



BANKENES
STANDARDISERINGSKONTOR



Annual Report 2014

Status concerning risk, priorities and activities



BSK's purpose is to perform administrative functions with regard to Distribution of payments and payments information in the collaborative infrastructure utilized by the Norwegian banking sector.

Introduction

Bankenes Standardiseringskontor (BSK) was founded in 1994 by Bankforeningens Servicekontor and Sparebanksforeningens Servicekontor. Its purpose is to perform administrative functions with regard to Distribution of payments and payments information in the collaborative infrastructure utilized by the Norwegian banking sector. Amongst other things, our responsibilities include establishment and maintenance of requirements and standards for coordination of payment systems, IT-security, formats for exchange of transactions and information between banks, as well as between associated product companies (BankID and BankAxept) as well as banks. The BSK Board of Directors is appointed by Finans Norge, and consists of the following representatives from the banks:

- Eldar Skjetne, board manager, Sparebank1 Alliansen
- Peer Theien, DNB
- Lorang Eriksen, Eika Alliansen
- Kristian Maubach, Sparebanken Vest
- Gunnar Senum, Skandiabanken
- Per Harald Fredriksen, NORDEA

- Bernt Ragnar Pettersen, Danske Bank
- Solveig Lie, Handelsbanken
- Einar Arne Engedahl, Storebrand

In addition Tor Johan Bjerkedal from Finans Norge regularly attends meetings as an observer.

BSK consists of 9 members of staff. In addition to this, we have associated ourselves with resources from banks in order to establish expert groups within the following areas:

- Card payment
- Online banking security
- Interbank
- Electronic invoicing and payment
- BankID

Approximately 40 people are currently associated with BSK through these expert groups. We also manage projects, task groups etc, where additional resources from banks and suppliers become involved in our work. This enables BSK to maintain an extensive and highly competent network, which we may utilize in order to perform our allocated tasks.

The purpose of this report is to give the banks an overview of, and an

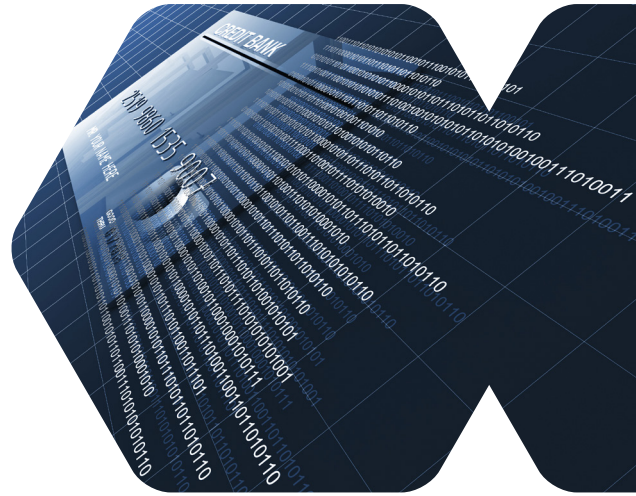
insight into the issues we are currently working on, in order to gain an understanding of the priorities and considerations our work is based on.

Priorities

The Board of Directors has outlined the following prioritized areas for BSK.

- Modernization and development of common infrastructure and systems.
- Adapting the industry to international standards and collaboration with relevant international partners.
- Further development of processes and competence.

The main priorities of the board are consistent with a clear overriding strategy, and executed through activities. The process of detailing activity plans is managed by the BSK administration in close collaboration with established expert groups, Finans Norge, and through dialogue with major suppliers. Furthermore, activities are based on decisions made by the Board of Managers through allocations made in our budget.



2014 – A year signified by change

2014 has been dominated by great changes, which have, and will continue to have an impact on BSK in the years to come.

In 2014 the banks have founded two product companies; BankID Norge AS and BankAxept AS. BSK will continue to be responsible for determining requirements, as well as overseeing security- and standardization processes. This includes requirements to be met by the product companies. Collaboration between BSK and the product companies is regulated through written agreements. A major concern is to maintain close collaboration with these companies, thus contributing to their continued success. This will remain of utmost importance to us in 2015, and in the years to come. We have worked closely with BankID with regard to the implementation of the BankID 2.0 project (aimed at making bankID java-free), and we are currently working alongside BankAxept in their effort to produce a solution for contactless payment cards. In the initial phase BankAxept have been co-located with BSK. FinansCERT celebrated its first year of operation on the 1st of October 2014. FinansCERT plays a key part in co-ordinating responses to security-related incidents from across Norwegian financial sector.

