REPORT

DANMARKS NATIONALBANK

4 MAY 2021 — NO. 3

Oversight of the financial infrastructure

- Denmark has a safe, efficient and resilient payments infrastructure. Danmarks Nationalbank considers the infrastructure to be largely compliant with the requirements of international standards for organisation, risk management and crisis response.
- The cyber threat is complex and rapidly evolving. The 2020 SolarWinds hacker attack exemplified the sophisticated techniques applied by the most advanced cyber threat actors.
- The evolution of the threat landscape means that cyber resilience is an area of work requiring persistent infrastructure development and adaptation. Progress is continuously made, but Danmarks Nationalbank finds that there is still room for improvement.

Infrastructure that is critical to society

Kr. 639 billion

in payments are settled each banking day on average in the core systems.

Read more

Collaboration across the financial sector

Cyber risk

Danmarks Nationalbank organises sectoral collaboration to reduce cyber risks and strengthen operational resilience.

Read more

CONTENTS

Denmark has a safe and efficient financial infrastructure

The exchange of goods, services and financial assets is key to the economy. This requires that payments and securities transactions can be effected in a safe and efficient manner.

The Danish financial infrastructure is the network of systems enabling consumers, corporations and financial actors to exchange payments and securities transactions. On an average banking day, payments totalling more than kr. 630 billion are cleared and settled through the core IT systems of the Danish financial infrastructure. See Box 1 for an explanation of the concept of clearing and settlement.

Due to the critical role of the core systems, they must meet high operational reliability and risk management standards. If the systems fail, disruption will follow that may, in a worst-case scenario, threaten financial stability. Danmarks Nationalbank oversees that the infrastructural core systems comply with international safety and efficiency standards.[1] This oversight also includes the most important payment solutions. The systems and solutions that make up the Danish financial infrastructure are described in Box 2.

This report presents the main conclusions of the oversight and the key areas of significance to the Danish financial infrastructure in 2020.

Safe, efficient and stable infrastructure
The conclusion of Danmarks Nationalbank's oversight is that the Danish payments infrastructure is efficient and resilient.

Operational reliability is high, and disruptions in the exchange of payments and the settlement of securities transactions are rare.

The core infrastructure systems/solutions to a large extent comply with the requirements of international standards. And efforts are continuously being made to strengthen safety and ensure compliance with Danmarks Nationalbank's recommendations for improvements.

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 based on international standards and guidelines and is described in its oversight policy (*link*).

The concepts of clearing and settlement Box 1

To enable consumers, corporations and financial actors to exchange payments and carry out securities transactions, these transactions must be cleared and settled in the core systems of the infrastructure.

Clearing is the process by which payments or securities transactions are prepared to be finally executed between the parties. Clearing includes the calculation, reconciliation and verification of transactions and, in most cases, also netting, i.e. offsetting of receivables and payables, so that each participant holds only a single net position against each of the other system participants.

Settlement is the actual exchange of amounts or securities between participants. In Kronos2, this is the process from a payment is debited to the remitter's account until the payment is credited to the recipient's account. In the settlement of a securities transaction, money and securities are exchanged. If settlement takes place immediately after the transaction is concluded, this is known as instant settlement. Once settlement has been completed, the transaction is final. Settlement may involve both individual transactions and net positions.

1 Oversight is based on the CPMI-IOSCO Principles for Financial Market Infrastructures (*link*).

The Danish payments infrastructure

Box 2

Each banking day[1], payments averaging kr. 639 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 when it comes to the 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.

Retail payments are payments between consumers, firms and public authorities, e.g. by payment cards, mobile phones or as credit transfers. When payments have been initiated and handled by a number of intermediaries, depending on their type, they are finally calculated and reconciled in the Sumclearing, Intradagclearing or Straksclearing system, the financial sector's retail payment systems. Settlement is subsequently effected through Kronos2 in accounts at Danmarks Nationalbank. The retail payment systems are owned by Finance Denmark.

Securities transactions may be entered into in different types of marketplaces, for instance the stock exchange, trading platforms or over-the-counter through a bank or broker. For professional investors, the subsequent settlement of transactions takes place on the trans-European securities settlement platform TARGET2-Securities (T2S), owned by the Eurosystem. Participation in T2S requires a dedicated cash account with Danmarks Nationalbank and a securities account with VP Securities (VP).

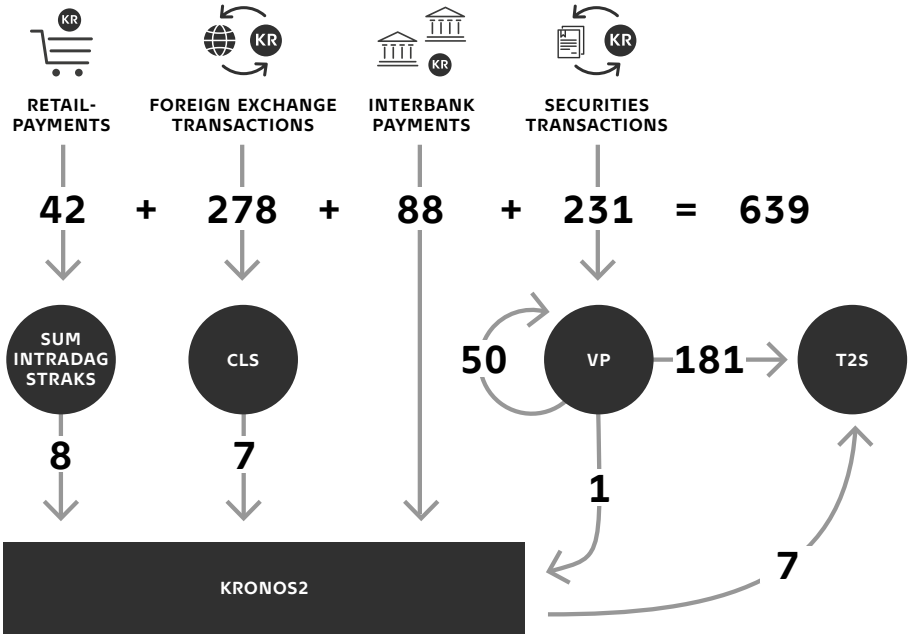
Hence VP, as the central securities depository (CSD), is responsible for regularly accounting for holdings of all Danish-issued securities on behalf of investors. Settlement of private investors' transactions takes place via VP settlement, VP's own settlement system.

Foreign exchange transactions are settled through CLS, an international system for foreign exchange transactions. Danmarks Nationalbank makes accounts available to banks settling transactions through CLS. CLS is owned by large, international banks.

The three retail payment systems, CLS and VP settlement settle their participants' net positions through accounts in Kronos2. Net positions are calculated by offsetting participants' claims and obligations in the respective systems. Netting reduces 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. 42 billion to kr. 8 billion, equivalent to a reduction of 81 per cent.

On T2S, settlement of professional investors' transactions is effected through so-called technical netting. Liquidity for settlement is transferred from participants' dedicated cash accounts with Danmarks Nationalbank and the settlement takes place in T2S.

Payment flows, kr. billion, averages per banking day in 2020



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.

However, due to the IT evolution, including, in particular, changes in the cyber threat landscape, infrastructure systems and solutions are constantly having to meet ever stricter requirements. In 2020, Danmarks Nationalbank focused on several areas of work in need of additional efforts, especially cyber resilience, crisis response, supplier management and organisation and governance in the corporations responsible for operating core infrastructure systems and solutions.

Covid-19 did not affect operational reliability
The operational reliability of the payments infrastructure was high in 2020 and not affected by the changing conditions during the covid-19 pandemic. Staff largely worked from home, and physical staffing levels were reduced to business-critical personnel, split into several teams to prevent potential spread of the virus. The resolution of any operational disruptions was coordinated through virtual meetings and remote communication.

SolarWinds attack hit the infrastructure
2020 saw the detection of one of the most comprehensive cyber attacks to date. A hostile actor had injected malicious code into updates of SolarWinds Orion, used by many private and public-sector organisations across the globe. The attack also hit the Danish financial infrastructure, but there are no indications that it caused any actual impact. As soon as the compromised updates of SolarWinds Orion were known, the relevant systems were contained and analysed.

The attack was not targeted at infrastructure systems, which may have helped to ensure that the incident was resolved without any real damage. The SolarWinds incident emphasises the need for effective cyber security measures to guard against the risk of cyber attacks via software provided by external suppliers. The SolarWinds Orion attack is described in more detail in Box 3.

