



FASS

FASS – External User Guide

External User Guide

Unicorn © 2026 – Unicorn Grid Systems a.s.
Jankovcova 1037/49, CZ – 170 00 Prague 7

Project: FASS
Project – Subject: FASS – External User Guide
Document Title: External User Guide

Author: Lukáš Žák, Jan Froněk, Miroslava Langová,
Martin Rohla, Pavel Bory, Ondřej Štverák

Contact: E-mail: info@unicorn.com
Tel.: (+420) 221 400 111



1. Content

1. Content.....	3
2. Revision History.....	8
3. Document Roadmap.....	9
4. Objective and Scope	10
4.1 Early release of information	10
4.1.1 Key to Figures:.....	10
4.1.2 Signposting of changes.....	10
5. Terms and Definitions.....	11
6. FASS Platform Overview	13
6.1 Platform & Process Overview	13
6.1.1 FASS Functional Modules.....	14
6.1.2 Registration and Qualification	14
6.1.3 DASSA Procurement	14
6.1.4 Secondary and Bilateral Trading	14
6.1.5 Lapsing	14
6.1.6 Residual Availability Determination (RAD)	15
6.2 Service Provider Interactions.....	15
6.2.1 Web-Based Graphical User Interface (GUI).....	15
6.2.2 Application Programming Interface (API).....	16
7. Generic Features and System Requirements	18
7.1 General System Requirements.....	18
7.1.1 Browser and Device Support	18
7.1.2 Other requirements	18
7.2 Security Considerations.....	18
7.3 Generic Features.....	19
7.3.1 Filtering Behaviour	19
7.3.2 Sorting Behaviour.....	19
7.3.3 On-screen reporting (Excel export)	20
7.3.4 Time Zone and daylight-saving time	20
7.3.5 Quantity and Prices Format	21
7.3.6 Landing Page.....	22
7.3.7 Menu navigation.....	22
7.3.8 Notifications	22
7.3.9 Manual File Upload	23
8. User Account Management	25
8.1 Service Provider User Roles.....	26
8.2 Registration	26
8.2.1 Party Authorised User Registration	27
8.2.2 User Registration by Party Authorised User.....	27
8.2.3 User Management by Party Authorised User.....	27
8.3 Log-in and Log-out	27
8.3.1 First login procedure	28

8.3.2	Forgotten Password	29
8.3.3	Password Policy	29
8.3.4	Multi-Factor Authentication	30
8.3.4.1	Remove MFA	32
8.3.4.2	Renew MFA	35
8.3.5	User Account Lifecycle (non-Machine Users)	36
9.	Step-By-Step Guides	38
9.1	Registration and Qualification	38
9.1.1	Introduction	38
9.1.1.1	Purpose of this guide	38
9.1.1.2	Who can use the Registration and Qualification module	38
9.1.2	Getting Started	39
9.1.2.1	Accessing the Registration and Qualification module	39
9.1.2.2	Role permissions summary	39
9.1.2.3	Key concepts and terminology	39
9.1.3	The Registration and Qualification Process — Service Provider View	40
9.1.3.1	End-to-end timeline	40
9.1.3.2	Registration and application business states	40
9.1.3.3	Notifications you receive	41
9.1.3.4	List and detail screens	41
9.1.4	Request for Information	41
9.1.5	Managing Attachments (File Manager)	43
9.1.6	Party Authorised User Registration	43
9.1.7	User Creation by PAU	44
9.1.8	Party Registration	45
9.1.8.1	Party Registration process — Service Provider view	45
9.1.8.2	Submitting Party Registration	47
	Form Step 1: Contact Details	47
	Form Step 2: Financial and Economic Capacity Declaration	48
	Option 1: Tax Clearance Certificate	48
	Option 2: e-Tax Clearance	49
	Option 3: e-Tax Clearance Application	50
	Option 4: Non-Irish Firm	51
	Form Step 3: Insurance	52
	Form Step 4: Health & Safety, Environment, and Employment	53
	Form Step 5: System Services Code	54
	Form Action Buttons	54
9.1.9	Unit Registration	55
9.1.9.1	Unit Registration process — Service Provider view	57
9.1.9.2	Submitting Unit Registration	57
9.1.10	Qualification Application	58
9.1.10.1	Qualification Application process — Service Provider view	58
9.1.10.2	Submitting Qualification Application	60
	Form Qualification Application	60
	Section 1 - General Party and Unit Information	61
	Section 2 - Technology Type Details	61
	Section 3 - Operating Mode Details	61
	Section 4 - Eligible Capacity per System Service Product	61
	Form Step 2: Reserve Characteristics Parameters (per Technology Type, and if applicable Operating Mode)	62
	Form Step 3: Qualification Pack	63
	Form Action Buttons	63