FinansCERT and BSKs standardization efforts within the domain of security are interlinked. FinansCERT are co-located with BSK.

There have been major changes affecting the banks main suppliers recently. The sale and reorganization of Nets has been significant in this regard. Such processes work



2014 has been a year in which the area of payments has undergone a revolution.

as a catalyst for our need to consider collaboration, and provide an opportunity for a re-evaluation of our own organization. Additionally we have become more familiar with SDC throughout the year. They have gained customers, and increasingly involved themselves with regard to the Norwegian banking infrastructure. Furthermore, EVRY is currently

settling in to a new situation with regard to a change of ownership.

Regulation of the payment – and security domains are equally in a time of transition. Crucially for our organization is the ongoing discussion in the EU regarding regulation of payments, which centers around Payment Service Directive 2 (PSD2). The main issue for us has been the authorities' drive to force banks to open the collaborative infrastructure (access to accounts) to Third Party Payment Providers (TPPs). The challenges surround the ability to accomplish this without compromising on security. Banks are not given the opportunity to demand regulated security agreements from those who are given access. At the same time the banks remain responsible for their customers in cases where they are subjected abuse, fraud, etc. Along with Finans Norge we are monitoring these issues by participating in the European Payment Council, Pan Nordic Card Association, and by direct dialogue with relevant authorities.

2014 has been a year in which the area of payments has undergone a revolution. There is every reason to believe 2015 will be even more eventful and hopefully a year during which the new payment solutions will increase in actual use.



Main activities during 2014

Considering the situation outlined previously, it is crucial that the banking community utilize their resources sensibly.

Main BSK projects

On the 20.06.2013, the BSK Board of Managers decided to launch the **Modernisation Project**, in order to replace BALTUS and BDM – the online interbank messaging transaction infrastructure. The project was launched as a recognition of the fact that the current infrastructure is obsolete (though still reliable). The project, aimed at releasing Baltus 2.0, will be terminated on the 31/12-15, by which time all traffic should be loaded onto the new infrastructure, and BSK will discontinue maintenance of the current one. The aim is to establish an infrastructure with increased reliability and security for online exchange of messages between banks, and to prepare for future solutions and services, as well as opening up for new stakeholders (suppliers and collaborators). The architecture of the solution also enables Finans Norge, on behalf of the banking community, to control network traffic through control of the Central Routing Table (CRT). Baltus 2.0 requirements, outlined by BSK are anchored in a new rule set for Baltus which has been established by Finans Norge, and agreed by Bransjestyret Betalingsinfrastruktur (BBI). The project is making good progress. Attached to this report is a white

paper which describes Baltus 2.0. Interested parties are welcome to contact BSK for further information.

The BSK Board of Managers on the 12.03.2014 decided on a **roadmap for implementation of ISO 20022** as the new standard for financial messages. This is set to replace the current customer-to-bank formats (such as Telepay, PAYMUL, CREMUL), and internal bank formats (NIBE, BOLS, NISOK). Internationally, ISO 20022 has gained increased market shares in the



The BSK Board of Managers decided on a roadmap for implementation of ISO 20022 as the new standard for financial messages.

messaging exchange domain within the financial sector. This standard is also supported by the EU as basis for their rule set for payments in Euro (SEPA). The aim of this change is to accommodate for increased transparency and ability to coordinate payments in NOK and other currencies, thus encouraging cost efficiency, increasing supplier competition,

simplifying governance and ensuring increased access to expertise.

BSK have worked on a **new design for debit cards** in close collaboration with the banks. The aim has been to increase card security, as well as giving it a more modern look. The entire back side of the card is now designed in a more holistic fashion. The new design integrates several security measures, making copying and forgeries much more difficult. The launch is planned so that the banks may start preparing their process of renewal in 2014.

