Nordea

Implementation Guide

Corporate eGateway

Table of contents

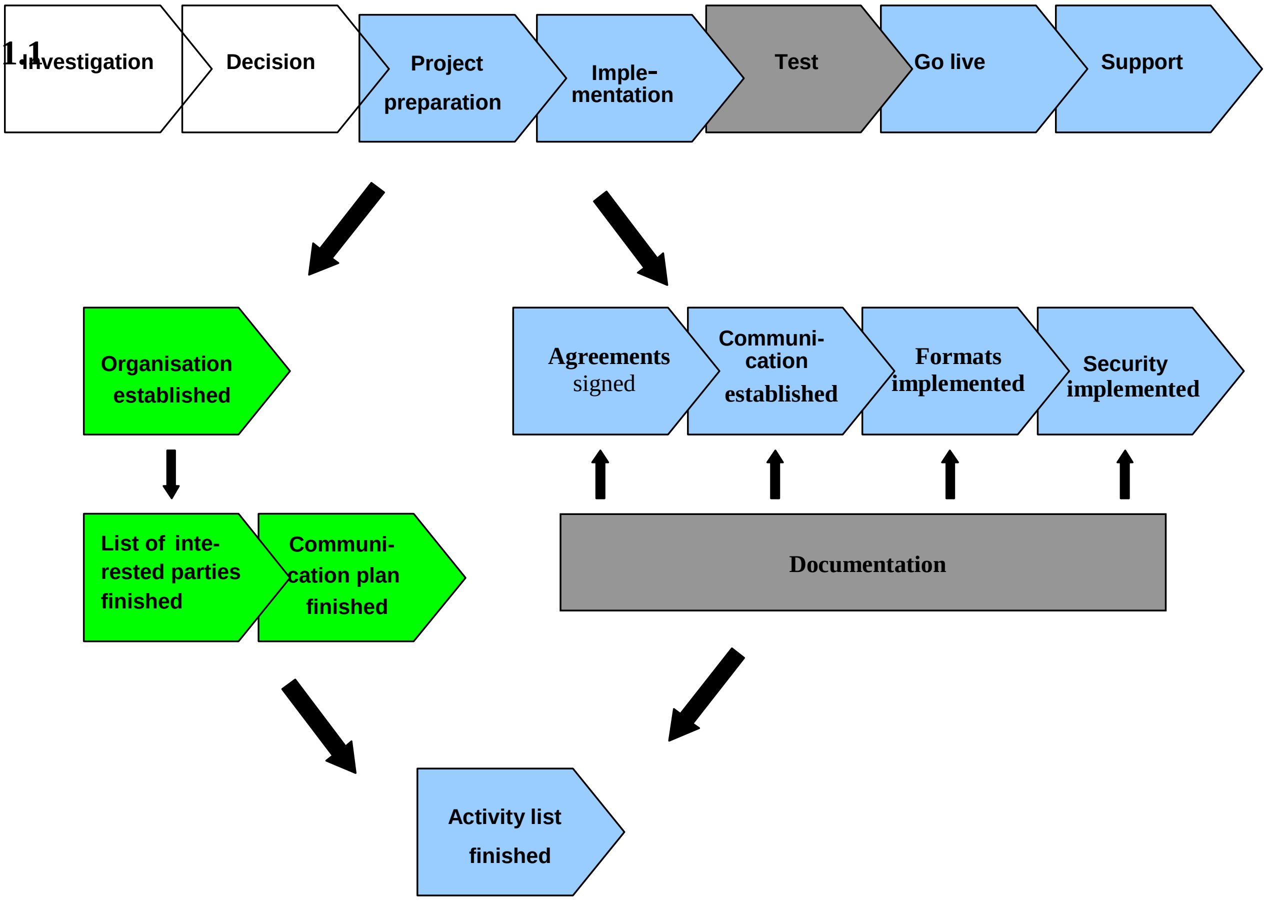
1 Purpose of this guide

This manual is aimed at integration suppliers and customers who are about to integrate a financial system with Corporate eGateway. The manual is primarily intended to support the project manager, but also members of the project team.

Implementation is a part of the total project and this manual describes the tasks for project organisation and the planning of the implementation (blue parts in the plan). Detailed information for the implementation team is available in *Project & activity plan*.

After each chapter you will find a checklist that should serve as inspiration for your work. Implementation of Corporate eGateway requires a good organisation and a good understanding of the product as well as good communication among the parties involved.

