DANMARKS NATIONALBANK

REPORT | Oversight of the financial infrastructure
4 May 2026 | No. 3

Oversight of the financial infrastructure 2025

Danmarks Nationalbank oversees the systems and solutions in the Danish financial infrastructure that enable consumers and businesses to exchange payments and securities. In this report, Danmarks Nationalbank presents the conclusions from its oversight operations in 2025.

Written by

Lone Natorp
Head of Oversight
ln@nationalbanken.dk
+45 3363 6109

Anne Hye Hedemann
Overseer, interbank payments and foreign exchange settlement
anhk@nationalbanken.dk
+45 3363 6262

Jonas Moltke-Aaen
Overseer, payment solutions and central securities depositories
jmaa@nationalbanken.dk
+45 2191 7443

Line Bolding Holmegaard
Overseer, retail payment systems
lbh@nationalbanken.dk
+45 3363 6087

Mathilde Bak Møller
Overseer, retail payment systems
mbm@nationalbanken.dk
+45 3363 6109

37 Pages

The payments infrastructure is secure, efficient and stable.

The central systems and solutions in the infrastructure are highly compliant with the requirements of international standards for organisation, risk management and contingency planning. This helps to ensure that the public and businesses in Denmark usually can exchange payments without delays and disruptions.

Threats to the infrastructure remain serious and are continuously evolving.

System owners have generally achieved a high degree of maturity in their development of cyber resilience, but the threat from cybercriminals remains high and is continuously evolving. Furthermore, several factors, including the use of hybrid techniques, contribute to making the threat landscape more complex. The robustness of the infrastructure must therefore continue to be strengthened to stay ahead of developments.

The need to focus on robust contingency arrangements remains.

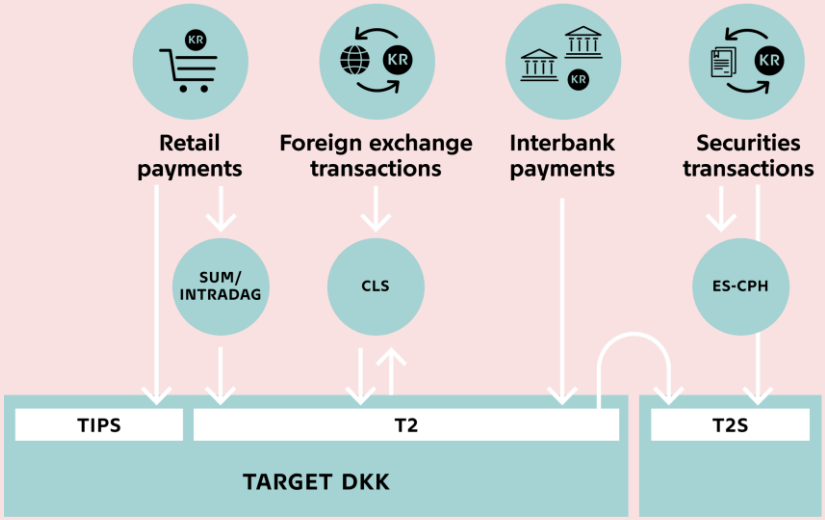
Full protection against cyberattacks and other operational incidents is not possible. System owners must therefore have contingency plans in place to restore operations quickly and safely after an attack or other forms of outage. Danmarks Nationalbank recommends that system owners also prepare to handle extreme situations such as failures at multiple data centres or corruption of critical data.

Why is it important?

On an average banking day, payments totalling kr. 838 billion – equivalent to a quarter of GDP – were sent through the systems that make up the Danish payments infrastructure in 2025, and it is crucial for the economy that payments and securities can be exchanged without problems. That is why Danmarks Nationalbank oversees whether the central systems and solutions in the payments infrastructure function securely and efficiently and comply with international standards in this area. This helps fulfil one of Danmarks Nationalbank's main purposes, which is to contribute to safe and efficient payments.

Main chart

Danmarks Nationalbank oversees the central systems and solutions in the payments infrastructure





Keywords

Oversight of the financial infrastructure
Oversight
Cyber security
Financial stability

1
Introduction

The payments infrastructure in Denmark consists of a number of interconnected systems and solutions that enable consumers, businesses and financial entities to exchange payments and securities with each other. It is crucial for financial stability and for the wider economy that these systems and solutions operate without disruptions or outages to ensure ease and efficiency when paying for goods and services. Payments totalling kr. 838 billion were exchanged through the payments infrastructure every day in 2025.

Because the payments infrastructure plays such a critical role in the economy, Danmarks Nationalbank oversees that the central systems in the infrastructure are well-functioning, secure and efficient. This oversight also includes the most important payment solutions. As part of its oversight, Danmarks Nationalbank assesses whether the overseen systems and solutions comply with the high requirements of international standards for security and efficiency, including requirements for cyber resilience. If the requirements are not met, Danmarks Nationalbank recommends changes to systems and solutions. Danmarks Nationalbank's oversight is described in more detail in box 1.

BOX 1

Danmarks Nationalbank's oversight in 2025

Danmarks Nationalbank oversees the core systems and solutions in the Danish payments infrastructure:

- TARGET DKK (settlement in Danish kroner via T2 and TIPS in TARGET Services, and Danmarks Nationalbank's system for monetary policy instruments and collateral management, SPI)
- Sumclearing and Intradayclearing (retail payments)
- Euronext Securities Copenhagen's settlement system (securities settlement)
- Dankort, Betalingsservice and account-to-account transfers (the most important payment solutions)

International systems Danmarks Nationalbank oversees:

- TARGET Services consist of:
  - T2 (interbank payments)
  - T2S (TARGET2-Securities): system for securities settlement
  - TIPS (TARGET Instant Payment Settlement), used for instant payments.
- CLS (foreign exchange transactions).

Danmarks Nationalbank's oversight is based on international standards and guidelines that require security and efficiency. Danmarks Nationalbank oversees the core Danish payment and settlement systems based on CPMI-IOSCO's[1], *Principles for Financial Market Infrastructures, PFMI*[2], and PFMI's supplementary *Guidance on Cyber Resilience for Market Infrastructures*[3]. Danmarks Nationalbank's oversight also incorporates the ECB's *Cyber resilience oversight expectations*[4], CROE, which implements the PFMI guidelines for cyber resilience in the ECB's oversight work. Oversight of the most important payment instruments in Denmark complies with the ECB's standards for payment instruments, PISA[5]. The organisation of the oversight is described in more detail in Danmarks Nationalbank's oversight policy[6].

Danmarks Nationalbank coordinates with the Danish Financial Supervisory Authority in this area. This collaboration is designed to ensure that duplicate regulatory controls are avoided, skills are utilised in the respective authorities and relevant information is shared.

Danmarks Nationalbank collaborates with other central banks on overseeing international systems relevant to Denmark.

Continues ...

... continued

[1] The Committee on Payment and Market Infrastructures, CPMI, is based at the Bank for International Settlements, BIS. The International Organization of Securities Commissions, IOSCO, is an international forum of cooperation between regulators of securities markets.
[2] See CPMI-IOSCO, *Principles for financial market infrastructures*, 2012 (*link*).
[3] See CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures*, 2016 (*link*).
[4] See ECB, *Cyber resilience oversight expectations for financial market infrastructures*, 2018 (*link*).
[5] See ECB, *The Eurosystem Oversight Framework for Payment Instruments, Schemes and Arrangements, PISA*, 2021 (*link*).
[6] See Danmarks Nationalbank, *Oversight policy 2025*, September 2025 (*link*).

The Danish payments infrastructure is described in more detail in box 2.

BOX 2

The payments infrastructure in Denmark

On banking days[1] in 2025, payments averaging kr. 838 billion per day were sent through the Danish payments infrastructure. This corresponds to about a quarter of Danish GDP.

Danmarks Nationalbank's payment system, TARGET DKK, plays a key role in the infrastructure for the settlement of large, time-critical payments between banks (interbank payments) and by virtue of the bank's role as settlement bank for the other payment and settlement systems. In Easter 2025, Danmarks Nationalbank transferred the settlement of Danish kroner from its own settlement system, Kronos2, to the pan-European platform for the settlement of payments and securities transactions, TARGET Services[2].

TARGET Services is a pan-European technical platform made available to participating central banks by the European Central Bank, ECB, and the Eurosystem. Three services are used for Danish kroner:

- T2 (formerly TARGET2), a payment system for large, time-critical payments between participants and settlement of net positions from connected payment and settlement systems
- T2S (TARGET2-Securities), the securities settlement system
- TIPS (TARGET Instant Payment Settlement), which is used for instant payments.

Denmark has its own monetary policy and collateral management, which is still handled in Danmarks Nationalbank's system for collateral management and monetary policy instruments, SPI. The collective term for the payments infrastructure that includes both TARGET Services and SPI is TARGET DKK. Danmarks Nationalbank is the system owner of TARGET DKK and has entered into an agreement with the ECB on the use of TARGET Services. Settlement in Danish kroner in TARGET Services is notified as a separate payment system in accordance with the Danish Capital Markets Act. The Danish payments infrastructure as it has been since Easter 2025 is shown in chart A in the box.

Retail payments are payments between consumers, businesses and public authorities, e.g. using payment cards and account-to-account transfers. Depending on the type, payments are settled and reconciled in one of the financial sector's retail payment systems. The participants' accounts at Danmarks Nationalbank are then credited. Before Easter 2025, the payments were calculated and reconciled in the Sumclearing, Intradayclearing and Straksclearing owned by Finance Denmark and subsequently settled in Kronos2. Net positions from the Sumclearing and Intradayclearing systems have been settled in TARGET DKK since Easter 2025. Instant payments have been settled through TIPS DKK since Easter 2025, where payments are processed individually and in real time. Danmarks Nationalbank is the system owner for TIPS DKK, the replacement for Straksclearing, which has now been closed. Sumclearing and Intradayclearing are owned by Finance Denmark.

Securities transactions may be carried out in different ways: On the stock exchange, through a multilateral trading facility or bilateral trades via a bank or broker (also called "over-the-counter"). The settlement of transactions in Danish-issued securities is handled by the central securities depository, Euronext Securities Copenhagen, ES-CPH.

Continues ...

