DANMARKS NATIONALBANK

17 MAY 2017 — No. 4

Dankort Assessment

- Dankort payments account for around 60 per cent of retail turnover, while cash and other payment cards make up the rest. A secure and well-functioning Dankort is important.
- Dankort's performance is stable with a high degree of availability, and Dankort fraud is low by international comparison.
- Danmarks Nationalbank has assessed Dankort, which is owned by Nets A/S, against the ECB standards for card payment schemes. Danmarks Nationalbank's assessment contains recommendations to Nets. Nets should ensure a more systematic knowledge management in relation to Dankort. Currently Nets conducts risk analyses of the Dankort IT platform. This work should be expanded by means of a risk assessment of all relevant aspects of Dankort. Nets should strengthen the framework for decision-making and communication as regards Dankort.

CONTACT

Ole Mikkelsen
Communications
and press officer

omi@nationalbanken.dk
+45 3363 6027

SECRETARIAT
AND COMMUNICATIONS

A secure

and well-functioning Dankort is important.

Read more

Low fraud

and stable performance.

Read more

Recommendations

in regard of the ECB standards

Read more

Dankort payments account for the largest share of Danish retail sales. A well-functioning Dankort and a low degree of Dankort fraud are important. Consequently, Dankort should meet international standards for card payment schemes.

The ECB has set up standards for well-functioning card payment schemes (link) that serve as the benchmark for assessment of e.g. VISA, MasterCard, American Express and local card payment schemes in Europe.

Danmarks Nationalbank has assessed Dankort's observance of the ECB standards for card payment schemes.

Nets is the owner of Dankort and authorises banks to issue Dankort. This makes Nets the scheme owner or governance authority for Dankort, and the responsibility for ensuring Dankort's compliance with the ECB standards rests with Nets.

Danmarks Nationalbank's Dankort assessment covers the elements of Nets' activities that contribute to the functioning of Dankort. The responsibility for ensuring a well-functioning Dankort is anchored in various parts of the Nets organisation. For instance, the responsibilities for the legal aspects of and rules concerning the Dankort, for customer contact and for the IT infrastructure are placed in different parts of Nets.

In this publication, the background and methodology of the assessment are first described, followed by a summary of Danmarks Nationalbank's assessment of Nets' observance of the ECB standards for card payment schemes. The subsequent sections describe Nets' compliance with the standards and Danmarks Nationalbank's recommendations and comments regarding improvements.

Facts about Nets

Headquartered in Denmark, Nets A/S is a Nordic provider of products related to payment systems and card and information services, among other products. Nets is the governance authority for Dankort, but also offers a range of other products, such as Betalingsservice (direct debit). Nets' customers are more than 240 banks and 300,000 retailers in the Nordic countries.

The company's history goes back to 1968, and its name has been Nets since 2010.

In 2014, Nets was sold to ATP and two US private equity funds, Advent International and Bain Capital. Nets went public in 2016.

Danes and Dankort in figures

Denmark is among the European countries with the largest shares of card payments relative to total payments. Dankort is the Danes' preferred payment solution; in 2016, Dankort payments accounted for around 60 per cent of total retail turnover. In 2016, 1.3 billion Dankort payments were made, with a total value of kr. 379 billion.

Approximately 5.4 million Dankort and VISA/Dankort have been issued. Each adult Dane has an average of 1.2 Dankort. Practically all stores in Denmark accept Dankort.

Key Dankort actors

Nets is the owner of Dankort and has several roles in the Dankort scheme. Nets

- is the sole acquirer of Dankort payments, i.e. Nets ensures that the payee receives the card payment;
- undertakes card issuer services, i.e. helps the issuer to e.g. process transactions, send out PINs, service customers and monitor fraudulent use;
- processes card payments, including by providing the infrastructure between the card issuer and the acquirer which ensures exchange of information between the parties. Nets as processor is responsible for netting out the day's Dankort transactions and calculating what each bank must pay or receive from each of the other banks;
- operates the Danish "Sumclearing" clearing and settlement system, in which final settlement of Dankort payments takes place on behalf of Finance Denmark.

Banks planning to issue Dankort must conclude a licence agreement with Nets. The licence agreement imposes various obligations on the banks, including an obligation to observe the Dankort scheme rules concerning security requirements, etc. A condition for obtaining a licence is that the bank is under the supervision of the Danish Financial Supervisory Authority, FSA, or a corresponding authority in another EU member state. Moreover, the issuer must have concluded an agreement with Finance Denmark, the owner of the Sumclearing.

Nets has concluded licence agreements with 77 banks, of which 6 are foreign banks' branches in Denmark.

A retailer wanting to receive Dankort must first conclude a payment card agreement with Nets. Standard conditions apply to all payees, although a distinction is made between physical and non-physical trading.

The cardholder is the person to whom the card has been issued and who has the right to use the card.

Other actors include
- providers of payment modules – or gateways – for e-commerce,
- suppliers of terminals, and
- card manufacturers.

Processing a Dankort payment

A Dankort payment involves a number of steps. The payment is initiated by the cardholder using the card in a store, and the final step is when the amount is deposited to the retailer's account. The Dankort payment steps in physical trading are described in Box 1. Nets' role in the individual steps is indicated in brackets, since Nets undertakes several payment processing functions, as mentioned above. Sumclearing settlement takes place at night, so the entire Dankort payment process typically takes one day, i.e. if payment is made on a Wednesday, the money will be deposited to the retailer's account on the Thursday. At weekends and on public holidays, the settlement process takes longer.