1.1



Four levels of information

1. (No colour) Level 1. The level to get an overview over the task, and primarily intended for the decision-makers. This level is not part of this manual.
2. (Blue colour) Level 2. The level at which you get more detailed information. You have to have sufficient knowledge to be able to react on the information, and you have to know where to collect more information about the subject. The target group is the project manager or project members who are not going to develop this task.
3. (Green colour) Level 3 is for the developers or persons with special responsibility. The information is detailed and easy to work with.
4. (Grey coloured) As level 2, but described in separate manuals.

Recommended information

If you have not been part of the previous part of the project, investigation and decision, you might need information about the functionality in Corporate eGateway. Please see the list of manuals for further information connected to the Corporate eGateway service.

This description serves two purposes:

1. To describe the rules for implementation, give inspiration for what processes the implementation will go through, bring out factual issues regarding Corporate eGateway and the implementation process, the organisation and who will participate.
2. To describe the support after implementation.

The Message Formats and advises are described in special manuals.

Most manuals can be downloaded in Adobe Acrobat Reader® PDF format from Nordea's website www.nordea.com.

Further information on the manual and general advice on integrated Messages can be obtained from Nordea's website www.nordea.com.

The terms and definitions used in this document are defined in a separate document, *Glossary for Corporate eGateway*, which can be found on Nordea's website: www.nordea.com.

1.2 How to get started?

There are many ways to start the implementation, depending on who is in your project, and how much they have been involved in the previous work around Corporate eGateway.

We cannot tell you exactly how to do or define roles and responsibilities for your organisation when starting up the project, but we can, out of previous experience and knowledge, offer you some advice from what we have learnt over the years, if you wish.

A good start would be to define the preferred results of the implementation. This means to make sure in detail what the end-user expects from the system. This has nothing to do with technique, but the functionality and the picture of the result in the end-user’s mind.
If you and the end-user have the same picture in mind, you have a much better chance to guide the technique in the right way, and create a result acceptable for the end-user.
In other words, less focus on the solution and more focus on the end-user. If your mind is on the end-user’s everyday work, and all it implies, there is a bigger chance that the final solution will be better than expected.

If you and the end-user can create a common idea of the starting point, you know exactly where you have to go and from where.

So as a project manager, a good way to start is to make a common understanding in your company of the starting point and the final result of the implementation. To reach a common understanding, you need acceptance of the start and final result from the end-user as well as from the sponsors or owners of the systems.