Operational disruptions are inevitable, but must be managed effectively
Generally, the risk of operational disruption in and between complex IT systems is inevitable. Covid-19 and the SolarWinds attack are two examples of operational disruptions that were managed by the systems and solutions of the financial infrastructure. Technical disruption also occurs intermittently, for instance in connection with system updates or due to human error; however, such disruption typically

The SolarWinds Orion attack Box 3

In December 2020, it was revealed that SolarWinds, a leading supplier of network monitoring solutions, had suffered a security breach. An advanced and likely state-sponsored hostile actor had maliciously modified certain updates of the SolarWinds Orion application used by numerous organisations across the globe. Through the installation of a malicious update, unsuspecting customers had their systems trojanised.

Using the malicious "Sunburst" code in SolarWinds Orion updates, the hostile actor created a backdoor to about 18,000 private and public-sector organisations. In several known instances, this backdoor was used for further hacker attacks on specifically selected targets – especially in the USA where confidential information was accessed in several ministries and other institutions. But FireEye, a renowned IT security services firm, and Microsoft also found themselves subject to intrusions into their systems.

In one instance, the core Danish payments infrastructure was also hit, as a trojanised SolarWinds Orion update was installed. However, there are no indications that this backdoor was used. In the specific case, swift action was taken, and the servers on which the application was installed were shut down as soon as the problem was detected.

The critical utility infrastructure in Denmark was also hit by the SolarWinds Orion attack. The backdoor was installed in the IT systems of several major power companies, but there have been no indications to suggest that this backdoor was used. In their follow-up on the attack, the companies identified a need for enhanced data logging to ensure that incidents can be investigated. Therefore, Danish Energy has proposed that key companies in the Danish infrastructure must store data logging and network monitoring data for 12 months. Moreover, in the near future monitoring sensors will be installed at 200 power and utility companies to help protect IT systems from hacker attacks.

impacts system availability to a lesser extent. There have also been a few examples of major incidents with noticeable implications for consumers and corporations in Denmark.[2]

Overall, those responsible for the core infrastructure systems/solutions are well prepared to manage traditional operational incidents. For instance, systems are required to be operated from two separate and geographically independent data centres to facilitate rapid change of platforms in case of disruption in one of the centres. Regular testing is carried out to ensure that it is possible to change platforms and resume operations within two hours. The two-hour requirement helps to ensure that critical transactions can be completed on the agreed settlement day.

However, due to cyber complexity, ensuring an effective cyber crisis response is a particular challenge. The core infrastructure systems/solutions must continuously identify and assess various types of threats and vulnerabilities that represent potential sources of cyber risk. Crisis response plans, IT system recovery plans and continuity plans for critical business areas must be structured based on the key risks identified by the assessments. These plans must also be tested based on extreme but plausible scenarios that could be caused by a cyber attack.

Danmarks Nationalbank regularly oversees the work by core systems to devise specific plans to ensure quick and safe recovery following a cyber attack. Progress is continuously made, but Danmarks Nationalbank finds that there is still room for improvement.

Cyber threat presents a challenge

The cyber threat is complex and rapidly evolving. The SolarWinds attack exemplified the sophisticated techniques applied by the most advanced cyber threat actors. The evolution of the threat landscape means that cyber resilience is an area of work requiring persistent development and adaptation. It is a job that never ends.

The cyber security threat potentially poses a risk to the business of financial corporations. Therefore, it is essential that the top management, i.e. the executive board and the board of directors of the corporations, assumes responsibility for the development of the overall risk management framework. This is to ensure strategic focus and the proper priorities in the cyber resilience work. Management is also responsible for ensuring the clear, visible and practised division of responsibilities and work in the organisation between those responsible for operations, those responsible for control and compliance and the independent auditors (the three lines of defence) of the corporations.

Danmarks Nationalbank has initiated a process in which the core infrastructure systems are assessed against separate international cyber resilience guidelines.[3] The preliminary results of this work show that the current level of cyber resilience is generally high. Management involvement in cyber resilience work has increased substantially compared with observations from previous years, which is a positive trend. Assessments also indicate progress in other organisation and risk management in the corporations responsible.

But Danmarks Nationalbank's assessments also show that there is room for improvement in some areas. As already mentioned, Danmarks Nationalbank finds that there is room for improvement when it comes to quick and safe system recovery following a cyber attack. A related area that also needs more focus is data protection. Effective encryption and use of backup are to ensure that data is not corrupted or otherwise compromised in a cyber attack. If critical data is not available, this will substantially impact the systems' ability to restore operations.

Danmarks Nationalbank's cyber assessment recommendations are shared with systems managers at bilateral meetings. For security reasons, these recommendations are not published.[4]

2 One such example was problems at IBM in January 2014, which resulted in a prolonged disruption of the Dankort system (the national debit card scheme). Another example was a system error in Danmarks Nationalbank's payment system, Kronos2, which delayed payroll and social benefit payments in August 2018.

3 The cyber assessments are based on the CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures (*link*), supplementing the standards generally applied in Danmarks Nationalbank's oversight.

4 Publication of assessments is otherwise standard practice for other types of assessments, see Danmarks Nationalbank's oversight policy (*link*).

Focus on supplier management
Cyber attacks may also occur via infrastructure suppliers. So, it is essential that the core infrastructure systems/solutions adequately incorporate risks from suppliers in their own risk management. This ensures that the corporations responsible have a comprehensive overview and, by extension, a good basis for prioritising and addressing risks. Danmarks Nationalbank continuously focuses on overseeing that the systems/solutions address the risks inflicted on them by suppliers in a structured manner.

The absence of separate regulatory responsibility for control of critical IT service providers is an issue in its own right, which could be problematic given the key role of these service providers. Work on this pan-European issue is ongoing in the EU, and the European Commission has proposed new powers in the Digital Operational Resilience Act (DORA), see Box 4.

Broader collaboration on operational risks
Part of the work to mitigate cyber risks and increase operational resilience takes place at sector level and through various sectoral collaborations.

Since 2016, at the recommendation of Danmarks Nationalbank, those responsible for the core infrastructure systems, i.e. Danmarks Nationalbank's Kronos2 system, VP settlement and Finance Denmark's retail payment systems, have engaged in formalised collaboration in which interdependencies and cross-system operational risks are identified and addressed. This collaboration is to help ensure that effective emergency procedures are in place and that redundant connections are established between systems and to the infrastructure participants.[5]

The core systems/solutions also participate in Financial Sector Forum for Operational Resilience (FSOR), in which a number of key financial sector actors and authorities have been collaborating on various aspects of cyber resilience since 2016. Danmarks Nationalbank chairs and provides secretariat services for FSOR.

Digital Operational Resilience Act (DORA) Box 4

On 24 September 2020, the European Commission published a proposal for a regulation on digital operational resilience for the financial sector ("DORA"). This proposal reflects a strategic priority of the Commission's Digital Finance Package: the need to address challenges and risks associated with the digital transformation of society. Against that backdrop, DORA sets out comprehensive requirements for IT risk management by financial corporations.

The proposal covers most types of regulated financial activities. Some of the provisions of the proposal apply to the IT service providers of these corporations, including cloud computing service providers. However, system operators (as defined in the Settlement Finality Directive) are not included – inter alia because the most important payment systems are already subject to central bank oversight and related separate regulation.

DORA aims to update, consolidate and harmonise rules on IT risk management and incident reporting currently addressed by national and pan-European legislation and standards. Thus, the proposal includes rules on governance and organisation, identification, protection, detection and business continuity, along with monitoring, registration and classification of incidents and related reporting to national and pan-European supervisory authorities and the European Central Bank (ECB).

Moreover, new or more detailed rules are introduced on information sharing arrangements between financial corporations and responsible disclosure of incidents or major vulnerabilities. This also applies to testing and risk management of IT service providers (for instance, IT contracts with service providers are regulated). Also included are general requirements relating to testing of IT systems and requirements relating to threat-led penetration testing of key financial corporations.

DORA also proposes the establishment of pan-European supervision of critical IT service providers in the EU. The relevant supervisory authorities will have powers to conduct inspections and submit recommendations and impose periodic penalty payments on service providers (for instance if a request for information is not complied with).

As regards the further process, the European Commission has submitted the proposal to the European Parliament and the Council of Ministers for review and negotiation. The adoption process for this type of extensive legislation could take up to two years.

5 E-nettet, a management company owned by Finance Denmark, also participates in the collaboration in the role of responsible for the e-connect network, connecting data centres with the retail payment systems and Kronos2.

Applying a risk-based approach, FSOR seeks to support individual actors' cyber resilience efforts in order to improve overall infrastructure resilience. 2020 saw the launch of a project focusing on enhancing data protection levels and strengthening the ability for quick and safe system recovery following a cyber attack. Throughout the financial sector, these are areas in which increased focus is generally required, as shown e.g. by the survey on cyber resilience in the Danish financial sector conducted by Danmarks Nationalbank in 2020.[6] In this survey, 25 key financial sector actors and suppliers self-assessed their current level of cyber resilience, including all operational members of FSOR.