Danmarks Nationalbank's oversight

Danmarks Nationalbank's oversight of the key Danish payment solutions is anchored in section 1 of the Danmarks Nationalbank Act, which states that the objective of Danmarks Nationalbank is to "maintain a safe and secure currency system in this country, and to facilitate and regulate the traffic in money and the extension of credit". Danmarks Nationalbank's oversight is described in detail in Danmarks Nationalbank's oversight policy (link). Oversight of Dankort takes place in accordance with ECB's general standards for payment instruments from 2009, implemented as specific standards for oversight of card payment schemes (link).

The ECB standards require:
1. a sound legal basis under all relevant jurisdictions,
2. access to comprehensive information for all actors, including appropriate information on financial risks,
3. an adequate degree of security, operational reliability and business continuity,

Dankort payment process Box 1

1. The cardholder initiates the payment by using the card in the in-store terminal, entering a PIN and pressing OK.
2. Via Nets or another transaction compiler, the retailer sends a request to Nets (acquirer) for authentication of the card and PIN.
3. Nets (acquirer) sends the request to Nets (card issuer service), which approves or rejects the payment request.
4. Nets (acquirer) receives a response from Nets (card issuer service), which is sent to the in-store terminal.
5. If the payment is approved, the transaction is effected, and the retailer releases the purchased goods.
6. The retailer sends a request to Nets (acquirer) for receipt of money for the purchase. Nets (acquirer) forwards the request to Nets (processor), which provides the infrastructure between the card issuer and the acquirer that ensures exchange of information between the parties.
7. 10 times a day, information about Dankort purchases is sent from Nets (processor) to the cardholder's bank – in one of these processes, the cardholder's account is debited.
8. Nets (processor) is responsible for and provides clearing and settlement facilities for the Dankort parties. Nets (processor) nets out the day's Dankort transactions and other payments included in the PBS clearing and calculates what each bank must pay or receive from each of the other banks. These amounts are sent to the Sumclearing, where they are added to the equivalent amounts from the electronic clearing. [1]
9. Final clearing and settlement takes place in the Sumclearing in the banks' settlement accounts at Danmarks Nationalbank.
10. After settlement in the Sumclearing, the retailer's bank deposits the amount to the retailer's account.

1. Dankort transactions are cleared in the PBS clearing and the electronic clearing, which are parts of the Sumclearing. For example, the PBS clearing comprises Dankort payments via physical online terminals in stores and for Internet purchases, payments abroad using a VISA/Dankort and payments using an international debit card issued by a Danish bank. The electronic clearing includes e.g. cash withdrawals using the Dankort in branches or in ATMs of banks other than the cardholder's bank.

4. effective, accountable and transparent governance arrangements,
5. management and containment of financial risks in relation to the clearing and settlement process.

Danmarks Nationalbank oversees clearing and settlement systems in another context, and the elements of Standard 5 that are comprised by this oversight have not been assessed in connection with the Dankort assessment.

For each standard, the ECB requirements are described in general terms later in this report.

Collaboration between Danmarks Nationalbank and the Danish FSA

Danmarks Nationalbank collaborates with the Danish FSA, cf. the Memorandum of Understanding concluded between the two authorities (link). The purpose of the collaboration is to avoid double regulatory control and to optimise regulatory resource utilisation.

The Danish FSA's supervision of Nets is described in Box 2.

As regards Nets, there are several interfaces between Danmarks Nationalbank and the Danish FSA. Generally, Danmarks Nationalbank and the Danish FSA keep each other informed of issues, and Danmarks Nationalbank participates as an observer in the Danish FSA's IT inspections at Nets.

The Danish FSA's IT inspections are described in more detail in Box 3. Danmarks Nationalbank's assessment of Nets' observance of the elements of Standards 3 and 4 that concern, inter alia, IT security management, operation, contingency plans, outsourcing and audit are based on the Danish FSA's work to the greatest possible extent. As a general rule, Danmarks Nationalbank does not assess areas that are under the supervision of the Danish FSA, except for those of specific Dankort relevance.

Nets holds a licence as a payment institution, one reason being that Nets offers acquiring of Dankort payments. The Danish FSA therefore supervises Nets' compliance with the requirements of the Danish Payment Services Act. In this connection, the Danish FSA oversees Nets' observance of the EBA guidelines on the security of Internet payments. Since the Danish Payment Services Act and the EBA guidelines on the security of Internet payments

The Danish FSA's supervision of Nets as a shared data centre and payment institution Box 2

Nets is a shared data centre of major importance to the Danish payments infrastructure, cf. section 343q of the Danish Financial Business Act (link). It appears from Part 20c of the Financial Business Act that shared data centres must observe rules on adequate control and security measures in the IT area. More detailed rules are stipulated in the Executive Order on Governance, Appendix 5 on IT security (link).

Nets is also subject to the Executive Order on system audits in shared data processing centres (link).

Moreover, Nets is subject to the same outsourcing rules as financial enterprises, such as banks, cf. the Executive Order on outsourcing of significant areas of activity (link).

