for instance Dankort for payments in supermarkets, Betalingsservice (direct debit) for paying rent or credit transfers via online banking or MobilePay. On average, daily retail payments totalled kr. 26.4 billion in 2017.

Danmarks Nationalbank oversees the most important payment solutions in Denmark, cf. Box 3.

Operational reliability
The operational reliability of Nets' systems concerning Dankort and Betalingsservice was overall satisfactory in 2017. However, two major incidents occurred in the 3rd quarter, affecting the availability of the card system whereby 250,000 and 1.2 million Dankort transactions, respectively, were rejected. In Danmarks Nationalbank's assessment, Nets followed up the incidents in a satisfactory manner.

In case of extended downtime, retailers may run the payment terminals in offline mode and thus continue to receive Dankort payments. Nets is currently reviewing how utilisation of this solution can be improved – possibly by automatically switching to offline mode in e.g. supermarkets.

No incidents affected the operation of Betalingsservice in 2017.

The incidence of Dankort fraud is low
Overall, the incidence of Dankort fraud is low. In absolute figures, Dankort fraud amounted to kr. 104 million[8] in 2017, or 0.23 per thousand of total turnover.[9]

Danmarks Nationalbank's oversight of payment solutions Box 3

Danmarks Nationalbank oversees Dankort, Betalingsservice and credit transfers.

Oversight of Dankort and Betalingsservice is aimed at Nets, the owner of these solutions.

Oversight of credit transfers is part of the oversight of the retail payment systems (the Sumclearing, Intradagclearing and Straksclearing), cf. the section "Clearing and settlement of retail payments".

Danmarks Nationalbank regularly monitors developments in the various other payment solutions to assess whether targeted oversight of them is required.

MobilePay is increasingly used for shopping in stores, online shopping, payment of recurring invoices and transfers between users. However, the average daily turnover for MobilePay of kr. 0.2 billion[1] is still limited compared to the payment solutions subject to oversight, e.g. Dankort, accounting for kr. 1.2 billion per day.

Moreover, the most system-critical parts of MobilePay are covered by Danmarks Nationalbank's oversight of the retail payment systems and Dankort, as MobilePay uses credit transfers and for instance Dankort to execute payments.

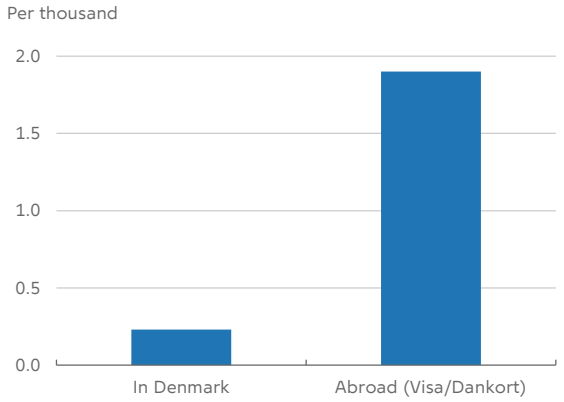
1. www.mobilepay.dk *(link)*.

7 The IT platform that supports the trans-European securities settlement system, Target2-Securities, T2S.

8 Danmarks Nationalbank's StatBank, Payments: (*link)* (*DNBSMIS, Type 1.1, Cat. 1, Denmark, Value, 2017 Q1-4*).

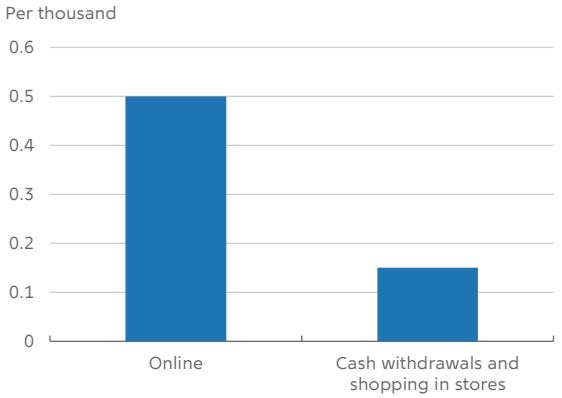
9 Danmarks Nationalbank's StatBank (*Payments*):(*link)* (*DNBSMIS, Type 1.1, Cat. 1, Denmark, Share of total value of transactions, 2017 Q1-4*).

