EUROPEAN CENTRAL BANK

EUROSYSTEM

Explainer on business configurations in the ECMS

September 2021

ECM project

Contents

1 Introduction

The ECMS provides flexible solutions for business configurations which are suitable for different ECMS counterparty needs. This document aims to describe the functionalities that allow a third party to act on behalf of a counterparty or provide connection to the ECMS to a counterparty. Some concepts have been already briefly explained and published on the ECB website. Please refer to the Business Description Document for the ECMS, the ECMS info pack - access and connectivity and the ECMS Connectivity Guide v1.0.

The document is structured as follows. The first chapters provide technical information on ECMS functionalities: Chapter 2 gives some basic information on connectivity; Chapter 3 describes authentication and authorisation processes; Chapter 4 explains the access rights; and Chapter 5 explains message subscription.

Finally, Chapter 6 shows how to configure ECMS parties and technical senders in different business scenarios, depending on counterparty needs.

2 Connectivity

The ECMS relies on the Eurosystem Single Market Infrastructure Gateway (ESMIG) for communication between the ECMS and ECMS parties. ESMIG is the common entry point for all interaction with the TARGET Services. The ECMS supports the connectivity of ECMS parties in A2A and U2A mode:

- A2A (Application-to-Application): Communication between software applications via XML messages or files using ISO 20022 messages or compliant with the ISO 20022 format. A file contains one or several messages.
- U2A (User-to-Application): Online screen-based activities performed by ECMS parties

Apart from the connectivity aspects, each NCB retains the business and legal relationship with its participants that are ECMS parties.

The ECMS does not provide technical connectivity or network services to ECMS parties. ECMS parties use a licensed network provided by an accredited connectivity services provider Network Service Provider (SWIFT and SIA Colt). Detailed information on the usage of network services is provided in the ECMS Connectivity Guide v1.0.

3 Authentication and authorisation

3.1 Introduction

This section provides information on the authentication and authorisation processes in the ECMS. In order to communicate with the ECMS, an ECMS party connects to its Network Service Provider (NSP) and has to successfully pass the authentication and basic authorisation processes carried out by ESMIG, and then the authorisation processes of the ECMS. For inbound A2A messages, the ECMS performs the schema checks on the message. For inbound U2A communication, the U2A interface of the ECMS ensures correct formatting.

An authorised person or authorised application may act on behalf of another ECMS party (via a proxy), i.e. one ECMS party can send messages on behalf of another ECMS party if both parties are under the same NCB Data Scope. Therefore, the business sender (the instructing party in the message and the party responsible for the business payload of the message) and the technical sender (delivering the message to ECMS via a licensed network NSP) can be different entities. The relationship between the business sender and the technical sender is established on a bilateral basis between the involved parties.

3.2 Main concepts

This section presents the main concepts related to authentication and authorisation processes in the ECMS. Authentication requires that each ECMS user has a login name and a certificate for access to the ECMS.

User

A user is a person or application that interacts with the ECMS triggering the available ECMS user functions. The set of available ECMS user functions stems from the set of privileges the user is granted (see section Access rights).

Each user defined in the ECMS corresponds to a person, i.e. an employee of a given ECMS party using the ECMS U2A, or to an application, i.e. a software component of a given ECMS party interacting with the ECMS in A2A mode. The ECMS uses a unique reference to identify each user (login name).

Certificate

A digital certificate is an electronic document binding the identity of an ECMS user to a pair of electronic keys; a private key (used to sign digital information to be sent to an ECMS party or to decrypt digital information received from an ECMS party, and a public key (used to encrypt digital information to be sent to an ECMS party or to perform the authentication and to ensure the integrity of digital information received from an ECMS party).

Association between users and certificates

ECMS parties assign certificates to their users (interacting with the ECMS in U2A mode) and applications (interacting with the ECMS in A2A mode). One certificate can be linked to one or more ECMS users, even users belonging to different counterparties and/or of different countries. One ECMS user can be linked only to one certificate. If an ECMS party uses two Network Service Providers (i.e. SWIFT and SIA Colt), separate certificates must be provided by each Network Service Provider. This information is used by ESMIG and stored in the Common Reference Data Management (CRDM).

Distinguished Name

A Distinguished Name (DN) is a sequence of attribute-value assertions separated by commas e.g.

<“cn=smith,ou=ECMSuser,o=bnkacct,o=nsp-1>

A DN is a sequence of comma-separated attributes that identifies the digital certificate. The NSPs are responsible for defining the DN for the ECMS party. Each user (human user or application) linked to a digital certificate is therefore given a Certificate DN. Each identity bound to a digital certificate is assigned a unique DN.

Technical sender

The technical sender is the entity that technically submits an A2A message to the ECMS. Each technical sender is identified by means of a certificate issued by NSP. The network infrastructure of the NSP authenticates the technical sender based on its certificate in A2A mode. The technical sender does not need to be configured as a party in the ECMS, but when technically sending a business message on behalf of other parties, the technical sender has to include the business signature of the business sender of the counterparty on whose behalf they are technically sending the message. The technical sender must be registered in the Closed Group of Users for the ECMS.

Business sender

The business sender is the ECMS party creating the business payload of an A2A or an U2A request to be submitted to and processed by the ECMS. In some instructing scenarios, the business sender and the technical sender can be different business parties.

Business sending user

The business sending user is the user creating the business payload of the request. This user corresponds to a person or to an application of the business sender ECMS party. Each business sending user is identified by the certificate DN, which is included in the business header of the request.

From a business perspective, the business sending user only needs to sign the business payload once, irrespective of whether this payload includes one request or as set of requests. If only one request is included in the payload, the business sending user signs the Business Application Header of the request[1]; if a set of requests is included, the business sending user signs the Business File Header of the file which contains these requests. One file cannot therefore include requests referring to different business sending users, i.e. requests related to different business sending users must be sent in separate files.

Business sending party

The business sending party is the party to which the business sending user belongs. The ECMS identifies the business sending party once it has identified the business sending user, as each business sending user belongs to one party.

The business sending party owns the business message identifier specified in the Business Application Header.

Instructing party

The instructing party is the party instructing the ECMS to process the business payload of the request. The instructing party is specified (as a pair of BICs) in the Business Application Header and is the owner of the business reference (i.e. the transaction identifier) specified in the business payload. The instructing party therefore defines the scope for the duplicate check at instruction level.