... continued

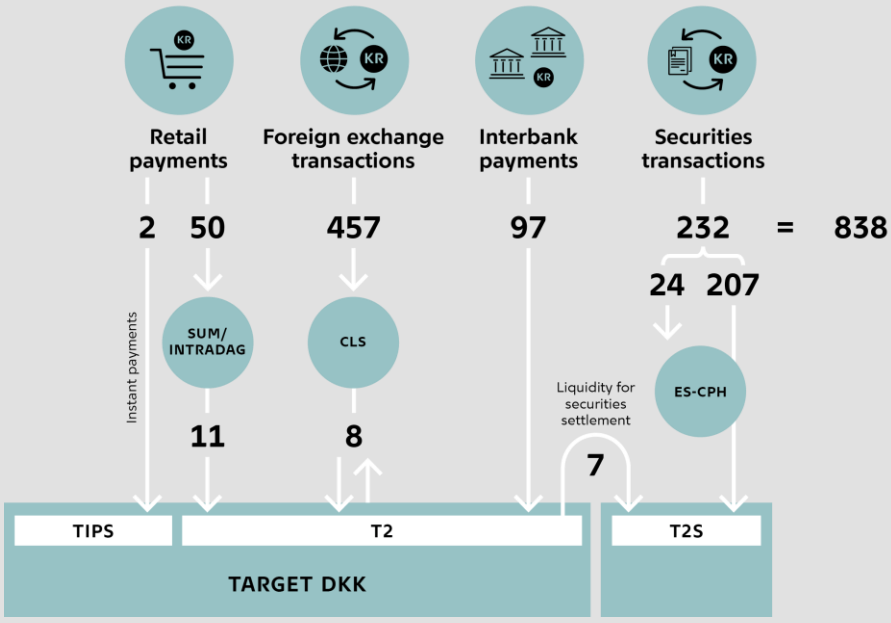
Securities transactions between banks and their own customers are settled via ES-CPH's own settlement system, the ES-CPH settlement, while securities transactions between banks and other financial institutions are settled via T2S. As the central securities depository, ES-CPH is responsible for keeping continuous records of the holdings of all Danish-issued securities on behalf of investors, and transfers of securities in accounts on T2S are subsequently reflected in accounts in ES-CPH's systems.

Foreign exchange transactions are settled through CLS, an international system for settlement of foreign exchange transactions, currently in 18 connected currencies, including Danish kroner. Danmarks Nationalbank makes accounts available to banks settling transactions through CLS. Participants reserve liquidity for CLS settlement by transferring funds to these accounts in TARGET DKK via T2. Before Easter 2025, participants reserved liquidity for the settlement of foreign exchange trades in CLS on accounts in Kronos2. CLS is owned by a number of large international banks.

Netting has a major impact on payment processing
As mentioned above, Sumclearing and Intradayclearing settle their participants' net positions on the participants' accounts in TARGET DKK. Net positions are calculated by offsetting participant claims and obligations in the respective systems. 'Netting' reduces participant liquidity needs significantly compared to a situation where all payments are settled individually. For example, netting reduces the liquidity need for settlement of retail payments from kr. 50 billion to kr. 11 billion daily, corresponding to a reduction of 78 per cent. T2S settlement also takes place using netting. The liquidity for settlement on T2S is transferred from the participants' cash accounts in TARGET DKK. Netting reduces the participants' need to reserve liquidity from kr. 207 billion to kr. 7 billion, which corresponds to a reduction of approximately 97 per cent.

CHART A

Payment flows, kr. billion, average per banking day in 2025



[1] Some types of payments can be made on all days and at any time, others only when banks are open. 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.
[2] See nationalbanken.dk, *Memo on TARGET DKK*, October 2024 (*link*).

The infrastructure is safe, efficient and stable

Danmarks Nationalbank's oversight shows that the Danish payments infrastructure is safe and efficient.

The central systems and solutions in the infrastructure highly compliant with the requirements set out in international standards for organisation, risk management and contingency planning. The owners of the systems and solutions generally have a high level of maturity when it comes to operational stability and cyber resilience. The threat landscape is also constantly evolving, requiring an ongoing need to strengthen resilience, see below.

In 2025, the operational stability of the infrastructure was generally high, and disruptions to the exchange of payments and the settlement of securities transactions in Denmark were rare. There were a few disruptions in the infrastructure in 2025, including three major incidents in TARGET Services and one in the card payments infrastructure. Danmarks Nationalbank's oversight has followed up with the owners of the systems to ensure that the response to the incidents is satisfactory. The incidents and the subsequent follow-up are described in more detail below in the sections on the respective systems.

Operational resilience is high, but needs to be continuously developed

The threat landscape for the financial sector is constantly evolving. The cyber threat to the financial sector remains high, and the payments infrastructure may be subject to serious cyberattacks or other operational incidents that could lead to disruptions and breakdowns in the financial sector. Several factors also contribute to making the threat landscape for Denmark more complex, including the emergence of hybrid threats.[1]

In August 2025, telecommunications provider Colt Technology Services was hit by a ransomware attack that affected the company's administrative systems. Colt's network is used to access TARGET Services. The attack did not cause any disruption to, or compromise of, services related to TARGET Services.[2]

Over recent years, the owners of the systems in the financial infrastructure have devoted considerable effort to enhancing its resilience against cyberattacks and other threats, and they generally exhibit a high level of maturity in this area. However, ongoing developments in the threat landscape mean that resilience against cyberattacks and other threats must continue to be strengthened.

In recent years, the owners of the systems have focused on contingency arrangements in particular in case cybercriminals succeed in penetrating the systems, and Danmarks Nationalbank's oversight has provided a number of the systems with recommendations to strengthen their work in this area. This includes recommendations to ensure strong frameworks for handling extreme but plausible scenarios, such as data corruption and outages at multiple data centres. In 2025, Danmarks Nationalbank followed up on how system owners select specific and relevant scenarios and incorporate them into their contingency planning. The work of system owners on these recommendations in 2025 is described in chapters 2, 3, 4 and 5 below.

In 2025, Danmarks Nationalbank analysed how to ensure that individuals and companies can continue to make payments and transfer money, even if central systems or data are unavailable. Based on that analysis, Danmarks Nationalbank

[1] For a more detailed description of the threat outlook for the financial sector, see Danmarks Nationalbank, *Uncertain times call for resilience and preparedness, Danmarks Nationalbank Analysis (Financial stability)*, no. 28, November 2025 *(link)*.
[2] Bleeping Computer, *Colt Telecom attack claimed by WarLock ransomware, data up for sale,* 15 August 2025 *(link)*.

issued a number of recommendations to financial companies to strengthen their operational preparedness.[3] These recommendations are also relevant to system owner compliance with international standards, and Danmarks Nationalbank's oversight will follow their implementation of the recommendations in 2026.

It is essential that systems in the infrastructure are well equipped to handle outages and other incidents, also if they are of an extreme nature. Work on cyber resilience also requires a holistic approach. It is therefore important that system owners continue to strengthen all aspects of security, including protection against intrusions into the systems and the ability to detect cyber incidents quickly, at an early stage. The requirements for the work of system owners on cyber resilience are described in more detail in box 3.

BOX 3

Cyber resilience is strengthened through a continuous and holistic approach to managing cyber risks.

Danmarks Nationalbank assesses the resilience of central systems based on CPMI-IOSCO's *Guidance on cyber resilience for financial market infrastructures*, Cyber Guidance, and the ECB's *Cyber resilience oversight expectation for financial market infrastructures*, CROE.

The standards set requirements for systems to work with cyber resilience in the following areas:

- **Governance** that defines cyber resilience frameworks, roles and responsibilities
- **Identification** of critical business activities, the supporting processes, procedures and systems and their risk assessments
- **Protection** through effective security controls and process design
- Early **detection** of cyber incidents through monitoring
- **Respond** to attacks and **recover** critical business operations quickly and securely after a severe and widespread outage.

There are also requirements for working with three cross-cutting elements:

Testing across all areas to ensure the efficiency of the work

Situational awareness, including intelligence on the cyber threat outlook and vulnerabilities

Learning and development to continuously strengthen cyber resilience, as the threat outlook also evolves.

It's important that system owners continuously focus on all areas to strengthen cyber resilience.

The five focus areas and the three common elements under CROE are illustrated in chart B.

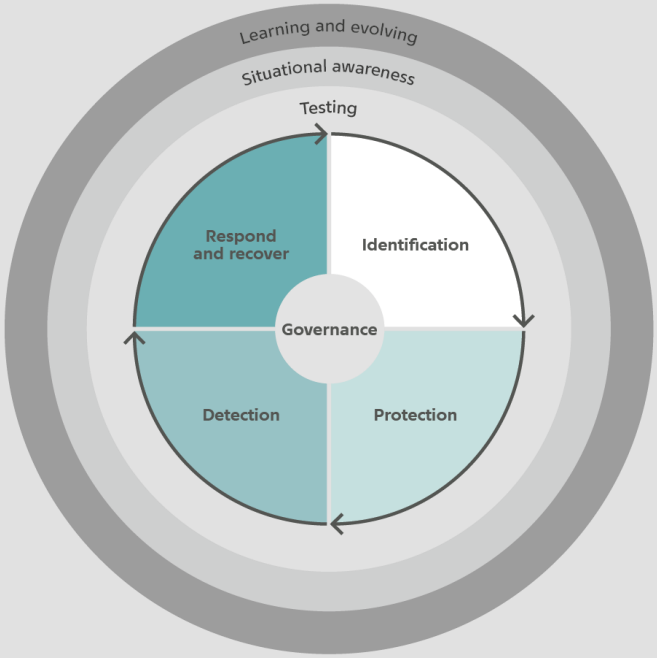
Continues ...

[3] Danmarks Nationalbank, Emergency preparedness for critical financial sector activities in extreme scenarios, *Danmarks Nationalbank Analysis*, no. 29, December 2025 (*link*).

... continued

CHART B

The five main focus areas and the three common elements of cyber resilience



Source: CPMI-IOSCO, Guidance on cyber resilience for financial market *infrastructures*, Cyber Guidance.
ECB, *Cyber resilience oversight expectations for financial market infrastructures*, CROE.

Sector-wide collaboration contributes to strengthening operational resilience.

Systems in the financial infrastructure are closely interconnected, making coordination and knowledge sharing in the work on operational resilience, including cyber resilience in particular, crucial. The international standards therefore set a number of requirements for participation in sector collaborations intended to increase the operational resilience of the sector as a whole, including resilience to cyberattacks. Furthermore, this type of collaboration also strengthens the work of individual companies on operational resilience. Danmarks Nationalbank's oversight continuously monitors system owner participation in Danish sector collaborations.

The international standards require system owners to continuously identify, monitor and manage risks related to participants in the system and to other systems. This particularly involves focus on managing risks arising from mutual dependencies between systems. Managing these risks requires close collaboration between all parts of the ecosystem. In Denmark, this cooperation is handled through the *Financial Sector forum for Operational Resilience*, FSOR[4], a public-private cooperation forum led by Danmarks Nationalbank. The members

[4] The bank acts as chair and secretariat for FSOR, which in addition to those in charge of the systems and solutions in the infrastructure includes banks, data centres, pension and insurance companies, relevant authorities and Nordic Financial CERT. See FSOR's 2025 Annual Report *(link)*.

of FSOR discuss risks, share knowledge and decide on joint mitigating initiatives. FSOR has also established a joint crisis management to coordinate efforts across the financial sector in the event of a crisis that could threaten financial stability.[5] FSOR maintains a common risk outlook, in which the cyber threat continues to constitute the primary risk. In 2025, FSOR also focused in particular on quantum-secure encryption, network connections, crisis management and communication. Danmarks Nationalbank's oversight has discussed work related to these topics with the owners of the systems and solutions under oversight.