Total Dankort fraud, 2017 Chart 3



Source: Danmarks Nationalbank.

Dankort fraud online versus cash withdrawals and shopping in stores, 2017 Chart 4



Source: Nets.

The incidence of Dankort fraud is also low relative to fraud in connection with Danish cards abroad.[10] Visa/Dankort fraud abroad amounted to 1.9 per thousand in 2017[11], cf. Chart 3.

Fraudulent use of Dankort cards to withdraw cash and shop in stores

Fraudulent use of stolen or lost Dankort cards to withdraw cash and shop in stores amounted to 0.15 per thousand in 2017,[12] cf. Chart 4.

Danmarks Nationalbank has asked Nets to review the possibility of strengthening the oversight of illegal cash withdrawals. Against that background, Nets developed a technical solution that is capable of including all cash withdrawals in the oversight. Nets has entered into a dialogue with the issuers about this possibility, and the matter will also be discussed at the meeting of the Danish Payments Council on 9 May 2018.

Fraudulent use of Dankort cards to shop online

Fraudulent use of Dankort cards to shop online was three times higher in 2017 than fraud in connection with cash withdrawals and shopping in stores, cf. Chart 4.

Fraudulent use of Dankort cards to shop online declined in 2017 and is now more or less on the same level as in the 1st half of 2015, cf. Chart 5.

In Nets' assessment, the decline is the result of the measures implemented by Nets in early 2017 to strengthen Dankort security, i.e. Fraud Prevention and Dankort Secured by Nets.[13]

International standards

In May 2017, Danmarks Nationalbank published a Dankort assessment in accordance with the ECB's standards for card payment schemes.[14] The main conclusion was that Dankort's performance is stable

10 See Danmarks Nationalbank, Fraud using Danes' payment cards occur above all in e-commerce, *Danmarks Nationalbank Statistics (Payments, 2nd quarter of 2017*), 12 December 2017 (*link*).

11 Danmarks Nationalbank's StatBank – (*Payments*) (*link*) (*DNBSMIS, Type 1.1, Cat. 1, Foreign countries, Share of total value of transactions, 2017 Q1-4*).

12 Nets' statistik for misbrug af Dankort (Nets' statistics on Dankort fraud – in Danish only) (*link*).

13 *Fraud Prevention* is a system that uses pattern recognition to reject transactions so unusual that they must be assumed to be made by someone other than the card owner. *Dankort Secured by Nets* is a solution based on strong authentication whereby the user must enter not only Dankort details but also a code received by text from Nets before finalising the purchase. This method, which is also used for purchases involving international cards, is used if the amount exceeds kr. 450.

14 Cf. Danmarks Nationalbank, Dankort Assessment, *Danmarks Nationalbank Report,* No. 4, May 2017 (*link*).

with a high degree of availability and a low level of fraud. The assessment also contained a number of recommendations for Nets.

Danmarks Nationalbank's recommendations included, inter alia, an expansion of the Dankort risk assessment by Nets, more systematic knowledge management in relation to Dankort and a strengthening of the framework for decisions and communication regarding Dankort.

Nets has subsequently been working to comply with Danmarks Nationalbank's recommendations. In the 1st quarter of 2018, Nets achieved its aim in terms of most of the recommendations:

- Nets has conducted an in-depth risk assessment of Dankort, comprising several types of risk as opposed to previously, when the focus was on the IT platform. It has also established a process for annual risk assessment updates.

