REPORT

DANMARKS NATIONALBANK

3 JUNE 2019 — NO. 3

Oversight of the financial infrastructure

- Denmark has a modern and well-functioning payments infrastructure. Kronos2 and the migration of Danish kroner to the trans-European securities platform, T2S, have contributed substantially to an up to date infrastructure.
- Danmarks Nationalbank is in dialogue with the owners of the financial infrastructure about their work on cyber security. Cyber security has high priority. Systematic effort is made to manage risks, although the level of maturity varies.
- At Danmarks Nationalbank recommendation, collaboration and a joint method for managing risks related to interdependencies between Kronos2, the VP settlement system and the retail payment systems is established. This is an important step to ensure a robust Danish payments infrastructure.

Not same level of maturity

Cyber security

was a focus area of Danmarks Nationalbank's oversight in 2018

Read more

Important infrastructure

Kr. 536 billion

Payments averaging kr. 536 billion are settled each banking day

Read more

CONTENT

Danmarks Nationalbank's oversight has focused on cyber resilience

Millions of payments are settled in Denmark every day. This is done via a network of systems that enables consumers, firms, financial institutions and public authorities to exchange payments and other financial transactions. The Danish payments infrastructure is described in Box 1.

Denmark has a modern and well-functioning payments infrastructure. In August 2018, Danmarks Nationalbank replaced Kronos by Kronos2, a newer and more robust system for interbank payments. In October, securities settlement in kroner was connected to TARGET2-Securities (T2S), the trans-European securities clearing and settlement platform.

As part of its oversight, Danmarks Nationalbank has monitored the work to migrate Danish kroner to T2S. This process and the problems that arose during the migration weekend and afterwards are described in the report's section on oversight of securities settlement.

The core payment and settlement systems and the most important payment solutions extensively observe the international standards for safe, stable and efficient systems and solutions. That is the conclusion of Danmarks Nationalbank's oversight.

However, the requirements for the infrastructure systems and solutions are regularly tightened to reflect changes in technology and the threat scenario. Especially the threat of cyberattacks makes new demands on the robustness of the payments infrastructure. Consequently, Danmarks Nationalbank's oversight in 2018 continued to have particular focus countering cyber risks in the 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. Its oversight comprises the core systems and solutions in the Danish payments infrastructure.

- Kronos2 (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.

Danmarks Nationalbank's oversight is described in its oversight policy (*link*).

This report presents the main conclusions of the oversight of the Danish payments infrastructure in 2018.

Cyber resilience efforts

In view of the increasing cyber threat, CPMI-IOSCO in 2016 published guidance for addressing cyber risks in payment and settlement systems.[1] The guidance elaborates on the more general CPMI-IOSCO principles from 2012.[2] Danmarks Nationalbank and those responsible for the core infrastructure systems keep up a dialogue on the efforts to comply with the guidance.

1 The CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures *(link)* was published by the Bank for International Settlements, BIS, and the International Organization of Securities Commissions, IOSCO. The Committee on Payment and Market Infrastructures, CPMI, is the BIS committee that contributed to preparing 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.

2 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.

The Danish payments infrastructure

Box 1

Each banking day[1], payments averaging kr. 536 billion, corresponding to almost one fourth of GDP, are settled via the Danish payments infrastructure.

Danmarks Nationalbank's payment system, Kronos2, 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. 83 billion are settled in Kronos2 on a daily basis.

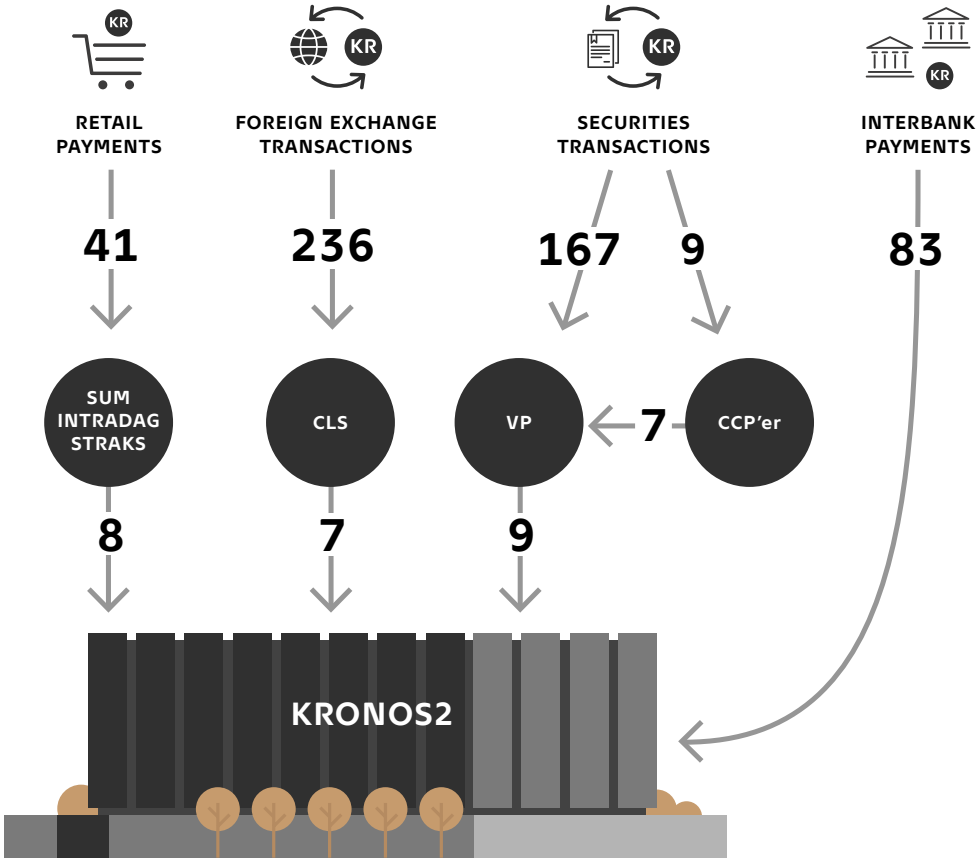
Retail payments are payments between consumers, firms and public authorities, e.g. by Dankort or as credit transfers. Depending on their type, retail payments are cleared and settled through the Sumclearing, the Intradagclearing or the Straksclearing (retail payment systems).

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, settle their participants' net positions in Kronos2. Net positions are calculated by offsetting participants' claims and obligations in the respective systems. This netting reduces the participants' liquidity requirement for settlement considerably compared with a situation in which all payments are settled individually. For example, netting reduces the daily liquidity requirement for settlement of retail payments from kr. 41 billion to kr. 8 billion, equivalent to a reduction of 80 per cent. In CLS and VP, netting reduces the liquidity requirement by 97 and 95 per cent, respectively.