The owners of the central systems in the infrastructure also cooperate in the *Risk Forum for Interdependencies*, RGA[6], to manage specific risks arising from interdependencies. RGA has previously worked on controlled shutdown and reopening in a number of scenarios. Danmarks Nationalbank followed up on the work of system owners on those plans in 2025.

Collaboration on cyber resilience is also supported by the TIBER-DK programme. In a TIBER test, companies must identify, prevent and respond to advanced cyberattacks simulated in actual production environments. The test thus provides specific input on how the company protects its critical activities against cyberattacks and avoids such attacks causing damage. TIBER-DK participants subsequently share the lessons from these tests with one another to further strengthen cyber resilience.[7]

Finally, the international standards also require common sharing of information about cyber threats and cyberattacks. The central systems and solutions in the infrastructure all participate in *Nordic Financial CERT*, NFCERT[8], a joint Nordic sectoral collaboration on the collection and sharing of information on cyber threats and cyberattacks.

Consolidation and internationalisation of the infrastructure continues

Over the years, the Danish payments infrastructure has become more closely integrated into the European infrastructure, and several systems and solutions are now part of international groups. This development continued in 2025.

In 2025, Finance Denmark, which is the system owner of the Sumclearing and the Intradayclearing for retail payments, initiated preparations to use EBA CLEARING as the new provider of clearing infrastructure. EBA CLEARING is a non-profit company owned by 48 European banks. EBA CLEARING currently clears retail payments in euros and will now develop a clearing solution in Danish kroner, which will replace the existing Intradayclearing.

In 2025, ES-CPH continued to work on the Euronext Group's *convergence programme*, which means that all five CSDs in the group must run on the same technical platform.[9] ES-CPH is scheduled to complete the programme in 2028, after which all key services will run on the Euronext Group's common technical systems.

[5] The FSOR's Crisis Management team supplements the members' own crisis plans as well as the national crisis response, NOST. Danmarks Nationalbank chairs FSOR's Crisis Management and is responsible for providing secretariat services.
[6] The Risk Forum for Interdependencies is a collaborative forum between the organisations responsible for the central payment and settlement systems in the infrastructure, i.e. Danmarks Nationalbank (interbank and instant payments), ES-CPH (securities transactions), Finance Denmark (retail payments) and e-nettet (communications network). The work of the RGA is coordinated with the FSOR.
[7] See Danmarks Nationalbank, TIBER-DK/TLPT – trusselsbaserede red team-test (TIBER-DK/TLPT – threat-based red team testing, in Danish only), 2026 (*link*).
[8] Nordic Financial CERT, NFCERT, is a member-driven non-profit organisation that aims to strengthen the Nordic financial industry's resilience to cyberattacks and enable Nordic financial institutions to respond quickly and effectively to cyber security threats and online crime. NFCERT collects and shares information about cyber threats and cyberattacks.
[9] Euronext, *Euronext Securities CSD Convergence Programme*, 2026 (*link*).

Nets, which operates Dankort, and MPS, which operates Betalingsservice, are also part of international groups where business functions and systems are shared across the group.

Danmarks Nationalbank's oversight function continuously monitors developments to ensure that system owners continue to comply with international standards.

2
Interbank payments and the central settlement of payments in Danish kroner

An interbank payment is a payment between financial institutions. These payments are typically time-critical and of high value. They are settled in an RTGS system, which stands for *Real Time Gross Settlement System,* meaning that payments are settled individually and immediately.

Interbank payments in Danish kroner were settled in Danmarks Nationalbank's Kronos2 until Easter 2025, when settlement was moved to TARGET DKK. TARGET DKK is a collective term for the settlement of payments in Danish kroner on TARGET Services and Danmarks Nationalbank's system for monetary policy instruments and collateral, SPI.

TARGET DKK functions as a central hub in the Danish payments infrastructure. In addition to interbank payments, monetary policy operations and net positions from, among others, retail payment systems are settled, and liquidity is transferred for the settlement of securities and foreign exchange transactions conducted in other systems.

With the migration, the Danish krone is the first currency, apart from the euro, to settle RTGS payments on the pan-European TARGET Services platform.

Use

Most Danish banks and mortgage credit institutions participate in TARGET DKK and hold accounts with Danmarks Nationalbank, in the same way that private individuals hold accounts with commercial banks. Branches of foreign banks also participate.

By the end of 2025, there were 71 participants in the settlement of payments in TARGET DKK, 29 of which were under co-management. Co-management is a new type of participation in Denmark, introduced via TARGET Services. Co-management is aimed at smaller credit institutions, which in this context are referred to as co-managees. A co-managee is an account holder at Danmarks Nationalbank but only holds an account for the safekeeping of liquidity. Co-managees enter into an agreement with a direct participant, typically a larger credit institution, which acts as the co-manager. The co-manager administers the co-managee's account and executes payment instructions on behalf of the co-managee. Co-managees do not have a direct connection to TARGET Services. A direct connection to TARGET Services requires compliance with a number of security requirements, including those set by the participant's chosen network provider, SWIFT or Nexi. The purpose of these security requirements is to ensure participants' resilience to potential cyberattacks. Ensuring and attesting compliance with the requirements for a direct connection to TARGET Services is a substantial task, which is one of the reasons why smaller credit institutions usually opt for co-management.

In 2025, interbank payments in TARGET DKK[10] averaged kr. 97.4 billion per banking day. This is a decrease of 3.5 per cent from 2024, see table 1.

Operational reliability

Operational stability in the settlement of interbank payments in Danish kroner was generally satisfactory in 2025.

In February and May 2025, respectively, there were two major incidents in TARGET Services, which meant that participants in Kronos2/TARGET DKK were unable to complete payments or securities transactions for several hours. For a more detailed description of the incidents, see chapter 6, Payments and securities settlement in euro.

In March, there was an incident in T2S on TARGET Services that led to a delay in the closing of the Danish monetary policy day and in the opening of the new day in Kronos2.

At the end of May, there was an incident in Danmarks Nationalbank's SPI. The incident meant that the ability of participants to deposit and withdraw collateral themselves was restricted between 26-29 May.

The incidents have subsequently been followed up with initiatives, and lessons have been learned from the course of events. Taken together, these measures help prevent similar incidents in future and strengthen the ability to respond should they nevertheless occur.

TABLE 1

Payments in TARGET DKK, billion kr. per banking day

	Billion kr., averages per banking day				
	2021	**2022**	**2023**	**2024**	**2025**
Interbank payments	88.7	101.5	95.8	100.9	97.4
- Of which customer payments	16.6	20.7	19.8	21.5	20.3

	Number, average per banking day				
	2021	**2022**	**2023**	**2024**	**2025**
Interbank payments	8,544	10,344	10,639	10,665	10,228
- Of which customer payments	3,076	4,294	4,670	4,482	5,380

Note: Data on interbank payments prior to the migration to TARGET DKK at Easter 2025 were sourced from Kronos2.
Source: Danmarks Nationalbank

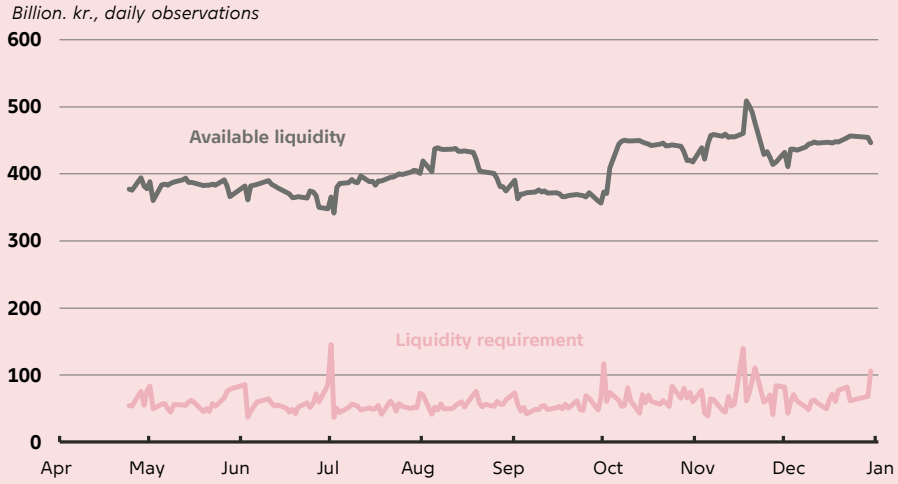
Liquidity

Participants still had ample liquidity to make payments in Kronos2/TARGET DKK in 2025. This covers interbank payments, securities trading in T2S, instant payments in TIPS DKK and payments resulting from settlement instructions from the connected payment and settlement systems (the retail payment systems and CLS), see chart 1.

[10] Including Kronos2 until the migration of the settlement of payments in Danish kroner at Easter 2025.

CHART 1

Available liquidity relative to liquidity requirements for participants in TARGET DKK in 2025



Note: The available liquidity of participants consists of the balances on their accounts in TARGET DKK as well as their ability to borrow on an intraday basis against collateral. The liquidity requirement is calculated by identifying the time of day when participants have used the largest amount of liquidity to complete their payments. This is then aggregated across participants to find the maximum total liquidity requirement.
Source: Danmarks Nationalbank.

In the initial period following the migration of krone payment settlement to TARGET DKK, there were incidents in which participants had not reserved enough liquidity for the settlement of retail payments. Such incidents were not due to a lack of liquidity, but to participants having to adapt their liquidity management to the new functionality. Read more about the incidents in chapter 3 on the Clearing and Settlement of Retail Payments.

Unlike the previous RTGS system, Kronos2, TARGET DKK has a queue function under which payments are queued if a participant does not have sufficient liquidity to settle the payments immediately. Payments are automatically settled once the participant has sufficient funds in the account. The queue function is also supported by prioritisation options under which payments can be assigned the priorities normal, high and urgent. TARGET DKK will attempt to settle the payments with the highest priority first, i.e. participant liquidity is prioritised for the most important payments. The queuing function helps reduce liquidity risk by preventing gridlock and ensuring that temporary liquidity shortages do not interrupt payment settlement.

Danmarks Nationalbank conducts regular liquidity stress tests in accordance with the requirements in CPMI-IOSCO's Principles for Financial Market Infrastructures, PFMI. The stress test includes, as a minimum, scenarios in which the largest participants cannot complete their payments, as well as a shock to participants' ability to draw on Danmarks Nationalbank's intraday credit facility against collateral. The first liquidity stress test using payment data from TARGET DKK is expected to be conducted in the first half of 2026.