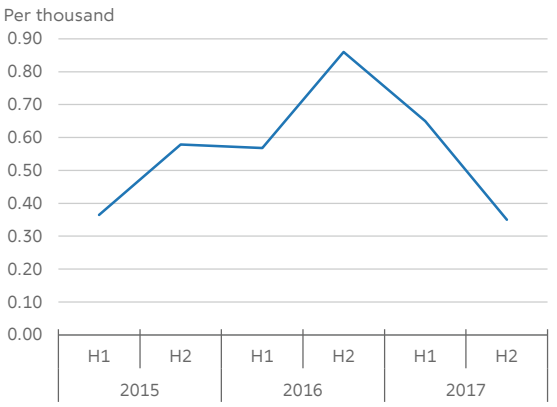
- Nets' outsourcing management has been strengthened. Nets' security requirements are transferred to external suppliers and more systematically followed up, e.g. by regular meetings and annual risk assessments of outsourced activities. A Vendor Management Board has been established to ensure information sharing and coordinated follow-up on Nets' external suppliers.

- In general, Nets has established a better organisational and operational Dankort-related overview.

Nets is still working on Danmarks Nationalbank's recommendation to strengthen the framework for Dankort-related decision-making processes and communication.

Danmarks Nationalbank recently initiated an assessment of Betalingsservice in accordance with the ECB's standards for direct debit systems.

Dankort fraud in connection with online shopping Chart 5



Source: Nets.

Regulation

A new Danish Payments Act came into force on 1 January 2018. The Act implements the new EU Payment Services Directive, PSD2.[15] This legislation has considerably changed the framework conditions for payments in Denmark and the rest of the EU.

Among other things, PSD2 has introduced a right for users with a payment account to use that account by means of a third party service provider without an agreement having been made between the user's bank and the third party service provider.[16] PSD2 thus allows new service providers to offer users the option of paying for instance invoices from their accounts without direct contact with their banks – i.e. without having to use Dankort or online banking.[17]

PSD2 ensures that almost all payment service providers will be subject to supervision, and that all online payments – apart from certain limited cases – must be approved by the user via strong (two-factor) au-

15 The Danish Payments Act also adjusts a number of special Danish rules, including the cash obligation.

16 The more detailed requirements regarding third parties' access to initiating a payment from the users' payment accounts will not enter into force until September 2019, however.

17 The emergence of services from new service providers allowing users to bypass the banks when using their bank accounts is often referred to as open banking.

thentication requiring the user to prove its identity in two different ways to reduce the risk of fraud.[18]

The purpose of the new rules is to increase market competition and improve security in connection with payments.

Clearing and settlement of retail payments

The Sumclearing, Intradagclearing and Straksclearing are the financial sector's systems for clearing and settlement of Danish retail payments. The systems are owned by Finance Denmark, managed by e-nettet, which is the financial sector's project and management company, and provided by Nets.

The Sumclearing is used for settlement of all card payments, Betalingsservice and Nets' other payment products. Settlement in the Sumclearing is carried out once a day on banking days. The Intradagclearing is used for settlement of credit transfers such as online banking transfers, payroll transactions and public-sector payments. Settlement is carried out at five fixed times a day on banking days. The Sumclearing and Intradagclearing are both net settlement systems.

The Straksclearing is a real-time settlement system where credit transfers of up to kr. 500,000 are made within seconds on a 24/7 basis. This is possible because the banks have prefunded the transfers. The Straksclearing is primarily used for online banking transfers and payments via MobilePay.

Use

There are 52 direct participants in the retail payment systems and 31 indirect participants, who settle via direct participants. The total transaction volume in the retail payment systems averaged kr. 38.4 billion per banking day in 2017, representing an increase by 5.5 per cent on 2016, cf. Table 2.