Third Party Access to the Banking Infrastructure (TIFI-project) was established as a consequence of a process in BSK where the Board of Managers challenged the administration to find a way of allowing third party providers access in a secure and controlled way. Considerations as to whether or not such access should be given is outside the scope of the project. Such consideration is an issue of industrial policy and will have to be made by Finans Norge and BBI. The TIFI project was established independently of signals from the PSD2 process, and aimed at exploring how banks may comply if new participants are to be allowed (following commercial considerations and in accordance to appropriate agreements) access to the infrastructure. Accommodating for this type of access was amongst the demands put to Baltus



2.0 from the Board of Directors, but while Baltus 2.0 focuses on message network infrastructure, TIFIs main focus is on the security requirements posed to the potential participants. The TIFI process has also proved valuable with regard to adapting our mindset to the idea of how we should prepare for the changed security situation when PSD2 is likely to be implemented, forcing banks to open account access to Third Party Payment Providers (TPPs).

Other important activities

BSK have realized other important changes throughout the year. Among other things, we have adapted in order to include more information regarding merchant information in financial transactions between banks, following card transactions by extending the BOLS format (LK27). This enables costumers to see more information regarding the transaction by using their online banking platforms.

Alongside BankID Norge, BSK have embarked on a feasibility study in order to test a possible solution for photo renewal on payment cards. The hypothesis is that one should be able to take a picture of oneself (selfie), and sign it using BankID via a mobile phone. The old photo is then collected from the card system vendor used by the bank, and a comparison is made between the old and the new picture by the use of face recognition software. If the photo is accepted, the file photo is replaced,

and the new photo used for the next card renewal. Part of this study is a legal review in order to consider whether there are any legislative restrictions in place blocking the use of this type of technology.

Further, BSK have, along with BankID Norge and Finans Norge, conducted an extended risk – and actions assessment of identity control when renewing BankID. The main focus has been on the PUM service provided by the National Postal service. The results have been reported to the BSK board of Managers BSK and BBI, and consequentially, a series of measures aimed at securing the continued issue of BankID with an absolute minimum of unwanted incidents have been put in place.

BSK have actively contributed to the realization of a Java free BankID alternative - The BankID 2.0 project. Our role has been to establish security acceptance criteria, as well as approving the solution for implementation. The project has been exciting as well as demanding, and we are proud of the success BankID Norge have had regarding the launch of BankID 2.0.

BSK continues to contribute to BankAxepts efforts to develop a solution for contactless payment cards. Our role is to establish security acceptance criteria, as well as approving the solution for implementation. The project is exciting as well as challenging, and we are proud to be involved in this important process.



BSK have actively contributed to the realization of a Java free BankID alternative - The BankID 2.0 project.

Furthermore, we have contributed to issuing acceptance criteria and standardization of the Account Address Project (KAR) and in the Immediate Payment Project. Both these projects are important for the development of the banking infrastructure, where KAR in particular will enable a connection to be made between mobile telephone numbers and bank accounts, thus simplifying solutions for mobile banking.

International work

BSK represents the banks in a series of forums and on several arenas. Our role is to attend to the interests of Norwegian banks. We are increasingly influenced by international initiatives on the payment area. This includes an increased subjection to international regulation, as well as our own decisions to utilize international standards more systematically (e.g. ISO 20022). During 2014,



Our aim is to make a contribution toward elevating the general level of security in the Norwegian community.



we have increased our willingness for participation on the international arena. An example of this is the establishment of the role of International Standards Manager.

In February 2014 we made a collaboration agreement with Standard Norge, making the establishment of the payment area one of their focus areas. This was implemented in close collaboration with SWIFT NNG, who had already initiated such a move. Working groups within the fields of payment and security were established, as well as a mirror committee for ISO TC68. Through these activities, we aim to enhance our opportunity for exerting influence on the future development of relevant standards, as well as our access to a broader field of competence, both nationally and internationally. As a consequence we have participated in relevant international committees: ISO (payment area), CEN (electronic invoicing) and ETSI (PKI).