Payment flows, kr. billion, averages per banking day in 2018



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

Cyber security efforts have high priority across infrastructure systems and solutions. Strategies have been prepared for this work, anchored at and monitored by the top management level. Systematic efforts are made to manage risks, including cyber risks, although the level of maturity varies. The cyber resilience efforts are described in more detail in the sections below on oversight of the individual payment and settlement systems.

An important part of the work relating to cyber resilience takes place in cooperation with other actors. One forum for cooperation is FSOR, the Financial Sector forum for Operational Resilience, which has worked with various aspects of cyber resilience since 2016. Participation in such sector activities supports the cyber resilience efforts of the individual actors and helps to ensure compliance with the CPMI-IOSCO cyber security guidance.

Red team testing of cyber security
Those responsible for the core systems and solutions participate in TIBER-DK, a Danish intelligence-led red team testing programme for live testing of critical systems against a simulated cyberattack. TIBER-DK is a joint framework aimed at ensuring that all participants will be subject to the same high minimum cyber testing requirements.

Red team testing is an important tool for strengthening cyber security and is part of the CPMI-IOSCO cyber security guidance.

Risks arising from interdependencies
At the recommendation of Danmarks Nationalbank's oversight function, cooperation has been established between VP, Finance Denmark and Danmarks Nationalbank to identify and address risks related to interdependencies between Kronos2, the VP settlement system and the retail payment systems.

The close interaction between the systems means that there is a risk that operational problems in one system will affect settlement in the other systems. Another risk is that external problems, such as a cyberattack, will spread between the systems. Risks may also arise because the systems use shared communication networks or the same critical service provider.

In mid-2018, this cooperation was formalised in the Risk Forum for Interdependencies (Risikoforum for Gensidige Afhængigheder – RGA) with a joint risk management method. RGA has identified and classified a number of risks that the system owners jointly seek to counter. In addition, RGA discusses issues related to interaction between the systems and addresses incidents that affect several systems.

RGA reports to FSOR and may also escalate issues requiring broader sector involvement to FSOR. The establishment of RGA and its interaction with FSOR constituted an important step in the work to ensure a robust Danish payments infrastructure.

Dialogue with critical service providers
As one of its first initiatives in relation to the risks identified, RGA in January 2019 held a joint meeting with critical infrastructure service providers. The aim was to achieve a common understanding of the interdependencies and to discuss the opportunities for knowledge-sharing and cooperation across service providers, operators and system owners.

The future dialogue with infrastructure service providers will take place under the auspices of FSOR. In this way, the focus will be broadened to cover all critical elements of the infrastructure, and experience from the dialogue can be included directly in FSOR's work to map the infrastructure and analyse risks.

The risk of criminal transactions
Against the background of, inter alia, the cyberattack on the central bank of Bangladesh in 2016, CPMI has published a strategy[3] aimed at strengthening end

3 *Reducing the risk of wholesale payments fraud related to endpoint security, (link).*

point security[4] and thereby reducing the risk of criminal transactions in core payment systems, primarily in relation to settlement of interbank payments. The key elements of this strategy are described in Box 2. A cardinal point is that payment system owners must impose adequate requirements on participants in order to support endpoint security. Since no actor can check all issues relating to endpoint security single-handedly, the strategy emphasises the importance of involving all relevant actors in the implementation of security measures at the endpoints checked.

Danmarks Nationalbank supports this strategy by implementing it in specific recommendations for the systems subject to oversight and by working with the issue in relevant forums such as FSOR. In 2018, an FSOR working group headed by Finance Denmark performed an analysis of the risk of criminal transactions, shedding light on issues such as risk of fraud in connection with interbank payments in Danish kroner and securities transactions.

Strategy for reducing the risk of wholesale payments fraud related to endpoint security Box 2

In 2018, the CPMI published the report Reducing the risk of wholesale payments fraud related to endpoint security. The strategy includes seven elements aimed at relevant stakeholders, i.e. operators of systems for settlement of interbank payments, messaging networks, service providers and system participants.

The seven elements require relevant stakeholders to identify and understand the risks of fraud related to endpoint security. In addition, operators must impose clear endpoint security requirements on participants as part of their participation requirements. Operators and participants must use information and tools that increase the opportunities to prevent and detect attempts at fraud and must have adequate procedures and sufficient resources to respond in a timely manner to actual or suspected fraud. All stakeholders must regularly support education in and awareness of endpoint security and where possible share relevant information. Moreover, they must develop and update endpoint security and coordinate relevant measures.

4 A payment system is linked to other financial infrastructures, service providers and participants (i.e. banks and other financial institutions) via messaging networks. Jointly, these parties and the associated networks make up a complex "ecosystem" for settlement of payments. In CPMI terminology, an endpoint is defined as a point in place and time at which payment instruction information is exchanged between two parties in the ecosystem.

Interbank payments

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, which settle payments individually and immediately.

In August 2018, Danmarks Nationalbank replaced the existing RTGS system for interbank payments in Danish kroner, Kronos, by an updated and more robust Kronos2 – see Box 3. Kronos2 settles not only interbank payments but also monetary policy operations and net positions from connected payment and settlement systems.

Use
There are 88 direct Kronos2 participants, mainly Danish banks, mortgage credit institutions and branches of foreign banks.

In 2018, an average of approximately 5,400 daily interbank payments with a total value of kr. 83 billion were settled in Kronos2, cf. Table 1. This was an increase from kr. 74 billion in 2017.

Transfers to the Sumclearing, Intradagclearing and Strakscleaning declined substantially in 2018. This fall reflects the new liquidity management functions in Kronos2 that allow participants to use their liquidity more efficiently, cf. Box 3.

Operational reliability
In connection with the transition to Kronos2 there has been an increase of incidents. This was attributable to factors such as operational errors in the interaction with other infrastructure systems.

On 31 August, an incorrect setting in Kronos2 contributed to delayed disbursement of wages and

Payments in Kronos2 Table 1

Kr. billion, averages per banking day	2014	2015	2016	2017	2018
Interbank payments	**92.0**	**99.3**	**83.0**	**74.0**	**83.0**
- Of which customer payments	11.0	12.8	11.5	11.5	13.6
Monetary policy operations	**25.5**	**37.5**	**28.7**	**39.9**	**36.9**
- Of which sale of certificates of deposit	24.9	37.3	28.6	39.9	36.9
- Of which monetary policy lending	0.6	0.2	0.1	0.0	0.0
Transfers to settlement systems	**320.2**	**380.0**	**283.4**	**316.3**	**237.4**
- Of which for the Sumclearing, Intradagclearing and Strakscleaning	274.6	334.9	242.7	273.8	177.2
- Of which for VP settlement	35.2	35.5	31.7	32.5	40.6
- Of which for CLS	10.4	9.6	9.0	10.0	19.6
Net positions settled	**25.7**	**27.5**	**25.1**	**24.8**	**24.0**
- Of which the Sumclearing, Intradagclearing and Straks clearing	7.0	7.6	10.6	8.0	8.1
- Of which VP settlement	12.2	12.7	10.6	10.1	9.1
- Of which CLS	6.5	7.2	6.9	6.7	6.8

Kronos2

Box 3

Kronos2 consists of an RTGS module for interbank payments and transfers for settlement of retail payments, securities, etc., a module for handling monetary policy operations and a module for collateral management, Calypso. The RTGS module, which is supplied by Perago, is also used by Sveriges Riksbank, Norges Bank and Seðlabanki Íslands, while the Calypso system is used by Banque de France and Banco de España.