Another FSOR task is responsibility for a crisis response plan at sector level to supplement its members' own crisis response plans and the national crisis response under the National Operative Staff (NOST). The crisis response plan is regularly updated, based, for instance, on experience gained from the tests performed twice a year. These tests are designed to ensure that the crisis response plan works in practice in the event of a serious incident in the sector. The most recent test was performed in November 2020 when, for the first time, coordination across six sectors that are critical to society was tested in connection with a fictitious cyber attack. The exercise was orchestrated by the Centre for Cyber Security.

An in-depth review of FSOR's work can be found in the forum's annual report, available on the Danmarks Nationalbank website (*link*).

The core infrastructure systems/solutions also participate in TIBER-DK, Danmarks Nationalbank's Threat Intelligence Based Ethical Red-teaming test programme.[7] In a TIBER test, a simulated cyber attack is launched against the participants' live systems to detect and correct vulnerabilities before they are exploited by cyber criminals. Several of the key infrastructure corporations were among the first to undergo a TIBER test procedure.

Financial infrastructure is dynamic

Financial infrastructure evolves over time to improve the payment methods made available to consumers and corporations and enhance the safety and efficiency of systems and solutions.

Currently work is ongoing at the European level to create a payment market with safe, efficient and competitive cross-European payments. The average use of electronic payment solutions is substantially lower in the EU overall than, in Denmark. The Commission's work on a "Digital Finance Package" is described in detail in Box 5.

There is also a clear trend towards cross-border consolidation of business activities. In Denmark, this trend has been evidenced, for instance, by Nets' sale of clearing activities to Mastercard and subsequent merger with Italian Nexi. Similarly, VP Securities A/S, the Danish central securities depository, now forms part of the Euronext Group, one of Europe's largest securities infrastructure companies. Increasing consolidation is driven, among other factors, by a tougher competition environment and economies of scale, but it also secures more resources for security efforts, for instance in the cyber security area.

In 2020, Danmarks Nationalbank announced its plans to consolidate the settlement of payments in Danish kroner in TARGET Services, the European payment and securities settlement platform. This will pave the way for closer collaboration with other central banks in Europe and provide economies of scale from joint use of the IT platform, and will all else equal add more resources for security efforts, including cyber security. The project also involves connection to TIPS, a platform for instant cross-border

6 Similar surveys were conducted in 2016 and 2018.

7 Find more information about TIBER-DK on the Danmarks Nationalbank website (*link*)

consumer-to-consumer and consumer-to-business payments in Europe. The possibility of cross-currency instant payments in Europe is being explored under the auspices of TIPS. The migration to TARGET Services and connection to TIPS are expected to be completed in 2024/25. Also see Box 6 in the interbank payments section.

Another ongoing project is P27, under which six Nordic banks are working to establish a new common infrastructure for clearing and settling retail payments in and between Denmark, Sweden and Finland. The work on P27 is described in detail in the section on clearing and settlement of retail payments.

Danmarks Nationalbank closely monitors financial infrastructure developments and, regardless of the country location of systems, will make determined efforts to shoulder the regulatory responsibility in order to contribute to a safe and efficient payments infrastructure in Denmark.

New strategic measures in the European payment market Box 5

In September 2020, the European Commission published "Digital Finance Package", including a European retail payments strategy[1]. The Commission's vision is to create a payment market with safe, efficient and competitive cross-European payments, for instance through an efficient and coherent payments infrastructure and pan-European payment solutions.

Over the coming years, the focus will be on the Payments Services Directive (PSD2) review, and the possibility of promoting the use of an EU-wide digital ID solution is being explored in collaboration between the Commission and the European Banking Authority (EBA). The Commission will also look into citizens' access to central bank money, in part in the form of cash and in part by supporting the investigative work on digital central bank money initiated by the ECB.

Finally, the Commission and the ECB have actively supported the European Payments Initiative (EPI), which aims to create a pan-European payment solution for both cards and instant payments (for instance through a mobile phone app), and which also supports person-to-person payments across Europe. The EPI is a private partnership between 16 major European banks and a number of card acquirers, including Nets.

1. European Commission, 24 September 2020, "Retail Payments Strategy for the EU" (*link*).

Interbank payments

Interbank payments are payments between financial institutions. Such payments are typically characterised by being time-critical and of high-value. Interbank payments in Danish kroner are settled in Kronos2, Danmarks Nationalbank's real-time gross settlement (RTGS) system, which settles payments individually and immediately.

In addition to interbank payments, Kronos2 also settles monetary policy operations and net positions from connected payment and settlement systems.

Kronos2 is the backbone of the payments infrastructure, see Box 2.

Use
There are 83 Kronos2 participants, mainly Danish banks, mortgage credit institutions and branches of foreign banks.

In 2020, an average of just under 6,100 daily interbank payments with a total value of kr. 87.6 billion were settled in Kronos2 per banking day, see Table 1.

Operational reliability
Overall, the operational reliability of Kronos2 was satisfactory in 2020.

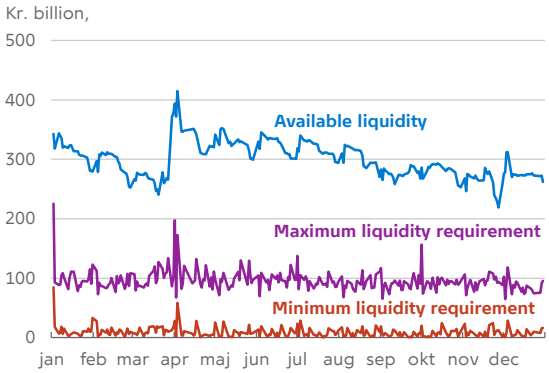
In a few incidents, Kronos2 was unavailable to some participants during the day. Emergency procedures ensured that critical payments were executed. A causal analysis has been performed, and measures have been implemented to prevent the recurrence of such incidents.

As part of the covid-19 crisis response, Kronos2 has been operated in split teams, based in different locations and not interacting physically with one another. The settlement of payments in Kronos2 has not been affected by the covid-19 pandemic.

Liquidity
Overall, participants had ample liquidity for settlement of payments in Kronos2, see Chart 1.

In March 2020, in connection with the coronavirus outbreak, Danmarks Nationalbank established an extraordinary lending facility to temporarily increase the access of monetary policy counterparties to liquidity, if needed.

Ample liquidity among Kronos2 participants in 2020 Chart 1



Source: Danmarks Nationalbank.

International standards
An assessment of Kronos2 against the CPMI-IOSCO Principles for Financial Market Infrastructures is being finalised. This assessment covers all areas of Kronos2 – both the legal basis, the overall organisation, IT security and the management of all risks that may arise in connection with payment settlements in Kronos2.

In 2021, Danmarks Nationalbank will also initiate an assessment of Kronos2's observance of the CPMI-IOSCO cyber security guidance, which elaborates on the cyber security aspects of the general CPMI-IOSCO principles.

Cyber resilience
In light of the evolving threat landscape, Danmarks Nationalbank is continuously working to strengthen the resilience of the Kronos2 systems.

Detection of anomalies that could signify a cyber attack is a key element in a strong cyber defence. Early detection enables faster response and mitigation of the impact of an attack. In 2020, Danmarks Nationalbank expanded its oversight capacity.

Cyber threat knowledge sharing from NFCERT and CIISI-EU also contributes to Danmarks Nationalbank's oversight of system and network vulnerabilities and anomalies.

Transactions in Kronos2 Table 1

Kr. billion, averages per banking day	2016	2017	2018	2019	2020
Interbank payments	**83.0**	**74.0**	**83.0**	**87.4**	**87.6**
- Of which customer payments	11.5	11.5	13.6	14.0	14.0
Monetary policy operations	**28.7**	**39.9**	**36.9**	**48.4**	**34.5**
- Of which sale of certificates of deposit	28.6	39.9	36.9	48.4	33.3
- Of which monetary policy lending	0.1	0.0	0.0	0.0	1.3
Transfers to settlement systems	**283.4**	**316.3**	**237.3**	**115.1**	**113.8**
- Of which to the Sumclearing, Intradagclearing and Strakscleaning	242.7	273.8	177.2	40.5	39.9
- Of which to VP settlement	31.7	32.5	40.6	46.4	41.2
- Of which to CLS	9.0	10.0	19.6	28.2	32.8
Net positions settled	**25.1**	**24.8**	**24.1**	**16.3**	**16.6**
- Of which Sumclearing, Intradagclearing and Strakscleaning	7.6	8.0	8.1	8.3	8.3
- Of which VP settlement	10.6	10.1	9.1	1.0	0.9
- Of which CLS	6.9	6.7	6.8	7.0	7.3

Danmarks Nationalbank has imposed restrictions on the use of a specific message type for transmitting payments from Danmarks Nationalbank's accounts. These restrictions help reduce the risk that a hacker will succeed in stealing funds from Danmarks Nationalbank's accounts.