Cyber resilience

Danmarks Nationalbank works continuously to strengthen the cyber resilience of its systems and business processes. Danmarks Nationalbank's management approved a new cyber resilience strategy in June 2025. The strategy sets out objectives that will guide how Danmarks Nationalbank's cyber resilience is to be strengthened towards 2028. One of the focus areas is to further strengthen the bank's preparedness for managing cyber incidents, including extreme but plausible scenarios.

Following the initial experience in 2024, purple team testing has become a permanent testing tool that helps strengthen the Danmarks Nationalbank's ability to detect, respond to and prevent cyberattacks. In a purple team test, external attack specialists – the red team – participate together with the bank's own employees responsible for operating the critical systems – the blue team. During the tests, the two teams work closely together, which gives the blue team insight into what an actual attack on the systems might look like. Identified areas for improvement are addressed and as far as possible, retested within the test period. Purple team testing supplements Danmarks Nationalbank's participation in the TIBER-DK test programme.

Danmarks Nationalbank complies with both SWIFT's Customer Security Controls Framework, CSCF, and SIAnet's Security Guidelines, which require the implementation of security controls aimed at strengthening cyber resilience in the event of cyberattacks. It is an ECB requirement that central banks and critical participants have two independent network connections to TARGET Services via SWIFT and Nexi, respectively. The purpose of this requirement is to ensure operational stability and resilience if the primary network connection fails.

International standards

In 2024, Danmarks Nationalbank's oversight completed an assessment of Calypso's compliance with CPMI-IOSCO's Cyber Guidance. Calypso supports SPI and is an important system for settlement in Danish kroner, as participants use the system to post collateral to obtain credit that can be used for payment settlement. In 2025, Danmarks Nationalbank has worked on the areas for improvement identified in the assessment. One of the initiatives introduced is a unit in the business area to further strengthen risk management, including proactive work on compliance with international standards.

An assessment has previously been made of Danmarks Nationalbank's compliance with CPMI's strategy to reduce the risk of criminal transactions in central payment systems relating to endpoint security. As follow-up to the assessment, response plans were strengthened and guidelines were updated on how to respond quickly and effectively in the event of suspected criminal transactions in TARGET DKK. The plans will be tested with participants in the first half of 2026. In addition, risks related to endpoints and existing control measures at the participants are being mapped. The mapping is intended to enhance the understanding of risks in the ecosystem surrounding TARGET DKK and how they are addressed. This work will also help provide the framework for an awareness training course that Danmarks Nationalbank will conduct with participants in 2026.

3
Clearing and settlement of retail payments

Retail payments in Danish kroner are cleared and settled in the Sumclearing and Intradayclearing and in the system for instant payments, TIPS DKK. Retail payments are payments made between consumers, businesses and public authorities.

In the Sumclearing, payments made with payment cards and Betalingsservice (direct debit) are settled once a day on banking days. In the Intradayclearing, account-to-account transfers such as online banking transfers, salary payments and public disbursements are settled five times a day on banking days. The banks' net positions – corresponding to the sum of payments to and from their customers – are calculated in the systems at fixed times. The net positions are sent to Danmarks Nationalbank's RTGS system, TARGET DKK, where the amounts are exchanged between the banks. The payments are then posted to the customers' accounts at the banks. The Sumclearing and the Intradayclearing are also called the batch clearings, as payments are settled in batches where payment data are processed collectively in groups.

In TIPS DKK, instant payments, i.e. account-to-account transfers, are settled within a few seconds, 24 hours a day, seven days a week. These include, for example, online banking transfers and payments via MobilePay. TIPS stands for *TARGET Instant Payment Settlement* and is part of TARGET Services. During Easter 2025, the settlement of instant payments in Danish kroner migrated to TIPS DKK, which replaced the previous instant payments system, Straksclearingen, which was owned by Finance Denmark.

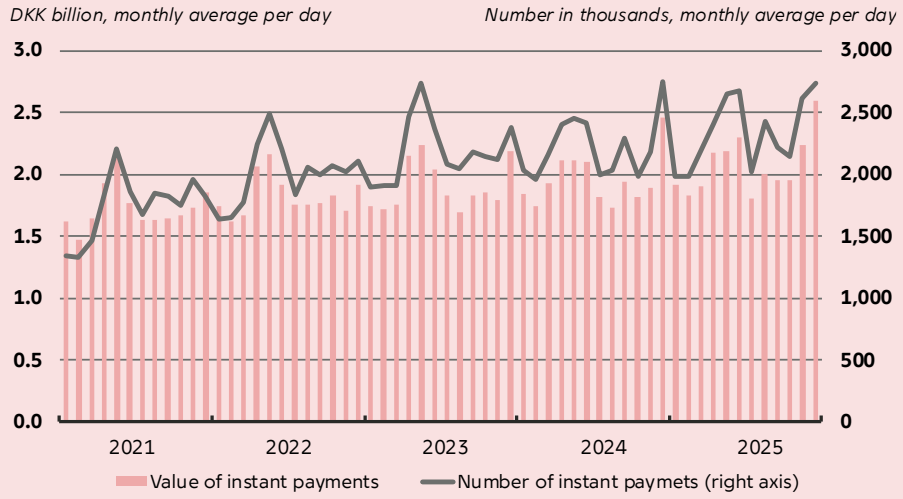
As shown in chart 2, the transition to TIPS DKK has not changed the trend in the use of instant payments. There is still a slight increase in both the average value and the number of transactions from 2024 to 2025, which is consistent with the generally upward going trend over the period 2021-2025, during which the volume has increased by 33.6 per cent. This can, among other thing, be attributed to increased use of MobilePay in e-commerce and payments between private individuals.[11]

[11] See Danmarks Nationalbank, *The digital retail payment market is changing*, *Danmarks Nationalbank Analysis*, no. 2, February 2025 (*link*).

CHART 2

Instant payments in Denmark

Value and number of instant payments, 2021-2025



Note: Data consists of transactions executed in Straksclearingen up to Easter 2025 and subsequently of transactions executed in TIPS DKK.
Source: Mastercard Payment Services A/S, MPS, and Danmarks Nationalbank.

The value of transactions in the retail payment systems averaged kr. 51.8 billion per banking day in 2025, see table 2. This is an increase of 6.6 per cent compared with 2024.

TABLE 2

Value of transactions in retail payment systems, 2021-2025, average per banking day

Billion kr., average per banking day

	2021	2022	2023	2024	2025
The Sumclearing	20.5	21.3	21.2	21.8	22.6
The Intradayclearing	23.9	25	24	24.9	27.1
TIPS DKK*	1.7	1.8	1.9	1.9	2.1
Total	46.1	48.1	47.1	48.6	51.8

Note: * Data consists of transactions executed in Straksclearingen up to Easter 2025 and subsequently of transactions executed in TIPS DKK.
Source: Mastercard Payment Services A/S, MPS, and Danmarks Nationalbank.

Batch clearings

The batch clearings are owned by Finance Denmark, managed by e-nettet and delivered by Mastercard Payment Services Danmark A/S, MPS.

Use

There are two types of participants in the batch clearings, direct participants and indirect participants.
Direct participation requires, among other things, that the participant holds a main account and a settlement account with Danmarks Nationalbank. If a participant does not have its own account, it can participate as an indirect participant. In this case, the indirect participant's payments are settled via a settlement account held by a direct participant. By the end of 2025, there were 33 direct participants in batch clearings and 29 indirect participants.

Liquidity

Banks reserve liquidity on accounts at Danmarks Nationalbank for settlement of their net positions in the Sumclearing and the Intradayclearing. If a participant does not reserve sufficient liquidity, it will be suspended, i.e. removed from the clearing, resulting in revised net positions for the other participants, who thereby risk not receiving the expected liquidity.

There were several suspensions in 2025 due to insufficient reserved liquidity on the participants' accounts. Most of the suspensions occurred in the period immediately following the transition from Kronos2 to TARGET DKK, during which participants, as part of the migration, had to adjust their liquidity management, including placing greater emphasis on the continuous, active management of liquidity throughout the day. Previously, participants were to a greater extent able to rely on automated tools for liquidity management.

Ahead of the migration, Finance Denmark focused on training the sector in liquidity management in TARGET DKK and, following the suspensions, has been in dialogue with the affected participants.

Operational reliability

In 2025, operational stability in the Sumclearing and the Intradayclearing was satisfactory.

There was a single major incident in the Sumclearing in connection with a group of banks transitioning from direct to indirect participation. This transition led to a misconfiguration in the production environment, causing some payments to be delayed by two days.

The oversight assesses that Finance Denmark's follow-up on the incident, and the suspensions has been satisfactory.

International standards and cyber resilience

Finance Denmark is continuously working to strengthen cyber resilience in the batch clearings and in 2025 continued its efforts to comply with the final outstanding recommendation from Danmarks Nationalbank's assessment based on the 2022 CPMI-IOSCO Cyber Guidance. Finance Denmark's primary focus has been on further developing and strengthening the ability to restore and/or maintain operations within set timeframes following cyber-related incidents, including in extreme but plausible scenarios. As part of this work, a scenario catalogue was conducted in the second half of 2025, which systematically links incident descriptions, assets, threats, controls and contingency plans. The first practical test based on the scenario catalogue was carried out in the third quarter of 2025 in cooperation with MPS.

A further element in Finance Denmark's work on cyber resilience is the Cyber Security Handbook for the batch clearings, which sets out IT security requirements for data centres and participating banks. The handbook covers the eight focus areas in CPMI-IOSCO's Cyber Guidance, cf. box 3. Finance Denmark

follows up annually on participants' compliance with the Cyber Security Handbook[12] and uses the results as a basis for ongoing dialogue and further work. Finance Denmark's follow-up takes place both in cross-sector forums and bilaterally with the individual banks and data centres.

Danmarks Nationalbank's oversight holds annual discussions on risk management and contingency planning with the system owners. In 2025, the oversight and Finance Denmark discussed the importance of Finance Denmark continuing to prioritise and ensure sufficient staffing in its crisis management planning, so that its own internal contingency planning and FSOR's Crisis Management can be handled effectively in the event of simultaneous activation.

In 2025, the oversight also discussed with Finance Denmark the work to ensure sufficient redundancy in network connections and preparations for the introduction of quantum-safe encryption.

Changes in the ownership model for the batch clearings

In 2025, Finance Denmark initiated work to establish a subsidiary, Clearing Services P/S, which will take over ownership of the Sumclearing and the Intradayclearing. As the owner of the clearings, Clearing Services will be responsible for day-to-day operation and maintenance, as well as for ensuring compliance with the international standards for financial market infrastructures.

Finance Denmark finds it necessary to separate its roles as a clearing house and business association as a result of an amendment to the Finality Directive[13], which enables payment institutions and e-money institutions to access to the retail clearing systems. The purpose of the new ownership model is to create a clearer distinction between members of the business association and participants in the clearing systems.

Prior to transition to the new ownership model, Danmarks Nationalbank's oversight function will review Clearing Services' compliance with selected parts of CPMI-IOSCO's Principles for Financial Market Infrastructures, PFMI, including Principle 2 on governance and Principle 15 on business risk.

