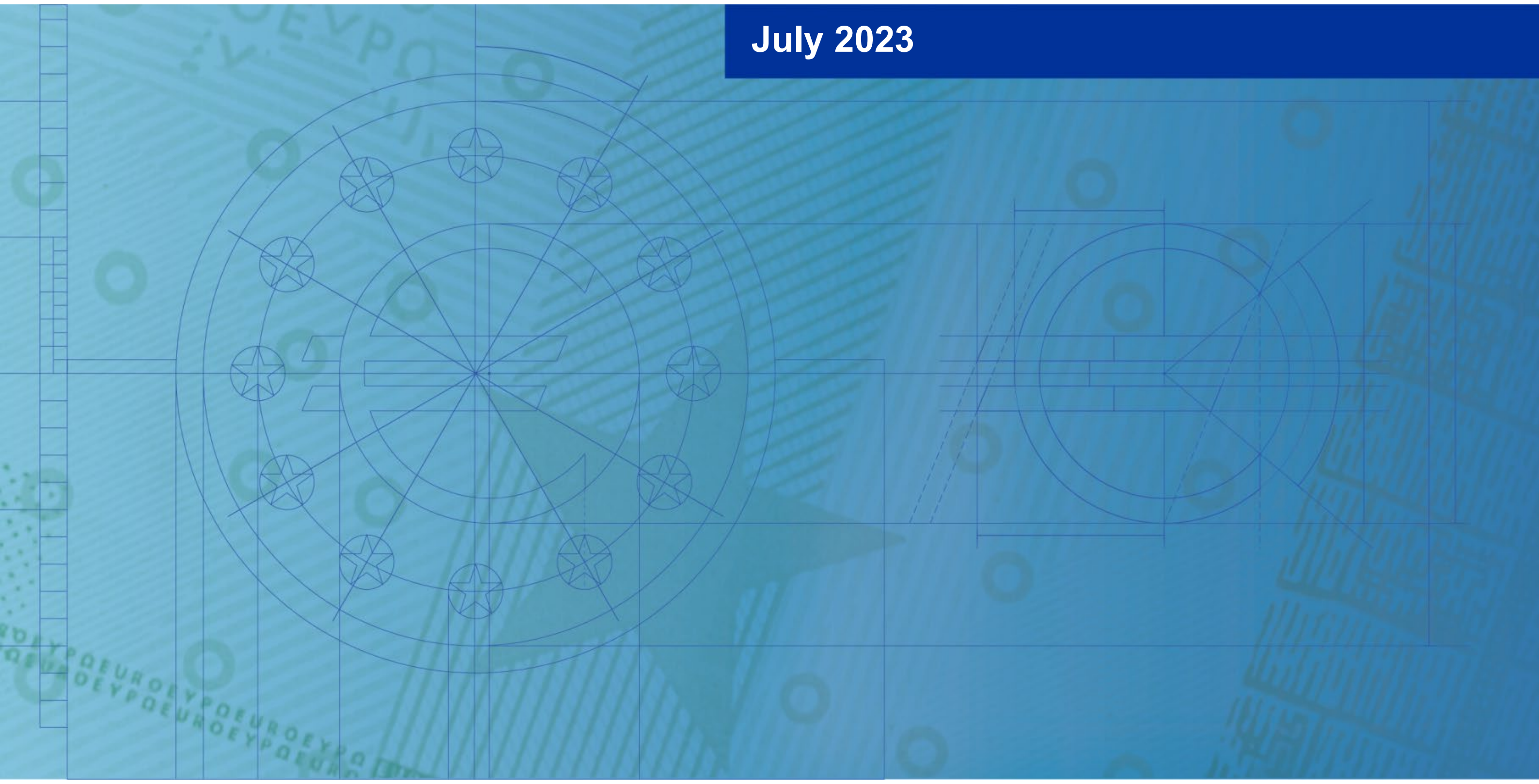
EUROPEAN CENTRAL BANK
EUROSYSTEM

U2A and A2A roles in the ECMS



July 2023

Introduction

Users belonging to counterparties, Central Securities Depositories (CSDs) and Triparty Agents (TPAs) interact with the ECMS (and all TARGET services) via the Eurosystem Single Market Infrastructure Gateway (ESMIG). These counterparties, CSDs and TPAs are defined in the ECMS as parties belonging to an NCB.

ESMIG is network-provider agnostic (i.e. it is not reliant on network-specific features) and therefore allows participants to connect to all TARGET Services, including the ECMS, in Application-to-Application (A2A) mode and/or User-to-Application (U2A) mode via a single certified network service provider of their choice.

ESMIG provides central authentication, authorisation and user management features to protect the connected systems/platforms against intrusion and unauthorised access. It ensures that only trusted parties transmit inbound communication via a secure channel.

A2A communication with the ECMS is based on ISO 20022 compliant messages. The ECMS offers functionality for message subscription, with each NCB responsible for configuring message subscriptions for its community.

A graphical user interface allows accessing to the ECMS via a desktop/laptop in U2A mode. Individual users can log on to the ECMS with the same sign-on used for any of the TARGET Services and common components and a single certificate.

ESMIG authenticates users, checks that they are authorised to address or use the ECMS, and manages access rights. The allocation of users to predefined roles is managed within the ECMS. Users are allowed to perform business functions based on their assigned roles and depending on their data scope.