[1] The BFH is used only in the communication with TPAs

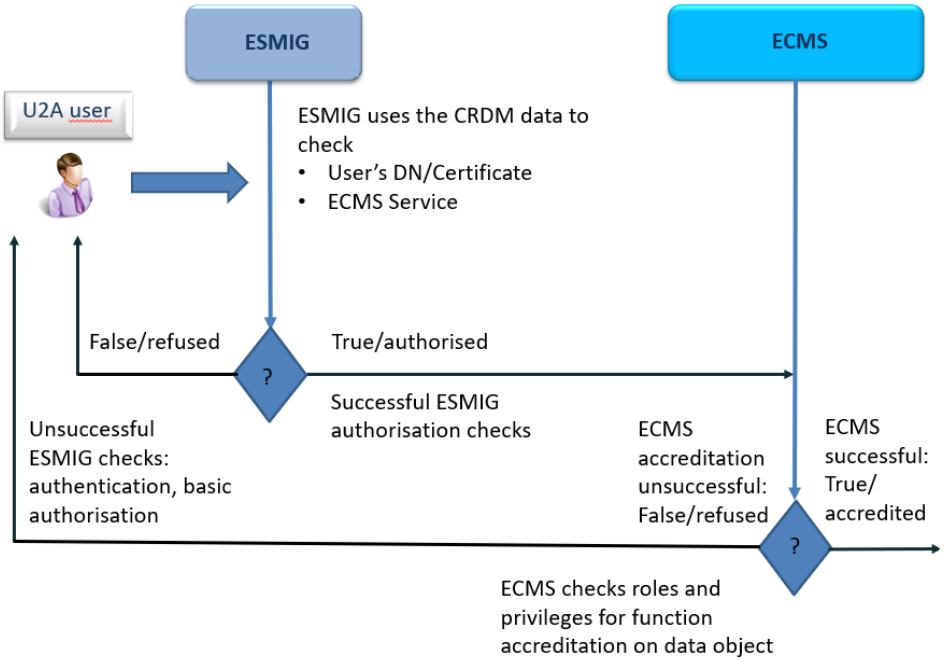
3.3 Authentication Process

The ECMS is not responsible for the sender strong authentication process, as this task is performed by the ESMIG. ESMIG checks the capacity of the user (application or person) to connect to the ECMS.

3.4 Authorisation Process

The purpose of this section is to provide a description of the Authorisation process carried out by the ECMS. The ECMS checks the rights of the user (application or person) to carry out a specific function in the ECMS. The authorisation is performed against the sender's privileges (User, Role, Function, Data object) stored in the ECMS reference data. Figure 1 shows the authorisation checks for U2A communication.

Figure 1- ECMS Authorisation

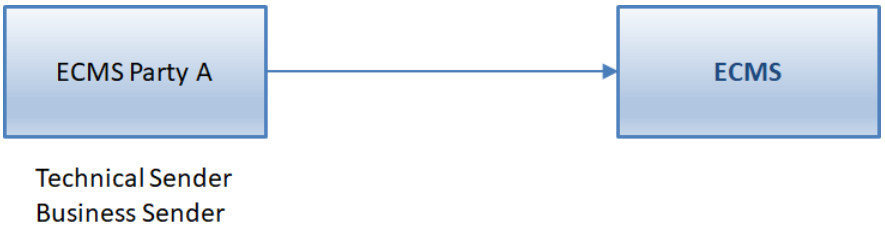


For detailed information on A2A authentication and the authorisation process please refer to Explainer on authentication and authorisation of instructions in the ECMS

3.5 Instructing Scenarios

The basic scenario is where an ECMS party instructs on its own behalf and receives notifications on the status of instructions. In this case, the ECMS party signs the instructions it intends to submit to the ECMS for processing, and therefore acts as both technical sender and business sender. The ECMS party can opt to use the same certificate to play both roles.

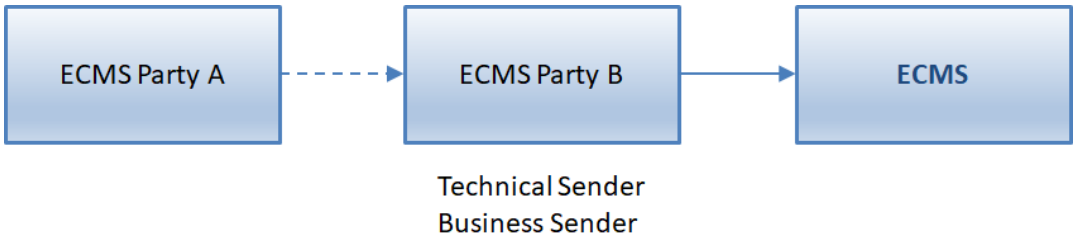
Figure 2 – Direct emission of messages



The other more complex scenario is where an ECMS party instructs on behalf of another ECMS party and receives notifications on the status of instructions. There are two possible cases.

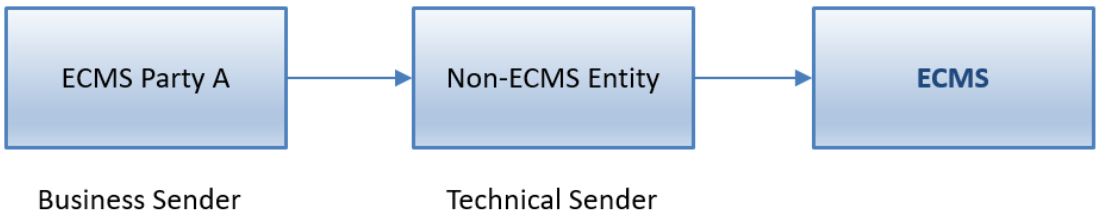
The first is where ECMS Party A does not sign the instructions it intends to submit to the ECMS for processing, and fully relies on another ECMS party to conduct its activities in the ECMS. In this case, ECMS Party B acts as both technical sender and business sender on behalf of ECMS Party A.

Figure 3– Indirect submission of messages (case 1)



The second case is where ECMS Party A keeps full responsibility for signing the instructions it intends to submit to the ECMS for processing. This means that ECMS Party A acts as business sender but relies on another non-ECMS entity to act as technical sender on its behalf, i.e. the non-ECMS entity acts as a pure technical router from ECMS Party A to the ECMS.

Figure 1 – Indirect submission of messages (case 2)



The Business Application Header (BAH) is part of each business message exchanged between the ECMS party and the ECMS. The BAH contains information on the instructing party and the business sender and, together with an ISO 20022 message, forms a Business Message.

4 Access rights

4.1 Access rights concepts

XML messages (authorised instructions) and GUI functions are the basic elements that applications and human users can trigger in A2A mode and in U2A mode respectively to interact with the ECMS. Based on these set of XML messages and GUI functions, it is possible to define the set of ECMS user functions. Users can trigger ECMS functions depending on the Privileges which have been granted to predefined Roles, and the Roles which have been granted to Users:

- A Privilege identifies the ability to trigger an ECMS user function.
- A Role is a set of Privileges. The Roles are predefined in the ECMS. A Privilege can only be assigned to one predefined Role, and Roles cannot therefore have overlapping Privileges.