Danmarks Nationalbank is still in the process of implementing the CPMI endpoint security strategy and has, inter alia, introduced the requirement that all Kronos2 participants connected through SWIFT must comply with the SWIFT Customer Security Programme's IT security requirements. This includes the largest Kronos2 participants.

System updates

In 2020, Danmarks Nationalbank's Extreme Contingency Facility (ECF) was tested with the largest Kronos2 participants. ECF is the solution designed to ensure that the settlement of payments will continue in the event that Kronos2 is affected by a serious incident or failure. The test performed increased the certainty that the settlement of payments can be handled in crisis situations. Danmarks Nationalbank will develop the ECF solution further and is planning to test the solution with the entire financial sector in 2021.

In 2020, Danmarks Nationalbank decided to migrate the settlement of Danish kroner to the new European consolidated payment and securities settlement platform TARGET Services in 2024/25. See Box 6.

Danish kroner on European and future-proof infrastructure

Box 6

In 2020, based on a preliminary analysis, risk assessment and dialogue with the financial sector, Danmarks Nationalbank decided to migrate the settlement of Danish kroner to the new European consolidated payment and securities settlement platform TARGET Services in 2024/25. Migration of Danish kroner to TARGET Services will ensure:

- a single platform for the settlement of Danish kroner
- strengthened information security and a common front against cyber threats
- a harmonised infrastructure with increased operational benefits in relation to maintenance and further development

TARGET Services consists of the TARGET2 payment system, the TARGET2-Securities (T2S) settlement system and the TARGET Instant Payment System (TIPS). Currently, TARGET2 supports only the settlement of euro payments, but as part of the European project to consolidate the three systems on a single platform, TARGET2 will be modernised and renamed T2, which will be able to support multiple currencies.

Since 2018, some of the Danish securities transactions have been settled in T2S. This made Danish kroner the first currency to use the T2S-system's multiple currency functionality. Following the migration of the settlement of payments in Danish kroner to TARGET Services, Kronos2 will be replaced by T2. Moreover, Danish kroner will be connected to TIPS, consolidating all settlements involving payments in Danish kroner in TARGET Services.

Substantial economies of scale and ongoing operational savings will be achieved by consolidating the Danish krone and securities settlement in TARGET Services rather than using the current solution. Furthermore, Danmarks Nationalbank, the Eurosystem and other participating central banks will be able to join forces against future cyber threats and collaborate on further developing the overall European payments infrastructure.

Access to TARGET Services is subject to high protection and security requirements, placing high demands on connected banks and users of the platform. All participants wanting direct access to TARGET Services must sign an agreement with one of the two prequalified network suppliers authorised to offer access. At any rate, participants in the euro settlement must sign an agreement with one of the prequalified network suppliers and may also use this access for the settlement of Danish kroner.

The consolidated TARGET Services will also support a new financial messaging format, ISO20022, which must be fully implemented by all payment systems by the end of 2025.

The migration of Danish kroner to TARGET Services will place Denmark in a stronger position with influence on the European payments infrastructure, and enhanced harmonisation will open up new longer-term opportunities in the payments area. In other words, the migration of Danish kroner to TARGET Services will streamline and future-proof Danish payment systems – in a Danish, Nordic and European context.

Denmark is a frontrunner in the instant payments area, and the migration of Danish kroner to TIPS will bring about significant new opportunities. In 2020, the Eurosystem decided that TIPS will be the settlement platform for all instant payments in euro. Enhanced harmonisation of instant payments is achieved by consolidating instant payments in multiple currencies on TIPS, including Danish kroner. This forms the basis of cross-currency instant payments for participating currencies in the longer term – a possibility that is being explored by a separate working group chaired by the ECB.

Danmarks Nationalbank has set up a project group which, in partnership and coordination with the ECB, the operator 4CB (the four central banks in Germany, France, Italy and Spain), the sector and other payments infrastructure system owners, will provide the framework for future settlement of payments in Danish kroner in TARGET Services. Danmarks Nationalbank and the Eurosystem must enter into Currency Participation Agreements (CPAs) on the settlement of payments in Danish kroner in T2 and TIPS. The existing T2S CPA is expected to continue.

A reference group and a sector group have been set up, consisting of sector representatives and representatives from Danmarks Nationalbank, to closely monitor the development project in all of its phases over the coming years. As part of the project launch, working groups with participation of sector experts were established. These working groups are to clarify liquidity and technical aspects of the new solution. Additional groups may be added during later stages of the project – for instance in connection with major sector testing etc. In early 2021, information meetings for interested account holders were also held.

Retail payments

In Denmark, most payments are made using electronic payment solutions such as the Dankort, MobilePay, online banking transfers and Betalingsservice (direct debit payment) etc. In 2020, the value of transactions by corporations and consumers averaged kr. 28.8 billion per day.[8]

Danmarks Nationalbank oversees the most important payment solutions in Denmark, see Box 7.

Over an extended period of time, the use of cash as a means of payment has been steadily declining. The share of cash in total payments in physical trade (for instance in supermarkets) decreased from 48 per cent in 2009 to 16 per cent in 2019.[9] In 2020, the coronavirus pandemic seems to have reinforced this trend.[10]

With the shift away from cash, electronic payment solutions are becoming increasingly important – including the solutions overseen by Danmarks Nationalbank.

Operational reliability
The operational reliability of the Dankort and Betalingsservice systems was high in 2020.

There were only minor incidents during the year, which did not affect consumers' ability to use the Dankort and Betalingsservice systems. As far as the Dankort system is concerned, minor disruptions were seen in the use of the *Dankort Secured by Nets* security solution in online transactions. Betalingsservice experienced a brief spell of problems with creditor access to the BS Creditor portal.

Operational reliability has not been impacted by the coronavirus pandemic. To prevent covid-19 infection and ensure daily operations, all Dankort and Betalingsservice employees have been split into two teams, only one of which may work from the office at a time. However, as far as possible, all employees are working from home.

Danmarks Nationalbank's oversight of payment solutions Box 7

Danmarks Nationalbank oversees the most important Danish payment solutions, currently Dankort, Betalingsservice and credit transfers (through oversight of the retail payment systems).

Danmarks Nationalbank regularly considers whether targeted oversight of other payment solutions in the Danish market is required. MobilePay is a growing payment solution. But turnover for MobilePay is still substantially lower than for the Dankort and Betalingsservice solutions and credit transfers. Average daily turnover for MobilePay was kr. 0.3 billion in 2020.[1] By comparison, Dankort payments totalled kr. 1.1 billion per day.[2]

1. MobilePay (*link*).
2. Nets' statistics for the Dankort.

Nets' sale of Betalingsservice to Mastercard
In August 2019, Mastercard entered into an agreement with Nets to acquire, inter alia, Betalingsservice. The requirements of the European Commission for approval of the agreement have been fulfilled, and the acquisition was closed in March 2021 (see also the section below on clearing and settlement of retail payments).

Nets and Mastercard have entered into a service agreement to help ensure the continued smooth, secure and stable operation of Betalingsservice. This means that, for a transitional period of up to three years after the acquisition, Mastercard will be able to obtain assistance from Nets to ensure that Betalingsservice will run smoothly.

8 The value of the transactions in the retail payment systems as calculated per calendar day, cf. the section *Clearing and settlement of retail payments.*

9 Danmarks Nationalbank, *Cash payments are declining*, 26 February 2020 (*link*).

10 Danmarks Nationalbank, *Payments before, during and after the corona lockdown*, 16 September 2020 (*link*).

Going forward, the oversight of Betalingsservice will be directed at Mastercard.

Merger of Nets and Nexi (and SIA)
In November 2020, Nets and Nexi signed a binding merger agreement. The European Commission approved the merger in March 2021, and Nets and Nexi expect to close the deal in the 2nd quarter of 2021.

The plan is then for the new consolidated company to complete the merger with SIA previously agreed by Nexi and SIA (independently of the merger of Nets and Nexi). However, the merger is subject to approval by the relevant authorities. Nets expects the consolidated company (Nets, Nexi and SIA) to be in place in the 2nd half of 2021.