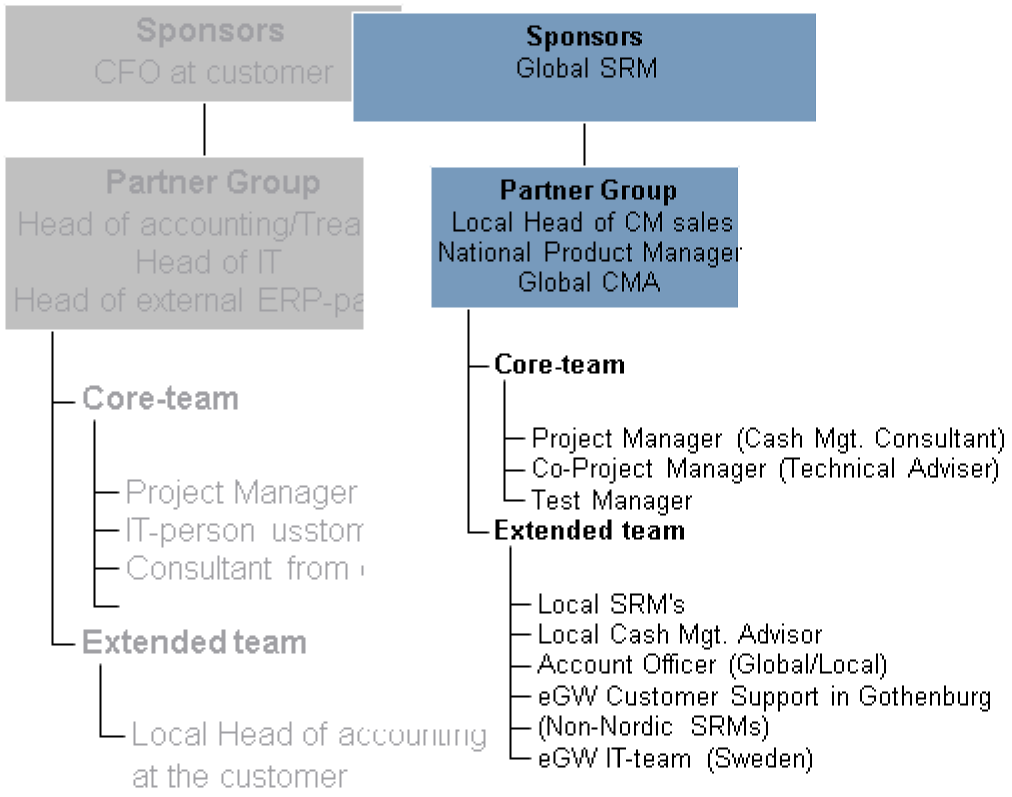
Organisation established

2 Project preparation

When it has been decided to implement Corporate eGateway the first and most important step is to build a proper organisation and agree on how this organisation has to work, how it has to communicate internally, and what the members have to expect from each other.
It is important for all parties to understand that this project organisation is not about sellers and buyers, but partners who work together to realise the same goal.

The project organisation described below is not only applicable to Corporate eGateway customer implementations, but could also be used in any cash management implementation. However, the work should be expanded to fully cover other CM strategic products.

The project organisation described below is recommended to be used in all Corporate eGateway implementations.



Further, in order to achieve fast implementations you should mirror this project organisation within your own organisation (illustrated with grey). Nordea do not require this but it may form a good basis for the discussion in relation to the allocation of sufficient resources, good communication and an appropriate escalation structure in the project.

The Project Sponsors are the top authority of the project; they fund the projects and are the receivers of the project result. The global senior relationship manager and, if needed, the Head of the implementation team in Nordea are the Sponsors from Nordea. The Sponsor's function is also to support and/or solve serious problems that may arise during the project process concerning resources, support and co-operation between different departments both in your company and in Nordea.

In smaller projects the Partner group and sponsor group can be merged.

The Project Partners are responsible for following-up on the project and to make sure that this agreement is followed and are responsible for keeping themselves up-to-date with the project and ensure that this activity plan is complied with. They must receive status reports on an ongoing basis, decided by the Core Team. Further, it is their responsibility to follow up on the project manager if any deviations occur. They should also help the core team with significant questions or problems that may arise during the project phase, for instance resource problems.

The project managers are responsible for the progress of the project and the daily project work. The project managers should handle all planning activities and exchange of information. The project manager may preferable participate in partner group meetings. However, formally she/he does not participate in the decisions in the group to prevent her/him from supervising his/her own actions.

The Core Teams consist of specialists from different areas like functional issues, data flow and messages, implementation and testing. The Core Teams play an active part in the project and there may be direct contact between the members of the two teams. The core team members will receive all relevant information from the project. The Core Team is where the hands-on work is done in the project.

The project manager is the driver of the Core Team and ultimately responsible towards the partner group.

The extended team is an internal reference group. The members of the extended team should be informed of the ongoing process through status reports in order to be prepared and informed about what is going on concerning the specific implementation. The extended team will most likely at some point during the project process be actively involved, i.e. when setting up local systems for Corporate eGateway.

If obstacles occur that may influence the progress or the end-result of the project, they should be brought to the attention of the two project organisations at a higher level. Example: The project managers will discuss issues with the project partner and if necessary the issues will be brought to the attention of the project partner in the other project, and so on.

A complete list with names and roles in the project will be exchanged between the parties, see the document *Project & activity plan*.

Communication plan finished

2.1 List of interested parties and communication plan

Where do you find the resources? – Who are pro and who are con the implementation?

It might be an idea to make an analysis of the interested parties in the project. You can avoid conflicts beforehand or even get important input to the functionality. Do not forget the end-users, they often have important information on how the system works, or they might be negative to the implementation.