Furthermore, in September, Finans Norge, BankID Norge, FinansCERT and BSK raised an initiative toward Standard Norge, prompting them to explore the possibilities for a

trans-sectorial initiative aimed at standardization of the IT security and privacy area in Norway, in order to utilize scarce resources more efficiently. BSKs managing director is a member of sector governing body for information technology within Standard Norge, and is as such responsible for following this up. At the time of writing, the outcome is uncertain, but work is in progress in order to secure funds and finding appropriate ways of organizing this effort. Our aim is to make a contribution toward elevating the general level of security in the Norwegian community. We consider this of utmost importance in order to reduce the vulnerability of the banks, as well as ensuring that good solutions may be re-utilized.

BSK is a member of the Pan Nordic Card Association (PNC) on behalf of Norwegian banks. PNC is a network of competence within the Nordic countries which also focuses on coordinating security regulation and standards for payment cards within the Nordic region. PNC further represents its members in international forums, such as EMVco, PCI, EPC etc.

The European Payments Council (EPC) was founded by the European financial sector in order to coordinate the sector within the payment area and to support the SEPA ambitions of the EU. DNB have become members of the EPC on behalf of the Norwegian banking community, while BSK covers any costs relating to this on behalf of the community. Several employees from Finans Norge, BSK and DNB attend the different expert groups within the EPC. Activities are coordinated through Fagutvalget for Internasjonale Rammevilkår Betalingsformidling (FIB). This allows us to exert influence relating to processes leading up to important decisions being made within the EU, as well as toward the setting of premises by the European Central Bank (ECB) and the European Banking Authority (EBA).

In addition to the above mentioned activities, BSK attends several other groups. Interested parties may receive further information upon request. If anyone wishes to participate and/or contribute to these efforts please contact us, and we will try to accommodate for that.



Risk assessment

BSKs activities will be adjusted to control risk toward an acceptable level. For that reason, BSK conducts an annual risk assessment on three different levels; strategic, tactical and operational. The consideration is a thorough and extensive process, which is detailed and documented in a separate report. We have summarized the risks BSK have considered in our recent planning process below. Please note that risk assessments which have led to implementation of measures in 2013 and 2014 (such as Baltus 2.0) have not been included in the summary below. We have only included risks which may trigger new actions and measures. Interested parties are encouraged to contact us for further information. However, the actual report is not intended for widespread distribution.

Strategic risk

We believe several factors will have an effect on our strategic risk situation in 2015. They include:

SELF GOVERNANCE

Change of regulation and scope of self governance. This is particularly relevant with regard to third party payment providers, as outlined elsewhere in this document, but it may also affect other areas. With regards to dealing with this situation, it is

essential that the industry focus their efforts towards following up relevant authorities. The ongoing process is spearheaded by Finans Norge.

THIRD PARTY ACCESS

Third parties who are to be given access to the banking infrastructure represent increased threats, as well as fresh opportunities. Threats relating to the increased security risk they may pose, as well as challenges to the control banks currently have with regard to their own infrastructure. However, they also bring with them opportunities with a broader field of cooperation and better access to innovation. Considering whether or not banks should embark on this venture is an issue of a Industry political nature, which needs to be considered by Finans Norge. If their conclusion is positive (and perhaps if PSD2 results in a situation where the move is enforced), BSK will be instructed to establish regulation and certification in order to ensure that risks remain within acceptable levels. BSK is closely monitoring this through the TIFI and BALTUS 2.0 projects presented above, while the discussions led by Finans Norge in BBI are ongoing.

SUPPLIERS

Changes within the landscape of suppliers may result in an altered

risk situation. Nets' journey towards ever increased commercialization is ongoing, following changes in ownership. This has so far resulted in organizational changes implemented from september 2014. BSK will continue to work closely with Nets in order to ensure continuing access to competence, and to ensure that there remains a mutual understanding of the security needs the industry is experiencing. Finans Norge, BankID Norge and BankAxept also keep in close contact with Nets in order to ensure the fulfillment of all agreements.

COMPETENCE

Access to competence concerning the Norwegian infrastructure is crucial in order to ensure successful governance and future development of existing solutions as well as for development of new solutions. During a time of reorganization and downscaling coinciding with changes as well as new developments in systems and solutions, taking steps to secure competence is essential. BSK have taken steps both to ensure the continued access to competence, as well as to ensure that systems comply with international standards. Furthermore, we have documented new requirements and standards (as with Baltus 2.0 and ISO 20022) in English.