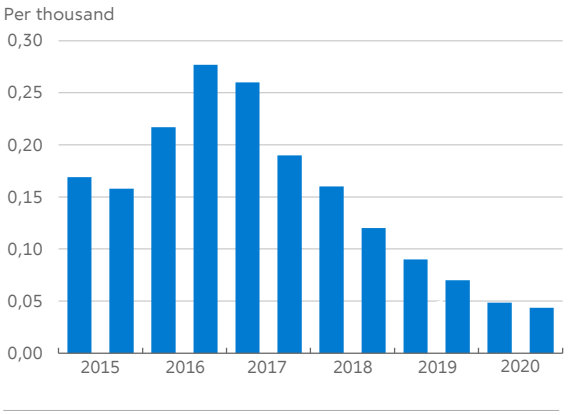
According to the three companies, the purpose of the mergers referred to above is to create a large, financially strong actor in the European payment market offering a broad range of solutions to banks and businesses across Europe – with a focus on the transition to digital payments.

Dankort will remain a part of Nets Denmark, which is part of the merger with Nexi. The merger will not have any immediate impact on Dankort and Danmarks Nationalbank's oversight of Dankort.

Sharp decline in Dankort fraud
According to Nets, Dankort fraud totalled kr. 17.9 million in 2020, corresponding to 0.05 per thousand of total consumption.[11]

The incidence of fraud decreased by a total of 42 per cent from 2019 to 2020. More specifically, the incidence of Dankort fraud in online transactions declined by 35 per cent from 2019 to 2020, while the incidence of Dankort fraud in physical trade was almost halved during this period (49 per cent reduction).[12] In other words, the positive trend seen in recent years with a substantial reduction in the incidence of Dankort fraud continued, see Chart 2.

Fraud as a proportion of total Dankort-based consumption Chart 2



Source: Nets

The reduction in the incidence of Dankort fraud in 2020 is attributable to several factors, one of which is believed to be the restrictions imposed due to the coronavirus pandemic. The lockdown of, for instance, nightlife venues has made it more difficult for criminals to steal Dankort cards.[13]

Nets, the police and banks have established regular collaboration to identify and monitor the ATMs often used by criminals after having glimpsed the PIN of the victims and stolen their cards. Nets has also expanded its systems for monitoring suspicious conduct. Nets has pointed out that these measures have helped to curb the incidence of fraud.

The contactless Dankort solution, used in more than three out of four Dankort transactions, may also have played a role. As shoppers generally do not need to enter their PIN for contactless payments below kr. 350, the criminals cannot catch a glimpse of the PIN. At the same time, the covid-19 pandemic seems to have boosted the use of contactless payments.[14]

11 Nets' statistics on Dankort fraud
(Note: Nets' data on fraud is not directly comparable with Danmarks Nationalbank's statistics on payment card fraud, which cover both Dankort and international cards used in Denmark.)

12 Nets' statistics on Dankort fraud.

13 Via Ritzau, *Nets: Dankort fraud halved (in Danish)*, 10 August 2020 (*link*).

14 Via Ritzau, *Nets: Corona fear boosts contactless payments (in Danish)*, 18 November 2020 (*link*).

Regulation and derived measures for secure payments

1 January 2021 was the deadline set by European supervisory authorities for the implementation of the PSD2 requirement of strong customer authentication (i.e. two-factor authentication)[15] of online card payments.[16]

The Danish Financial Supervisory Authority has announced that, from 11 January 2021, they expect banks and other card issuers to start declining card payments that have not been approved by strong customer authentication.[17]

In preparation, during 2020, Danish online stores were rolling out the *Dankort Secured by Nets* security solution with a requirement for use of a one-time SMS code for online Dankort purchases above a specified amount. From 2021, the security of *Dankort Secured by Nets* has been enhanced due to the PSD2 requirements stated above. Since the New Year, two-factor authentication by one of the following procedures has been a requirement for online Dankort transactions:

1. A one-time SMS code and a password.
2. NemID user name and password with verification through the NemID key app or the NemID key viewer.

In addition to this enhancement of security, PSD2 has also lowered the spending limit for when *Dankort Secured by Nets* must to be applied, from kr. 450 to kr. 225, from the start of 2021. These measures will presumably help curb the incidence of Dankort fraud in future.

International standards

During 2020, Nets continued its follow-up on Danmarks Nationalbank's assessment of Betalingsservice's observance of ECB standards[18]. Nets has addressed most recommendations and remarks in the assessment, but in three respects it has proved difficult to finalise the relevant projects due to covid-19-related obstacles. This applies to efforts to strengthen IT risk management, network monitoring and management of critical suppliers. Danmarks Nationalbank followed up on these issues at the quarterly meetings with Nets.

15 Strong customer authentication is a control measure under which at least two factors must be used to approve a payment. The two factors must be something the payer knows (e.g. a PIN), something the payer has (e.g. a mobile phone for receiving a one-time code) or something the payer is (e.g. a fingerprint) – cf. the EU Regulation on strong customer authentication and common and secure open standards of communication (*link*).

16 Finance Denmark, Facts on new EU rules on payments (in Danish), 28 December 2020 (*link*).

17 Danish Financial Supervisory Authority, *Danish online stores must be ready for new EU rules starting on 1 January 2021 (in Danish)*, 21 October 2020 (*link*).

18 Danmarks Nationalbank, Betalingsservice Assessment, *Danmarks Nationalbank Report*, no. 4, October 2019 (*link*).

Clearing and settlement of retail payments

Danish retail payments are cleared and settled in the Sumclearing, Intradagclearing and Straksclearing systems, also known as the retail payment systems. The systems are owned by Finance Denmark and operated by Mastercard.

The Sumclearing system is used for clearing of e.g. card and Betalingsservice payments once a day on banking days. The Intradagclearing system is used for clearing of credit transfers such as 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.

In the Straksclearing system, 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 interbank exchange of liquidity takes place six times a day on banking days. The Straksclearing is used for online banking transfers and payments via MobilePay.

Use

There are 50 direct participants in the retail payment systems and 25 indirect participants, who settle via direct participants.

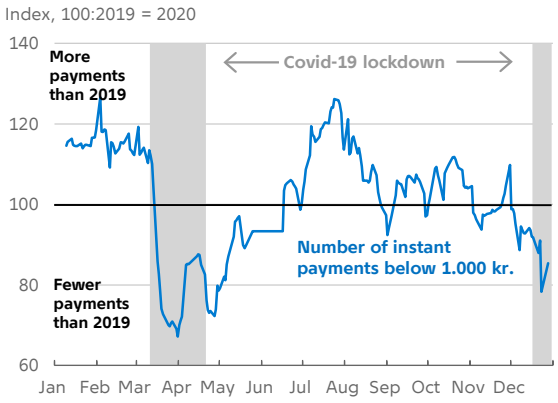
The value of transactions in the systems averaged kr. 42.2 billion per banking day in 2020, see Table 2.

During covid-19 lockdowns in March and December, the number of instant payments below kr. 1,000 declined, see Chart 3. The Straksclearing system is used, in particular, for person-to-person payments, for instance through MobilePay. So, the lockdowns did affect that type of payments to some extent.

Operational reliability

Retail payment system operations were satisfactory in 2020. However, there were a few incidents during the year. For instance, a number of payments were delayed when a small bank – in a voluntary resolution process – did not have sufficient liquidity after transferring its funds to an account with another bank as part of the resolution process. The incident has been followed up to prevent a recurrence in future bank resolutions.

Drop in number of instant payments below kr. 1,000 during the covid-19 lockdowns Chart 3



Note.: Index=100: 2019 equals 2020. This means that the development through 2020 is compared with the development through 2019. The series shows a seven-day moving average with the last observation. Adjusted for public holidays in 2019 and 2020, respectively, except for the period 25 May to 16 June for which an average has been applied to avoid outliers.
Source: Nets.

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

Kr. billion, average per banking day	2016	2017	2018	2019	2020
Sumclearing	17.2	17.8	18.3	19.2	18.7
Intradagclearing	18.4	19.7	20.1	20.8	21.9
Straksclearing	0.8	0.9	1.2	1.4	1.6
Total	36.4	38.4	39.6	41.4	42.2

Source: Nets.

In connection with covid-19, staff that must be physically present on site to manage operations have been split into several teams to prevent potential spread of the virus. Moreover, a special information crisis response system has been set up between Finance Denmark, e-nettet, Mastercard and the data centres.

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 will be postponed, and new net positions are calculated for the other participants, who risk not receiving the expected liquidity.

Most of the participants use the automated liquidity management tools of the systems, and in addition to the above incident there has only been one case in 2020 where a participant's settlement was postponed due to lack of liquidity.