Given the central position of Kronos2 in the Danish financial infrastructure, safety and efficiency requirements are high.

Kronos2 has been specifically designed to meet high security requirements as regards confidentiality, integrity and accessibility. The system has been built on an isolated and dedicated IT platform. This makes it possible for Danmarks Nationalbank to test the entire platform and to perform its own security updates on an ongoing basis. Furthermore, all key components have been duplicated, which supports the target of a maximum time limit for resumption of system operations of two hours following a major incident or failure.

The functionality of Kronos2 has enabled Danish kroner to be migrated to the trans-European securities platform, T2S. As a result of the migration to T2S, the monetary policy day[1] has been extended to run from 5:30 pm to 4:45 pm the following day. Previously it ran from 4:30 pm to 3:30 pm.

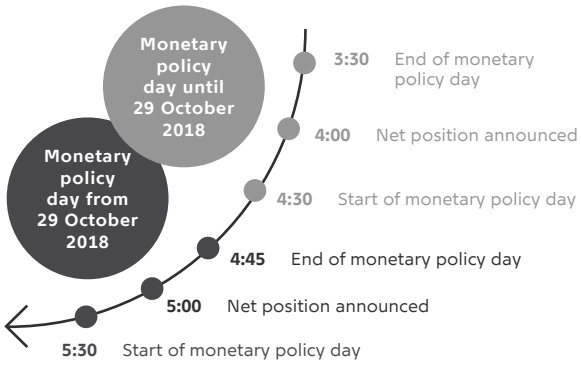
Kronos2 is accessible 24/7, thereby enabling participants to make more efficient use of their liquidity. For example, Kronos2 continuously transfers liquidity on behalf of participants for use in the Straksclearing and liquidity is automatically sourced for night-time settlement in the Sumclearing and Intradagclearing. The new liquidity management functions have replaced the "Maximum liquidity" function, which transferred all the participant's available current account liquidity for night-time settlement. This has led to a substantial reduction in participants' transfers to the retail payment systems, cf. Table 1 and the chart below showing use of liquidity in the retail payment systems.

Unlike Kronos, Kronos2 has no queuing function. This has not led to problems as participants have ample liquidity for settlement of their payments.

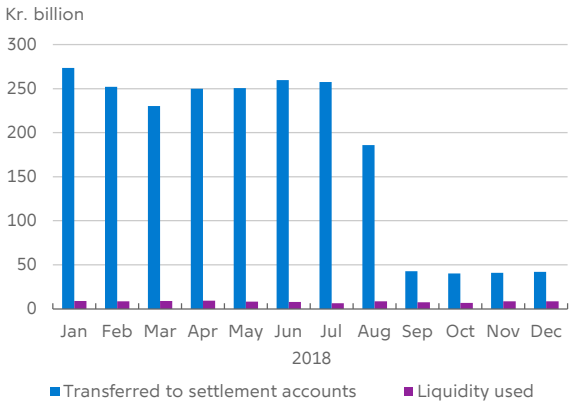
With Kronos2, a new pricing model[2] has been introduced for participants, based primarily on equal weighting of the participants' shares of the total number and value of all transactions in Kronos2.

The monetary policy day and use of liquidity in the retail payment systems

The monetary policy day



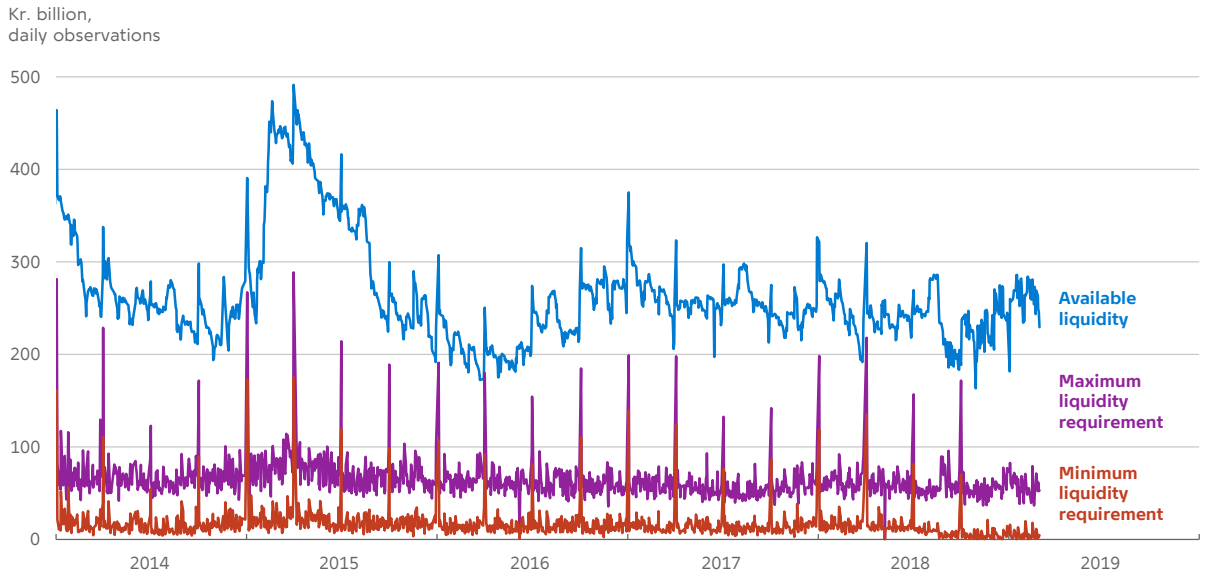
Use of liquidity in the retail payment systems



Source: Danmarks Nationalbank.

1. The monetary policy day is the period during which the banks can withdraw liquidity from and deposit liquidity in their accounts at Danmarks Nationalbank when various payments are settled.
2. Pricing Model in Kronos2, (*link*).

Ample liquidity among Kronos2 participants Chart 1



Note: Available liquidity is the participants' lines plus their current account balances when Kronos2 opens at 7:00 am. Any credit available under the automatic collateralisation arrangement has not been included. 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.

salaries. The fault arose because the upper limit in Kronos2 for the amount that may be drawn on Danmarks Nationalbank's account had accidentally been set at too low a value. As a result, transfer of central government payments from Danmarks Nationalbank to the banks did not take place. The Kronos2 setting was soon corrected, but a chain reaction was triggered so that problems at the data centres led to further delays – see the section on clearing and settlement of retail payments.

It is assessed that this and other incidents in relation to Kronos2 in 2018 were satisfactorily followed up.