Each individual user is assigned one or more predefined roles by the party administrator in each party. A role consists of a set of privileges that determine what functionality the user has access to within the ECMS. Each privilege relates to a business function that the user can perform in either “read-only” or “take action” mode. In U2A mode, the ECMS may be configured to require four-eye verification.

Counterparties can fully manage their pool in U2A mode only, and do not need an A2A connection.

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

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. The first party administrator needs to be configured by the party responsible for the party (i.e. the NCB should configure this first party administrator for a counterparty). 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.

U2A roles

The predefined U2A roles may be created in two variants: read-only and execution. The execution variant allows the user to manage a business need, e.g. create instructions and/or by make changes in the database, while the read-only variant allows the user to monitor their business activities.

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;

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 role applies.

The following U2A roles can be granted to ECMS Actors.

Role	Overview	Variant
ECMS Entity U2A Administrator	The role allows the user constellation configuration and the counterparty security management in regards of roles related with the own counterparty data scope. With this role the user is able, for example, to create/delete users, groups, to assign/remove a set of roles to users and groups, etc.	Execution Read Only
ECMS Entity U2A General Reference Data	The role allows the access to all relevant reference data constellation for the counterparty data scope. With this role the user is able, for example, to see its asset accounts, settlement possibilities, etc.	Read Only
ECMS Entity U2A Triparty Reference Data	The role allows the access to all relevant triparty reference data constellation for the counterparty. With this role the user is able, for example, to see the triparty transaction details.	Read Only
ECMS Entity U2A Pool Reference Data	The role allows access to all relevant reference data information related to the pool configuration under the counterparty data scope.. With this role the user is able, for example, to see the pool configuration details.	Read Only
ECMS Entity U2A Marketable Asset (De)Mobilisation	The role allows the management and monitoring of marketable assets (de)mobilisations under the counterparty data scope.	Execution Read Only
ECMS Entity U2A Cash Collateral	The role allows the management or monitoring of the cash collateral related processes in the ECMS.	Execution Read Only
ECMS Entity U2A Externally Managed collateral	The role allows the monitoring of the externally managed collateral.	Read Only
ECMS Entity U2A Open Market Operations	The role allows the monitoring of open market operations.	Read Only

Role	Overview	Variant
ECMS Entity U2A Standing Facilities	The role allows the management or monitoring of the marginal lending on request and automatic marginal lending functionalities.	Execution Read Only
ECMS Entity U2A Credit Freezing	The role allows the management or monitoring of the credit freezing functionalities.	Execution Read Only
ECMS Entity U2A Credit Line	The role allows the management of the maximum credit line functionality, and the monitoring of the credit line covered by an ECMS pool. With this role the user is able, for example, to monitor the maximum credit line.	Execution Read Only
ECMS Entity U2A Pool Position	The role allows the counterparty pool monitoring. The user is able to see the pool overview, pool valuation and pool position.	Execution Read Only
ECMS Entity U2A ELA Management	The role allows the monitoring of ELA operations.	Read Only
ECMS Entity U2A Banking Group Manager Processes	The role allows the monitoring of the banking group pool details.	Read Only
ECMS Entity U2A Credit Claim Management	This role allows the management or monitoring of credit claims.	Execution Read Only
ECMS Entity U2A Corporate Actions and Tax Management	The role allows the management and monitoring of corporate actions and taxes related processes.	Execution Read Only
ECMS Entity U2A Statements	The role allows the generation and downloading of U2A statements, as well as the downloading of the pre-generated A2A statements in xml format.	Execution Read Only

A2A roles

In A2A, 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 Entities are also created and maintained by the ECMS Operator.

The following A2A roles can be granted to CSDs, TPAs or Counterparties.

Role	Overview	Relevant message(s)
CSD A2A	The role allows the central securities depository participating in the ECMS and used as custodian or depository only by an NCB and counterparties to send messages related to securities events.	camt.077, seev.001, seev.002, seev.003, seev.006, seev.007, seev.008, seev.031, seev.032, seev.034, seev.035, seev.036, seev.037, seev.039, seev.041, seev.042, seev.044
TPA A2A	The role allows the eligible triparty agent to send messages related to the provision of triparty collateral management services.	camt.077, colr.020, colr.021, colr.022, colr.024, seev.001, seev.002, seev.003, seev.006, seev.007, seev.008, seev.031, seev.032, seev.034, seev.035, seev.036, seev.037, seev.039, seev.041, seev.042, seev.044, reda.028
ECMS Entity A2A Credit Freezing	The role allows the counterparty A2A user to send messages to execute credit freezing functionalities.	camt.998 Credit Freezing
ECMS Entity A2A Marketable Assets	The role allows the counterparty A2A user to send messages to execute marketable assets functionalities.	sese.023, sese.020
ECMS Entity A2A Credit Claims	The role allows the counterparty A2A user to send messages to execute credit claims functionalities.	camt.998 Credit Claims
ECMS Entity A2A Marginal Lending	The role allows the counterparty A2A user to send messages to execute marginal lending on request functionalities.	camt.056, pacs.009 for Marginal Lending
ECMS Entity A2A Corporate Actions	The role allows the counterparty A2A user to send messages to execute corporate actions functionalities.	seev.004, seev.005, seev.033, seev.040
ECMS Entity A2A Cash Collateral and Maximum Credit Line	The role allows the counterparty A2A user to send messages to execute cash collateral and maximum credit line functionalities.	pacs.009 and pacs.010 for cash collateral, camt.011.
ECMS Entity A2A Reporting	The role allows the counterparty A2A user to send messages to execute reporting functionalities.	admi.005