We consider the Norwegian infrastructure to be essentially sound and well governed.

Tactical risk

For 2015 we consider these to be some of the most important tactical risks:

APT

Well planned attacks on the central infrastructure and across value chains - Advanced Persistent Threat (APT) - are difficult to guard against, as it requires broad insight and that measures are taken across organizations. Even so, this risk needs to be thoroughly addressed, and BSK have made this a major issue for 2015. APTs have triggered a need to establish a new expert group for security, where chief information security officers (CISO) from banks and major suppliers are represented. We envision the founding of a security program designed to monitor this risk continuously. The fact that the APT risk may arise across sectors, has led to our initiative put to Standard Norge, prompting them to make this an agenda point.

CONTROL ASSURANCE

Ensuring quality of systems and suppliers, by ensuring that they comply with BSKs requirements and standards is important to us. This is particularly true when facing a world where major transformation is taking place and many attacks are

targeted toward known weaknesses. As a result, BSK will initiate activities and increase focus on certifications during 2015.

Operational risk

We are monitoring a series of operational risks as part of our governance activities. We consider the Norwegian infrastructure to be essentially sound and well governed. However, there are some risks requiring more active management at different times. Pinpointing these is done through discussions in the expert groups, and as a result of incidents and threats experienced within the market. For 2015 we consider these to be some of the most important operational risks:

SOCIAL ENGINEERING

Social engineering, whereby criminals trick the banks customers into divulging their secrets (like personal codes, etc) and/or to download malware is an ever-present risk which is not likely to diminish. Protective measures are difficult, because they rely on building a general security awareness in the society, while avoiding a situation where one contributes to spreading unnecessary insecurity. BSK have addressed this by building alliances

and by contributing to information campaigns. We have been, and will continue to be, platinum sponsors of the Security Month led by NORSIS, and we have initiated a cross-sectorial collaboration within the field of security to Standard Norge, in order to contribute to a generally increased security awareness. We also keep in contact with the Lysne Committee (Sårbarhetsutvalget) in order to raise this issue. In addition to this, banks regularly conduct extensive information campaigns targeting customers.

IDENTITY CONTROL

Issues surrounding identity control when issuing electronic IDs is outlined above. We will be following up the plan of measures compiled following the risk evaluation conducted late 2014 and through 2015.

COUNTERFEITING

Counterfeiting BankAxept cards with photos is a risk we have addressed through establishing a new card design, as well as testing technology for self-renewal of photos as outlined above. There will still be old cards in circulation throughout 2015, and we will be monitoring the situation in order to uncover any indications suggesting that counterfeiting increases. If we experience an increase, we will be able to take appropriate measures.

2015 Activities

The BSK Board of Directors annually compiles a list of activities to be conducted by BSK. All activities are prioritized using a labelling system where each activity is given a label, adding it to an A, B or C-list. The A-list consists of obligatory activities, the B-list of activities which should be conducted, while the C-list consists of activities which may be conducted through the year. The following list is that of A-list activities for 2015:

ACTIVITY	DESCRIPTON
The modernization project	Realization of av Baltus 2.0 (terminated by 31/12-15)
BAX Contactless cards	Requirements, realization(including key centre)
ISO 20022	Customer/bank realization, Bank/bank planning.
Interface TSM	Standardization requirements for bank systems interface to Trusted Service Manager (eg. TSM Nordic)
Electronic invoicing B2B, B2C og CEN	Monitoring and requirements
Increasing and facilitating supervision	Analysis, requirements and implementation , incl register of terminals etc. Main priority to strengthen the role as gatekeeper.
BankID 2.1	Requirements and approval
Advanced Persistent Threat	Analysis, plan of actions and measures related to well planned attacks on the bank infrastructure.
Account address register (KAR)	Realization
Management of BSK	Management of BSK, expert groups and participation in relevant forums, eg. PNC board, NS etc

Contact



Lars Erik Fjørtoft,
managing director, BSK



lars.erik.fjortoft@bsk.no



+47 974 74 469