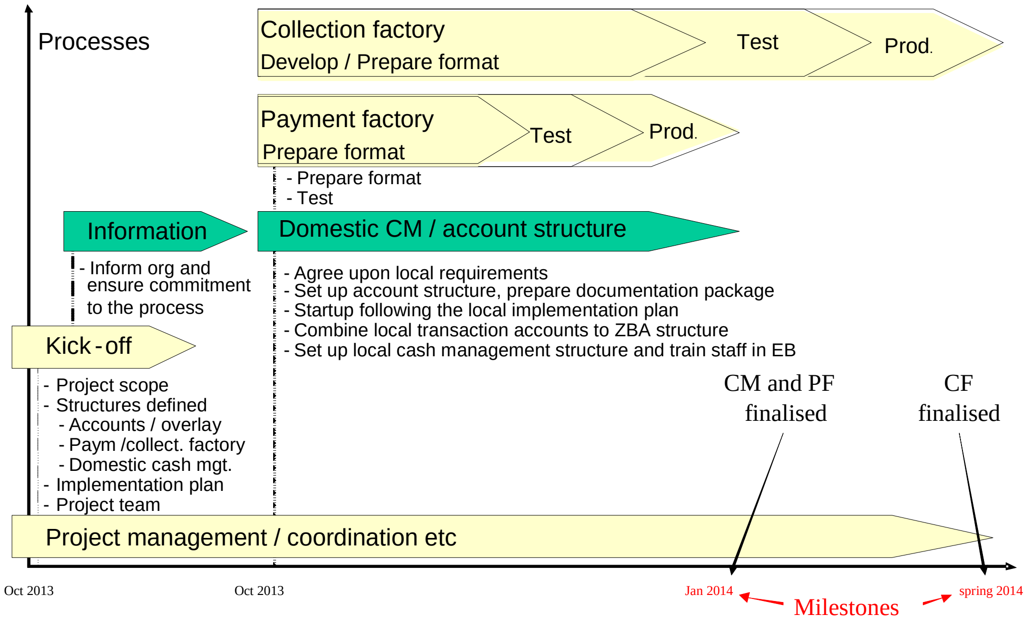
An important part of the analysis is to make a plan for the communication in the project.
There are two parallel organisations, and it is very important that information between you and the bank and vice versa is informative.

Activity list finished

2.2 Project progress

It is recommended to agree on a plan about the progress in the project. This project plan should contain the various implementation milestones, the responsible persons and the timetable.

Timetable and processes


Processes
Collection factory
Develop / Prepare format
Test
Prod.
Payment factory
Prepare format
Test
Prod.
- Prepare format
- Test
Information
Domestic CM / account structure
- Inform org and ensure commitment to the process
- Agree upon local requirements
- Set up account structure, prepare documentation package
- Startup following the local implementation plan
- Combine local transaction accounts to ZBA structure
- Set up local cash management structure and train staff in EB
Kick-off
- Project scope
- Structures defined
- Accounts / overlay
- Paym /collect. factory
- Domestic cash mgt.
- Implementation plan
- Project team
CM and PF finalised
CF finalised
Project management / coordination etc
Oct 2013
Oct 2013
Jan 2014
Milestones
spring 2014

The project plan will differ depending on the company and the technique involved and many other things and it are not possible to make a general project plan. Many of the tasks will be common for all but will depend on the ERP system and platform.

The above figure shows an example of the timetable and processes, including the account opening processes, which are not described in this manual.

Before completing the activity list, please read chapter 4 about implementation. You will find an example of the activity list in a separate document *Project & activity plan.*

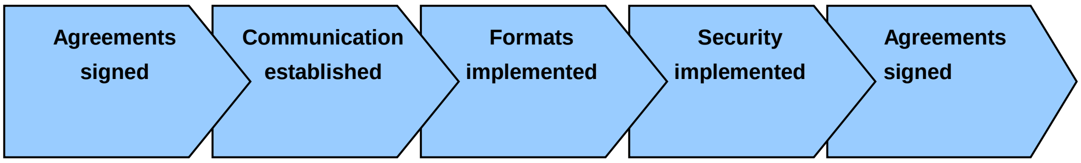
2.2.1 Checklist

Project start

- Project initiation, definition of project organisation, roles and responsibilities
- Decision on which business transactions will be exchanged, as well as the exchange of security and control Messages with each business transaction
- Establish test and go live dates with Nordea

3 Implementation

The implementation task consists of four different subtasks:



Each subtask will be described to give you the possibility to estimate time, resources, and define goals for the final implementation. It is not possible to define a detailed activity list as customers differ and have different demands to the solution, but you will get a checklist based on our experience so that you can check whether you have touched all aspects in the implementation.

3.1 Agreements signed

Agreements have to be signed by the persons authorised to sign on behalf of the company. The customer relationship manager at Nordea will provide you with the relevant agreements based on the decisions in the previous phase.

We know from experience that this task may take some time as the persons authorised to sign for the company may not be available at the moment when the signing is needed.