Liquidity

Overall, participants had ample liquidity for settlement of payments in Kronos/Kronos2. Chart 1 shows the participants' excess liquidity cover.

Previously, the liquidity requirement was particularly high on days when auctions of fixed rate bullet bonds for financing adjustable rate mortgage loans were settled, which is reflected in the periodic increases in the liquidity requirement, cf. Chart 1. After the migration of kroner to T2S in October 2018, redemption of maturing and financing of new bonds can take place in the same process so that the liquidity requirement is reduced via netting.

The ample liquidity among Kronos2 participants contributes to smooth settlement of payments.

International standards

In the most recent assessment of Kronos observance of the CPMI-IOSCO principles, four areas with potential for improvement were identified.[5] In 2017, this was followed up by an analysis of the risks related to

5 Assessment of Kronos, 2016 (*link*)

indirect participants.[6] In connection with the implementation of Kronos2, the target for the maximum time limit for resumption of system operations has been reduced from four to two hours. Work is still underway in the remaining two areas for improvement, including strengthening of the management of risks related to interdependencies in the infrastructure, cf. above. The risks identified in collaboration with VP and Finance Denmark still need to be anchored in the Kronos2 risk management.

As part of the ongoing oversight, risk management of Kronos2 has been reviewed in relation to the CPMI-IOSCO principles. The conclusions will be taken into account in Danmarks Nationalbank's future work to manage risks.

Cyber resilience
Danmarks Nationalbank's Risk and Security Policy was revised in 2018. This led to strengthening of the framework for risk management, including management of cyber risks. For example, targets and requirements for risk management and security levels have been specified in more detail and a clearer distribution of roles and responsibilities has been established.

The transition from Kronos to Kronos2 entailed substantial strengthening of cyber resilience. Kronos2 has been designed with high security requirements and has been built on an isolated IT platform, which makes it possible to perform necessary security updates on an ongoing basis.

During 2018, Danmarks Nationalbank worked to improve the mapping of risks in relation to Kronos2. A technical risk assessment of the central components of Kronos2 was performed, as well as a business risk assessment of core Kronos2 processes.

Also in 2018, work was carried out to meet the requirements of the SWIFT Customer Security Programme (CSP) and the ECB's Connectivity Guide. These requirements are aimed at strengthening security throughout the payments network, i.e. in relation to payment and settlement systems, communications networks and at participants. Kronos2 is compliant with both SWIFT CSP and the ECB's Connectivity Guide.

System updates
With the implementation of Kronos2, a major milestone was reached. Danmarks Nationalbank continues its work to modernise its core systems; for example, a strengthened Extreme Contingency solution is being established for settlement of payments in the event that Kronos2 is hit by a major incident or failure.

6 Analysis of risks related to indirect participants (*link)*

Retail payments

Payments between consumers and firms can be made using banknotes and coins or various electronic payment solutions. Most payments take place electronically, e.g. credit transfers via online banking or MobilePay, Dankort for payments in supermarkets, Betalingsservice for paying rent. In 2018, the daily value of electronic retail payments averaged kr. 27.9 billion.[7]

Danmarks Nationalbank oversees the most important payment solutions in Denmark, i.e. Dankort, Betalingsservice and credit transfers, cf. Box 4.

Operational reliability
The operational reliability of Nets' Dankort and Betalingsservice systems was satisfactory in 2018.

However, there were a few episodes where some Dankort holders experienced problems in relation to approval of online payments using SMS codes. In Danmarks Nationalbank's assessment, Nets followed up the incidents in a satisfactory manner.

In January 2018, Nets initiated preventive replacement of 36,000 co-branded Dankort cards (Visa/Dankort). The background was suspicion that card details had ended up in the wrong hands via a compromised foreign website. All Visa/Dankort cards that had been used on that website were replaced.

No incidents of consequence affected the operation of Betalingsservice in 2018.

The incidence of Dankort fraud is falling
According to Nets, fraudulent use of Dankort totalled kr. 57.5 million in 2018, corresponding to 0.14 per thousand of total consumption.[8] That is the lowest level in four years, cf. Chart 2.

7 Kr. 27.9 billion per calendar day corresponds to kr. 41.1 billion per banking day, cf. Table 2 in the section "Clearing and settlement of retail payments".

8 Nets' statistics of fraudulent use of Dankort: (*link*)
Nets' data for fraudulent use is not directly comparable with Danmarks Nationalbank's statistics of fraudulent use of payment cards, which cover both Dankort and international cards used in Denmark.

Danmarks Nationalbank's oversight of payment solutions Box 4

Danmarks Nationalbank oversees Dankort, Betalingsservice and credit transfers.

Oversight of Dankort and Betalingsservice is aimed at Nets, the owner of these solutions. Oversight of Dankort comprises the pure Dankort cards as well as the Dankort side of co-branded cards (primarily Visa/Dankort).

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".

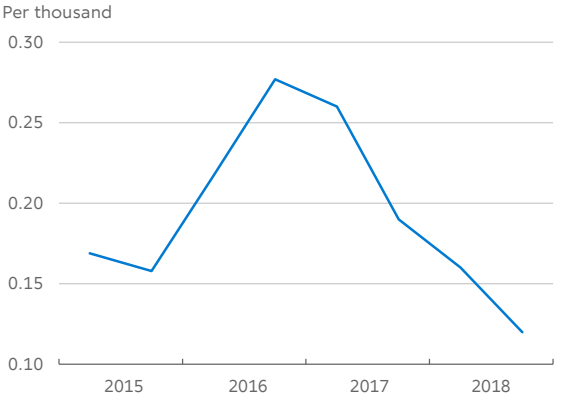
Developments in the various payment solutions offered in the Danish market are monitored on an ongoing basis to assess whether targeted oversight of these solutions is required.

MobilePay is increasingly used for shopping in stores, online purchases, payment of recurring invoices and transfers between users. Average daily turnover for MobilePay was kr. 0.2 billion in 2018.[1] By comparison Dankort payments totalled kr. 1.1 billion per day in 2018.[2]

The new payment solutions in the Danish market, Apple Pay and Google Pay, still have only quite limited market shares.

1. Press release from MobilePay, 27 December 2018 (link)
2. Nets' statistics on fraudulent use of the Dankort: (link)

Fraudulent use as a share of total Dankort-based consumption Chart 2



Source: Nets.

Fraudulent use of stolen or lost Dankort cards for trading in stores or withdrawing cash from ATMs has more than halved since the 2nd half of 2017, to 0.065 per thousand in the 2nd half of 2018.[9]

Nets has stated that in cooperation with the police targeted efforts were made to prevent fraudulent use of stolen cards in 2018. Together Nets and the police have identified the places in Denmark where cardholders are most frequently watched when they enter their PINs. This has led to the arrest of criminal groupings.