The number of transactions in the Straksclearing has continued to rise, cf. Chart 6. The increase is mainly attributable to MobilePay payments being settled in the Straksclearing. Statistics show that more than 3.7 million Danes use MobilePay.[19]

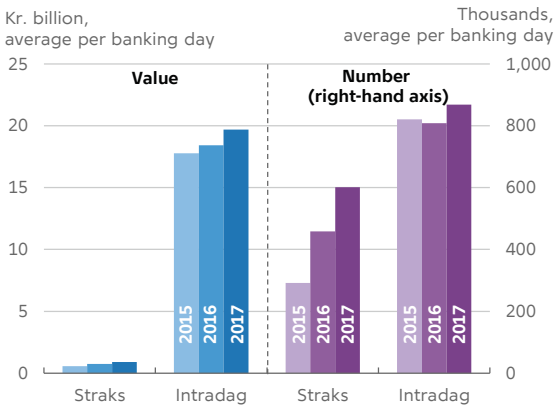
Although there has been an increase in the number of instant payments, the Straksclearing only accounts for a small share of total retail payments in terms of value, cf. Table 2.

Payments in the Sumclearing, Intradagclearing and Straksclearing Table 2

Kr. billion, averages per banking day	2013	2014	2015	2016	2017
Sumclearing	29.1	17.9	16.7	17.2	17.8
Intradagclearing	13.8	17.0	17.8	18.4	19.7
Straksclearing	-	0.5	0.6	0.8	0.9
Total	42.9	35.4	35.0	36.4	38.4

Source: Nets.

Payments in the Intradagclearing and Straksclearing, 2015-17 Chart 6



Source: Nets.

18 The more detailed requirements regarding strong customer authentication and the related exceptions will not enter into force until September 2019, however.

19 www.mobilepay.dk (*link*).

Operational reliability
Retail payment system operations were in general satisfactory in 2017. A major incident occurred on 26 April when an underground main cable was cut in two. The cable damage affected the central network of the sector and meant that, for more than eight hours, no transactions could be submitted for clearing, and that the normal settlement activities between Nets and Danmarks Nationalbank were not carried out as planned. The reason for the more than eight hour delay in restoring network traffic was an unclear network governance structure. In view of the incident, it was decided to implement a new network, cf. below on system updates.

Liquidity
Participants reserve liquidity in accounts at Danmarks Nationalbank for settlement of their net positions. If a participant does not reserve sufficient liquidity, its settlement is postponed, and new net positions are calculated for the other participants who risk not receiving the expected liquidity for settlement. There were no incidents of participants having their settlement postponed in 2017. One reason is that all participants use at least one of the automated liquidity management tools.

International standards
Danmarks Nationalbank is finalising an assessment of the retail payment systems' observance of the CPMI-IOSCO principles. The assessment will be published in mid-2018.

Danmarks Nationalbank previously recommended that Finance Denmark perform an analysis of the retail payment systems' observance of the CPMI-IOSCO cyber guidance. Finance Denmark will initiate this analysis when the above assessment has been completed.

System updates
The financial sector is establishing a whole new network for clearing and settlement of retail payments to replace the old network. The network is called e-connect, and TDC has been chosen as supplier. The project is handled by e-nettet to ensure supplier management on behalf of the sector. e-nettet is also in charge of overall governance for the participants in the new network. The network is expected to be implemented in the course of 2018.

The opening hours of Kronos will be extended when the Danish krone joins T2S, which will enable later settlement in the retail payment systems. In that connection, it was previously decided to move the last settlements in the Intradagclearing and Straksclearing to take place later in the day. This means that a larger share of transactions will be settled within the same day.

A group of larger Swedish, Danish, Norwegian and Finnish banks are currently exploring the possibilities to establish a pan-Nordic payment infrastructure for all the Nordic banks. The vision is to create the first area in the world, where domestic and cross-border payments in multiple currencies (SEK, DKK, NOK and EUR) can be made fast and easy.