The Danish FSA supervises compliance with the rules and performs activities in connection with the supervision of Nets. The Danish FSA

- carries out IT inspections, applying a risk-based approach (see also Box 3);
- is regularly informed of major incidents;
- reviews the system audit reports.

According to the Danish Payment Services Act, the Danish FSA authorises and supervises payment institutions, including Nets (link). The authorisation is based on a review of compliance with the statutory requirements.

The Danish FSA regularly supervises Nets' compliance with the Payment Services Act and approves outsourcing of important operational functions. The Danish FSA has incorporated the EBA's guidelines on the security of Internet payments (link) into its supervision of the Payment Services Act.

overlap the ECB standards forming the basis for Danmarks Nationalbank's Dankort assessment, Danmarks Nationalbank and the Danish FSA collaborate on issues of relevance to both authorities. For example, Danmarks Nationalbank has followed the discussions between the Danish FSA and Nets about the "Dankort Secured by Nets" security solution introduced for Dankort payments on the Internet. This solution, which entails strong authentication for Internet payments, is also key to Nets' compliance with the requirements under Standard 3, i.e. the requirements for strong authentication in connection with card payments for physical and non-physical transactions.

Interfaces with other authorities

There are several interfaces between Danmarks Nationalbank and authorities other than the Danish FSA.

One such authority is the Danish Competition and Consumer Authority, which, inter alia,

- supervises compliance with access to payment systems, cf. section 40 of the Danish Payment Services Act (link),
- carries out cost studies of the Dankort as described in Executive Order no. 605 of 03.06.2016 (link), and
- supervises Nets' compliance with the Regulation on interchange fees for card-based payment transactions, also called the MIF Regulation (link). The MIF Regulation seeks to contribute to enhancing competition for the services provided in connection with card payments.

Another interface for Danmarks Nationalbank is to the Danish Data Protection Agency, which oversees compliance with the Danish Act on Processing of Personal Data (link).

Danmarks Nationalbank did not assess areas within the remit of the authorities mentioned above.

Delineation and methodology

Danmarks Nationalbank's Dankort assessment is based on Nets' self-evaluation, which contains Nets' responses to a large number of questions concerning the ECB standards for card payment schemes. Moreover, Nets has submitted extensive documentation, including sets of agreements with the Dankort actors, organisation plans, security policies, risk analyses, etc. Danmarks Nationalbank and Nets were in ongoing dialogue about the assessment.

The Danish FSA's IT inspections Box 3

The Danish FSA adapts its IT inspections to the company at hand on the basis of, inter alia, an assessment of importance and risk. An IT inspection will often comprise the following areas:

- IT strategy, IT security strategy and IT governance, including IT security management and IT risk management
- IT contingency plans and testing of IT contingency procedures.
- Outsourcing – compliance with the Executive Order on outsourcing, and control of suppliers
- Granting of rights, access management and logical access controls
- Physical security and access management
- IT operational management and oversight
- Internal and external system audits
- Change management and project management
- Administration and maintenance of network and system software
- Strategy and security measures to combat IT crime.

Source: Danish Financial Supervisory Authority's website (link).

On the basis of the assessment, Danmarks Nationalbank has issued a number of recommendations and comments to Nets, which are detailed below.

Overall assessment

Danmarks Nationalbank has assessed Dankort against the ECB standards.

In the assessments against the five standards, the following five categories have been applied: Observed, broadly observed, partly observed, not observed and not applicable, cf. Box 4.

Danmarks Nationalbank's assessment of Dankort is as follows:

Standard 1 (A sound legal basis under all relevant jurisdictions): Broadly observed

Standard 2 (Access to comprehensive information for all actors, including appropriate information on financial risks): Broadly observed

Standard 3 (An adequate degree of security, operational reliability and business continuity): Partly observed

Standard 4 (Effective, accountable and transparent governance arrangements): Broadly observed

Standard 5 (Management and containment of financial risks in relation to the clearing and settlement process): Observed

Dankort complies with many of the ECB requirements for card payment schemes. Nevertheless, Danmarks Nationalbank has identified potential for improvement. Recommendations have been issued in respect of key issues. Comments have been issued in respect of other issues.

Nets should address the recommendations and comments. Danmarks Nationalbank will monitor the progress as an element of its continuous oversight.

Danmarks Nationalbank's assessment of Nets' compliance with the requirements under the ECB standards for card payment schemes is described below. For each standard, the ECB requirements are first described, followed by Danmarks Nationalbank's overall assessment of Nets' compliance with the requirements. Finally, Danmarks Nationalbank's recommendations and comments for the individual standards are listed.

Rating scale for assessment against the standards Box 4

In the assessment against each standard, the following categories have been applied:

- *Observed* is used when all significant criteria have been observed and any deficiencies are only minor and adaptation can take place on a continuous basis as part of the normal operations.
- *Broadly observed* is used when one or more deficiencies have been identified which should be addressed within a given deadline.
- *Partly observed* is used when one or more major deficiencies have been identified which could be serious if they are not immediately addressed. Remediation of such deficiencies should be given high priority.
- *Not observed* is used when one or more serious deficiencies have been identified which require immediate action. Remediation of such deficiencies should be given top priority.
- *Not applicable* is used when the standard does not apply due to structural, legal or institutional circumstances.