International standards
Danmarks Nationalbank is in the process of assessing the retail payment systems' observance of the CPMI-IOSCO cyber security guidance. The assessment is expected to be completed in 2021.

Finance Denmark has previously reviewed the cyber security requirements. Against that backdrop, Finance Denmark has initiated work to strengthen the cyber resilience of the retail payments infrastructure. Among other measures, a cyber security rulebook has been prepared, describing IT security requirements to be implemented and reported on by participants.

System updates
In the past, there have been examples of incidents in the night-time settlement that have significantly delayed entry to customers' accounts. Therefore, night-time settlement has been adjusted 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 gives the data centres more time to complete their book-entry before the start of the day.

In the Straksclearing system, liquidity for bank payments is reserved automatically 24/7. To mitigate the risk of rapid liquidity outflows from a participant, for instance as a result of a cyber attack, the time interval for reservation of new liquidity has been changed from every 15 minutes to every two hours. Moreover, participants have been given the opportunity to set their own individual time intervals for reservation of new liquidity and a backstop for the number of times new liquidity may be reserved between two settlement blocks.

Mastercard assumed responsibility for the operation of the retail payment systems
In August 2019, Mastercard entered into an agreement with Nets on the acquisition of, among other things, Nets' retail payment systems.

The European Commission's competition authority approved the deal subject to the condition that Nets' instant payments technology be licensed to a third party with exclusivity to offer the solution within the EEA.

Since then, Nets and Mastercard have obtained the requisite approvals from the relevant competition and supervisory authorities, and the European Commission's condition for closing the deal has been fulfilled. So, in March 2021 Mastercard assumed responsibility for the operation of the retail payment systems.

Danmarks Nationalbank and the system owner, Finance Denmark, as well as Nets and Mastercard all focus on ensuring that operations of the retail payment systems are not affected by the transfer to Mastercard.

P27 – common retail payment system for Denmark, Sweden and Finland
Six Nordic banks collaborate on the establishment of a Nordic infrastructure, known as P27, for clearing and settlement of retail payments in and between Denmark, Sweden and Finland.[19] The banks have established the company P27 Nordic Payments in

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

Sweden, which will manage P27. In addition, the banks have chosen Mastercard as the supplier responsible for the development and operation of the system.

Being a foreign company, P27 will not automatically be subject to Danish law and Danmarks Nationalbank's powers of supervision and oversight[20]. Therefore, efforts are being made to ensure that there will be adequate supervision and oversight of clearing and settlement of retail payments in Danish kroner.

The parties are discussing a model in which P27 will incorporate a provision into their contractual agreements with the banks, stipulating that clearing and settlement of Danish kroner in P27's system will be governed by Danish law. This will make settlement subject to Danmarks Nationalbank's powers, and oversight may be directed at P27's Swedish-based company.

The P27 project is also being discussed by the Nordic central banks and financial supervisory authorities. It is the ambition to establish a Nordic cooperation on oversight and supervision.

Danish instant payments in TIPS

In 2020, the ECB continued the development of TIPS, the ECB's system for instant payments. TIPS is part of the ECB's consolidation project and will be consolidated with TARGET2 and T2S on a single platform in TARGET Services.

With Danmarks Nationalbank's decision to migrate the settlement of Danish kroner to TARGET Services, Danish kroner will also be connected to TIPS, enabling settlement of Danish instant payments in TIPS.

Sveriges Riksbank has also decided to join TIPS, and from mid-2022, Sveriges Riksbank's instant payments system will be settling payments in TIPS. Furthermore, Sveriges Riksbank and the ECB are exploring the possibility of developing a cross-currency functionality to enable account holders in different countries to send and receive cross-currency instant payments, see Box 8.

TIPS to develop cross-currency functionality Box 8

The ECB and Sveriges Riksbank are exploring the possibility of developing a cross-currency functionality in TIPS to enable account holders across currencies to send and receive instant payments.

To this end, it is being examined whether a central exchange hub may be connected to TIPS to ensure that the sender of a cross-currency payment gets the best possible exchange rate in the market. The ambition is a fully automated procedure in which an instant payment may be settled in less than 10 seconds, regardless of whether the payment is a national or a cross-currency payment.

The ECB and Sveriges Riksbank expect to decide in 2021 whether to proceed with the project and envisaged implementation in 2023. If the project is realised, cross-currency payments will be an option for Danish account holders when Danish kroner migrate to TARGET Services in 2024/25.

The work is anchored in a working group in which Danmarks Nationalbank participates.

20 Under the Danish Capital Markets Act (*Kapitalmarkedsloven*), the duty of supervision of the retail payments system rests with Danmarks Nationalbank. The Capital Markets Act stipulates that Danmarks Nationalbank oversees payment systems of major significance to the settlement of payments.

Securities settlement

Securities transactions may be entered into in different types of marketplaces, for instance the stock exchange, trading platforms or over-the-counter through a bank or broker. The final settlement of transactions, i.e. the exchange of funds and securities in participants' accounts, takes place in VP settlement and TARGET2 Securities, T2S.

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.

In July 2020, the Danish Financial Supervisory Authority approved Euronext Group's acquisition of VP, which has, since then, been part of the pan-European stock exchange and market infrastructure group. Euronext has corporations in a number of European countries, including central securities depositories in Norway, Portugal and now also in Denmark.

T2S is a European securities settlement platform. Since October 2018, a large portion, in value terms, of the securities settlement in Danish kroner has taken place in T2S. T2S is owned by the Eurosystem and operated by the 4CB (the four central banks of the largest euro area countries), with the ECB as coordinator. Settlement of krone transactions in T2S is carried out through VP, which is connected to T2S in its capacity as central securities depository. Danish kroner for the money leg of the transactions are transferred from the participants' accounts at Danmarks Nationalbank.

Use

The VP settlement system has 110 participants, of which 56 are non-resident market participants, including four CCPs, see Box 9. Settlement of securities transactions between professional participants takes place on T2S, while private investors' securities transactions are settled on VP's own platform.[21] So, large, high-value transactions are typically settled in T2S, while the highest number of transactions is settled in VP settlement.

Central counterparties (CCPs) Box 9

A CCP intermediates between the parties to a securities transaction, taking on the risk for both the buyer and the seller from the transaction date until the transaction has been finally settled. The four foreign CCPs in VP – EuroCCP, LCH Clearnet and Six X-clear – clear equities transactions, while Nasdaq Clearing clears repo transactions. Regulatory control of CCPs is conducted in collaboration with supervisory colleges consisting of authorities from the countries in which, based on objective criteria, the respective CCPs have been deemed as systemically important, see the EMIR Regulation.[1]

Currently, Danmarks Nationalbank does not participate in any supervisory colleges because the value of cleared transactions in Danish kroner is relatively low compared with that of other currencies in the four CCPs settling transactions in VP. The Danish Financial Supervisory Authority participates in the supervisory colleges of Nasdaq Clearing and EuroCCP.

1. 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.

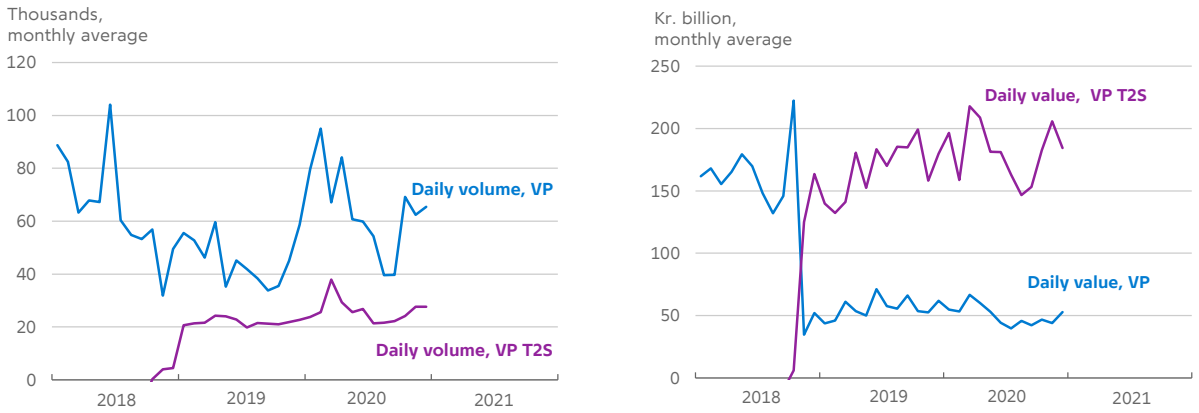
Securities transactions totalling an average of kr. 231.5 billion per banking day were settled in 2020, see Table 3, a record level. A driving factor was a surge in market activity at the start of the year when covid-19-related uncertainty impacted investor sentiment. In the course of the summer and autumn, activity slowed, only to pick up again towards the end of the year.