9.2 DASSA Procurement.....	64
9.2.1 Introduction	64
9.2.1.1 Purpose of this guide	64
9.2.1.2 Key concepts and terminology.....	64
9.2.1.3 Who can use the DASSA module	65
9.2.1.4 Prerequisites for participation	65
9.2.2 Getting Started.....	65
9.2.2.1 Accessing the DASSA module	65
9.2.2.2 Role permissions summary	65
9.2.3 The DASSA Process — Service Provider View	66
9.2.3.1 End-to-end timeline (Happy Day Scenario)	66
9.2.3.2 DASSA auction business states	66
9.2.3.3 Timing and gates	66
9.2.3.4 Notifications you receive.....	67
9.2.4 Viewing DASSA Auctions.....	67
9.2.4.1 Opening the DASSA Auctions list.....	67
9.2.4.2 Viewing auction detail	68
9.2.4.3 Navigating to related screens	68
9.2.4.4 Understanding the Auction Information Pack.....	68
9.2.5 Submitting DASSA Offers	69
9.2.5.1 Overview.....	69
9.2.5.2 Viewing DASSA offers	69
9.2.5.3 Entering offers via the GUI	70
9.2.5.4 Copy Previous offers	71
9.2.5.5 Submitting offers via file upload.....	72
9.2.5.6 Submitting offers via API	72
9.2.5.7 Validation rules and common errors	72
9.2.6 Submitting Forecast Capability.....	73
9.2.6.1 Overview.....	73
9.2.6.2 Viewing forecast capability	74
9.2.6.3 Entering forecast capability via the screen	74
9.2.6.4 Submitting forecast capability via file upload	75
9.2.6.5 Submitting forecast capability via API.....	75
9.2.6.6 Validation rules and common errors	75
9.2.7 Viewing DASSA Results	76
9.2.7.1 When results are available	76
9.2.7.2 Viewing public results in the GUI	76
9.2.7.3 Retrieving public results via API	77
9.2.7.4 Retrieving private (party-specific) results via API	77
9.2.8 Viewing DASSA Orders	77
9.2.8.1 Overview.....	77
9.2.8.2 Viewing the DASSA Orders list.....	77
9.2.8.3 Viewing order detail	79
9.2.8.4 Retrieving DASSA Orders via API	79
9.2.9 Special Situations and Impacts on Service Providers	79
9.2.9.1 Auction cancellation.....	79
9.2.9.2 DASSA fallback (auction state Failed).....	79
9.2.9.3 Suspended Party or Unit.....	80
9.2.9.4 Concurrent editing in the GUI	80
9.2.10 Reference.....	80
9.2.10.1 Screen quick-reference.....	80
9.3 Secondary Trading	81
9.4 Lapsing.....	81

9.5	Residual Availability Determination (RAD)	81
10.	API Guide	82
10.1	API Overview	82
10.2	Reliability And Operations	83
10.2.1	API Versioning	83
10.2.2	Deprecation Policy	83
10.2.3	Rate Limit	83
10.2.4	Idempotency	83
10.2.5	Availability	83
10.2.6	Retry Behaviour	83
10.2.7	IP Whitelisting	83
10.2.8	Response Timeout	83
10.2.9	Trouble Shooting Logs	83
10.2.10	Pagination	83
10.3	Architecture and Vocabulary	84
10.3.1	HTTP Request Methods	84
10.3.2	HTTP Request Headers	84
10.3.3	HTTP Response Headers	85
10.3.4	HTTP Status	85
10.3.5	Common Method Properties	86
10.3.5.1	Request Body	86
10.3.5.2	Response body	86
10.4	Machine User Management	86
10.5	Authentication and Authorisation	87
10.5.1	API Key	87
10.5.2	Client Credential Flow	87
10.5.3	oidc/grantToken Request Description	87
10.5.3.1	Basic information	87
10.5.3.2	HTTP request headers	88
10.5.3.3	Request body example	88
10.5.3.4	Request body object description	88
10.5.4	oidc/grantToken Response Description	88
10.5.4.1	Response body example	88
10.5.4.2	Response body object description	88
10.6	API Endpoints	89
10.6.1	DASSA Offers	90
10.6.1.1	Introduction	90
10.6.1.2	Submission Rules	90
10.6.1.3	Example	91
10.6.2	Forecast Capability	91
10.6.2.1	Introduction	91
10.6.2.2	Submission Rules	91
10.6.2.3	Example	92
10.6.3	DASSA Auction Information Pack (to Service Provider)	92
10.6.3.1	Introduction	92
10.6.3.2	Response Description	93
10.6.3.3	Example	93
10.6.4	Publish DASSA Results - Private (to Service Provider)	93
10.6.4.1	Introduction	93