4.2 Users, groups and roles

The authorisation mechanism is based on user/group/role assignment. Access control to the ECMS is based on user privileges and the ECMS user functions granted to that privilege. A user has the access right to trigger a given ECMS user function if the user has been granted with the role that contains the privilege for this function.

Privileges to system resources (data and services) are assigned by predefined roles. Predefined roles can be assigned to users either individually or in groups.

Access rules are defined for each role. They control access to the data, services and the user interfaces.

The same user cannot be linked to an U2A role and an A2A role at the same time (as each user is either a U2A or an A2A user). If a user is granted with multiple roles, the privileges granted to the different roles are cumulative. It is not possible to be granted with contradictory privileges/roles, as the ECMS will always apply the least restrictive privilege.

4.3 Data scope

The data scope of an ECMS actor consists of all reference and dynamic objects for which it is responsible.

The ECMS Operator can view all data objects but can only modify objects belonging to participants in exceptional circumstances and with specific agreement.

NCB users can view all reference and dynamic data objects that are linked to the NCB and to the entities created by the NCB.

Users of ECMS parties can view all reference and dynamic data objects that are linked to their ECMS party.

The data scope of an ECMS party can be extended using the proxy functionality. An NCB can extend the data scope of one ECMS party (acting as a proxy) to allow it to operate on behalf of a different ‘delegating’ ECMS party or several different ‘delegating’ ECMS parties, provided that all counterparties fall under the data scope of the same NCB. The extension will allow the users of the party acting as a proxy to use their roles to manage the data scopes of all ‘delegating’ counterparties.

Figure 5- Default data scope. (Note: Entity = party)

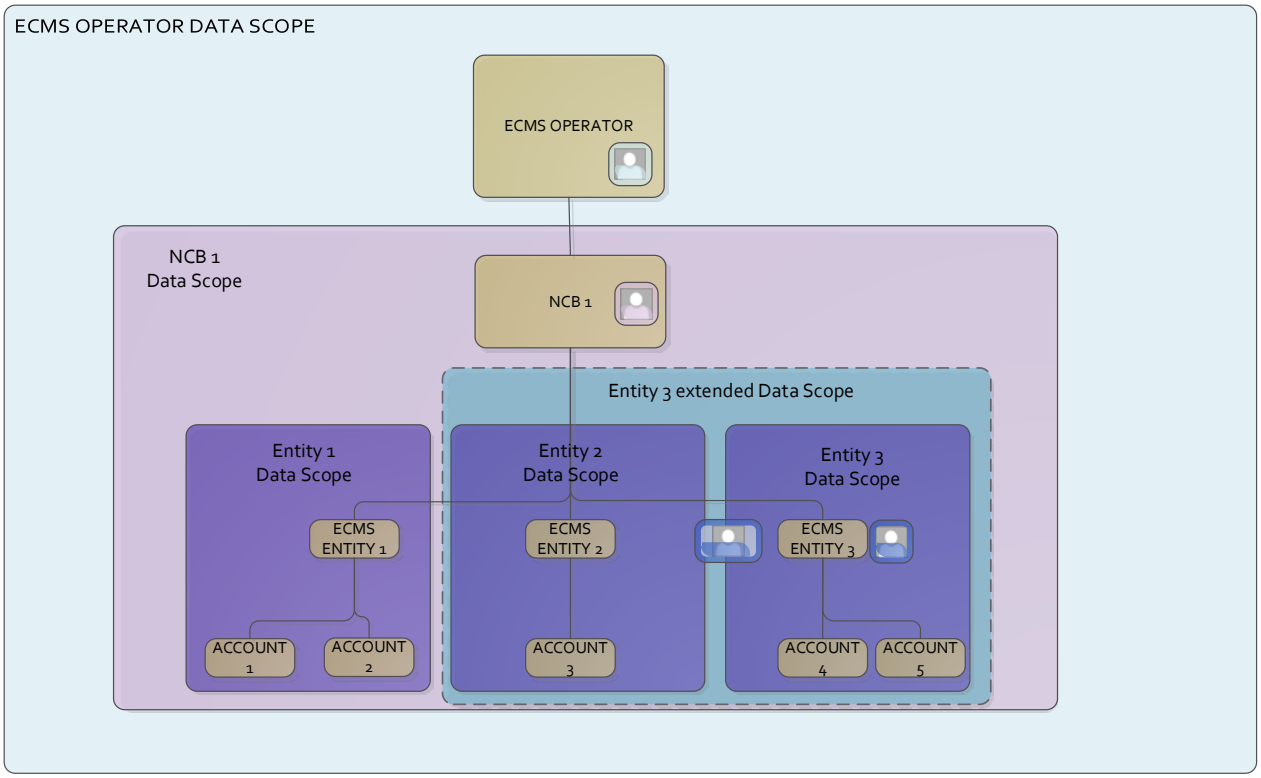


Figure 5 shows the default data scope model. In this figure the user of party 3 has access to a wider scope (including party 2 objects) due to a scope extension made possible through the proxy functionality. As such, party 3 users allocated with the relevant predefined roles are allowed to perform the required user functions on data elements of party 2 (e.g. a user of party 3 can send a mobilisation instruction on party 2's ECMS Account).

4.4 Configuration of administrators and users

The allocation of users and predefined roles is managed in the ECMS platform.

When the NCB creates a new counterparty in the ECMS reference data, the counterparty data scope is automatically created by the ECMS. The NCB links the party administrator user to the counterparty.

All users created by the party administrator are linked to the same data scope as the party administrator user.

4.5 Administrators

Each party must have at least one party administrator, i.e. a user which is granted the specific roles allowing the parties falling under its administrator privilege to

themselves grant roles to their own users. If a new party is to be administered in 4-eyes, it must be created with at least two administrators, each of them with the relevant predefined roles allowing for the confirmation of actions.

4.6 Roles

The ECMS supports a role-based access control (RBAC) model. A user can inherit the privileges for more than one role.

Roles are predefined in the ECMS and are based on the different business roles that a user can have in the system.

Predefined roles in the ECMS are segregated per ECMS party (NCB, Counterparty, CSD and TPA), per communication mode (U2A and A2A) and per business area (e.g. one role for Marketable Asset (De)Mobilisation and a different role for Counterparty U2A Credit Claim Management).

A2A roles allow the execution of the set of messages related to a business area, e.g. the role Counterparty A2A Marketable Assets allows the user to send the set of messages related to bilateral (de)mobilisations (sese.023, sese.020 messages), whereas the role Counterparty A2A Corporate Actions allows the user to send the set of messages related to corporate instructions (seev.004, seev.005, seev.033, seev.040). This segregation of roles provides multiple technical configurations that can be used to support the counterparties in their business needs.