Standard 1: A sound legal basis under all relevant jurisdictions

Standard 1 concerns the legal basis for the card payment scheme, including the following:

- Legislation and jurisdiction should be clearly identified.
- Relevant national and EU law should be observed, and the governance authority should perform regular reviews of this compliance.
- The rules and procedures of the card payment scheme should be complete, unambiguous and enforceable.
- The card payment scheme actors should conclude legally binding agreements, which should be complete, unambiguous and enforceable.

Danmarks Nationalbank has reviewed whether Nets has a process in place for ensuring compliance with relevant legislation. Danmarks Nationalbank has not assessed Nets' compliance with relevant legislation, as this is supervised by other authorities, including primarily the Danish FSA, the Danish Competition and Consumer Authority and the Danish Data Protection Agency.

Assessment
The Dankort scheme operates in Denmark only and is governed by Danish law.

In 2016, Nets established a "regulatory forum" with the purpose of ensuring a harmonised process for following up new statutory and regulatory rules or amendments to existing statutory or regulatory rules.

The rules and procedures for Dankort are implemented in the Dankort scheme rules. Actors involved in the scheme should submit to Nets, on an annual basis, a report by the management and a statement signed by the auditor about compliance with the security requirements of the scheme rules. Nets ensures that the rules are enforced by following up comments and qualifications. Nets regularly updates the Dankort scheme rules. For example, the rules were amended when cards with contactless functionality began to be issued. Nets has stated that they have not received any complaints about the scheme rules. If an actor points out a drawback, Nets will initiate a dialogue about it and amend the rules, if deemed appropriate.

Nets has prepared standard contracts for card issuers and retailers, i.e. a licence agreement and a payment card agreement, respectively. The agreements include provisions on enforcement, including courses of action in the event of default, and on dispute resolution. Nets ensures that the agreements are unambiguous by making amendments if Nets becomes aware of ambiguities. For example, the payment card agreement was changed so as to clarify that it is the retailer's responsibility to inform Nets if the store closes down. Completeness is ensured by amending relevant agreements and rules, e.g. when new functionalities are introduced. A case in point is contactless functionality.

Standard 1 is assessed to be broadly observed, subject to the following recommendations and comments:

Recommendation re Standard 1
Danmarks Nationalbank recommends that the work in Nets' "regulatory forum" should be more formalised and structured. Roles and responsibilities should be clear and well-documented, including the distribution of roles and responsibilities between Nets' first, second and third line of defence, i.e. operative units, the compliance function and the internal audit function.

Comment re Standard 1
Nets amends relevant agreements and rules as required. There is no formal procedure for updating agreements and rules concerning the Dankort scheme. Nets should establish such a procedure. That would ensure that any relevant amendments are made on a clear, systematic basis, and it would also reduce the drain of knowledge if key employees leave Nets.

Standard 2: Access to comprehensive information for all actors, including appropriate information on financial risks

Standard 2 relates to clear distribution of roles and responsibilities and access to information, including the following:

- Roles and responsibilities derived from the rules and contractual arrangements for card payment scheme actors should be clearly documented and regularly updated.
- There should be a procedure in place for classification of information.
- Relevant information should be available to existing actors and potential actors.
- There should be specific requirements in place concerning information on (1) prices and fees, (2) financial risks associated with Dankort participation, (3) complaints, (4) fraud and (5) mitigation of fraud, including disclosure requirements for the information which the card organisation should ensure that cardholders get from their issuers.
- Provisions should be in place for communication with relevant actors in the event of operational disruptions. Provisions for communication in the event of major changes should also be in place.

Assessment

The roles and responsibilities of the various Dankort actors are stated in the Dankort scheme rules. The scheme rules have a systematic structure, making it clear which actors are responsible for meeting which requirements.

Nets has established procedures for classification of information.

All Dankort actors can access information about Dankort at nets.eu and dankort.dk. Moreover, issuers have access to a closed site, INFONET, where e.g. price lists for licensees can be found, while retailers can find prices at Nets' website. Information on financial risks appears from relevant agreements and rules.

Nets makes a complaints system, CLARA, available to issuers, and all complaints are submitted to Nets via this system.

Information on fraud and the latest trends in fraud are published at nets.eu. Nets' efforts to combat fraud are described in detail under Standard 3.

There are requirements in place as to the information which Nets should ensure that cardholders get from their issuers, e.g. information on various security measures. Nets has imposed some of these requirements on the card issuers, as the requirements are included in the Dankort scheme rules, e.g. in the form of cardholder rules to be applied by all issuers. Not all ECB requirements are included in the scheme rules, meaning that Nets is not imposing all the requirements of the ECB standard on issuers.

Nets informs relevant stakeholders of any operational disruptions via Nets' information system (infocast). In addition, Nets has an incident management procedure in place.

Major changes are communicated to the Dankort scheme actors via Kortudvalget, Bankgruppen and Samarbejdsforum, where the changes are discussed. Representatives of Dankort-issuing banks are members of Kortudvalget and Bankgruppen. Representatives of retailers and Dankort-issuing banks are members of Samarbejdsforum. Moreover, there is a degree of stakeholder involvement in projects in Nets.