10.6.4.2	Response Description.....	94
10.6.4.3	Example.....	94
10.6.5	Publish DASSA Results - Public (to Service Provider).....	94
10.6.5.1	Introduction.....	94
10.6.5.2	Response Description.....	95
10.6.5.3	Example.....	95

2. Revision History

Version	Date	Author	Description
TLG v1 (v0.7.2)	26.08.2026	Unicorn and EirGrid	First version for sharing via the TLG

3. Document Roadmap

Version	Date*	Description
TLG v1 (v0.7.2)	Complete by end August	Chapters 3 to 8, and 10.1 to 10.5 Available parts of Chapter 9 9.1 Registration and Qualification, 9.2 DASSA Procurement Available parts of section 10.6 10.6.1 to 10.6.5 API Endpoints for DASSA Procurement ZIP file with Open API description and example JSON
TLG v2 (v0.8)	Complete by end October	7.3.8 Notifications – further details on notifications re: manual file upload 8.2.3 User Management by Party Authorised User – more detailed information on functionality and figures to be added 8 User management updates (open issues, if needed) 9.1.5 Managing Attachments (File Manager) 9.2.8.4 Retrieving DASSA Orders via the API 9.3 Secondary and Bilateral Trading 10.3.1 HTTP Request Methods (consideration of PATCH) 10.4 Machine User Management (open issue, lifecycle management) 10.5.n API endpoint details for Secondary and Bilateral Trading – overview, Open-API description and example JSON (including ZIP file updates)
TLG v3 (v0.9)	Complete by end November	7, 8, 9.1, 9.2 Updated screenshots from test system 9.4 Lapsing 10.5.n API endpoint details for Lapsing – overview, OpenAPI description and example JSON (including ZIP file updates)
TLG v4 (v0.10)	Complete by end January	9.3 Updated screenshots from test system 9.5 RAD 10.2.9 Trouble Shooting Logs 10.5.n API endpoint details for RAD – overview, OpenAPI description and example JSON (including ZIP file updates)
	Timeline to be confirmed	9.4, 9.5 Updated screenshots from test system Move from ZIP file with Open API description and example JSON to availability from website Include email addresses, URLs, and confirm parameters New name for FASS Platform

* Please note that these Dates are indicative only and might change based on internal design dependencies.

4. Objective and Scope

The User Guide is a document created for Users of the FASS platform to help with navigation in the system, its usage and to provide step-by-step guides on how to achieve important use cases available in the system.

This User Guide consists of main parts:

- **Terms and Definitions**
Introduces and explains terms and definition used in this document.
- **Generic Features and System Requirements**
Specifies technical requirements for using the system and describes general principles which are applied within the system.
- **User Account Management**
Describes User and Party Management, User Registration and log in/out procedures.
- **Step-by-Step guides**
A "cookbook" describing individual use cases.
- **API Guide**
Documentation on API integration using HTTP/REST and OpenAPI.

4.1 Early release of information

This User Guide is developed on an iterative basis. Information is initially provided after detailed design which has yet to be validated through testing phases. Details are subject to change and updates will be applied during the project development as necessary. Where possible, details that are subjected to change are highlighted as below.

4.1.1 Key to Figures:

-  Mock-up with indicative look and feel
-  Screenshot from the test system
-  Screenshot for the system after vendor testing

4.1.2 Signposting of changes

Details in blue background indicate where more detail will be provided as the User Guide is developed.