For more information, please refer to U2A and A2A roles in the ECMS.

The party administrators are automatically able to manage all predefined roles assigned to the party to which they belong.

Each predefined role is created in two variants: read only and execution. The execution variant allows the user to manage a business need by sending instructions and/or by making changes in the database, while the read only variant allows the user to monitor their business activities. This is an exception to the general rule stating that each predefined role can only encompass a unique set of privileges.

One of two additional roles will be granted alongside the execution roles: 2-eyes allows the user to execute available actions without need of validation by another user; and 4-eyes allows the user to execute available actions only when validated by another user. These roles do not apply to the read-only roles. As the ECMS always applies the less restrictive role, if a user is granted both variants of a predefined role, the execution variant applies (as the less restrictive). Similarly, if a user is granted both the 2-eyes role and the 4-eyes role, the 2-eyes roles applies.

4.7 A2A privileges

In A2A, applications can trigger authorised instructions (XML messages). The administrator of the party can grant granular A2A privileges to the application user.

All A2A privileges (all A2A authorised instructions) are granted in 2-eyes-mode.

Predefined roles encompassing all authorised instructions in A2A for NCBs and for ECMS parties are also created and maintained by the ECMS Operator.

4.8 Configuration of groups

Administrators can use groups to gather U2A users with the same business profile. The usage of groups is meant to facilitate the allocation of business roles to the users. Once the users are allocated to one group, the administrator only needs to grant the role to the group and all the users included in the group inherit the predefined role.

Figure 6- Access rights configuration

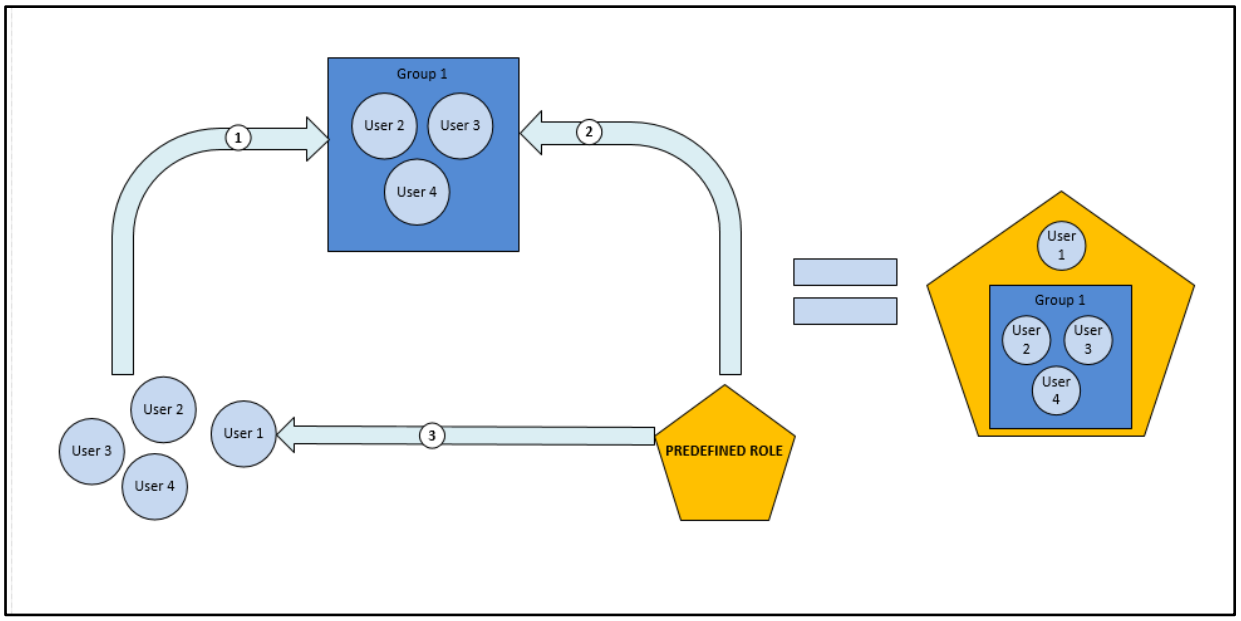
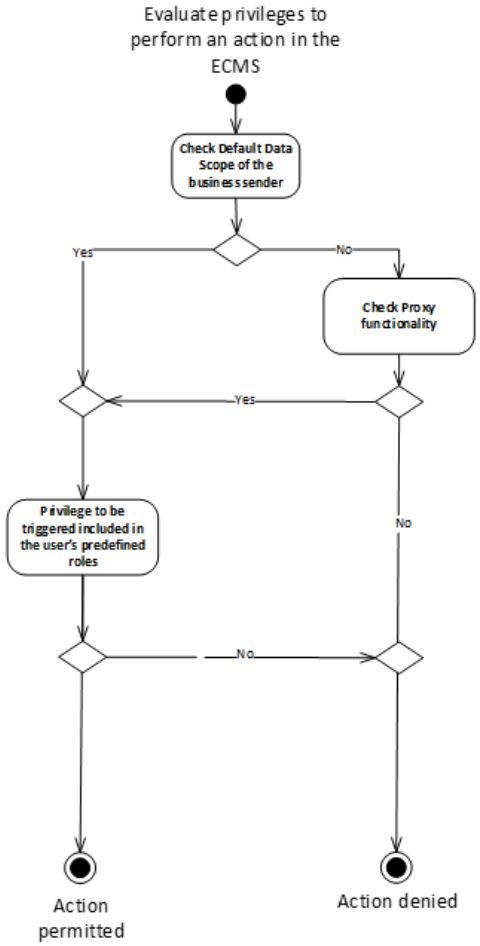


Figure 6 summarises the access rights configuration of the users of an ECMS party.

- In Step 1, the selected users are included by the administrator in a functional group. The step is optional as business roles can also be granted individually to a user.
- Step 2 represents the granting of a particular predefined role to the functional group that has been created in step 1.
- Step 3 represents the possibility of granting a business role in an individual basis

The result of these actions is that the users in the functional group 1 and the User 1 can trigger the functions included in the predefined role.

Figure 7 – Summary of privilege evaluation



In figure 7 the privilege evaluation process is summarised. In the first stage, the data scope of the user is checked. If the object on which the action is intended to be triggered is not in the default data scope of the party to which the user belongs, then the system checks if the party has extended data scope on other parties through the proxy functionality.

When the data scope check is resolved positively, then the ability of the user to perform the required action is checked against the user privileges included in the user roles.

5 Message subscription

This section provides a detailed description of the functionality offered by the ECMS to filter messages sent to ECMS parties.