System changes in the clearing infrastructure in 2025

As part of the Sector Programme for the Future Payments Infrastructure, Finance Denmark has prepared a long-term strategic plan for the modernisation of the Danish clearing infrastructure, see box 4. Consequently, Finance Denmark has entered into an agreement with EBA CLEARING to establish a new STEP2 DKK clearing solution to replace the existing Intradayclearing. With the establishment of STEP2 DKK, part of the batch clearing infrastructure will be migrated to a standard platform that is NPC-compatible (see box 4). Finance Denmark expects the new clearing to be more resilient. At present, no decision has been made regarding the modernisation of the Sumclearing. Danmarks Nationalbank's oversight has underlined the importance of also preparing a plan for the clearing.

[12] In 2024, elements of the Cyber Security Handbook were updated with new requirements for data centres and participating banks to work more systematically on resilience, emergency plans and recovery options, including contingency plans and emergency procedures. The aim is to ensure sustained, sector-wide focus on these areas. The implementation period ran until the end of 2025, and the requirements now apply in full.

[13] In April 2025, amendments to the so-called Finality Directive entered into force (Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations (EU) No. 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro). The changes allow payment institutions (non-bank payment service providers) and e-money institutions to participate directly in the settlement of payments in the core payment systems without having to go through a bank. However, payment institutions will only have access to settlement accounts at Danmarks Nationalbank and will not have access to monetary policy instruments.

Finance Denmark expects that testing and development activities for the technical component of the STEP2 DKK solution will be completed by November 2026, and that the STEP2 DKK clearing will go live in the first half of 2027. Danmarks Nationalbank's oversight is closely following the STEP2 DKK project, with particular focus on governance, risk management and contingency planning, as well as on Clearing Services' readiness to operate the new STEP2 DKK clearing.

Focus on reducing digital fraud

As part of the Sector Programme for the Future Payments Infrastructure Finance Denmark initiated work in 2024 to select a provider of a Verification of Payee service, VoP, for the Danish sector. The initiative was launched as a result of new EU legislation, which requires that a payer's payment service provider must offer a service that verifies the identity of the payee to whom the payer wishes to send a credit transfer or instant payment.[14] In April 2025, Finance Denmark entered into an agreement with SurePay to assume the role of national provider of the VoP service.[15] The VoP service has been operational for euro payments since October 2025 and is expected to be operational for payments in Danish kroner in the first half of 2027. The VoP service is a key tool in efforts to combat digital fraud.

Finance Denmark is also working on establishing a joint freeze scheme, which should make it possible to freeze fraudulent transactions before they can be moved on from fraudsters' accounts.[16] In 2025, Finance Denmark initiated an analysis of options for a joint solution for the financial sector. The work is still ongoing, as its implementation requires a legislative amendment.

BOX 4

Sector Programme for the Payments Infrastructure of the Future

A comprehensive sector plan has been prepared under the auspices of Finance Denmark, with the aim of ensuring continued modernisation and resilience of the Danish retail payments infrastructure. Work on the sector plan is embedded in a sector programme under Finance Denmark's Board of Directors, with a broadly composed steering committee led by e-nettet in cooperation with Finance Denmark.

As part of the sector programme, Finance Denmark has developed a long-term strategic plan for the Danish clearing infrastructure, including the establishment of STEP2 DKK, which will replace the Intradayclearing. The initiative stems from a sector decision to apply the Nordic Payments Council's, NPC[1], payment standards. This means that clearing systems must be able to send and receive NPC-compatible message formats for account-to-account transfers. The Sumclearing and the Intradayclearing currently use older message formats and are therefore not NPC-compatible.

[1] NPC was established in 2018 as an independent non-profit organisation by the four Nordic banking associations (Bits A/S (Norway), Finance Denmark (Denmark), Finassiala (Finland) and Svenska Bankföreningen (Sweden)). The NPC's main purpose is to harmonise payment standards in the Nordic region, and work towards this goal continues across the Nordic banks. NPC's payment standards are based on the European Payment Council's, EPC, rulebooks and guidelines, with some adaptations to Swedish legislation and to the context of local payment landscapes in the Nordic region.

[14] See ECB regarding EU legislation for standard credit and instant transfers, Instant Payment Regulation, IPR, March 2024 (*link*).
[15] SecurePay, Denmark becomes the first non-Euro country to implement a nationwide VOP solution, April 2025 (*link*).
[16] See Finance Denmark, *Her er 18 anbefalinger, der kan bremse it-svindlen i Danmark* (Here are 18 recommendations to inhibit IT fraud in Denmark, in Danish only), November 2024 (*link*).

TIPS DKK

Danmarks Nationalbank is the system owner of TIPS DKK. TIPS DKK is overseen as part of TARGET DKK

Use

There is a total of 53 participants in TIPS DKK. Of these, 25 participate indirectly and therefore settle their payments via a direct participant's TIPS-account in TARGET DKK.

Liquidity

The execution of instant payments requires that the participant has made the necessary liquidity available in TIPS DKK. Participants transfer liquidity from their main account in TARGET DKK to a settlement account dedicated to instant payments.

The settlement of instant payments takes place 24/7/365, but liquidity transfers to and from a participant's TIPS settlement account can only take place during TARGET DKK's opening hours, which are 19:30-17:00 on banking days. Participants must therefore ensure that they have transferred sufficient liquidity to their TIPS account ahead of weekends and public holidays, when other services are closed and liquidity adjustment is therefore not possible.

Operational reliability

In December, an incident at a data centre meant that many members of consumers were unable to make instant payments for several hours. Danmarks Nationalbank activated the TIPS contingency arrangements, and contingency meetings were held until the incident was resolved. TARGET DKK, including TIPS, was not affected by the incident, which meant that the settlement of payments proceeded normally throughout the incident. The incident was caused by capacity constraints at the data centre, which meant that instant payments could not be processed. Remedial measures have subsequently been implemented at the data centre to safeguard against similar incidents in future.

Development of an instant payment system across currencies

Since 2024, Danmarks Nationalbank, in collaboration with the ECB and Sveriges Riksbank, has been working on the establishment of TIPS Cross-Currency, which is intended to enable cross-border instant payments in euro, Danish kroner and Swedish kronor via TIPS. The aim is to provide businesses and individuals access to fast, low-cost and secure instant payments across currencies. The first version of the technical solution was made available in November 2025, and work will continue in 2026.

4
Retail payments

When consumers and businesses in Denmark buy goods and pay bills, they mostly use digital payment solutions. The most commonly used payment solutions in Denmark are Dankort, international payment cards from Visa and Mastercard, MobilePay, Betalingsservice and account-to-account transfers via online or mobile banking. Payments worth approximately kr. 52 billion were made on average per day using digital payment solutions in 2025.[17]

Danmarks Nationalbank oversees Dankort and Betalingsservice. Oversight of these payment solutions is based on the PISA standards, see box 1. Account-to-account transfers are also subject to oversight. This takes place as part of Danmarks Nationalbank's oversight of retail clearings, see Chapter 3 *Clearing and settlement of retail payments*. Visa and Mastercard are overseen by the Eurosystem.

Danmarks Nationalbank regularly considers whether targeted oversight of other payment solutions is needed if they have become more important in the Danish market.

Dankort

Danmarks Nationalbank's oversight of Dankort is directed at Nets, which is the system owner of Dankort.

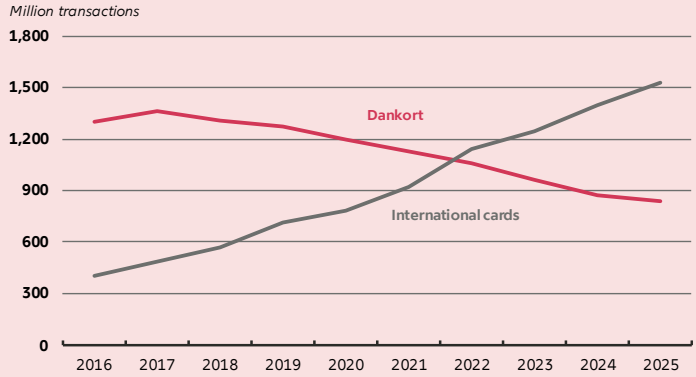
Since 2017, there has been a significant decrease in Dankort usage. This trend reversed in 2025. There is still a decline for the year as a whole, but it is smaller than in previous years, and in the fourth quarter of 2025 the use of Dankort increased. The decrease in Dankort usage is mainly due to increased use of Visa and Mastercard, see charts 3 and 4. However, Dankort still plays a central role in Danish retail payments.

[17] This includes all payments passing through the Danish retail clearing systems, including card payments, MobilePay, account transfers, bill payments through Betalingsservice, Leverandørservice and FI-kort as well as salary and Pension payout, etc. through Overførselsservice. The calculation method differs from that used in previous years' reports, and the figures are therefore not directly comparable.

CHART 3

Dankort and international card usage in Denmark (volume)

Total number of transactions made with payment cards in Denmark

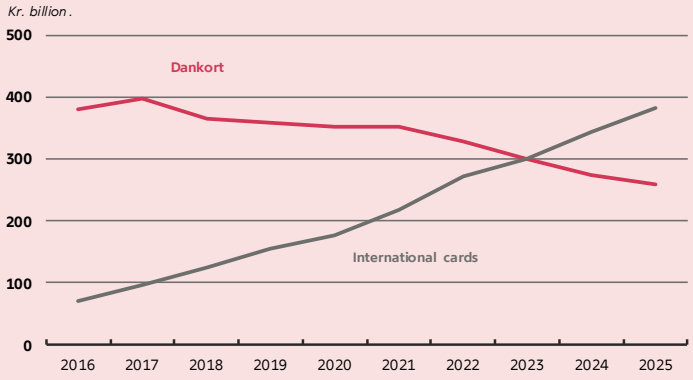


Note: The calculation covers card payments in physical trade, online and self-service environments in Denmark.
Source: Nets and Danmarks Nationalbank.

CHART 4

Dankort and international card usage in Denmark (value)

Total value paid with payment cards in Denmark



Note: The calculation covers card payments in physical trade, online and self-service environments in Denmark.
Source: Nets and Danmarks Nationalbank.