Securities settlement

VP settlement is the Danish securities settlement system. VP Securities A/S, VP, also undertakes registration of ownership of securities and handling of periodic payments, issues, redemptions, etc.

Use
The VP settlement system has 145 participants, of which 60 are non-resident market participants. Securities transactions totalling an average of kr. 162.7 billion per banking day were settled in 2017, cf. Table 3, a fall of 7.5 per cent relative to 2016. The decline was strongest for bonds, while the value of investment fund shares settled continued its upward trend from the previous years.

Operational reliability
VP system uptime[20] was 100 per cent in 2017. In a few cases, delays in Target2-Securities, the trans-European securities settlement system, delayed night-time settlement in VP's systems, but did not affect the availability of VP.

20 The uptime is the technical uptime supplied by VP's IT service provider.

Equities, investment fund shares and bonds settled in VP Table 3

Year, daily averages	Total		Bonds		Equities		Investment fund shares	
	Number of trades, thousands	Value, kr. billion	Number of trades, thousands	Value, kr. billion	Number of trades, thousands	Value, kr. billion	Number of trades, thousands	Value, kr. billion
2013	51.5	172.0	3.3	146.1	25.7	21.3	22.5	4.6
2014	61.1	178.2	3.1	144.4	32.3	28.2	25.6	5.6
2015	67.1	206.2	3.4	158.5	33.4	41.4	30.2	6.3
2016	63.6	175.9	2.8	131.8	30.9	37.6	29.9	6.6
2017	66.9	162.7	2.7	118.4	32.4	36.6	31.8	7.7

Note: Values have been calculated on the basis of the securities leg of a trade, i.e. the market value of the securities transferred from the seller to the buyer.
Source: VP Securities A/S.

VP and Danmarks Nationalbank regularly monitor incidents in VP to be able to assess operational risks. Overall, the operational reliability of the VP settlement system is assessed to have been satisfactory in 2017. VP has followed up any incidents in a timely manner, and their consequences have been limited.

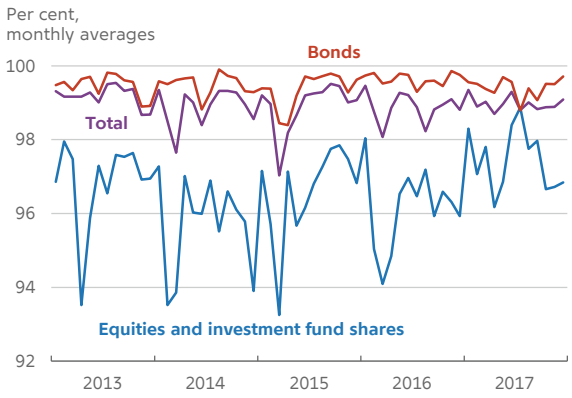
Settlement ratio

According to best practice, securities transactions must be settled two days after the transaction date. The settlement ratio indicates the percentage, in value terms, of the transactions settled in a timely manner. In 2017, the overall settlement ratio in VP was 99.0 per cent, which was a little higher than in the previous year, cf. Chart 7. Sanctions, including fines of up to kr. 100,000, will be imposed on VP settlement participants if their settlement ratios remain too low for a prolonged period of time. In 2017, two fines were issued to participants with too low settlement ratio.

Liquidity

VP participants reserve liquidity in accounts at Danmarks Nationalbank for VP's net settlement cycles. If VP's checks for adequate cover show that a buyer does not have sufficient liquidity, the reported purchases will, as a main rule, be postponed until the subsequent settlement cycle. Participants who have overdrawn their liquidity lines may be fined.

Settlement ratios in VP Chart 7



Note: In the chart, the settlement ratios are stated on the basis of settlement values. For equities and investment fund shares, the settlement ratio has been calculated as a weighted average of the two types of securities, while the total is a weighted average for all types of securities.
Source: VP Securities A/S.

The size of the fine depends on how many times the participant has overdrawn its liquidity line within the last six months.