This is a risk for the timetable in the project, and you might prevent this at an earlier stage, if possible.

3.1.1 Checklist

Agreements

- Sign the required agreements with the payment systems in the countries where the relevant Nordea Companies are located
- Sign the required account and other service agreements with the relevant Nordea Companies
- Sign a Testing Agreement and an Corporate eGateway Agreement with the relevant Nordea Company

3.2 Communication

Communication is about how to deliver and receive data to and from the bank. In other words, which line and protocol are we going to use? Many customers have their own way to communicate and Nordea also has its own way of communicating. If we cannot agree, we use a VANS operator to support the communication.

If you decide to use a VANS operator, you are responsible for the connection between yourself and the VANS operator, and Nordea will take care of the connection between the VANS operator and Nordea. We have to co-operate about the addresses of the VANS operators.

The present standard communication towards Corporate eGateway is FTP/VPN, SFTP, AS2, WebServices (only for XML ISO20022) and SWIFTNet FileAct. You will find some detailed technical specification at Nordea's website www.nordea.com.

3.2.1 Checklist

Communication

- Order FTP/VPN, SFTP, AS2, WebServices or SWIFTNet FileAct service
- Install any required communication software if it is not a part of the message software
- Configuration of communication software
- Configuration of addresses
- Test communication software and set-up

Formats implemented

3.3 Formats

The format in Nordea's Corporate eGateway service is EDIFACT D96.A or XML ISO20022, version 3.

This chapter will give you an overall view of the formats, the flow and Message Formats.
You will find detailed information about the EDIFACT and/or XML format to be used for mapping in the documents *Message Implementation Guides* and *Message flow and use of EDIFACT* / XML at Nordea's website www.nordea.com.

This subtask might be the most complicated. At the investigation and decision tasks, the formats and the use of data are usually not discussed in details. At this stage you will go into detail with the format, and you will discover that small details make big difficulties.

First of all you need to be sure of how you want to use the Message Format in your own system, which fields are important and which is not. At this point the information you got from the end-user in the beginning of the project might be of great value.

This subtask requires a good understand of the business and the demands from the users, and also a good understanding of the format and the content in the format. You as the customer know the demands, and we as the bank know the content in the format, so to be successful in this task, close co-operation is a must.

By using the EDIFACT and/or XML format, you will have the benefit of using the same syntax for all Message Formats in Corporate eGateway, but the content, however, will differ from country to country due to:

What payment routines/products you use in each country
What invoicing routine/system you use
What payment routines/products your creditors use in each country
The infrastructure and common practice of each country and each local clearinghouse

The following types of Messages Formats will be supported between the Customer and Corporate eGateway:

From the Customer to Corporate eGateway when using EDIFACT:

Message name	**Message type**	**EDIFACT directory**
Payment orders	PAYMUL	UN/EDIFACT D.96A directory
Direct Debit Message	DIRDEB	UN/EDIFACT D.96A directory
Authorisation Message	AUTHOR	UN/EDIFACT D.96A directory
Message Acceptance Acknowledgement and Syntax errors	CONTRL	UN/EDIFACT, R.1186
Authentication	AUTACK	UN/ECE/TRADE/WP.4/R.1245 and R.1246. Adapted to the Recommended Practice - SJWG

From the Customer to Corporate eGateway when using XML ISO20022:

Message name	**Message type**	**XML ISO20022**
Payment orders	pain.001	"*CustomerCreditTransferInitiation*" Message (pain.001.001.03).

See an example of the use and Message flow of these Message Formats in the scenarios above. For a more detailed description, see the documentation – *Functional specification* for each service, *Message flow and use of EDIFACT / XML* and *Message implementation guides* which all can be found on Nordea's website www.nordea.com.

Before starting the mapping, a meeting between the programmers and Nordea should be held to explain the format and the differences in each country.

3.3.1 Checklist

Application system interface

- Investigation of information requirements to Nordea.
- Is it possible to deliver all mandatory information from the internal application system?
- Investigation of return information from Nordea.
- How can we process the status information, bank statements etc from Nordea into our system?
- How can we achieve automated reconciliation?
- What set-up and modifications need to be made to our system in order to achieve the above?
- What internal controls do we need to apply?