Standard 2 is assessed to be broadly observed, subject to the following recommendations and comments:

Recommendation re Standard 2 (1)

The ECB standard lays down requirements as to the information which Nets should ensure that cardholders get from their issuers. Nets should impose on issuers an obligation to comply with all requirements appearing from the ECB standard concerning issuers. This will ensure that the issuers implement the measures in a harmonised and appropriate manner, and it will allow Nets to follow up the implementation.

Recommendation re Standard 2 (2)

Nets should prepare a general and formal communication plan to ensure that relevant information

concerning Dankort is available to relevant actors via suitable communication channels, including communication to relevant actors in connection with major operational disruptions and major changes.

Comment re Standard 2
Nets has established procedures for classification of information. Nets should ensure that the procedures are followed.

Standard 3: An adequate degree of security, operational reliability and business continuity

Standard 3 imposes requirements in a number of areas supporting operational security and stability. These areas are described separately below:

- The governance authority's security management
- Manufacture and distribution of cards
- Transactions
- Clearing and settlement
- Contingency planning
- Outsourcing

It should be noted that Nets is focusing on meeting the requirements of international card companies, such as VISA. The international card companies oversee compliance with their requirements. Cases in point are requirements concerning PCI-PIN (link) and PCI-DSS (link).

Standard 3 is overall assessed to be partly observed. The assessments of the areas mentioned above have been reviewed one by one, followed by recommendations and comments for each one.

Requirements relating to the governance authority's security management

The standard's security management requirement comprises requirements concerning:

- the security policy and risk management of the card payment system;
- operational requirements concerning operation, incident management, change management, access policy, separation of duties, protection of sensitive data and IT and data security;
- management and employees, including requirements concerning documentation of roles and responsibilities;
- assistance to customers 24/7.

There are interfaces with other authorities. The Danish FSA supervises Nets' general IT security management, strategy, security policies and guidelines, as well as Nets' procedures for system access management and separation of duties. Moreover, the Danish FSA supervises Nets' incident management and change management. The Danish Data Protection Agency oversees Nets' compliance with the Danish Act on Protection of Personal Data. Danmarks Nationalbank did not assess Nets' compliance with the Danish Act on Protection of Personal Data.

Assessment

Nets' security policy focuses on security in Nets as a company, while the Dankort scheme rules represent implementation of rules and security requirements for Dankort actors.

Nets' security policy sets out the general guidelines for IT and data security at Nets. The security policy also imposes a number of requirements on Nets employees, e.g. mandatory security awareness training.

Nets carries out risk analyses of the Dankort IT platform. All risks are assessed in collaboration between the owner of the IT system and Group Risk Management. Risks which are found to have major consequences or high probability are communicated to the owner, and an action plan is prepared. Risk reduction activities should be described, and ownership and a deadline for implementation should be defined. Progress will be monitored.

Nets monitors technological developments and improves the security features of the Dankort on an ongoing basis.

The operation of Dankort is stable. There are only few incidents and disruptions influencing operational stability. In connection with disruption, Nets encourages stores to use the offline functionality of the card terminals so that payments can still be received. Nets has formalised procedures for incident and change management, access management and separation of duties. These procedures apply throughout the organisation.

Nets has submitted organigrams for the parts of the Nets organisation that are involved in the Dankort scheme.

Nets provides assistance to customers 24/7.

Recommendation re Standard 3 (1)
Currently Nets conducts risk analyses of the Dankort IT platform. This work should be expanded by means of a risk assessment of all relevant Dankort aspects, including organisation, staff, infrastructure, technical issues, potential security threats and operational functions. The purpose is to gain a comprehensive overview of Dankort-related risks with a view to implementing appropriate control and security measures and ensuring the right prioritisation.

Recommendation re Standard 3 (2)
Nets should document and maintain a comprehensive overview of the Dankort organisation, including clear documentation of roles and responsibilities. This overview is to create awareness and an overview of the various functions in Nets tasked with aspects of Dankort.

Recommendation re Standard 3 (3)
The Nets unit responsible for Dankort should create and maintain a comprehensive overview of incidents and other relevant information concerning IT and data security in relation to Dankort. Such inputs are material elements of the overall assessment of the functioning of Dankort and should be used, inter alia, for Dankort risk assessment purposes.

Requirements for manufacture and distribution of cards
The standard imposes security requirements regarding

- cards and terminals;
- personalisation and delivery of cards;
- production and installation of terminals, etc.

Moreover, the governance authority should ensure strong authentication tools for cardholders.

Assessment
Nets defines security requirements for cards and terminals in the Dankort scheme rules. Nets approves all terminals that can be used under the payment card agreement. No cards are issued without Nets. The scheme rules contain requirements for procedures and controls concerning personalisation and delivery of cards. For example, the card design must be to particular specifications. Furthermore, there are requirements for ordering Dankort and PINs, returned PIN letters, deliveries from the card supplier, initialisation of cards, card handling by the issuer, renewal and replacement of cards, blocking or deleting cards and handling of withdrawn cards/cards handed in. Approved suppliers and manufacturers must always be used for personalisation and delivery of Dankort. Nets has no experience of fraud in connection with personalisation and delivery of cards.

Nets has prepared requirement specifications for terminals, as well as a written procedure for terminal approval. Moreover, Nets has requirements in place regarding terminal installation. Nets has no knowledge of breach of controls as regards terminals.