According to Nets, use of contactless payments has also contributed to reducing fraud: since the PIN is not used for contactless payments, no-one can watch the cardholder enter it. This reduces the risk of incidents where knowledge of the PIN and theft of the card are used to withdraw cash or make large purchases in stores. The upper limit for contactless Dankort payments was increased from kr. 200 to kr. 350 from 1 February 2018. According to Nets, some 85 per cent of payments in stores are below that limit.[10] For security reasons, cardholders are, however, from time to time asked to enter the PIN when making purchases below the limit.

The incidence of fraudulent use of Dankort on Danish websites has also fallen. Fraudulent online use typically takes place if the card number and accompanying CVV/CVC code are stolen. From 2017 to 2018, fraud of this type declined from 0.5 to 0.38 per thousand.[11]

In early 2017, Nets introduced two measures to enhance the security of Dankort: Dankort Secured by Nets is a solution based on strong authentication, whereby the user in online transactions must not only state the Dankort details but also enter a code sent by SMS from Nets before purchases exceeding kr. 450 can be completed; and Fraud Prevention is a system that uses pattern recognition to reject transactions which are so unusual that they must be assumed to be made by another person than the cardholder.

International standards

As part of Danmarks Nationalbank's oversight of Dankort and Betalingsservice, Nets' risk management is followed up on a regular basis. It is assessed that Nets' risk management is mature, based on well-established standards and used widely within the organisation. Nets has functions in both the first and second organisational lines of defence that follow up the work with risk and associated controls.

In 2018, Nets achieved compliance with the last two recommendations in Danmarks Nationalbank's 2017 assessment of Dankort in relation to ECB's standards for card payment schemes.[12] Nets has prepared a plan for communication to relevant stakeholders in connection with major operational disruptions and changes affecting Dankort. Furthermore, Nets has strengthened the overall decision-making processes for Dankort via an updated formal framework for cooperation with banks.

Danmarks Nationalbank is finalising an assessment of Betalingsservice in relation to the ECB's standards for direct debit schemes.

Regulation

Among other things, the EU's new Payment Services Directive, PSD2, aims to make electronic payments more secure and to enhance competition in the EU payments market. The new Danish Payments Act implemented PSD2 in Danish law and also introduced a number of national rules on 1 January 2018.

However, many of the most important provisions applying to new and existing actors in the market will not take effect in their final formulation until 14 September 2019. From that date, the banks must inter alia be ready with technical solutions allowing customers to make payments via a payment service provider in the market without any agreement existing between the bank and the service provider in question.

9 Nets' statistics on fraudulent use of Dankort: (*link*)

10 Press release from Dankort, 13. December 2017: (*link*)

11 Nets' statistics on fraudulent use of Dankort: (link)

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

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 and operated by Nets.

The Sumclearing is used for clearing of all card payments, Betalingsservice and Nets' other payment products once a day on banking days. The Intradagclearing is used for clearing of credit transfers such as online banking transfers, payroll transactions and public sector payments. At fixed times, the systems calculate the participants' net positions, corresponding to the sum of payments to and from the banks' customers. The net positions are sent to Kronos2, which exchanges the amounts between the banks.

The Straksclearing is a real-time settlement system in which credit transfers are entered to customer accounts as they are made. This is possible because the banks in advance reserve liquidity in Kronos2 for the transfers. The actual exchange of liquidity between the banks takes place six times a day on banking days. The Straksclearing is used primarily for online banking transfers and payments via MobilePay.

Use

There are 54 direct participants in the retail payment systems and 29 indirect participants, who settle via direct participants. The value of transactions in the retail payment systems averaged kr. 41.1 billion per banking day in 2018, cf. Table 2.

The number of transactions in the Straksclearing has continued to rise, cf. Chart 3. One reason is that since 2017 transactions in MobilePay has increasingly been based on credit transfers via the Straksclearing rather than Dankort transactions in the Sumclearing[13].

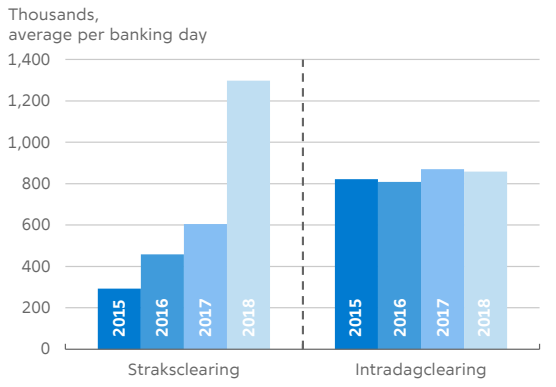
Although there has been an increase in the number of transactions in the Straksclearing, these account for only a small share of the total retail payments in terms of value, cf. Table 2.

Value of transactions in the Sumclearing, Intradagclearing and Straksclearing Table 2

Kr. billion, averages per banking day	2014	2015	2016	2017	2018
Sumclearing	17.9	16.7	17.2	17.8	19.8
Intradagclearing	17.0	17.8	18.4	19.7	20.1
Straksclearing	0.5	0.6	0.8	0.9	1.2
Total	35.4	35.0	36.4	38.4	41.1

Source: Nets.

Number of Intradagclearing and Straksclearing transactions, 2015-18 Chart 3



Source: Nets.

Operational reliability

Retail payment system operations were in general satisfactory in 2018. On 31 August, disbursement of wages, pensions, etc. was delayed considerably. An incorrect setting in Kronos2 meant that there was insufficient liquidity for night-time settlement, and

13 The number and value of transactions in the Straksclearing are not equal to the volume of payments. For example, a MobilePay payment may entail two transactions in the retail payment systems.

consequently transactions were not settled until the morning. This incident led to resultant errors and capacity pressure at the data centres due to the accumulation of transactions that should have been book-entered during the night. Since it was the end of the month, the number of transactions was higher than normal. This delayed entry to customer accounts.

In view of the incident on 31 August, it has been agreed to adjust the night-time settlement so that – in the event of an incident – the settlement cycles at 3:00 am and 6:00 am can be settled manually and therefore earlier. This will give the data centres more time to complete their book-entry before the start of the day. It is assessed that the incident has been satisfactorily followed up.

Liquidity
Participants reserve liquidity in accounts at Danmarks Nationalbank for settlement of their net positions in the Sumclearing, Intradagclearing and Straksclearing. If a participant does not reserve sufficient liquidity, it may generate a domino effect of delayed payments. Besides the incident on 31 August, there were only two cases in 2018 in which participants had not reserved sufficient liquidity.

International standards
In 2018, Danmarks Nationalbank published an assessment of the retail payment systems observance of the CPMI-IOSCO principles.[14] The systems extensively observe the safety and efficiency requirements stated in the principles. All the same, there is room for improvement in some areas. Danmarks Nationalbank recommends, inter alia, further strengthening of governance and risk management, testing in selected areas and intensification of the cyber security effort.