In 2017, there were a total of 71 overdrafts in VP, and 29 fines were issued, cf. Chart 8. This was a lower number of overdrafts than in 2016 and the number of fines was reduced by half. The development in the number of overdrafts is being monitored to assess the efficiency of the sanctioning system.

New regulations and legislation

The Central Securities Depositories Regulation, CSDR, was implemented in Danish law with effect from 2015. The purpose of the CSDR is to ensure consistent regulation of central securities depositories in the EU with a view to increasing international competition. In future, firms must apply for a licence to act as central securities depositories.

VP applied for a licence under the CSDR in May 2017. Danmarks Nationalbank and the ECB participated in the assessment of VP's application as relevant authorities, i.e. authorities with right of consultation. The ECB is a relevant authority for VP, because more than 1 per cent of VP's total settlement is in euro.

VP was given its CSDR licence with effect from 3 January 2018 as one of the first central securities depositories in the EU. In future, VP must report to the Danish Financial Supervisory Authority, Danmarks Nationalbank and the ECB according to the CSDR. At the turn of the year 2017/18, the existing Danish Securities Trading Act was repealed and replaced by the Capital Markets Act. One of the reasons for this change was to ensure greater coherence with the CSDR as VP is to function in accordance with the new legal basis.

International standards

The rules of the CSDR are aligned with the CPMI-IOSCO principles, which form the basis for Danmarks Nationalbank's oversight of the financial infrastructure.

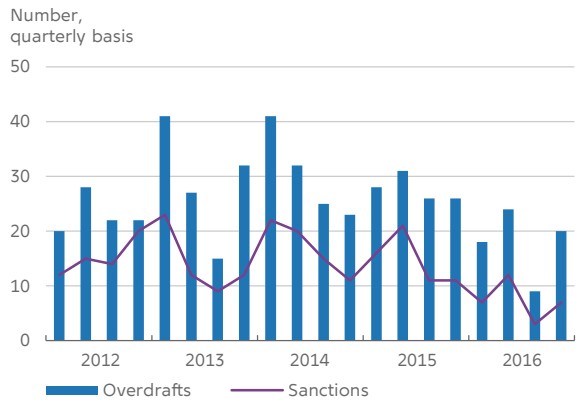
VP complies with the vast majority of the requirements in the CPMI-IOSCO principles. That was the conclusion in the assessment published by Danmarks Nationalbank and the Danish Financial Supervisory Authority in 2016.[21]

In the assessment, four recommendations were given to VP – including to ensure the independence of the Board. In connection with its review of VP's CSDR application, the Danish Financial Supervisory Authority's assessed that the independence of VP's Board was sufficiently ensured.

VP collaborates with Finance Denmark and Danmarks Nationalbank on management of the risks related to interdependencies. Once this collaboration has been formalised, VP will be assessed to comply with the CPMI-IOSCO principle for managing risks related to interdependencies.

VP has also presented its plan to observe the CPMI-IOSCO principle for the handling of a participant's operational failure, resolution or default. Based on the documentation available, Danmarks Nationalbank assesses that VP is observing the principle.

Overdrafts and sanctions in VP settlement Chart 8



Anm.: A participant is fined only if the overdraft is the participant's own fault. In other words, no fine is imposed if the overdraft is due to non-payment by another participant who has reserved insufficient liquidity for settlement.
Source: VP Securities A/S.

21 Cf. Danmarks Nationalbank and the Danish Financial Supervisory Authority, Assessment of VP Securities, February 2016 (*link*).

Finally, Danmarks Nationalbank made a recommendation regarding management of business risks. According to the recommendation, VP must ensure closer links between its risk management, recovery plan and resolution plan. This recommendation was also issued in connection with the review of the CSDR application.

Danmarks Nationalbank regularly assesses the measures implemented by VP in order to comply with the requirements of the CPMI-IOSCO principles.