Nets has requirements in place for authentication procedures. In connection with in-store trading, a PIN must be used, except for contactless payments below kr. 200. Moreover, the principle of strong authentication may be deviated from in connection with e.g. bridge crossings and payment of parking fees. The justification is that these goods are non-marketable and that the transaction speed is of material importance. Nets makes "Dankort Secured by Nets" available on the Internet for transactions exceeding kr. 450, thereby enabling execution of such payments with strong authentication. In "Dankort Secured by Nets", when the purchase exceeds kr. 450, the cardholder receives a code by text message, and the code must be used to finalise the purchase.

Transaction requirements
The standard contains requirements for

- validity periods for payment cards, payment sessions, etc.;
- monitoring of, response to and prevention of fraud;
- evidence of transaction validity;
- transaction logging, system and data access, etc.;
- capacity management and planning.

The Danish FSA supervises Nets' logging and capacity management and planning.

Assessment
The scheme rules state the validity period, which must not exceed 4 years for the VISA/Dankort, calculated from the month of issue plus three months. The PIN follows the card. This means that the PIN can follow the new card as long as the card is just renewed. After maximum 3 wrong PIN attempts, the card is blocked. A blocked Dankort can be unblocked. If the card has been compromised, it must be cancelled and a new card issued.

Nets monitors all Dankort transactions based on its experience and regularly carries out analyses of

Dankort fraud. Nets has launched two initiatives in 2017 with focus on fraud reduction. One is a fraud prevention tool that applies artificial intelligence to analyse fraud tendencies and uses the results to identify fraud attempts. The other is "Dankort Secured by Nets", as described above. Dankort fraud is low by international comparison.

For Internet payments, Nets requires a time-out for the browser window after a maximum of 15 minutes. There is no mechanism to prevent double login to the Internet, e.g. simultaneous login from a PC and an iPad. Nets is closely monitoring fraud developments and has not experienced any fraud as a consequence of double login.

Nets has clear rules in place regarding when and how a Dankort transaction can be reversed if rejected by the user. Where the cardholder cannot accept an in-store transaction made using a PIN/signature, but the chip has been read, special rules apply to the processing of the complaint, as the card may be fake or counterfeit. If Nets asks for documentation of a card payment, the retailer must provide it to Nets. Retailers are required to store transaction documents for 20 months as from the date of payment.

Nets has procedures in place for logging system and data access, actions carried out in the production environment, etc.

Nets monitors the card payment scheme with a view to ensuring adequate capacity, also at peak load. Nets can provide additional capacity at short notice.

Comment re Standard 3 (1)
Fraud is reported manually to Nets. Nets already has a project for electronic fraud reporting on the drawing board. Nets should launch this project.

Comment re Standard 3 (2)
The ECB standard specifically requires an option for the cardholder to deselect Dankort use for Internet trading. Nets should analyse cardholders' need for this option and the possibilities of developing such a solution.

Comment re Standard 3 (3)
Nets should investigate the possibilities of including all cash withdrawals from ATMs in the centralised authorisation process at Nets. This will strengthen Nets' oversight and prevention of Dankort fraud.

Clearing and settlement requirements
The governance authority should define technical and organisational security requirements for clearing and settlement, e.g. relating to capacity, availability, stability, confidentiality and audit possibilities.

Assessment
A Dankort transaction is first included in the PBS clearing (or electronic clearing), then in the Sumclearing. These clearing systems are subject to oversight by Danmarks Nationalbank in another context. Consequently, any issues relating to these systems have not been assessed in connection with the Dankort assessment, cf. the review of Standard 5 in this report.

Contingency planning requirements
The standard imposes contingency planning requirements. There must be:

- business impact analyses (BIAs) identifying the components that are crucial to the functioning of the card payment scheme;
- contingency plans and testing procedures.

The Danish FSA supervises Nets' contingency planning and testing of the plans.

Assessment
Since 2016, Nets has prepared BIAs for critical services, including Dankort. Several BIAs are relevant to Dankort, including BIAs concerning transaction processing, Internet trading, card production, card initialisation and authorisation.

Nets has a contingency plan in place, including requirements for re-establishment times based on the BIAs. The plan comprises, inter alia, the contingency plans in connection with Dankort. Moreover, Nets has a crisis management plan in place, including crisis communication.

Nets regularly tests the contingency plan and the crisis management plan. Improvements are documented and responsibilities placed.

Comment re Standard 3 (4)
Nets should reconsider which BIAs are relevant in a Dankort context, such as BIAs concerning clearing systems. Nets should finalise the BIAs in all areas of Dankort relevance.

Outsourcing requirements
The standard contains the following outsourcing requirements:

- Outsourcing-related risks should be analysed by the outsourcing actor, and the external service provider should be required to analyse own risks related to the outsourced activities.
- Contracts should comprise all relevant issues in connection with the outsourced activities, including descriptions of expected service levels.
- A process should be in place for monitoring and following up the security and availability of the outsourced services.

The Danish FSA supervises Nets' outsourcing of IT functions.

Assessment
Nets outsources several Dankort-related functions.

Nets has an outsourcing process in place. Contractual provisions include, inter alia, expected service levels. Nets performs risk assessments of outsourced services and requires service providers to carry out their own risk assessments. However, for a small external service provider to Dankort, Nets has not updated its risk assessment on an annual basis.