Message software

- Install Message software, if not already in place
- Create a test environment and prepare a production environment
- Create conversion programs for selected Message Formats
- Test outgoing Message Formats (test data can also be exchanged via mail for initial tests of incoming Message Formats before the communication is working)

Security implemented

3.4 Security

In order to prevent attempted fraud, it is important for the participants to make sure that the message formats are valid instructions to the bank. This means ensuring that the instruction is made by a valid party, who cannot subsequently deny having sent it, and that the instruction is not changed or manipulated by any other party during the transfer. To ensure this you should cover the transactions by Integrity, Origin Authentication, and Non-repudiation of origin techniques.

The Secure Authentication and Acknowledgement Messages AUTACK or is used to give origin authentication for EDIFACT Messages. In addition Nordea can offer PGP (Pretty Good Privacy) as a security method towards Corporate eGateway for both EDIFACT and XML ISO20022 users.

Validation of sequence integrity (assuming a system of sequentially numbering messages is used and is covered by authentication).

Non-repudiation of origin.
For details, please see the document *Security and communication description,* which can be found on Nordea's website www.nordea.com

Corporate eGateway follows the recommendations from UN/CEFACT regarding security when using EDIFACT and therefore supports AUTACK as a security message for EDIFACT Messages sent by you to Corporate eGateway. Nordea does not as standard use security methods, such as AUTACK, in EDIFACT Messages sent from Corporate eGateway to you.

In addition Corporate eGateway offers PGP (Pretty Good Privacy) for both EDIFACT and XML ISO20022 users. This security method may be used both from Nordea as well as from our customers.

For XML ISO20022 users, Nordea also offers WebServices, using PKI as security method.

It is assumed that normal professional standards of internal security are in operation, in particular covering access and modification of security keys, and their use in authorising the electronic transmission of transactions. The function of the security described here is simply to authenticate data while it is in transit, and a single signature is adequate. This would most probably be an automated signature.

Nordea's policy concerning AUTACK (or PGP and/or PKI for WebServices) is not to recommend or provide any software. We will, however, upon request inform you about relevant software.

The authentication is implemented in the following steps:

- Calculation of the hashed value of the interchange
- The hash value is then used as input to calculate the digital signature, i.e. it is encrypted under the originator's private key
- The digital signature is put into the AUTACK (or PGP and/or PKI for WebServices)

If necessary, a second, or more, authentication(s) can be made by another signatory. The hash value is calculated again (to allow detection of changes to the data between signatures) and the Signature may be computed using a second, or more, private key(s) and put into the AUTACK to provide a double, or more, key(s). To use several signatures may form a "personalised" authentication/authorisation process in order for you to identify (authorise) individual persons in your company.

The recipient will check that the received interchange matches the hash value extracted from the sender's digital signature, and this verifies both the validity of the content and the origin.

The ordering party is responsible for assigning a unique customer reference to each Message. Corporate eGateway may detect duplicate Messages immediately after acceptance and before booking. The reference number of accepted Messages is stored in Nordea for a period of 90 days. Duplicate messages received after this period will be processed as normal messages.

For information on the security messages PGP or PKI for WebServices, please contact your local cash manager adviser.

3.4.1 Checklist

Security

- Purchase security software that handles digital signatures, if none exists
- Install security software and investigate interface to Message software creating AUTACK, PGP (or PKI for WebServices) Messages
- Investigate exchange and management of keys and/or certificates

4 Test

TEST

Tests are a project of its own, and are not described in detail in this manual.

4.1 How are tests performed in Corporate eGateway?

The test period in Nordea is mainly divided into two steps;

1. *Format test – Part 1*. The Nordea Test manager will do a number of format test cases based on the services and payment types needed by you. The format testing is a very basic testing of the format itself and normally this part doesn't involve any from the business side.

2. *Functional test – Part 2*. Functional test cases will also be created by the test manager on the basis of the same criteria as for Part 1. The Functional testing is aimed to replicate an end-to-end scenario at the customers' side and therefore it normally involves also the business side. In some cases it might even be possible to pass the Functional test cases on to an in-country Nordea test environment.

Before go-live we do always suggest our customers to do a *Production Verification test*:

3. *Production Verification test – Part 3*. These tests will be performed in Nordea's production environment. No test cases are created by Nordea's test manager, but can be done jointly with you, if wanted. For this purpose it is recommended to open two new accounts in each Nordea Company, and send a very limited number of payments carrying small amounts between these accounts. The project team will monitor these payments closely together with you. It is, however, important to understand that Nordea cannot take any responsibility for these types of payments, since they are booked automatically in Nordea's production environment. **Note:** Please note that both the Corporate eGateway Agreement and the Security keys must be in place before performing this kind of tests.