In particular, the use of international cards to make mobile payments via wallet solutions Apple Pay and Google Pay is driving developments in the card payments area.[18] From the beginning of 2025, Nets has mandated that card issuers/banks that enable the use of a card co-badged with Dankort in a wallet solution must ensure that the Dankort functionality is also available in the solution. If a bank issues a Visa/Dankort card where the Visa functionality can be used in a wallet, it must also ensure that the Dankort functionality can be used in the same wallet. All Danish banks now meet these requirements with regard to Apple Pay.[19]

The Danish Parliament passed a bill in June 2025 clarifying that payment systems must provide payment service providers with access to their payment systems on objective, non-discriminatory and proportionate terms.[20] This means that Nets must give other acquirers access to Dankort payments. In June 2025, the political parties behind the Dankort agreement (i.e. the Government, Green Left, the Conservatives, the Danish Social Liberal Party and the Danish People's Party) also entered into an agreement to strengthen Dankort, which is intended to ensure the issuance of significantly more Dankort cards. This will be achieved through the development of Dankort with balance monitoring and a business card, as well as the possibility of financing other initiatives that ensure the future development of Dankort. In this context, the agreement will form the basis for covering costs incurred by Nets associated with developing the new functions and the initiatives to give new acquirers access to Dankort payments.[21] Danmarks Nationalbank's oversight discussed the consequences of these changes with Nets in 2025. Discussions will continue in 2026, focusing on compliance with the PISA standards, including Nets' establishment of

[18] See Danmarks Nationalbank, *The digital payments market is changing, Danmarks Nationalbank News*, February 2025 *(link)*.
[19] Google Pay does not currently support payments with co-badged payment cards such as Visa/Dankort. The process of banks complying with Nets' requirements for Google Pay has therefore not yet begun.
[20] Act No. 711 of 20/06/2025 *(link)*.
[21] Ministry of Industry, Business and Financial Affairs, *New agreement to strengthen Dankort,* June 2025 *(link)*.

appropriate management of the risks associated with companies other than Nets acquiring Dankort transactions.

Operational reliability

Operational stability in the Dankort system was satisfactory in 2025, with full uptime apart from one major incident.

On 19 July 2025, there was a major incident in Nets' card payment systems, including the Dankort system. The incident was caused by an overload of a database in Nets' card platform and resulted in downtime of approximately 3.5 hours and long response times in Nets' systems, with only a limited share of card transactions being completed. In addition, the incident led to some payments being posted/reserved multiple times, and some payments being posted to incorrect accounts. Finally, the communication channels on Nets' website were down as it was overloaded by heavy traffic, and Nets was unable to handle the many enquiries. Nets' emergency solution in the form of offline card payments worked as expected during the outage, but many payees were unfamiliar with how to use this solution.

Danmarks Nationalbank has followed up on the handling of the incident together with Nets. The discussions focused on identifying the cause of the incident, including how payments came to be incorrectly posted, Nets' supplier management, and its crisis management and communication. In this context, Danmarks Nationalbank also participated as an observer in the IT inspection that the Danish Financial Supervisory Authority conducted at Nets in December 2025. The inspection was intended to follow up on how Nets handled the incident. The inspection has not yet been completed.

In connection with the follow-up to the incident, Danmarks Nationalbank and Nets also discussed the transition to a new operating platform for card payments. Nets expects that Dankort payments will be able to be processed on the new platform in 2027 and that the platform will increase resilience in the Dankort system.

Finally, Danmarks Nationalbank's oversight has followed Nets' work to further expand the possibility of making offline card payments, including card payments with mobile phones through, for example, Apple Pay or Google Pay. This is a key element of the work on the national contingency arrangements for payments[22], intended to ensure that consumers can pay for basic food and medicine for at least a week if digital payment solutions do not function normally. In this context, Danmarks Nationalbank has also focused on how the lessons learned from the incident in July 2025 are incorporated into Nets' further work to strengthen offline contingency arrangements both at Nets itself and at Nets' customers, i.e. shops and other payees.

Fraud

Dankort fraud remains low. It totalled approximately kr. 28 million in 2025, corresponding to approximately 0.1 per mille of total Dankort payments. The development from 2024 to 2025 has been broadly stable, and total fraud for the year has remained broadly unchanged.

Fraud related to card theft or loss continues to make up the majority of fraud. This type of fraud amounted to approximately kr. 21 million in 2025, while online shopping fraud totalled approximately kr. 7 million.

[22] This process is being led by Danmarks Nationalbank through its chairmanship of the Danish Payments Council. Read more about the Danish Payments Council on Danmarks Nationalbank's website (*link*).

International standards and cyber resilience

Danmarks Nationalbank assessed Dankort against PISA's requirements for risk management and contingency arrangements in 2024, leading to recommendations for Nets' work in these areas. One of the recommendations is that Nets strengthens its procedures for handling extreme but plausible scenarios. This is intended to help ensure that Nets has a strong framework for developing and maintaining its cyber contingency arrangements. Nets has started implementing the recommendations in 2025, and Danmarks Nationalbank and Nets are now discussing the results. Against this background, Danmarks Nationalbank will then assess whether Nets has complied with the recommendations. The bank will take into account the conclusions from The Danish Financial Supervisory Authority's IT inspection in its assessment.

In 2025, Danmarks Nationalbank also discussed how Nets is working to ensure sufficient redundancy in network connections and preparations for the introduction of quantum-safe encryption.

Betalingsservice and the PBS clearing

Danmarks Nationalbank's oversight of Betalingsservice and the PBS clearing is directed at Mastercard Payment Services Denmark A/S, MPS, the system owner of Betalingsservice and PBS clearing. PBS clearing is a partial clearing system used to collect transactions from MPS' own products, including Betalingsservice[23], and card transactions from Nets before they are included in Sumclearing, see chapter 3 *Clearing and settlement of retail payments*.

Operational reliability and fraud

Operational stability in Betalingsservice and the PBS clearing was high in 2025. There were no operational disruptions in Betalingsservice. The PBS clearing likewise had full uptime, with only a single minor delay in June due to the lack of timely delivery of settlement files for card payments from Nets. The contingency procedure in the PBS clearing functioned as expected in this context.

There was no fraud in Betalingsservice in 2025.

International standards and cyber resilience

Danmarks Nationalbank monitored the work of MPS on compliance with the PISA standards in 2025. The bank concluded that MPS has worked systematically to ensure that Betalingsservice complies with the PISA standards. The bank has focused in particular on the work of MPS on contingency arrangements and its ability to handle extreme but plausible cyber scenarios. These discussions will continue in 2026.

MPS strengthened its internal organisation in 2025 to ensure ongoing compliance with the PISA standards.

Danmarks Nationalbank and MPS also discussed the latter's efforts to ensure sufficient redundancy in network connections and to explore options for introducing quantum-secure encryption.

[23] In addition to Betalingsservice, Leverandørservice and Overførselsservice are included in the PBS clearing.

5
Securities settlement

Securities transactions can be concluded in different ways: on the stock exchange, through a multilateral trading facility or bilaterally between the parties through a bank or a stockbroker. After the trades have been concluded, there must be final settlement, i.e. where money and securities are exchanged between the participants.

The central securities depository Euronext Securities Copenhagen, ES-CPH[24], handles the settlement of trades in Danish-issued securities, and registrations of changes in the holdings of securities are made in the participants' accounts in ES-CPH.

Securities transactions between banks and other financial investors are initially settled on accounts in the pan-European system TARGET2-Securities, T2S, which handles the settlement process on behalf of ES-CPH. Movements of securities in accounts on T2S are subsequently mirrored in accounts in ES-CPH's systems. In legal terms, the final settlement of the securities trades only takes place when the relevant securities accounts in ES-CPH are updated. The settlement of the money side also takes place on accounts on T2S. Participants must therefore transfer liquidity to their settlement accounts in Danish kroner on T2S. Trades between banks and their own customers continue to be settled in ES-CPH's own settlement system.[25] In recent years, ES-CPH has gradually reduced the use of ES-CPH settlement and will fully phase it out; see the section below on system changes.[26]

ES-CPH is also responsible for handling periodic payments, issues, redemptions, etc.[27] ES-CPH is the only company in Denmark authorised by the Danish Financial Supervisory Authority to operate a central securities depository.

Use

ES-CPH has 88 participants, of which 35 are foreign market participants, including four central counterparties, CCPs.[28] 45 of the participants in ES-CPH also have an account in TARGET DKK so that they can transfer liquidity to their settlement account in T2S. It is also possible to transfer liquidity to settlement accounts on T2S via a co-manager in TARGET DKK without themselves being participants in TARGET DKK, see chapter 2, *Interbank payments and the central settlement of payments in Danish kroner*[29].

An average of approximately 102,000 trades per day in Danish kroner were settled through ES-CPH in 2025, an increase of 9.1 per cent compared to 2024,

[24] Until November 2020, ES-CPH was called VP Securities. VP Securities was then acquired by the pan-European stock exchange and the market infrastructure group Euronext Group. The change of name is only commercial, and the Danish company is still registered as VP Securities A/S in the CVR register.
[25] The division of settlement between T2S and ES-CPH settlement is also known as the layered settlement model. Settlement of securities transactions via the local ES-CPH settlement in Danish kroner and euro takes place only as free-of-payment trades, FoP. Settlement of trades in Swedish kronor continues to involve the exchange of funds between participants.
[26] You can also read more about this development in the section *System changes* below.
[27] Also known as corporate actions.
[28] The four foreign CCPs in ES-CPH are Cboe Clear Europe N.V, LCH Clearnet and Six x-clear, which clear equity trades, while Nasdaq Clearing AB clears repo trades. The regulatory control of the CCPs is conducted in so-called supervisory colleges, where the Danish Financial Supervisory Authority participates in the supervision of Cboe Clear Europe N.V and Nasdaq Clearing AB.
[29] Before Easter 2025, this transfer of liquidity took place in the same way, only from accounts in Kronos2 instead of TARGET DKK. See chapter 2, *Interbank payments*.

see table 3. This is due to an increase in the number of trades in shares and investment fund certificates. The average daily value of settled trades was approximately kr. 232 billion per banking day, which is an increase of 4.4 per cent compared with 2024, see table 3. This is due in particular to an increase in the value of trades in bonds and investment fund certificates. According to ES-CPH, the increase in the number of trades can be attributed to increased market activity as a result of the frequently changing US tariff announcements.

TABLE 3

Number and value of securities transactions

	Total		Bonds		Equities		Investment fund certificates	
Year, average per day	Number of transactions, thousand	Value, kr. billion	Number of transactions, thousand	Value, kr. billion	Number of transactions, thousand	Value, kr. billion	Number of transactions, thousand	Value, kr. billion
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	34.8	29.8	7.6
2020	90.5	231.5	3.8	178.1	49.0	43.5	37.7	9.9
2021	101.7	226.4	3.9	163.6	49.1	51.0	48.7	11.8
2022	91.3	255.4	5.2	194.6	39.6	51.3	46.5	9.5
2023	84.7	226.3	4.6	165.0	39.8	53.1	40.4	8.2
2024	93.6	221.9	3.8	144.4	43.3	68.6	46.5	9.0
2025	102.1	231.7	3.8	159.6	46.4	62.3	51.9	9.8

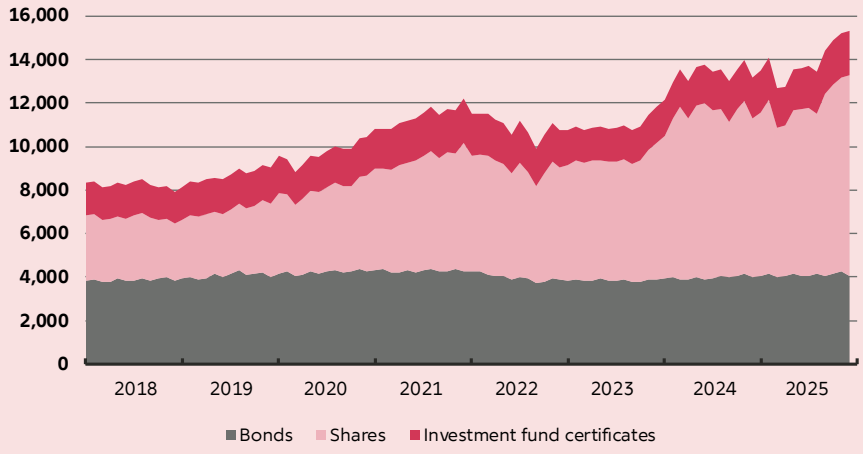
Source: ES-CPH.