Cyber resilience
In the autumn of 2017, VP participated in the ECB's questionnaire survey concerning VP's cyber security response plans. Its responses show that VP strengthened its cyberattack response plans in 2016 and 2017.

In 2018, VP will conduct a red team test as a simulated cyberattack on systems in production, but without damaging those systems or the operation of VP. Initial test results confirm that VP has a strong cyber defence.

System updates
In an effort to strengthen its Nordic position, VP concluded an agreement with Sveriges Riksbank for settlement of securities transactions, etc. in Swedish kronor in VP. The solution was implemented in March 2017. VP will also establish a link to Euroclear Sweden, the central Swedish securities depository, in the course of 2018 to allow securities transactions in Swedish kronor via VP.

Target2-Securities
T2S is a trans-European securities settlement system owned by the ECB. The purpose of T2S is for cross-border securities transactions to be handled as safely, inexpensively and efficiently as domestic transactions.

A total of 20 central securities depositories from 18 countries now settle via T2S, including VP. Settlement in euro, accounting for just over 1 per cent of total settlement, mainly takes place on T2S.[22] So far, the euro is the only T2S settlement currency, but from October 2018, settlement in Danish kroner via the system is possible.

13 Danish banks are direct participants in T2S and thus currently hold T2S settlement accounts at Danmarks Nationalbank. Three of those banks have established accounts in euro with central banks in the euro area in order to have direct access to euro. The other banks have concluded agreements with correspondent banks.

CCP clearing
In Denmark, equities and repo transactions are settled via a central counterparty, CCP, cf. Box 4.

The three CCPs, EuroCCP, LCH Clearnet and Six X-clear, clear equities transactions, while Nasdaq Clearing clears repo transactions. After CCP clearing, transactions are settled in VP.

Ongoing supervision to ensure that CCPs comply with the regulatory requirements is conducted by the national supervisory authorities in collaboration with supervisory colleges, comprising supervisory authorities and central banks from the most important countries in which the CCP is operating. Danmarks Nationalbank monitors developments, via its participation in e.g. the EuroCCP supervisory college.

What is a CCP? Box 4

A CCP intermediates between the parties to a transaction, assuming the risk for both the buyer and the seller from the transaction date until the transaction has been finally settled. So if either of the parties to the transaction defaults within this period, the CCP still has an obligation to the other party. However, this also means that risks are concentrated in the CCP, and therefore the CCP is subject to a number of regulatory requirements[1] to ensure the completion of the transaction.

1. Cf. Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (*link*).

22 It will still be possible to settle in euro in VP's own systems in cycle 50 at 2:15 pm.

Settlement of foreign exchange transactions

A foreign exchange transaction consists of two opposite payments in two different currencies.[23] Traditionally, foreign exchange transactions are settled as two independent payments, often executed via correspondent banks in the currencies in question. If the two payments are not settled simultaneously, the parties incur settlement risk. The international foreign exchange settlement system, CLS, mitigates settlement risk by simultaneous settlement of the two payments (payment-versus-payment, PvP).

CLS is owned by large, international banks and settles transactions in 18 participating currencies, including Danish kroner.

Danmarks Nationalbank participates in the cooperative oversight of CLS, cf. Box 5.

Use

More than 80 per cent of all foreign exchange transactions in Danish kroner are settled via CLS.[24] Both financial institutions and firms participate in the CLS settlement of Danish kroner. If a company does not settle directly in CLS itself, FX trades can be settled via one of the four settlement members with direct access to the CLS settlement in Danish krone.

In 2017, the value of CLS transactions remained stable, cf. Chart 9. The average daily value of CLS transactions was kr. 225 billion in 2017. The value of trades is particularly large around quarter change and on days around foreign holidays. CLS settlement set a new record in Danish kroner on the first banking day of 2nd quarter 2017, 3 April, reaching kr. 612 billion.