Overview

The ECMS offers functionality for message subscription, with each NCB responsible for configuring message subscriptions for its community.

Counterparties have the option of requesting subscriptions to a specific set of reports on a daily, weekly, monthly, annual or ad-hoc basis, depending on the type of message.

Multiple addresses of a recipient

Depending on the business area, different addresses can be configured in the ECMS by NCBs for its counterparties.

At internal asset account level, NCBs can specify a technical address for the following business areas:

- Corporate Actions
- Securities Management
- Securities Settlement

Depending on the business need, the same technical address can be defined, or different technical addresses can be used.

At counterparty level the NCBs can specify a technical address for the following business areas:

- Corporate Actions
- Securities Management
- Securities Settlement
- Cash Management
- Payment
- Margin call
- Credit Claims

The ECMS sends the message to the address defined in the reference data at the level of the account. When no address has been defined at the account level, the

ECMS sends the message to the address defined in the reference data at the level of the counterparty. When no address has been defined at either the account or the counterparty level, no outbound message is sent.

When the recipient is directly an ECMS party (i.e. no technical address has been defined at the account level) , for example the refinancing NCB, the ECMS sends the message to the address indicated in the ECMS party reference data for the relevant business areas.

Technical address per business area

Technical addresses are configured per business area (Cash Management, Payment, Corporate Actions, Securities Management, Securities Settlement and Margin Call). Each business area has a set of messages.

The messages related to different business areas can be routed to different technical addresses. The technical address can be the counterparty's technical address or the technical address of a service provider. For further information please refer to the Annex on message subscription at the end of this document.

Message subscription per message and business status

An NCB can configure the message subscription for the counterparties in its community and can configure which reports will be sent to the Counterparties.

Each business areas contains a set of messages. Each message has several statuses. Message subscription can be configured at message level and business status level, depending on the specific message.

For details on the available messages and statuses, please refer to the Annex on message subscription at the end of this document.

In conclusion, counterparties can decide which messages they want to receive and to which technical address they are routed.

6 Potential business configurations

This section describes how to configure ECMS parties and technical senders for different business scenarios. The explanations are based on the following basic business needs/conditions and the functionality that can be used in the ECMS to support the counterparties:

Business need	Functionality
A person or application needs access to several counterparties under the data scope of the same NCB.	Data scope extension (proxy functionality)
A counterparty needs a service provider for A2A communication	Technical senders (technical sender signature can be different from the business sender signature).
A counterparty needs a service provider specialised in a specific area of the business (e.g. management of bilateral mobilisations)	Creation of dedicated A2A users within the counterparty granted with the appropriate roles
The counterparty does not have a contract with a Network with a Service Provider	Data scope extension.
A person or application in a counterparty in one country needs access to a counterparty located in another country	Association of one DN certificate to multiple users

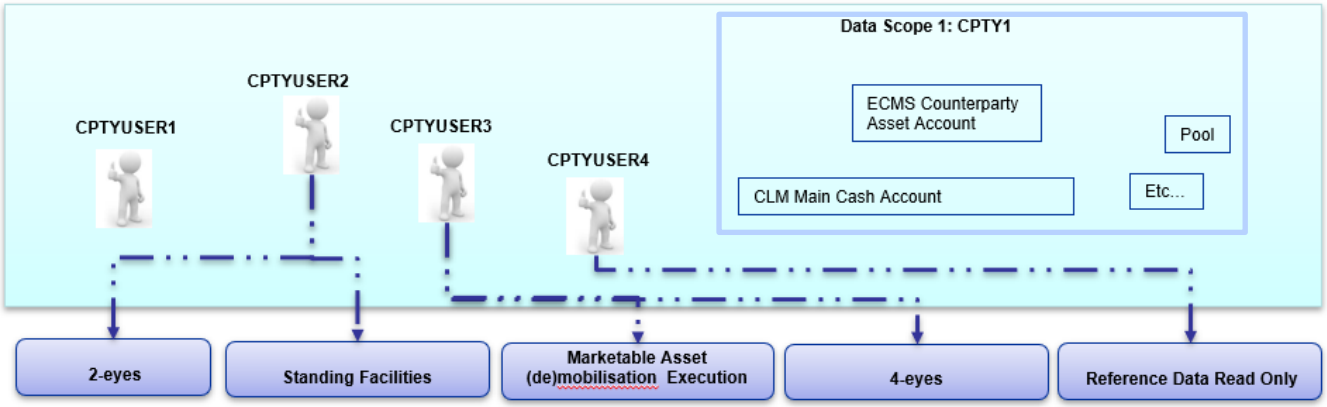
The examples below also combine these scenarios.

6.1 Data scope extension

NCB users can extend the data scope of an existing counterparty (CPTY) in the ECMS. Data scope extension can be achieved by modifying an existing data scope or by creating a new data scope.

Example. The initial set up is the following: CPTY1 has 4 users. CPTYUSER1 is the party administrator and configures CTPYUSER2, CTPYUSER3 and CPTYUSER4 with different roles in 2-eyes and 4-eyes and read only access. All these users have access to objects under the scope of CPTY1 (Data Scope 1)