The market value of securities held in ES-CPH increased by 16 per cent in 2025, see chart 5. This rise is mainly due to increases in the value of shares and investment fund certificates.

CHART 5

Market value of securities held in ES-CPH

Kr. billion, current prices



Source: ES-CPH

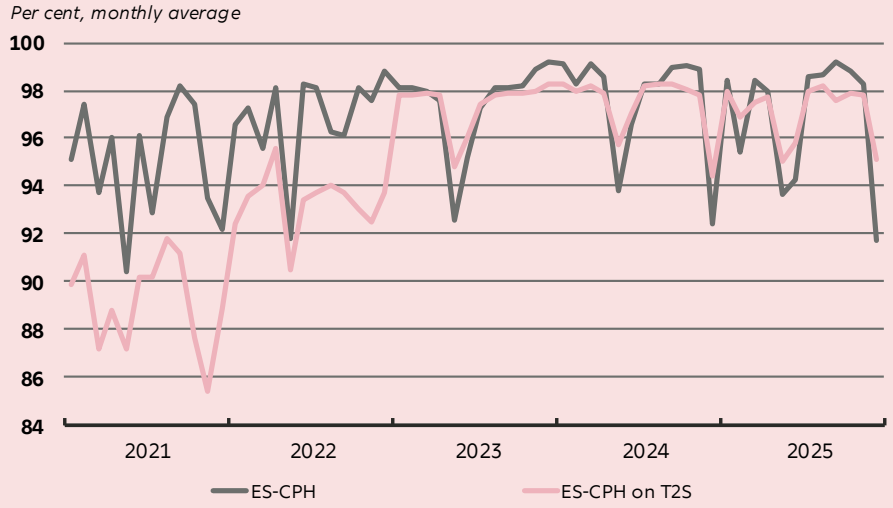
Settlement ratio

The settlement ratio measures the proportion of trade turnover settled on time, i.e. within two days of the trading day.[30]

Chart 6 shows the settlement ratio for ES-CPH's settlement on T2S and for ES-CPH's own system. It is satisfactory that the settlement ratio in 2025 is generally maintained at a high level. The only exception is February, when there was a decrease in the settlement ratio due to the incident in TARGET Services on 27 February, see below. The fluctuations in May, June and December are due to T2S being open on Danish bank closing days and do not reflect a decline in settlement discipline among participants.[31]

CHART 6

Settlement ratio



Source: ES-CPH

Operational reliability

The operational stability in the settlement of Danish securities transactions in the ES-CPH settlement was generally satisfactory in 2025. Three major incidents in TARGET Services had a significant impact on operations at ES-CPH. The incidents occurred on 27 February, 13-14 March and 5 May 2025, and all three were caused by communication problems between T2S and the associated central securities depositories and participants. As a result of the incidents, ES-CPH had to suspend the settlement of trades in a number of securities, which led to delays in the closure of the settlement day and in the settlement of securities trades. Managing the incidents required substantial work at ES-CPH to enable the correct reconciliation of participants' securities accounts. Danmarks

[30] According to article 5 of CSDR, securities trades must be settled within two days of the trading day. From 11 October 2027, the settlement time will be shortened so that trades must be settled no later than the day after the trading day.
[31] On Danish bank closing days, when T2S is also open, there is a decrease in settlement efficiency due to the lack of activity among Danish participants. The decrease in May is due to 30 May, the day after Ascension Day. The decrease in June is due to Constitution Day. The decrease in December is due to 24 and 31 December. T2S is open on these days. In years when the special Danish bank closing days fall at a weekend, this does not cause fluctuations in the settlement ratio.

Nationalbank's oversight has followed up on ES-CPH's handling of the incidents and assesses that the follow-up has been satisfactory.

For a more detailed description of the incidents in T2S, see chapter 6, *Payments and securities settlement in euro*.

International standards and cyber resilience

Danmarks Nationalbank oversees that the settlement of Danish securities transactions in ES-CPH and T2S complies with international standards for financial market infrastructures.

The bank's oversight of ES-CPH is closely coordinated with the Danish Financial Supervisory Authority, as it concerns many of the same elements as the authority's supervision of ES-CPH's compliance with the requirements of the pan-European legislation on central securities depositories, CSDR.[32] In this regard, Danmarks Nationalbank contributes to the Danish Financial Supervisory authority's ongoing evaluations of whether ES-CPH fulfils the requirements of CSDR (also called Review and Evaluation). Here Danmarks Nationalbank pays particular attention to ES-CPH's management of operational risks and its contingency arrangements, especially for handling extreme but plausible scenarios.

The oversight of T2S is carried out in collaboration with all central banks connected to the platform, with the ECB as lead overseer and coordinator, see chapter 6, *Payments and securities settlement in euro*.

Danmarks Nationalbank performed an assessment of ES-CPH against CPMI-IOSCO's Cyber Guidance in 2020.[33] The assessment showed that ES-CPH complied with the Cyber Guidance in most areas. In a few, but key, areas Danmarks Nationalbank made recommendations to ES-CPH on how to strengthen its cyber resilience. This includes ES-CPH's procedures for handling extreme but plausible cyber scenarios. This should help ensure that ES-CPH has a robust framework for developing and maintaining its cyber preparedness. The bank found that ES-CPH complied with further two of the recommendations in 2025. One of the original 16 recommendations remains open.

Danmarks Nationalbank is continuously monitoring ES-CPH's efforts to improve the cyber resilience of its systems. In 2025, Danmarks Nationalbank and ES-CPH discussed the importance, in ES-CPH's crisis management planning, of ensuring sufficient staffing to be able to handle the simultaneous activation of both its own internal crisis management and FSOR's Crisis Management. Danmarks Nationalbank and ES-CPH also discussed the need to ensure better integration of escalation to FSOR's Crisis Management in ES-CPH's own internal contingency plans.

In 2025, Danmarks Nationalbank and ES-CPH also discussed ES-CPH's work to ensure sufficient redundancy in network connections and ES-CPH's preparations for introducing quantum-secure encryption.

System updates

ES-CPH began using the Euronext Group's corporate actions platform, CA4U, to handle corporate actions for bonds in 2024. ES-CPH decided to postpone the

[32] 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 etc., abbreviated CSDR (link), aims to harmonise the timing and conduct of securities settlement as well as the rules for the central securities depositories, CSs, that operate the settlement infrastructure.
[33] Danmarks Nationalbank's assessment of ES-CPH according to Cyber Guidance has not been published.

planned use of CA4U in 2025 for other types of securities from the end of 2025 to September 2026.

In October 2025, the European Parliament and the Council of Ministers adopted the European Commission's proposal to shorten the settlement period for securities transactions to the day after the trading day (also known as T+1).[34] This will require a number of changes to current market practices and to IT systems in the financial sector. Ahead of the transition to T+1 settlement on 11 October 2027, ES-CPH will make adjustments to the local settlement platform so that it can support the shorter settlement period. ES-CPH had previously planned to phase out the tiered settlement model during 2027. In 2025, ES-CPH agreed with the settlement participants to postpone the phasing out of the local settlement platform until August 2028. After that, all securities trades must be settled on T2S. After August 2028, ES-CPH is scheduled to have completed its part of the Euronext Group's *convergence programme*, under which all five CSDs will run on the same technical platform.[35]

[34] Regulation (EU) 2025/2075 of the European Parliament and of the Council of 8 October 2025 amending Regulation (EU) No 909/2014 as regards a shorter settlement cycle in the Union (*link*).
[35] In addition to ES-CPH, the CSDs in Greece, Italy, Norway and Portugal are part of the Euronext Group.

6
Payments and securities settlement in euro

Settlement of payments and securities transactions in euro takes place through TARGET Services. TARGET Services consists of three services, namely T2, T2S and TIPS. T2 is the pan-European RTGS system for the settlement of large and time-critical payments as well as for the transfer of liquidity for settlement in other systems, including T2S and TIPS. T2S, TARGET2-Securities, is the pan-European system for the settlement of securities transactions. TIPS is the settlement system for instant payments.

TARGET Services can handle multiple currencies, including Danish kroner. This chapter focuses on the settlement of payments in euro.

TARGET Services is owned by the European Central Bank, ECB, and the national central banks of the euro area and is operated by the 4CB (the four central banks of Germany, France, Italy and Spain) with the ECB acting as coordinator.

The oversight of TARGET Services is carried out in collaboration between the ECB oversight function and the other central banks connected to T2 or T2S. 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.

Use

In total, around 1,000 banks use T2 to process payments in euro, including 18 Danish banks and branches of foreign banks in Denmark. In 2025, Danish participants carried out interbank payments averaging EUR 5.4 billion per day. Danish participants mainly use T2 to execute intra-group payments and payments to foreign participants. The largest euro flows are exchanged with participants in Germany, France, Finland and Belgium.

There is a total of 24 CSDs operating in 23 EU countries connected to T2S, including ES-CPH. A bank may settle securities transactions via T2S as either a direct participant, if the bank has a T2S settlement account, or as an indirect participant via a direct participant. A T2S settlement account is set up through one of the central banks in the EU, including Danmarks Nationalbank. There are 11 Danish participants that have a T2S settlement account in TARGET Services via Danmarks Nationalbank and use it to pay or receive euro in connection with T2S settlement.

There are currently no Danish participants offering instant payments in euro via TIPS, but this will change from 2027, when participants that offer credit transfers in euro will also be required to offer instant payments in euro, cf. the Instant Payments Regulation. The Instant Payments Regulation, IPR, was adopted by the European Parliament and the Council on 13 March 2024 and aims to accelerate the roll-out of instant payments across Europe. The regulation applies to credit transfers in euro within the EU.

Operational reliability

The operational stability of TARGET Services was not fully satisfactory in 2025. There have been several major incidents that have affected both the settlement of payments and securities transactions in euro, as well as settlement in other

systems; see the chapters on interbank payments in Danish kroner, securities settlement and settlement of foreign exchange trades.