The same service provider to Dankort does not comply with Nets' IT security policy, and in some cases Nets does not have a coherent and consistent procedure in place for monitoring and following up the security and availability of outsourced services.

Recommendation re Standard 3 (4)
Nets should update, on an annual basis, its risk analyses of all outsourced Dankort-related functions. In this connection, Nets should incorporate the external providers' own risk analyses of the outsourced activities. This risk analysis should form the basis for establishing appropriate control and security measures, and outsourcing risks should constitute an important element of the Dankort risk assessment.

Recommendation re Standard 3 (5)
Nets should ensure that Dankort service providers comply with Nets' IT security policy. Nets' monitoring and follow-up of the security and availability of the outsourced services should generally take place in a systematic and regular way, which should be documented and subject to quality assurance.

Standard 4: Effective, accountable and transparent governance arrangements

The standard requires:

- clearly defined, efficient and transparent processes for decisions on business objectives and policies. Roles and responsibilities should be clearly defined;
- objective, fair and transparent access criteria for issuers and acquirers;
- efficient and transparent processes for assessment of the services offered to customers;
- an effective internal control framework, including an audit function;
- ongoing control of the stores handling sensitive payment data.

The Danish FSA supervises Nets' requirements and procedures concerning control and reporting. The Danish Competition and Consumer Authority is the authority for competition issues. Danmarks Nationalbank has not examined competition issues.

Assessment

As owner of Dankort, Nets makes the final decisions about the product. Nets collaborates with representatives of issuers and retailers. This collaboration takes place in Bankgruppen, Kortudvalget and Samarbejdsforum. Other working groups are established as required.

Issuers must meet a number of criteria to obtain a licence, and they must apply for a licence to Nets, which makes a decision on granting the licence on the basis of a specific assessment. Nets has never rejected an issuer's application for a licence. According to the terms and conditions for licences, Nets is the sole acquirer of Dankort. The acquirer fee is regulated by law and depends on the costs of operating Dankort.

Nets carries out a Continual Service Improvement, CSI, measurement once a year. The CSI measurement is targeted at Nets' customers, e.g. issuers and retailers. The result is presented to the Board of Directors. Since the measurement is not product-related, it is not possible for Nets to generate separate Dankort-related results. Nets is only aware of cardholders' assessments of Dankort if issuers include Nets in the customer feedback loop.

The responsibility for control and security is organised in three lines of defence (first, second and third), i.e. operative units, the compliance function and internal audit, respectively. Both internal and external system audits are carried out. Moreover, Nets initiates audits of its outsourcing partners, e.g. IBM. Internal Audit follows up auditors' qualifications on a monthly basis, and prepares, on a quarterly basis, an overview of auditors' qualifications to the management. Internal Audit requires all auditors' qualifications to be closed within 12 months from the final meeting. If this is not possible, the qualification must be presented to the Audit Committee, after a discussion with the CFO. The auditor in charge is responsible for closing the qualification.

The physical retailers do not store payment data. Nets requires that in-store terminals transmitting data must be approved by Nets and thus meet Nets' security requirements, including compliance with the PCI-DSS standard. Online stores must use an Internet payment module approved by Nets, whereby they comply with the PCI-DSS standard. Nets monitors once a year whether PCI-DSS certificates have been renewed.

Standard 4 is assessed to be broadly observed, subject to the following recommendations and comments:

Recommendation re Standard 4 (1)

Nets should strengthen the framework for decision-making processes in Kortudvalget, Bankgruppen and Samarbejdsforum. Nets should ensure that clearly defined, efficient and transparent processes are in place for decisions on business objectives and policies.

Recommendation re Standard 4 (2)

The Nets unit responsible for Dankort should create and maintain a comprehensive overview of the audit qualifications directly and indirectly related to Dankort. This overview is to contribute to a comprehensive picture of the functioning of Dankort and should be used, inter alia, for Dankort risk assessment purposes.

Comment re Standard 4

Nets does not perform satisfaction surveys regarding feedback from the cardholders on Dankort. Nets should examine the possibilities of establishing a satisfaction survey in collaboration with the card issuers. The purpose would be to ensure an efficient Dankort that meets cardholders' requirements.

Standard 5: management and containment of financial risks in relation to the clearing and settlement process

The standard requires:

- an overview of clearing and settlement;
- management and containment of financial risks in relation to the clearing and settlement process.

Most of the requirements under Standard 5 have not been assessed, as they concern clearing and settlement, i.e. PBS clearing, electronic clearing and the Sumclearing. Danmarks Nationalbank oversees these clearing processes in another context, and consequently they are not part of the Dankort assessment.

Assessment

Dankort transactions are cleared in the PBS clearing and the electronic clearing, which are parts of the Sumclearing. For example, the PBS clearing comprises Dankort payments via physical online terminals in stores and for Internet purchases, payments abroad using a VISA/Dankort and payments using an international debit card issued by a Danish bank. The electronic clearing includes e.g. cash withdrawals using Dankort in branches or in ATMs of banks other than the cardholder's bank.