After successfully having performed the *Production Verification test* you are now ready to go into production. However, Nordea strongly recommends that new Security Keys are first sent to Nordea's Security department. Outside consultants and/or other internal staff in the company not related to the normal day-to-day business have often participated in the above test scenarios, and therefore this is necessary to prevent any unauthorised access when in production.

4.2 What can be tested?

For information about what kind of Messages that can be tested in each local Nordea Company through Corporate eGateway please refer to either your cash management adviser or technical adviser in Nordea.

4.3 Test accounts to be used

For information about which test accounts to use please through Corporate eGateway please refer to either your cash management adviser or technical adviser in Nordea.

4.4 Security and/or Authorisation Keys for the test period

Test period: The responsible project manager, technical adviser or test manager will inform Nordea Bank AB's Security Department about any new customer's name, contact persons, test plans etc. As soon as you are ready to start testing your preferred security solution, the test period can start.

The purpose of these tests is to ensure that you can create the relevant Message Formats for each service used in each chosen country. It is also aimed at giving you the possibility of getting familiar with and adopts the different types of Message Formats that Corporate eGateway provides.

Nordea Bank AB's security department will send an e-mail to Nordea's responsible project manager, technical adviser or test manager, when the public test keys have been installed. Nordea's project manager or test manager will then inform you that you can start testing messages with your preferred security solution.

Before going into full production, new security keys must be sent to Nordea's Security Department.

4.5 Go live and Service Support

When the test period has finished, and you have signed and accepted the performed tests, the time has come to go live. It is recommended to go live with one country at a time and with small volumes in order to see that the service is acting and performing as expected – but also to enable you to react correctly to and understand the Message Formats sent by Corporate eGateway.

During the first week of production the project management, test manager and Corporate eGateway Service Support will have full attention to the project and alert routines will be in place in case any unexpected errors should occur but also to help and support in any situation related to Corporate eGateway.

4.6 Security and/or Authorisation Keys for production

Before you can go live with Corporate eGateway, new security keys have to be sent to the security department in Nordea Bank AB (publ). To do this, certain requirements have to be fulfilled, all of which can be read in the document.
The Corporate eGateway Agreement has to be signed together with Schedule 3 (Authorisation document). *Guideline for support including Contact List* has to be filled in by you, stating the persons authorised to create and send new Security/ Authorisation Keys to Nordea Bank AB's Security Department, which also include the authority to block any payment services within Corporate eGateway, if such action will be required.

4.7 Back-up systems

Things might go wrong. It is a fact that sometimes the lines are down, damaged by accident, or whatever your fantasy can imagine. The keys are invalid, your ERP systems experience major break downs, lots of things that put you in the situation - You are not able to deliver your Messages to the bank - or - you can not receive data from the Corporate eGateway.

On the basis of the solution you have implemented you are recommended to think about an alternative solution for the situation mentioned above, and an emergency plan has to be documented.

Discuss the alternatives with the project manager in Nordea, and find the back-up system you need or a procedure for emergency cases.

4.8 Service Support

Guideline for support including Contact List

Situations may occur when it is necessary to re-transmit one or more Messages and a standard solution is therefore needed for handling re-transmissions.

In this document cancellation routines describes in detail how you can achieve this service through our Corporate eGateway Service Support. For this purpose it is important that authorised persons at your company sign Appendix 3 to the Corporate eGateway Agreement, to ensure a correct processing by Nordea.

You will also find information on cover control routine, security related issues etc as well as opening hours and other contact information to Nordea's Corporate eGateway's Service Support.

4.8.1 Checklist

Go live

- Create and document routines for operation and error handling
- Appoint contact persons for questions and for error handling
- Create and document routines for emergency cases

5 Documents to be read in relation to Corporate eGateway

There are a number of documents for Corporate eGateway that you should read in order to ease the implementation and to get a true understanding of the Corporate eGateway services and its Message Formats.

For implementation purposes, the following documents are recommended:

- Nordea's interpretation of how a test procedure or project in Corporate eGateway may be performed, which can be found within the *Testing Agreement for Corporate eGateway*
- *Project & activity plan*

For descriptions, guides and other specifications, please us the following documents:

- *Main product description*
- *Message implementation guides*
- *Functional Specifications* (for each relevant service)
- *Message flow and use of EDIFACT / XML*
- *Guideline for Support including Contact List*