At the end of February, a major incident in TARGET Services meant that payments and securities settlement in T2 and T2S could not be carried out for approximately eight hours during the middle of the day. As a result of the incident, the closure of the European monetary policy day was postponed by six hours. During the incident, the enhanced contingency solution in TARGET Services, ECONS II, was activated to process the most time-critical payments.

On 13 and 14 March, there were problems sending confirmations to T2S participants that the securities settlement had been completed. The incident meant that central securities depositories were unable to reconcile participant holdings and, as a result, had to suspend the settlement of trades in certain securities. The incident caused delays in the closing of the monetary policy day, including the DKK business day, as well as significant delays in the settlement of securities transactions.

On Monday 5 May, there were difficulties accessing TARGET Services. The ECB decided that operations should be transferred to another data centre, a process, which takes an hour and a half, during which TARGET Services was unavailable. The consequence was that payments and securities transactions could not be carried out during this period.

At the end of November, there were two incidents in TARGET Services where operational failures delayed the settlement of securities and delayed the settlement day in euro and Danish kroner, respectively.

Those responsible for the operation of TARGET Services have followed up on the incidents, and measures have been initiated to prevent similar incidents in future. Danmarks Nationalbank's oversight participates in the follow-up of incidents under the auspices of the joint oversight. Assessments of TARGET Services' follow-up to incidents and compliance with international standards are communicated by the ECB's oversight function. In addition, Danmarks Nationalbank's oversight follows up on the handling of the connected systems of the consequences of those events; see chapter 2 *Interbank payments*, chapter 5 *Securities settlement* and chapter 7 *Foreign exchange settlement*.

International standards

The ECB and the joint oversight are in the process of finalising two assessments: a so-called comprehensive assessment of T2 and TIPS under the SIPS Regulation, Regulation on oversight requirements for systemically important payment systems[36], and an assessment of T2S under the CPMI-IOSCO Principles for Financial Market Infrastructures, PFMI.

In 2022, ECB oversight completed an assessment of T2S's compliance with the Cyber Resilience Oversight Expectations, CROE. Danmarks Nationalbank's oversight participates in the follow-up to the action plan prepared by the ECB to address identified areas for improvement under the joint oversight of TARGET Services.

[36] European Union, Regulation (EU) No 795/2014 of the European Central Bank of 3 July 2014 on oversight requirements for systemically important payment systems, July 2014 (*link*).

System updates

In June 2025, the Eurosystem's collateral management system, ECMS (Eurosystem Collateral Management System), was launched.[37] ECMS only handles collateral in euro and not in Danish kroner.

[37] European Central Bank, *Eurosystem launches single collateral management system,* June 2025 (*link*).

7
Settlement of foreign exchange transactions

The foreign exchange market is the largest of all financial markets globally in terms of turnover. Central banks, financial institutions, companies and private individuals all need to buy or sell currency. Foreign exchange transactions in which Danish kroner are bought or sold against another currency can either be settled via correspondent banks or through the international foreign exchange settlement system, CLS.

When a foreign exchange trade is settled via correspondent banks, the settlement of the two payments does not necessarily occur simultaneously. Foreign exchange transactions are often settled across time zones, and payments can be in transit for many hours. This happens, for example, if a Danish bank sells Danish kroner and buys dollars from an American bank. The Danish bank may send the krone payment in the morning, Central European Time. By this time, it is night in the US, and the US bank may not send dollars via the US payment system until its usual opening hours, which could be many hours later. In the intervening period, the Danish bank has therefore made the payment without having received the purchased currency. This can result in significant losses if the other party to the foreign exchange transaction defaults or becomes insolvent before the counterpayment is made and can potentially lead to systemic consequences.

When settlement takes place through the foreign exchange settlement system, CLS, settlement risk is significantly reduced because both sides of the foreign exchange transaction are settled simultaneously (payment-versus-payment, PvP). In addition to PvP settlement, the CLS settlement system is a multilateral netting arrangement that produces a consolidated account of participant payments across currencies and counterparties, thereby reducing participants' liquidity needs by over 96 per cent.[38]
CLS currently settles foreign exchange transactions in 18 connected currencies, including Danish kroner, euro and US dollar. Only FX trades where both currencies in the trade are connected to CLS can be settled in CLS. On average, foreign exchange trades worth over USD 8,000 billion are settled in CLS each banking day.

CLS also offers a bilateral netting calculation service covering 120 currencies, CLSNet[39], which provides participants with a comprehensive overview of their net payment obligations. Netting reduces the settlement risk in foreign exchange transactions, as netting reduces the amounts that are to be exchanged between the parties to foreign exchange transactions. CLSNet therefore helps to reduce settlement risk for foreign exchange transactions that cannot be settled in the CLS settlement system.

CLS is owned by the major international banks participating in the CLS settlement, including Danske Bank and Nordea.

[38] CLS Bank, *CLSSettlement,* March 2026 (*link*).
[39] CLS Bank, CLSNet, March 2026 (*link*).

Danmarks Nationalbank collaborates with the central banks of the other member currencies on overseeing CLS, see box 5.

BOX 5

Oversight of CLS

Oversight of CLS is carried out by a joint CLS Oversight Committee[1], which is a forum for collaboration between the central banks of the participating currencies, through which they can handle their national oversight responsibilities. Danmarks Nationalbank participates in the collaboration, which is led by the US Federal Reserve, which is also the supervisory authority for CLS. Danmarks Nationalbank's oversight focuses especially on issues that affect the settlement of transactions in Danish kroner. Oversight of CLS is based on the CPMI-IOSCO principles for safe and efficient payment systems (Principles for Financial Market Infrastructures, PFMI). CLS published its most recent description of how the system complies with CPMI-IOSCO's principles in August 2024.[2]

[1] See Federal Reserve System, Protocol for the Cooperative Oversight Arrangement of CLS (*link*)
[2] See CLS, Principles for financial market infrastructures (PFMI) disclosure, 2024 (*link*)

Use

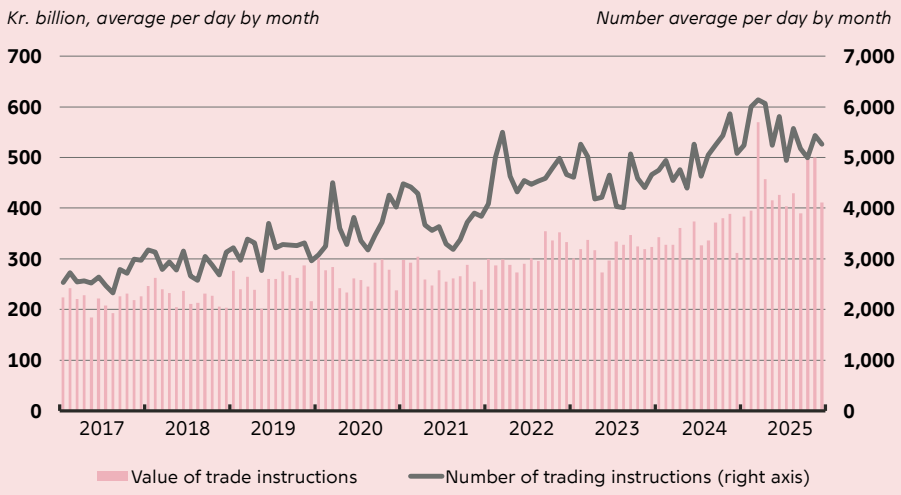
The Danish krone is the 21st most traded currency in the world.[40] The average value of trades in Danish kroner settled in CLS was kr. 457 billion per banking day in 2025. This is a substantial increase of 26.6 per cent relative to 2024, see chart 7. This development is in line with a general global trend, where heightened volatility in international financial markets, for example in connection with repeated US tariff threats, has contributed to increased activity in the global foreign exchange markets.

Danish banks and companies can settle foreign exchange transactions via CLS. There are four direct participants in CLS that make payments in Danish kroner to the CLS settlement. In addition, a number of Danish banks and companies participate indirectly in the CLS settlement via one of the four direct participants.

[40] See Danmarks Nationalbank, Trading in Danish Kroner has increased – especially in Denmark, *Danmarks Nationalbank Statistical News*, December 2025 (*link*).

CHART 7

Trading instructions in CLS



Source CLS Bank.

Operations and liquidity

The Danish participants reserved sufficient liquidity for CLS settlement in 2025.

CLS settlement takes place during a relatively short period of time during the day when the RTGS systems of the connected central banks are open simultaneously across time zones. Pay-ins and pay-outs related to CLS are made via the connected central banks' RTGS systems. For Danish kroner, this means through TARGET DKK. The stability of CLS settlement is therefore dependent on the stability of the connected RTGS systems. Due to the interdependencies between CLS and the RTGS systems of the 18 associated currencies, an event in one RTGS system can propagate to other systems. This was the case, for example, in February 2025, when CLS settlement was affected by a major incident in TARGET Services; see chapter 6, Payments and securities settlement in euro. The incident delayed payments in several currencies, including USD, CAD, CHF, GBP and SEK, because CLS was waiting for incoming euro payments. In CLS settlement, the settlement and funding processes are closely interconnected, so currency payments can only be executed once the necessary incoming payments in other currencies have been received.

Publications



ANALYSIS

Analyses focus on current issues of particular relevance to Danmarks Nationalbank's objectives. The analyses may also contain Danmarks Nationalbank's recommendations. They include our projections for the Danish economy and our assessment of financial stability. Analyses are targeted at people with a broad interest in economic and financial matters.



STAFF PAPER

Staff Papers provide insights into the analytical work being done by employees of Danmarks Nationalbank. Staff Papers include, for example, background analyses and method descriptions. They are primarily targeted at people who already have knowledge of economic and financial analyses. The conclusions expressed in Staff Papers are the authors' own and should not be interpreted as views held by Danmarks Nationalbank.



WORKING PAPER

Working Papers present research work by both Danmarks Nationalbank's employees and our partners. Working Papers are primarily targeted at professionals and people with an interest in central banking research as well as economics and finance in a broader sense. The conclusions expressed in Working Papers are the authors' own and should not be interpreted as views held by Danmarks Nationalbank.



NEWS

News may be a news article or an appetiser offering quick insight into one of Danmarks Nationalbank's more extensive publications. The series is targeted at people who need an easy overview and like a clear angle.



STATISTICAL NEWS

Statistical news focuses on the latest figures and trends in Danmarks Nationalbank's statistics. Statistical news is targeted at people who want quick insight into current financial data.



REPORT

Reports consist of recurring reports on Danmarks Nationalbank's areas of work and activities. Here you will find Danmarks Nationalbank's annual report, among other documents. Reports are targeted at people who need a status and update on the past period.

The analysis 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
2100 Copenhagen Ø
+45 3363 6363

This edition closed for contributions on 30 March 2026

DANMARKS NATIONALBANK