As the scheme owner, Nets cannot suffer losses in connection with clearing and settlement of transactions. However, losses may occur as a result of Nets' role as acquirer of Dankort if the cardholder submits a complaint to a retailer and the retailer is unable to accommodate it. The cardholder's bank has an obligation to try to collect Nets' claim from the retailer, but if this is impossible, Nets as the acquirer is liable for any losses. In order to minimise the risk of losses, and based on an assessment of the retailer, Nets may require the retailer to provide a bank guarantee as part of its application before a payment card agreement can be concluded. Moreover, Nets ensures that a maximum per card per day has been introduced for certain types of payment card agreements, such as gambling.

Standard 5 is assessed to be observed.

Overview of recommendations and comments

Table 1 provides an overview of Danmarks Nationalbank's recommendations and comments. Danmarks Nationalbank and Nets have agreed on a timeframe for Nets' follow-up on recommendations and comments.

Recommendations and comments for Nets – to be continued Table 1

Recommendations	Comments
Standard 1 *A sound legal basis under all relevant jurisdictions:*	
• Danmarks Nationalbank recommends that the work in Nets' "regulatory forum" should be more formalised and structured. Roles and responsibilities should be clear and well-documented, including the distribution of roles and responsibilities between Nets' first, second and third line of defence, i.e. operative units, the compliance function and the internal audit function.	• Nets amends relevant agreements and rules as required. There is no formal procedure for updating agreements and rules concerning the Dankort scheme. Nets should establish such a procedure. That would ensure that any relevant amendments are made on a clear, systematic basis, and it would also reduce the drain of knowledge if key employees leave Nets.
Standard 2 *Access to comprehensive information for all actors, including appropriate information on financial risks:*	
• The ECB standard lays down requirements as to the information which Nets must ensure that cardholders get from their issuers. Nets should impose on issuers an obligation to comply with all requirements appearing from the ECB standard concerning issuers. This will ensure that the issuers implement the measures in a harmonised and appropriate manner, and it will allow Nets to follow up the implementation. • Nets should prepare a general and formal communication plan to ensure that relevant information concerning Dankort is available to relevant actors via suitable communication channels, including communication to relevant Dankort actors in connection with major operational disruptions and major changes.	• Nets has established procedures for classification of information. Nets should ensure that the procedures are followed.

Recommendations and comments for Nets – continued Table 1

Recommendations	Comments
Standard 3 *An adequate degree of security, operational reliability and business continuity:*	
• Currently Nets conducts risk analyses of the Dankort IT platform. This work should be expanded by means of a risk assessment of all relevant Dankort aspects, including organisation, staff, infrastructure, technical issues, potential security threats and operational functions. The purpose is to gain a general overview of Dankort-related risks with a view to implementing appropriate control and security measures and ensuring the right prioritisation. • Nets should document and maintain a comprehensive overview of the Dankort organisation, including clear documentation of roles and responsibilities. This overview is to create awareness and an overview of the various functions in Nets tasked with aspects of Dankort. • The Nets unit responsible for Dankort should create and maintain a comprehensive overview of incidents and other relevant information concerning IT and data security in relation to Dankort. Such inputs are material elements of the overall assessment of the functioning of Dankort and should be used, inter alia, for Dankort risk assessment purposes. • Nets should update, on an annual basis, its risk analyses of all outsourced Dankort-related functions. In this connection, Nets should incorporate the external providers' own risk analyses of the outsourced activities. This risk analysis should form the basis for establishing appropriate control and security measures, and outsourcing risks should constitute an important element of the Dankort risk assessment. • Nets should ensure that Dankort service providers comply with Nets' IT security policy. Nets' monitoring and follow-up of the security and availability of the outsourced services should generally take place in a systematic and regular way, which should be documented and subject to quality assurance.	• Fraud is reported manually to Nets. Nets already has a project for electronic fraud reporting on the drawing board. Nets should launch this project • The ECB standard specifically requires an option for the cardholder to deselect Dankort use for Internet trading. Nets should analyse cardholders' need for this option and the possibilities of developing such a solution. • Nets should investigate the possibilities of including all cash withdrawals from ATMs in the centralised authorisation process at Nets. This will strengthen Nets' oversight and prevention of Dankort fraud. • Nets should reconsider which BIAs are relevant in a Dankort context, such as BIAs concerning clearing systems. Nets should finalise the BIAs in all areas of Dankort relevance.
Standard 4 *Effective, accountable and transparent governance arrangements:*	
• Nets should strengthen the framework for decision-making processes in Kortudvalget, Bankgruppen and Samarbejdsforum. Nets should ensure that clearly defined, efficient and transparent processes are in place for decisions on business objectives and policies. • The Nets unit responsible for Dankort should create and maintain a comprehensive overview of the audit qualifications directly and indirectly related to Dankort. This overview is to contribute to a comprehensive picture of the functioning of Dankort and should be used, inter alia, for Dankort risk assessment purposes.	• Nets does not perform satisfaction surveys regarding feedback from the cardholders on Dankort. Nets should examine the possibilities of establishing a satisfaction survey in collaboration with the card issuers. The purpose would be to ensure an efficient Dankort that meets cardholders' requirements.

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

This edition closed for
contributions on 10 May 2017

Anne Dyrberg Rommer
ady@nationalbanken.dk

Mikkel Steen Madsen
msn@nationalbanken.dk

FINANCIAL STABILITY

DANMARKS
NATIONALBANK