Equity trading showed a particular increase relative to the previous year. In terms of value, equities totalling kr. 8.7 billion more than the previous year were traded on average per banking day, up 25 per cent, while the number of transactions rose by close to 50 per cent. In other words, the increase was primarily driven by many small equity transactions between private investors, which is reflected in the sharp increase in the number of transactions settled on VP's platform, see Chart 4.

21 See Oversight of the financial infrastructure 2018, page 15, for a more detailed description of VP settlement in T2S (*link*).

Number and value of securities transactions

Chart 4



Note: The left-hand chart shows the number of transactions settled, while the right-hand chart shows the value of transactions, calculated based on the market value of the securities transferred from the seller to the buyer.
Source: VP.

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

Table 3

	I alt		Obligationer		Aktier		Investerings-foreningsbeviser	
Year, average per day	Number of trans-actions, thousand	Value, kr. billion	Number of trans-actions, thousand	Value, kr. billion	Number of trans-actions, thousand	Value, kr. billion	Number of trans-actions, thousand	Value, kr. billion
2017	66.9	162.7	2.7	118.4	32.4	36.6	31.8	7.7
2018	65.5	168.5	2.6	119.0	29.4	40.8	33.5	8.8
2019	67.0	223.1	4.2	180.7	33.0	34.8	29.8	7.6
2020	90.5	231.5	3.8	178.1	49.0	43.5	37.7	9.9

Note: The number and value of transactions have been calculated collectively for VP and VP on T2S. 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.

Operational reliability

Overall, operational reliability in the settlement of Danish securities transactions was satisfactory in 2020, but there were several incidents.

During the covid-19 pandemic, both VP and T2S staff largely worked from home, and on-site staffing levels were reduced to only business-critical personnel for both systems. The changed conditions did not affect system operations, and the incidents that did occur were managed for instance through virtual meetings and remote communication.

In March, covid-19-related uncertainties resulted not only in higher trading activity in Denmark, but also in a sharp increase across European securities markets. The rise in the number of transactions caused capacity pressures in the settlement in VP and T2S. Therefore, both systems had to add additional capacity to be able to cope with the rising transaction volumes.

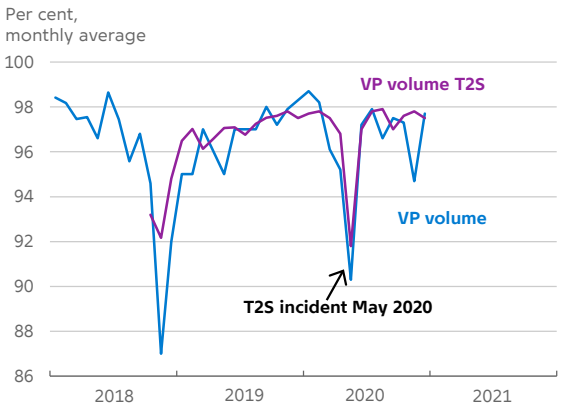
In May, a technical error in T2S led to issues in the platform's business controls. When the error was detected and resolved, erroneous entries had already been made. Therefore, several of the central securities depositories connected to the T2S platform, including VP, had to carry out correcting activities. For several attemps, VP had to wait for sufficient and necessary information from T2S to get up running again, and as a result VP had to block the settlement of 99 ISINs for 55 hours until correct data had been received from T2S.

This was a serious incident, and T2S subsequently performed extensive analyses to map its causes. Measures have been implemented to prevent similar incidents in future. VP has also prepared a report, assessing VP's management of the incident, among other things.

In September, VP had to ask the ECB to postpone the start of the night-time settlement due to T2S connectivity issues. The ECB granted VP's request, and VP managed to send all messages to T2S, meaning that the settlement could start and be conducted with a limited delay. The incident occurred on the night before the start of a new quarter, making it particularly critical due to large settlement volumes from mortgage refinancings. A long delay would have caused the mortgage refinancings to be late. VP subsequently identified the cause of the incident: a software error that was subsequently resolved and tested.

Settlement ratio

Chart 5



Note: In the chart, the settlement ratio is based on the number of transactions (trading volume).
Source: VP.

Settlement ratio

The settlement ratio indicates the percentage of the transactions settled in a timely manner. According to Article 5 of the Central Securities Depositories Regulation (CSDR),[22] all securities transactions traded on a trading venue must be settled two days after the transaction date.

Chart 5 shows the settlement ratio for VP's own system and for VP's settlement in T2S. The low level at the end of 2018 was due to a number of incidents occurring in the weeks following VP's connection to T2S. As the issues were resolved, the settlement ratio stabilised at a level similar to VP's pre-T2S migration level, only to drop sharply in May 2020. The underlying cause was the serious T2S incident described above, which delayed the settlement of a large num-

22 Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories.

ber of transactions. The low VP settlement ratio towards the end of 2020 was due to a relatively large number of new share issues to be settled in the month of November.

Penalties
A pan-European penalty system is being developed in the T2S platform designed to sanction participants whose transactions cannot be settled in a timely manner due to a lack of securities or liquidity. If the transactions of a participant are not settled in a timely manner, this may cause problems for that participant's counterparties, which may not be able to meet their obligations as a result. A penalty system can help to discipline participants so that they make sufficient funds and securities available for settlement.

In 2020, work on the pan-European penalty system, which was already delayed, was delayed further by the challenges posed by the covid-19 pandemic. At this point, the system is not expected to be commissioned until the 1st quarter of 2022. VP has suspended its penalty system pending the entry into force of the new system, in order for VP to follow the pan-European standard.

International standards
Danmarks Nationalbank oversees VP and participates in the joint European oversight of T2S, led by the ECB.

In 2016, four recommendations were issued to VP in connection with Danmarks Nationalbank's assessment of the VP settlement system's observance of the CPMI-IOSCO Principles for Financial Market Infrastructures. VP has complied with three of the recommendations, while the final recommendation, relating to VP's recovery plan, must be reassessed following the changes in VP's ownership. Primary responsibility for the assessment rests with the Danish Financial Supervisory Authority, which, as the competent authority, supervises VP's compliance with the requirements of the pan-European Central Securities Depositories Regulation (CSDR) for financial recovery plans.

As prescribed by the CSDR rules, the recovery plan has been presented to the Danish Financial Supervisory Authority, and the plan has subsequently been approved by VP's Board of Directors.

In 2020, under the auspices of the ECB, Danmarks Nationalbank participated in an assessment of T2S based on a selection of the CPMI-IOSCO principles. This assessment, completed in 2019, has not been published, but Danmarks Nationalbank participated in the work.

Cyber resilience
In 2020, Danmarks Nationalbank completed an assessment of VP's compliance with the CPMI-IOSCO cyber guidance. This assessment shows that VP has a high level of maturity and complies with the cyber guidance in most respects. VP and Danmarks Nationalbank have agreed on a process for the 1st half of 2021 for follow-up on the recommendations issued by Danmarks Nationalbank in the assessment.

In 2020, Danmarks Nationalbank also contributed to the assessment of T2S against the Cyber Resilience Oversight Expectations (CROE), which is the ECB's implementation of the CPMI-IOSCO cyber guidance. The assessment, conducted under the auspices of the ECB, is expected to be completed in 2021.

System updates
Following acquisition by Euronext, VP is aligning its organisation and processes with those of Euronext. This also involves the consolidation of services and business models offered across the group. There are no current plans to roll out a joint IT platform for the three central securities depositories in Denmark, Norway and Portugal, all of which are part of the Euronext Group.

Payments and securities settlement in euro

Payments and securities transactions by Danish banks in euro are settled in TARGET2 and TARGET2-Securities (T2S), owned and operated by the Eurosystem.

TARGET2 is the trans-European RTGS system for the settlement of large, time-critical payments in euro. In TARGET2, liquidity is also transferred for the settlement of other euro systems, including T2S. T2S is the trans-European system for settlement of securities transactions in euro and in Danish kroner.[23]

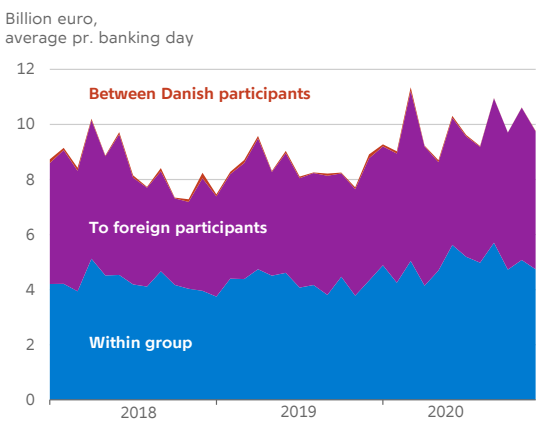
Use

More than 1,000 banks use TARGET2 for the settlement of euro payments, including 22 Danish participants. In 2020, Danish participants' daily interbank payments averaged kr. 9.8 billion euro. Danish participants use TARGET2 mainly for intergroup payments and payments to non-resident participants, see Chart 6. Exchange of euro mostly takes place with participants in Germany, Finland, France and Belgium.