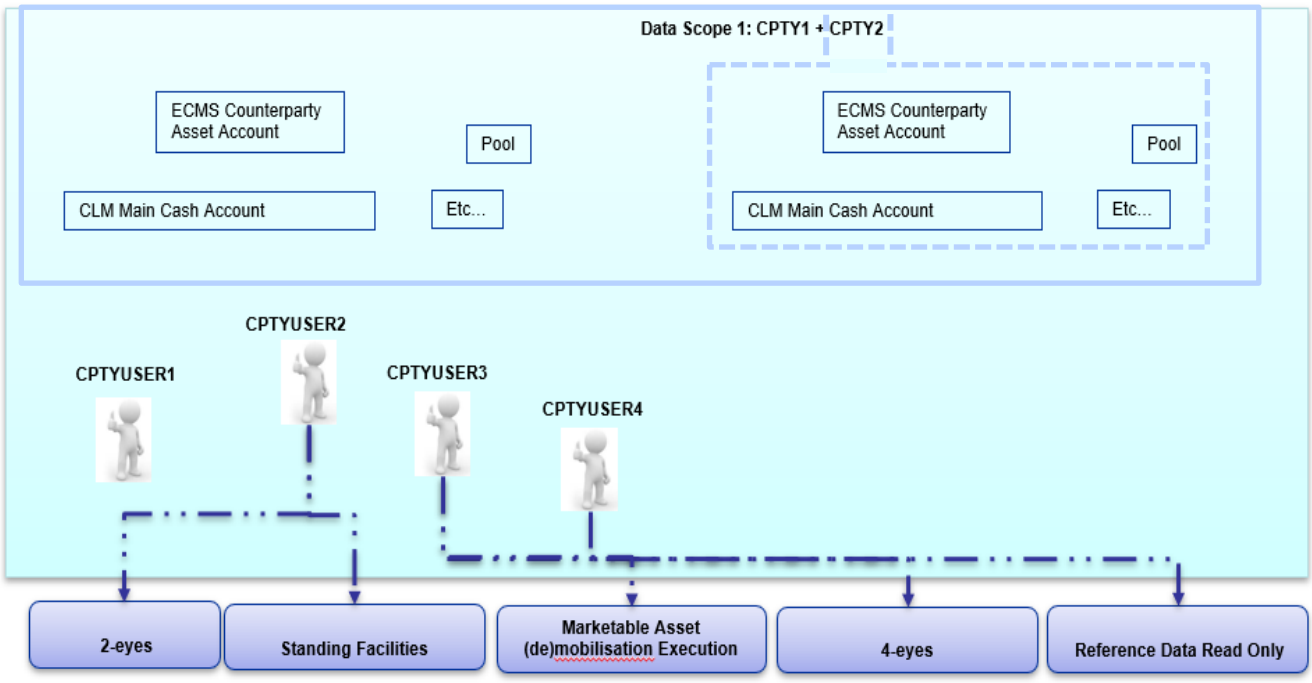
Figure 8 – Initial set up



Data scope extension: modification of an existing data scope

CTPY1 needs to work on behalf of another counterparty, CTPY2. One way of achieving this is to modify the existing data scope. The NCB user extends Data Scope1 to include all the objects under the scope of CTPY2. As the users of CPTY1 already have access to Data Scope 1, these users have automatic access to all objects under the scope of CPTY2. Users of CPTY1 can now work on behalf of CPTY2 using the same ECMS user and the same certificate DN. It should be noted however that the extension of Data Scope 1 does not give users of CTPY2 access to the data objects of CTPY1.

Figure 9 - Modification of an existing data scope



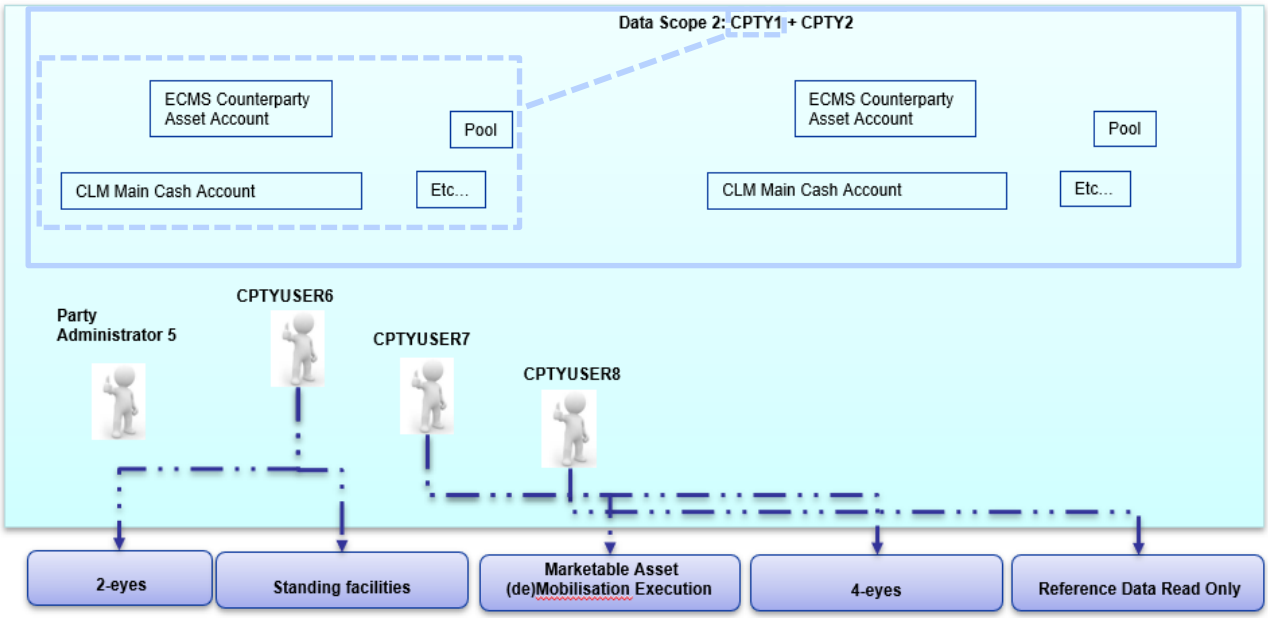
Data scope extension: creation of a new data scope

Depending on the needs, the NCB user can, instead of enlarging Data Scope 1 to allow users of CTPY1 to act on behalf of CTPY2, create a new data scope which would allow users of CTPY1 to act on behalf of CTPY2

To achieve this, the NCB user creates Data Scope 2: CPTY1 + CPTY2. The NCB user then creates the party administrator for Data Scope 2 and the party administrator create new users.

The new user constellation would be CTPYUSER5 as party administrator, with users CPTYUSER6, CPTYUSER7 and CPTYUSER8.

Figure 10 – Creation of a new data scope



With this configuration CPTYUSER1, CTPYUSER2, CTPYUSER3 and CPTYUSER4 only have access to the initial Data Scope 1: CPTY1. The new users Party Administrator 5, CPTYUSER6, CPTYUSER7 and CPTYUSER8 have access to data objects under the scope of both CPTY1 and CPTY2.

The data scope can be extended to many counterparties (e.g. CTPY3, CPTY4, CPTY5 in addition) and new data scopes can be created for multiple counterparties, as long as all counterparties within the data scope belong to the same NCB. Data scope extension applies to both U2A and A2A users.