Finance Denmark has complied with a number of the recommendations, e.g. by preparing a cyber strategy for the retail payment systems, testing default procedures and contingency plans and by publishing a description of the retail payment systems observance of international standards. In addition, Finance Denmark has strengthened its controls to ensure that tasks in relation to the retail payment systems, including risk management, are carried out efficiently and in accordance with applicable policies and procedures. Finance Denmark has laid down a plan for observance of the remaining recommendations.

In 2018, Finance Denmark, VP and Danmarks Nationalbank agreed on a joint method for managing risks related to interdependencies between the systems, and Finance Denmark has incorporated the risks identified in its own risk management. This closes a previous recommendation from Danmarks Nationalbank.

Danmarks Nationalbank has initiated an assessment of the retail payment systems observance of the CPMI-IOSCO cyber security guidance.

System updates
The financial sector has established a new network, e-connect, for communication between data centres, Nets and Kronos2 in connection with the clearing and settlement of retail payments. The new network meets high standards for security, redundancy and operational reliability. It is managed by e-nettet, which is responsible for governance and supplier management on behalf of the entire sector. Migration of network traffic to e-connect is expected to be completed in mid-2019.

The opening hours of Kronos2 have been extended after the migration of Danish kroner to T2S. In that connection, it has been discussed whether the last settlement cycles in the Intradagclearing and Straksclearing should take place later in the day so that a larger share of transactions are settled the same day they are made. These discussions are part of a project to review the settlement times for retail payments and securities settlement, the aim being to achieve a more robust settlement day.

A group of large Swedish, Danish and Finnish banks[15] are working to establish a Nordic retail payment system called P27. According to the banks, economies of scale can be achieved by sharing a single platform, just like a common

14 Assessment of the Danish retail payment systems, 2018 (*Link*)

15 The banks behind this initiative are Danske Bank, Nordea, Handelsbanken, SEB, Swedbank and OP Financial Group. DNB was part of the initiative but withdrew from the project in March 2019.

system will pave the way for shared products across the Nordic region. The vision is efficient cross-border payments.

Securities settlement

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

On 29 October 2018, a part of the krone-denominated securities settlement migrated from VP's own platform to the trans-European securities settlement platform, TARGET2-Securities (T2S). Go forward, securities settlement will take place either on T2S or on VP's own platform, depending on the parties to the transaction (see Box 5).

Use

The VP settlement system has 126 participants, of which 62 are non-resident market participants. Three participants have direct access to T2S. The rest have indirect access to T2S via VP.

Securities transactions totalling an average of kr. 174.5 billion per banking day were settled in 2018, cf. Table 3. This equals an increase of 7.3 per cent relative to 2017. The settlement for each of the three main asset classes - equities, bonds and investment fund shares - increased. Thus, recent years' downward trend in equities and bonds has been reversed.

Danish kroner on T2S – a dual settlement system

Box 5

The trans-European securities settlement platform, T2S, was launched in 2015 with the aim to make cross-border securities settlement just as inexpensive and efficient as domestic securities settlement. One of the ways to achieve this was to give national central securities depositories, CSDs, access to settle securities transactions on the T2S platform. Historically, cross-border securities settlement has been handled by a network of international custodian banks with custody accounts in various CSDs or via participation in an international CSD.

In 2016, Danish participants were given access to settle securities transactions in euro on T2S, and on 29 October 2018, Danish kroner migrated to T2S. Hereafter, settlement of securities transactions between participants will take place on T2S, while investors' securities transactions are still settled in VP's own systems via their respective banks.

Going forward, securities settlement will be handled in two systems. Via T2S, professional actors will have easier access to settlement of cross-border transactions involving Danish securities. The transactions of the many private investors with lower trading volumes will still be settled on VP's platform, and their custody accounts will be managed by VP.

The T2S platform is operated by the Eurosystem and connected to the central banks' RTGS systems. So far, only the euro area's TARGET2 system has been connected, but now Danmarks Nationalbank's Kronos2 system is also connected to T2S.

Hence, the Danish krone is the first currency besides the euro to be settled on T2S. In the longer term, better integration with the European infrastructure should strengthen the liquidity of Danish securities and support the vision of a single European financial market.

For the securities settlement that takes place via T2S, changes have been introduced in relation to liquidity management. Participants settling on T2S hold a Dedicated Cash Account containing krone liquidity for securities transactions on T2S. Participants settling via VP's platform will still have to reserve liquidity in accounts at Danmarks Nationalbank for VP's net settlement cycles.

For both platforms trades surpassing the reserved liquidity put up by the participant will be postponed for settlement at a later time when sufficient liquidity is made available. T2S does not have a sanction system in the event that provided liquidity is insufficient, but according to the Central Securities Depository Regulation (CSDR[1]), a penality mechanism is to be established so that participants with insufficient liquidity or securities for a transaction must compensate their counterparties. This mechanism is still being developed and is planned to take effect in 2020.

In the coming years, participants will have to adapt to the new opportunities offered by the infrastructure, and the Eurosystem will continue its work to harmonise the rules for dividends and taxation – two areas in which differences between the individual member states currently impede cross-border securities trading and settlement.

1. Regulation of CSDs in the EU takes place via the CSDR.

Equities, investment fund shares and bonds settled in VP, averages per banking day Table 3

	Total		Bonds		Equities		Investment fund shares	
Year, daily averages	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
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
2018	71.4	174.5	2.8	125.1	34.2	40.6	34.3	8.9

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

In 2018, VP closed its subsidiary in Luxembourg – VP Lux. Among other things, this company had assisted Danish issuers of euro-denominated securities that were eligible as collateral in the Eurosystem. Since 2014, issues outside of euro area have been eligible too and hence the need for VP Lux has been reduced. In connection with the close down, all pledged securities in VP Lux had to be transferred to VP, and access to T2S had to be closed down. Neither had been done before, but both the transfer and the closing-down went according to plan.

Operational reliability
The operational reliability of the VP settlement system was affected by several incidents in connection with the migration of Danish kroner to T2S in 2018. These incidents caused lengthy delays in securities settlement and in two specific cases transactions were postponed until the next monetary policy day.

During the first week after the migration, VP operations were unstable, partly due to problems with external and internal network communication. VP performed a number of adjustments to systems and processes, and around two weeks after the migration, operations were stable and settlement cycles were completed on time.

VP has followed up all incidents and addressed the problems incurred. As a result of the extensive system changes and related incidents, VP has had to strengthen its processes and controls in connection with system changes.

Unmatched trades
After the migration to T2S, there were unusually many unmatched trading instructions. They were primarily attributable to errors in participants' instructions. The implementation of new exchange formats and change of country code for one large participant was the root cause to many incorrect instructions. Furthermore, some participants' T2S account relationships were not finalised until after the migration.

VP and the participants worked together to identify the problems, and by the turn of the year the number of unmatched trading instructions had been reduced considerably.

The high number of unmatched trades shows the importance of preparation and efficient system support among participants, who need to adapt, test and implement changes to their own systems. Some participants still need to make the necessary adjustments following the migration of kroner to T2S.