A total of 21 central securities depositories from 20 countries now settle via T2S, including VP. A bank may settle via T2S as either a direct participant, if the bank has a so-called Dedicated Cash Account, or as an indirect participant via another participant's access.

A Dedicated Cash Account must be set up through one of the central banks in the EU. Fifteen Danish participants hold a Dedicated Cash Account in euro at Danmarks Nationalbank for payment in or receipt of euro in connection with T2S settlement. Other Danish participants may have set up a Dedicated Cash Account through other EU central banks.[24]

Interbank payments in TARGET2 Chart 6



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

Operational reliability

The operational reliability of the local TARGET2 components for which Danmarks Nationalbank is responsible was satisfactory in 2020.

In 2020, one serious incident occurred in the Eurosystem's TARGET2. Following an operational disruption of TARGET2 on Friday, 23 October, payments could not be settled and liquidity could not be transferred to or from the connected systems, including T2S, for several hours. TARGET2 has several data centres, and operations were resumed after a switch of operations to a centre in another region. The incident was

23 T2S can handle multiple currencies. Besides the euro, Danish kroner is the only other currency connected to T2S. Read about the settlement of Danish kroner in the section *Securities settlement*.

24 As euro cannot be deposited permanently in Dedicated Cash Accounts, banks must also have access to a TARGET2 account to which euro can be transferred at the end of the settlement day. Most of the Danish banks have concluded agreements with correspondent banks, while some of the largest banks have established a TARGET2 account through their branch in a central bank in the euro area.

caused by a network error that impacted the TARGET2 infrastructure. The ECB is taking steps to reduce the risk of a recurrence.

There were few major incidents on the T2S platform in 2020. Given that these incidents also impacted the settlement of securities transactions in Danish kroner, they are described in the securities settlement section above.

International standards
Oversight of TARGET2 and T2S takes place in collaboration with the EU central banks. Danmarks Nationalbank participates in the joint oversight headed by the ECB which takes place in working groups with the participation of the national central banks.

In 2020, Danmarks Nationalbank participated in various assessments of T2S's compliance with international standards for securities settlement systems. These efforts are described in more detail in the securities settlement section above.

System updates
In 2016, the ECB initiated a major project to modernise the European payments infrastructure and has been working to consolidate TARGET2, T2S and TIPS on a single IT platform since then. The aim is to meet new market requirements and optimise participants' liquidity management across all TARGET Services.

The consolidation was scheduled to take effect in November 2021, but has been postponed for one year until November 2022. The rationale for the decision to postpone was a request from the entire European financial industry, requesting postponement due, among other factors, to the covid-19 pandemic and SWIFT's delayed global migration of cross-border payments to the ISO 20022 format from November 2021 until end-2022.

In March 2020, TARGET2 participants began the software development needed to adapt their internal systems to the new consolidated platform.

Settlement of foreign exchange transactions

A foreign exchange transaction consists of two opposite payment instructions in two different currencies. Foreign exchange transactions can be settled bi-laterally via correspondent banks or via the international foreign exchange settlement system, CLS, which settles payment instructions in 18 participating currencies. The vast majority of foreign exchange transactions in Danish kroner are settled in CLS.

CLS Bank International (CLS) is owned by large, international banks. CLS reduces the settlement risk associated with foreign exchange transactions because CLS settles the two payment instructions in a foreign exchange transaction simultaneously (Payment-versus-Payment, PvP).

Danmarks Nationalbank participates in the cooperative oversight of CLS, cf. Box 10.

Use

Both financial institutions and firms participate in the CLS settlement of Danish kroner. Only one Danish bank participates directly in CLS settlement. Those who are not direct participants can settle foreign exchange payment instructions in CLS via one of the nine domestic and foreign participants who offer indirect participation to the Danish market.

More than 95 per cent of all foreign exchange transactions in Danish kroner are settled via CLS.[25] The average daily value of transactions in Danish kroner was DKK 278 billion in 2020. This is an increase of 5 per cent compared to 2019 cf. Chart 7.

During March, the number and value of settled transactions in CLS was particularly high. In April, numbers and value were back to pre-covid-19 levels.

Operational reliability and liquidity

CLS settlement takes place during a relatively short period, where the participating central banks' RTGS systems - across time zones - are open at the same time. Pay-ins to CLS take place via the national RTGS

25 BIS, *Triennial Central Bank Survey, Foreign exchange turnover in April 2019* (*link*) and CLS Bank.

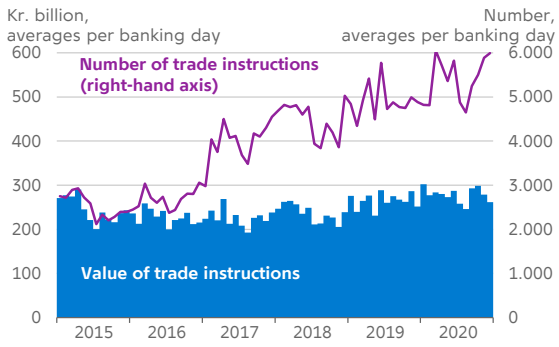
Oversight of CLS Box 10

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 (OC), 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 the OC, which is organised by the Federal Reserve. The Federal Reserve 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, 2019 (*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 7



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.

systems, in the case of Danish kroner via Kronos2. The operational stability of CLS is therefore dependent on the stability of the RTGS systems.

In 2020, one incident in Kronos2 affected CLS settlement. Monday morning, November 23rd Kronos2 was down for an hour and a half. Contingency procedures were initiated but Kronos2 was up running again and able to transfer the participants' pay-ins to the CLS settlement, which was completed within business deadlines. Measures have been taken to prevent a recurrence.

The Danish participants reserve sufficient liquidity for CLS settlement.

Brexit

Brexit has not had any effect on Danish participation in CLS or on the settlement of Danish kroner.

When the United Kingdom left the European Union on 31 January 2020 and the transition period ended on 31 December 2020, CLS lost its previous protections under the Settlement Finality Directive, SFD. To ensure that European Economic Area (EEA) participants could continue to settle their foreign exchange payment instructions in CLS, certain jurisdictions had to specify under their relevant local law that the Directive's provisions on settlement finality also apply to systems outside the EEA.

The Directive is in Denmark implemented in the Capital Markets Act. According to this, the Danish Financial Supervisory Authority had prior to Brexit approved CLS as a third country payment system. This means, that Danish participation in CLS is protected in the way as it is the case with European Union systems. Thus, the CLS settlement of payment instructions in Danish kroner is still protected by SFD.

PUBLICATIONS

NEWS

News offers quick and accessible insight into an Analysis, an Economic Memo, a Working Paper or a Report from Danmarks Nationalbank. News is published continuously.

ANALYSIS

Analyses from Danmarks Nationalbank focus on economic and financial matters. Some Analyses are published at regular intervals, e.g. *Outlook for the Danish economy* and *Financial stability*. Other Analyses are published continuously.

REPORT

Reports comprise recurring reports and reviews of the functioning of Danmarks Nationalbank and include, for instance, the *Annual report* and the annual publication *Danish government borrowing and debt.*

ECONOMIC MEMO

An Economic Memo is a cross between an Analysis and a Working Paper and often shows the ongoing study of the authors. The publication series is primarily aimed at professionals. Economic Memos are published continuously.

WORKING PAPER

Working Papers present research projects by economists in Danmarks Nationalbank and their associates. The series is primarily targeted at professionals and people with an interest in academia. Working Papers are published continuously.

The report consists of a Danish and an English version. In case of doubt regarding the correctness of the translation the Danish version is considered to be binding.

DANMARKS NATIONALBANK
LANGELINIE ALLÉ 47
DK-2100 COPENHAGEN Ø
WWW.NATIONALBANKEN.DK

This edition closed for contributions on 14 April 2021

DANMARKS NATIONALBANK

CONTACT

Ole Mikkelsen
Communications and Press Officer

omi@nationalbanken.dk
+45 3363 6027

SECRETARIAT AND COMMUNICATIONS