6.2 Counterparties without Network Service Provider

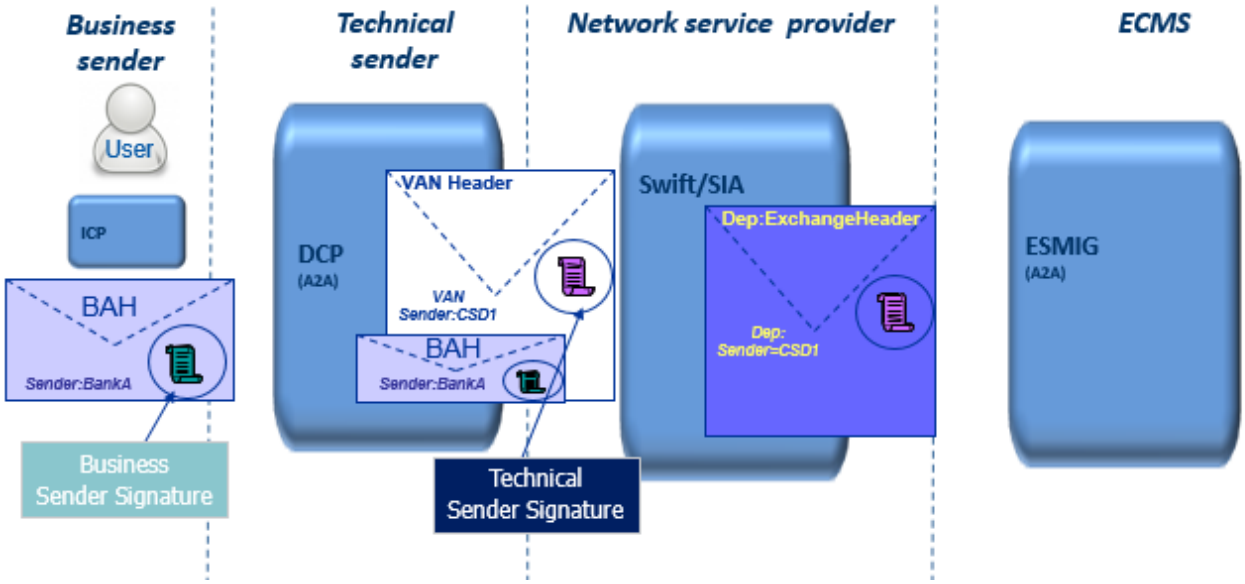
Even if a counterparty has not signed a contract with a Network Service Provider (NSP) and therefore has no connection to the ECMS, the counterparty can still be managed by users from a different counterparty, provided that counterparty is an ECMS party.

The ECMS counterparty without an NSP (CPTY2) can make an agreement with the ECMS party (CPTY1) which allows the users of CPTY1 to act on behalf of CPTY2, in both U2A and A2A mode. This agreement is reflected in the ECMS reference data by extending the data scope of CPTY1 to include the data scope of CPTY2, i.e. Data Scope 1: CPTY1+CPTY2.

6.3 Counterparties with a technical service provider for A2A communication

CTPY1 has access to ESMIG in U2A but does not want to itself use A2A. CPTY1 makes an agreement with a technical service provider that specialises in A2A communication. The technical service provider acts as technical sender and sends messages to the ECMS on behalf of CPTY1. The technical sender needs to be registered in the Closed Group of Users for the ECMS but does not need to be a registered entity in the ECMS reference data. The business payload of the message is signed by the ECMS user of CPTY1 and can be linked to the DN certificate of the technical service provider. The technical address of the technical service provider is configured in CPTY1's reference data to receive messages sent by the ECMS to CTPY1.

Figure 11 – Technical sender check



In A2A, the distinguished name is obtained from the business signature included in the Business Application Header of each message. The technical sender authentication is performed by the network infrastructure of the NSP. This is an

additional security check, only for A2A communications, that takes into account whether a message can be technically sent for a specific party. It does not broaden the scope or the privileges of the sending business user.

For further information please refer to Explainer on authentication and authorisation of instructions in the ECMS.

6.4 Counterparties with a service provider for marketable assets

CTPY1 has access to ESMIG in U2A but does not want to itself use A2A. CPTY1 has an agreement with a service provider A that is specialised in the management of bilateral mobilisations of marketable assets in A2A. The service provider sends the messages to the ECMS on behalf of CPTY1. The party administrator of CPTY1 creates an A2A user for service provider A. and links it to the relevant certificate DN of service provider A. This A2A user is granted with the role Counterparty A2A Marketable Assets, which allows the A2A user dedicated to the service provider A to send sese.023 and sese.020 messages on behalf of CTPY1. CPTY1 subscribes to the related outgoing messages sent by the ECMS (sese.024, sese.025 and sese.027). The technical address of the service provider is configured in the CPTY's reference data for this set of messages. The outgoing messages are routed to the service provider.

The service provider could for example also manage the corporate actions of CPTY1 using the same A2A user of CPTY1 and the same technical address. The A2A user would also need to be granted with the role Counterparty A2A Corporate Actions to allow the user to send seev.004, seev.005, seev.033, seev.040 messages. CPTY1 subscribes to the related outgoing messages sent by the ECMS. The technical address of the service provider is also configured in the CPTY's reference data for this set of messages (responses to the sent messages), as well as for the notifications on CA sent by the CSDs to the ECMS (e.g. seev.031) that are relayed by the ECMS to the service provider's technical address.

6.5 Counterparties with two service providers

CTPY1 has access to ESMIG in U2A, but does not want to itself use A2A. CPTY1 has an agreement with service provider A (which specialises in the management of bilateral mobilisations of marketable assets and corporate actions in A2A), and an agreement with service provider B (which specialises in the management of non-marketable assets). For the configuration of service provider A, please see section 6.4 above. service provider B is configured as follows:

The party administrator of CPTY1 creates an A2A user for service provider B. This A2A user is granted with the role Counterparty A2A Credit Claims, which allows this user to send credit claims files. The technical address of service provider B is configured in the CPTY's reference data for the related outgoing messages sent by the ECMS (the Processing Report file, which contains the responses to the

instructions sent in the credit claim file). The Processing Report file is routed via service provider B.

Service provider A and service provider B can have the same NSP or different NSPs, i.e. technical addresses of both SWIFT and SIA Colt can be configured within CPTY1.

6.6 Counterparties with A2A connection and a service provider

CTPY1 has access to ESMIG in both U2A and A2A mode, but would like to outsource the management of marketable assets and corporate actions. CPTY1 has an agreement with a service provider which specialises in the management of bilateral mobilisations of marketable assets and corporate actions in A2A. All messages related to other business areas (e.g. credit claim files, credit freezing instructions, etc) are managed directly by CPTY1.

The party administrator of CPTY1 creates an A2A user (A2AUser1) for the messages managed directly by CPTY1 and creates another A2A user for the service provider (A2AUser2). User1 is granted with all A2A roles apart from Counterparty A2A Marketable Asset and Counterparty A2A Corporate Actions, which are both granted to A2AUser2. The technical address of CPTY1 is configured for receiving all messages apart from those routed to the technical address of the service provider.

6.7 Same A2A technical service provider for many counterparties

The configuration of a service provider for a counterparty is explained above. If one service provider is used by several counterparties, the same configuration steps are repeated for each counterparty. The party administrator of each counterparty creates a dedicated A2A user for the technical service provider and assigns the corresponding role(s) to the A2A user. The NCB user configures the message subscription and the service provider’s technical address in the counterparty’s reference data. The same technical address can be configured for many counterparties.