Settlement ratio
According to article 5 of the CSDR, securities transactions must be settled two days after the transaction date. The settlement ratio indicates the percentage of the transactions settled in a timely manner.

In 2018, incidents in connection with the migration to T2S caused the settlement ratio to fall, cf. Chart 4. The settlement ratio stabilised in the 1st quarter of 2019 as the problems related to e.g. unmatched trading instructions were gradually solved.

The settlement ratio was at a stable high level until 2017, when a single significant incident in October had a negative impact on the settlement ratio.

Liquidity

When a participant has insufficient liquidity in its securities settlement account, one or more transactions cannot be executed. This may cause problems for that participant's counterparties, which may not be able to meet their obligations as a result. A sanctioning system can help to discipline participants so that they make sufficient liquidity available for settlement.

In 2018, there were 116 cases in which a participant had not made sufficient liquidity available for securities settlement on VP's own platform. This is also known as "overdraft". In 43 of these cases, fines were issued.

The number of cases where insufficient liquidity was provided/fines issued was higher than in 2017, but on a par with previous years, cf. Chart 5.

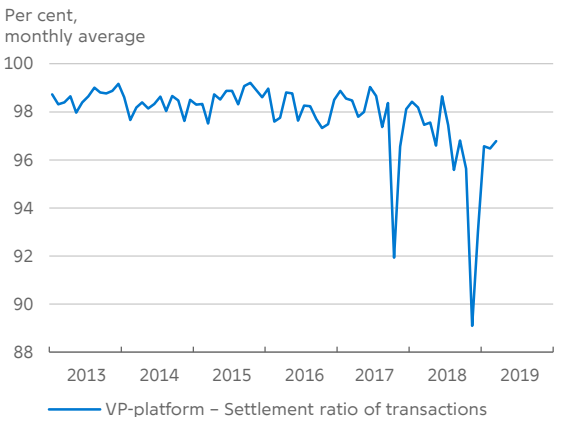
Fines are not issued if there is insufficient liquidity on the T2S platform. Instead, a trans-European penalty mechanism based on compensation between counterparties is being developed. This penalty mechanism is planned to take effect in 2020. It will apply to both T2S and VP and will thus replace the existing sanctioning system on VP's platform.

International standards

As part of its ongoing oversight, Danmarks Nationalbank reviewed VP's risk management in the spring of 2018. The conclusion was that VP's risk management is mature, based on approved standards and the framework is well integrated in the organisation.

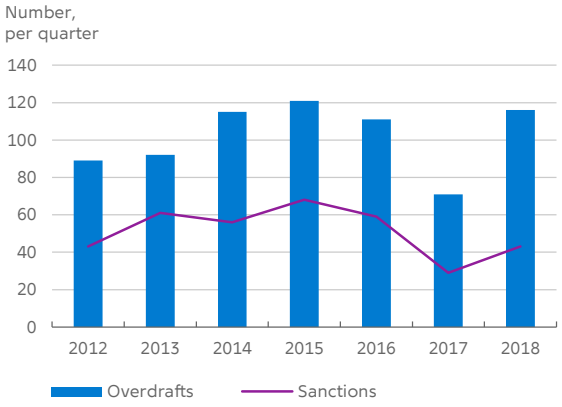
In connection with Danmarks Nationalbank's assessment of the VP settlement systems observance of the the CPMI-IOSCO principles in 2016, four recommendations were issued to VP. Two of them were complied with in the autumn of 2017. In 2018, VP, Finance Denmark and Danmarks Nationalbank agreed on a joint method for managing risks related to interdependencies, and VP has incorporated the risks iden-

The VP settlement ratio fell in 2018 due to the migration of kroner to T2S Chart 4



Note: In the chart, the settlement ratio is stated on the basis of the number of transactions. The total is a weighted average of the settlement ratios for the VP and T2S platforms.
Source: VP.

Overdrafts and sanctions in VP settlement on a par with previous years Chart 5



Note: The figures relate to sanctions and insufficient liquidity on the VP platform only.
Source: VP.

tified in its own risk management. This means that VP complies with the third recommendation.

The final recommendation stipulates that VP should adjust its recovery plans to take better account of the critical scenarios, as described in the technical standards under CSDR. VP is currently revising its recovery plan.

VP has strengthened its cyber resilience on an ongoing basis. More specifically, VP has strengthened its data protection, access controls and system and network security and has introduced training and awareness campaigns for employees.

In 2018, Danmarks Nationalbank initiated an assessment of VP's compliance with the CPMI-IOSCO cyber security guidance.

System updates
In connection with the migration of Danish kroner to T2S, the end of the monetary policy day was postponed until 4:45 pm, which has made room for a new VP settlement cycle 80 at 3:00 pm.

Adjustment of the monetary policy day was aimed at achieving better alignment with the settlement schedule of the T2S platform. T2S starts its night-time settlement at 8:00 pm. At 5:00 am, T2S day-time settlement begins, and Delivery-versus-Payment, DvP, settlement takes place until 4:00 pm.

Based on the experience from the migration, VP, Finance Denmark and Danmarks Nationalbank are assessing whether further adjustments of the timing of clearing and settlement cycles over the monetary policy day are required.

CCP clearing
In Denmark, equities and repo transactions are settled via a central counterparty, CCP, cf. Box 6.

Three CCPs – EuroCCP, LCH Clearnet and Six X-clear – clear equities transactions, while Nasdaq Clearing clears repo transactions. After CCP clearing, the transactions are settled in T2S, to which EuroCCP has direct access.

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 primary countries in which the CCP is operating. Danmarks Nationalbank monitors developments, e.g. via its participation in the EuroCCP supervisory college.

What is a CCP? Box 6

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)*.

Settlement of foreign exchange transactions

CLS Bank International (CLS) is a settlement system for foreign exchange trades. CLS is owned by large, international banks and settles transactions in 18 participating currencies, including Danish kroner.

Traditionally, the two payments in a foreign exchange trade are settled as independent payments, often executed via correspondent banks in the currencies in question. If the two payments are not settled simultaneously, the parties incur a settlement risk i.e. a risk that one party fails to uphold its obligation. With CLS, settlement risk is reduced, as the two payments in a transaction are settled simultaneously (Payment-versus-Payment, PvP).

Danmarks Nationalbank participates in the cooperative oversight of CLS, cf. Box 7.

Use

More than 80 per cent of all foreign exchange transactions in Danish kroner are settled via CLS.[16] Both financial institutions and firms participate in the CLS settlement of Danish kroner.

One Danish bank participates directly in CLS settlement. Those who are not direct participants can settle foreign exchange transactions in CLS via one of the nine participants who offer indirect participation to the Danish market. Four participants have CLS settlement accounts at Danmarks Nationalbank and offer handling of incoming and outgoing payments for CLS settlement on behalf of other participants.