Operational reliability and liquidity

Pay-ins to CLS take place via the national RTGS systems; in the case of Danish kroner via Kronos.

Hence the operational reliability of CLS depends on the stability of the RTGS systems. In 2017 one Kronos

23 For example, trading kroner against euro entails a payment in kroner by one party to the other and an opposite payment in euro.

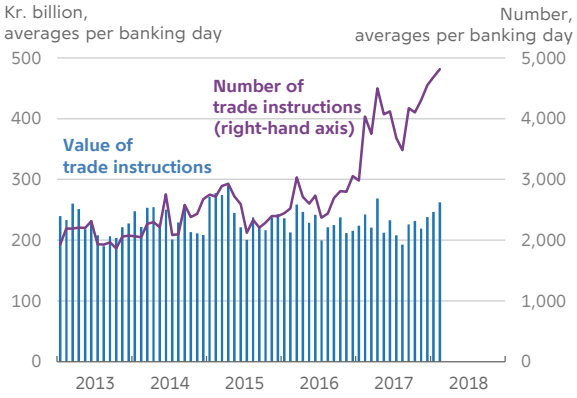
24 BIS, *Triennial Central Bank Survey, Foreign exchange turnover in April 2016* (*link*) and CLS Bank.

Oversight of CLS Box 5

Oversight of CLS is based on the CPMI-IOSCO principles for financial market infrastructures (PFMI). Every second year CLS publishes an updated disclosure of the system's observance of the PFMI.[1] Oversight of CLS is carried out by a joint CLS Oversight Committee, which is a forum for cooperation between the central banks of the participating currencies[2], whereby they can carry out their national oversight responsibilities. Danmarks Nationalbank participates in this work, which is organised by the Federal Reserve, Fed. The Fed is also the supervisory authority for CLS. Danmarks Nationalbank's oversight is focused on matters of importance to the settlement of transactions in Danish kroner.

1. CLS, Principles for Financial Market Infrastructures Disclosure, 2016 (*link*).
2. Federal Reserve System, Protocol for the Cooperative Oversight Arrangement of CLS (*link*).

Trade instructions in CLS Chart 9



Note: Daily averages calculated on a monthly basis. On 23 January 2017, CLS changed the threshold amount for which a trade is split into several instructions. This has led to a higher number of instructions per day.
Source: CLS Bank.

incident affected CLS settlement. On 30 March 2017 settlement in Kronos was affected by network issues resulting in CLS not receiving payments. Manual procedures were launched to ensure CLS settlement within key business deadlines.

The Danish participants reserve sufficient liquidity for CLS settlement.

System updates

CLS continues to work towards the launch of CLSNet[25], a standardised, automated bilateral payment netting service intended for FX transactions settled outside the CLS settlement service. Participants will be able to submit FX instructions for trades in more than 125 currencies. The service will be launched on a distributed ledger technology (DLT) based platform. CLSNet can be accessed either directly via DLT or indirectly via SWIFT channels.

Furthermore CLS plans to launch a separate settlement service for cleared FX products. The first CCPs to join the new service are expected to be Eurex Clearing and LCH Clearnet.

Another new initiative underway is CLSNow[26] which will allow participants to mitigate settlement risk associated with same day FX transactions, including the out legs of CLS in-out swap transactions[27]. CLSNow will provide simultaneous settlement of both legs (PvP) on a gross basis. The service will be open for all CLS eligible currencies in the future[28].

25 CLS, CLSNet (*link*).

26 CLS, CLSNow (*link*).

27 In CLS in/out swaps reduce large positions to minimise liquidity risk in settlement.

28 At go-live, only CAD, CHF, EUR, GBP, and USD will be included.

DANMARKS NATIONALBANK
HAVNEGADE 5
DK-1093 COPENHAGEN K
WWW.NATIONALBANKEN.DK

This edition closed for contributions on 16 April 2018

DANMARKS NATIONALBANK