The certificate DN of the technical service provider can be linked to each dedicated A2A user on a 1 to 1 basis, meaning that the technical service provider uses one certificate DN for each A2A user (i.e. one certificate DN per counterparty), or the certificate DN of the technical service provider can be linked to many A2A users.(i.e. 1 to n).

6.8 A2A technical service provider for many counterparties within the same data scope

The configuration of a technical service provider for a counterparty is explained above. If several counterparties within the same data scope need to use the same

technical service provider, it is unnecessary to repeat the configuration process for each counterparty.

Instead, the party administrator with access to the extended data scope creates one A2A user for the service provider. The A2A user has access to all the counterparties within the data scope. The party administrator assigns the corresponding role(s) to the A2A user. The NCB user configures the message subscription and the service provider's technical address for each counterparty within the extended data scope.

6.9 Cross NCB scenario

As explained above, it is only possible to extend the data scope for counterparties which belong to the same NCB. It is however still possible for a person or application of a counterparty (CPTY1) belonging to one NCB to manage a counterparty (CPTY2) which belongs to another NCB.

To achieve this, the party administrator of CPTY2 needs to create a separate dedicated user profile in CTPY2 for the user of CPTY1. The same person or application will thus has two separate user profiles for the two different counterparties. If CPTY2 does not have a U2A connection, the configuration of the dedicated user can be carried out by the NCB user on behalf of CPTY2.

The certificate DN of the user of CPTY1 can be linked to the user profile in CPTY2. This means that the person or application with a user profile in both CPTY1 and CPTY2 can use the same digital certificate to connect to both CPTY1 and CPTY2.

7 Configuration of CSDs and TPAs

The configuration of CSDs and TPAs is performed by the ECMS operator.

CSDs and TPAs have their own roles which differ from counterparty roles, which allow them to send messages to the ECMS in A2A mode only. For example, a CSD is authorised to send a sese.031 message (corporate action notification), but cannot send a sese.023 message (marketable asset (de)mobilisation instruction).

If a counterparty has an agreement with a service provider for the management of its marketable assets and this service provider is also a CSD, the counterparty needs to create an A2A user for the CSD and grant the counterparty role(s) to this A2A user. Once the role(s) are granted, the CSD is allowed to send sese.023 messages to the ECMS on behalf of the counterparty.

For more information on CSD and TPA roles please refer to U2A and A2A roles in the ECMS.

8 Annex on message subscription

8.1 Business area: Securities Settlement

For sese.024, the subscription can be made at ECMS Status Level[2]:

Message	Status	Sub-Status
sese.024	Rejected	N/A
	Validated	Waiting Settlement Date
		Waiting Global Collateral
	Matched	N/A
	Cancelled	N/A

With a subscription to the sese.025, the user will receive the only possible status specified in the sese.025 (i.e. Confirmed). Therefore, the status is not configurable (N/A).

Message	Status	Sub-Status
sese.025	N/A	N/A

With a subscription to the sese.027 message, the user will receive all possible statuses (i.e. Rejected, Denied, Accepted, Pending Cancellation, Cancelled). Therefore, the status is not configurable (N/A).

Message	Status	Sub-Status
sese.027	N/A	N/A

[2] Message subscription cannot be made at Sub-Status level.

8.2 Business area: Corporate actions

Some corporate action messages can be subscribed at status level:

Message	Status
seev.034	Cancelled
	Accepted for further processing
	Rejected
	Pending
	Standing Instruction
	Default Action
seev.041	Cancellation Completed
	Accepted
	Rejected

Message	Status[3]	
seev.006	Instruction status	Processing status
		Rejected
		Pending
	Cancellation Status	Processing status
		Rejected
		Pending Cancellation

For other corporate action messages, the subscription is made at message level:

Message			
seev.001	seev.007	seev.032	seev.037
seev.002	seev.008	seev.035	seev.039
seev.003	seev.031	seev.036	Seev.044

[3] The subscription for the seev.006 can be taken out at the Instruction Status level (all or none) and/or the Cancellation Status level (all or none).

8.3 Business area: Cash Management

For Cash Management messages, the subscription can be done at status level:

Message	Status
camt.025	COMP
	REJT
camt.029	CNCL
	RJCR

For Pacs.002, subscription is also made at status level:

Message	Status
pacs.002	ACSC
	RJCT

8.4 Business area: Credit claims

Camt.998_PR (credit claims processing report) is made at message level. Therefore, the status is not configurable (N/A).

Message	Status
camt.998	N/A

8.5 Admi.007

Admi.007 (Receipt Acknowledgement) does not require a subscription. It is sent automatically the sender of the message (technical address of the inbound message).

8.6 Report subscription

Reports can be subscribed to at a predefined frequency, or on an ad-hoc basis.

Counterparties which have been subscribed to ad-hoc reports can request the generation of the ad-hoc reports by sending an admi.005.

The counterparties subscribed to reports at a predefined frequency can also send an admi.005 to ask the ECMS to resend an already generated report.

Message	Subscription				
semt.002	Daily	Monthly	Weekly	Yearly	Ad-Hoc
semt.017	Daily	Monthly	Weekly		Ad-Hoc
semt.018	Daily	Monthly	Weekly	Yearly	Ad-Hoc
colr.016	Daily	Monthly	Weekly	Yearly	Ad-hoc

8.7 Technical Address

For each ECMS business area shown in the table below has a dedicated technical address can be specified. It is also possible for all or some business areas to use the same technical address, e.g. TA1 for cash management and payments, and TA2 for corporate actions.

Business Area	Related messages	CPTY Technical Address
Cash Management	camt.025	Technical address for cash management
	camt.029	
Payment	pacs.002	Technical address for payments
Corporate Actions	All related seev messages	Technical address for corporate actions
Securities Management	For semt messages	Technical address for securities management[4]
Securites Settlement	For sese messages	Technical address for securities settlement
Margin Calls	colr.003	Technical address for margin calls
Credit Claims	CC processing report file (camt.998)	Technical address for credit claims

[4] Statement of holdings for both, marketable and non-marketable assets (semt.002) are communicated using the same technical address.

Counterparties can specify the technical address of the related business area in the internal asset account for the following business areas:

Business Area	Related messages	CPTY Technical Adress
Corporate Actions	All related seev messages	Technical address for corporate actions
Securities Management	For semt messages	Technical address for securities management
Securites Settlement	For sese messages	Technical address for securities settlement

In case the technical address is not specified at internal asset account level, the ECMS will search for the technical address of the related business area at Counterparty Level (same business areas as specified in the previous table).

8.8 No message subscription for CSDs and TPAs

CSDs and TPAs do not need to subscribe to any messages. The ECMS will send any messages intended for TPAs and CSDs.