The value of CLS transactions in Danish kroner continued its stable development in 2018, cf. Chart 6. The average daily value of transactions in Danish kroner was kr. 236 billion in 2018. The number and value of trades are particularly large around quarter change and on days around foreign holidays.

Brexit

CLS is governed by English law and designated by the Bank of England as a system protected by the Settlement Finality Directive. This means that pay-

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

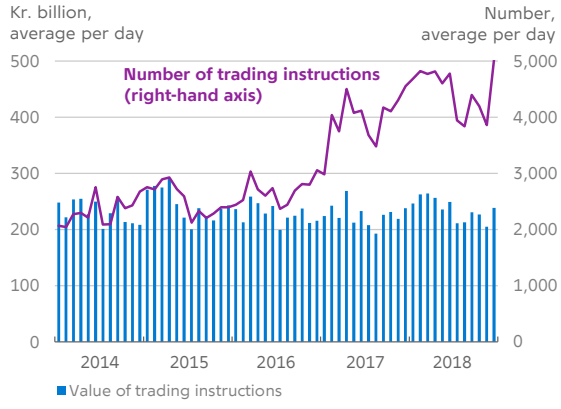
Oversight of CLS Box 7

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*).

The value of trading instructions in CLS shows a stable trend Chart 6



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

ments in CLS are final and cannot be revoked in case of insolvency.

When the United Kingdom leaves the EU, CLS will lose its protection under the Directive. If EU participants are to continue to settle their foreign exchange transactions via CLS, it must be stipulated in national legislation that the Directive's provisions on settlement finality also apply to systems outside the EEA. In Denmark, the Capital Markets Act contains such provisions. According to this, the Danish Financial Supervisory Authority has approved CLS as a third-country payment system and Danish participants can continue to settle via CLS after Brexit.

Operational reliability and liquidity
Pay-ins to CLS take place via the national RTGS systems, in the case of Danish kroner via Kronos2. Hence the operational reliability of CLS depends on the reliability of the RTGS systems. In 2018, one incident in Kronos2 delayed the participants' pay-ins for CLS settlement due to network problems. Contingency procedures were initiated to ensure CLS settlement within key business deadlines. It is assessed that the incident was satisfactorily followed up.

The Danish participants reserve sufficient liquidity for CLS settlement.

System updates
In 2018, CLSNet was launched. CLSNet is a standardised, automated bilateral payment netting service[17] intended for FX transactions settled outside the CLS settlement service. In CLSNet participants can submit trades in approximately 120 currencies. The service is built on a distributed ledger technology (DLT) and can be accessed via SWIFT channels.

CLS also launched CLSClearedFX in 2018. This is a service that can settle payments resulting from CCP-cleared products. LCH Clearnet participates in CLSClearedFX, and it is expected that Eurex Clearing will join the service in 2019.

CLSNow[18] is still underway and is subject to regulatory approval. CLSNow will make it possible to settle transactions individually within the same day via PvP. CLSNow will potentially be expanded to all CLS currencies[19].

17 CLS, CLSNet *(link)*.

18 CLS, CLSNow *(link)*.

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

Payments and securities settlement in euro

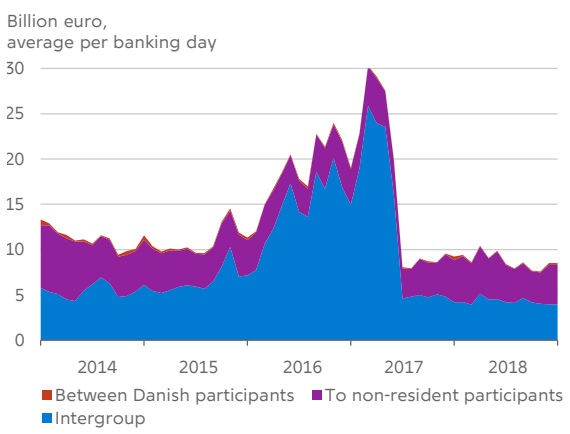
Denmark is connected to TARGET2 and TARGET2-Securities (T2S). TARGET2 is the trans-European RTGS system for settlement of interbank payments in euro. TARGET2 also handles transfers for settlement in other euro payment systems such as T2S. T2S settles securities transactions in euro and now also in Danish kroner – see Box 5.

Use

There are 28 Danish participants in TARGET2. In 2018, Danish participants' daily interbank payments averaged 8.8 billion euro. Exchange of euro mostly takes place with participants in Germany, Finland, France and the Netherlands.

Danish participants use TARGET2 mainly for intergroup payments and payments to non-resident participants. As Chart 7 shows, there has been a decline in intergroup payments in the 2nd half of 2017. This can be attributed to a change in market participants' liquidity management practice.

Interbank payments in TARGET2 Chart 7



Note: The chart shows payments submitted by Danish participants via TARGET2. Daily averages have been calculated on a monthly basis.
Source: Danmarks Nationalbank.

A total of 21 central securities depositories from 20 countries now settle via T2S, including VP. 13 Danish banks hold a Dedicated Cash Account in euro at Danmarks Nationalbank. Three of them have, via branches, established accounts in euro with central banks in the euro area in order to be able to borrow euro intraday. The rest have concluded agreements with correspondent banks.

Operational reliability

The operational reliability of the local TARGET2 components for which Danmarks Nationalbank is responsible was satisfactory in 2018. In 2018 there were only minor incidents that did not affect the execution of payments in euro.

International standards

Oversight of TARGET2 and T2S takes place in collaboration with the EU central banks in the Payment and Securities Oversight Working Group, PSOWG, and the Market Infrastructure and Payments Committee, MIPC, in which Danmarks Nationalbank participates.

Along with other European central banks and supervisory authorities, Danmarks Nationalbank and the Danish Financial Supervisory Authority participate in a Cooperative Arrangement that defines common frameworks and coordinates oversight of T2S.

System updates

In 2018, the ECB launched TIPS, TARGET Instant Payment Settlement, as a service under TARGET2 – see Box 8.

The ECB continues its modernisation of the European payments infrastructure and is working to replace TARGET2 with an updated RTGS system running on the same platform as T2S[20]. This will increase security and reduce operational costs. The consolidated platform is expected to be launched in November 2021. It will offer new RTGS services, in

20 The IT platform supporting the European securities settlement system, TARGET2-Securities, T2S.

cluding improved liquidity management procedures and a multi-currency service.

TIPS has gone live Box 8

The European Central Bank, ECB, has been modernising the European payments infrastructure in recent years. The ECB's system for instant payments, TIPS, went live in November 2018. The system allows banks to clear and settle instant payments in euro. At the same time, TIPS supports multi-currency, i.e. the system can be used to process instant payments in other currencies than the euro.

The purpose with TIPS is to offer a solution whereby instant payments can be made between all account holders in Europe. It is the ECB's ambition that such a service can minimise the risk of a fragmented European retail payments infrastructure and the need for national instant payment systems.

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

This edition closed for contributions on 26 April 2019

DANMARKS NATIONALBANK