For example, email address(es) to be used for communications from the FASS Platform.

5. Terms and Definitions

Term	Abbreviation	Description
Day-ahead System Service Auction	DASSA	Type of system services auction held for day-ahead timescale to select providers of system services.
Future Arrangements for System Services	FASS	FASS Programme is a framework developed by EirGrid for the procurement of system services.
FASS Platform	SSP or SSMP	A system/platform implemented to manage the registrations and qualifications and carry out the actual DASSA auctions. The platform may include other auction types in the future. A different name will apply to the FASS Platform before testing/go-live – this reflects the fact that FASS is the Programme to deliver the future arrangements. In short-form (for API interactions) it is referred to as SSP or SSMP, which is consistent with the System Services Code references to System Services Market Platform.
Generic Features	–	General Functionality covers the system functionalities, such as GUI, notifications and further features related to the whole system.
Registration and Qualification	–	Registration and Qualification covers the process by which capabilities required for Service Providers to participate in the System Services Markets are verified, and by which Service Providers are registered as participants by the TSOs.
DASSA Procurement	–	DASSA Procurement covers the capabilities required to run the daily DASSA arrangements auctions, provide the Auction Information Pack, receive/validate Service Provider offers, auction clearing and publication of results and reporting.
Secondary and Bilateral Trading	–	Secondary and Bilateral Trading covers the capability to Secondary Trade and/or execute Bilateral Trades via a central trading platform. This will cover assessing eligibility to trade, the submission and validation of trade offers, Order Book management, trade matching via a periodic batch matching process (secondary) and instant matching (bilateral), storing trades, amendment of Service Provider obligations where applicable, and ensuring resulting trade positions are available to Settlement processes.
Lapsing	–	Self-Lapsing Notification covers the capability for Service Providers to Self-Lapse when they are aware they will not be able to fulfil their commitment obligation. The Service Provider can (optionally) Self-Lapse by Gate Closure. TSO Lapsing covers the capability for the TSO to conduct ex-post analysis of the DASSA Orders and real-time availability to determine if any orders have failed to meet their DASSA obligation.
Residual Availability Determination	RAD	Residual Availability Determination (RAD) focuses on identifying any additional System Services volumes necessary to meet system requirements (compared with what is supplied or paid for through confirmed DASSA orders) via calculation of the residual availability volume requirement, execution of RAD Auction, and the creation of RAD Orders.

Party Authorised User	PAU	The first User of a given Party requests a new User account and submits basic information necessary for the registration of a new Party. Once the account request is approved by the TSO Administrator, the Party is automatically created together with the User account. The Party is assigned to the User who is granted the access rights of Service Provider Approver and Party Authorised User role. Party Authorised User role enables the User to create other User accounts for the relating Party directly in the system.
------------------------------	-----	---

6. FASS Platform Overview

6.1 Platform & Process Overview

The FASS Platform supports the Future Arrangements for System Services (FASS) market arrangements, including the procurement of upward and downward system service products. It provides a secure and centralised platform through which Service Providers can register and qualify units, participate in system services procurement processes, manage ongoing obligations and view relevant market information.

The FASS Platform hosts the Day-Ahead System Services Auctions (DASSA), through which Service Providers submit offers for System Services and receive auction outcomes on a daily basis. It also facilitates the exchange of information between Service Providers, the System Operators (TSOs & DSOs) and associated downstream systems including settlement and publications.

The platform supports the full participant lifecycle through five core functional modules:

- Registration and Qualification
- DASSA Procurement
- Secondary and Bilateral Trading
- Lapsing
- Residual Availability Determination (RAD)

Service Providers may interact with the platform through a web-based graphical user interface (GUI) and, where available, through system-to-system integration using the FASS Application Programming Interface (API). The appropriate interaction method will depend on the activity being undertaken and the participant's operational requirements.

This chapter provides a high-level overview of the FASS Platform, its key functional areas and the ways in which Service Providers can interact with the system. Detailed instructions for each process are provided in the subsequent chapters of this User Guide.

Figure 1 provides a high-level overview of the principal processes supported by the FASS Platform. It shows how participant registration and qualification support entry into the market and the provision of procured services, how DASSA requirements and offers are brought together to produce auction outcomes, and how the platform supports subsequent activities including Secondary and Bilateral Trading, Lapsing and Residual Availability Determination (RAD).

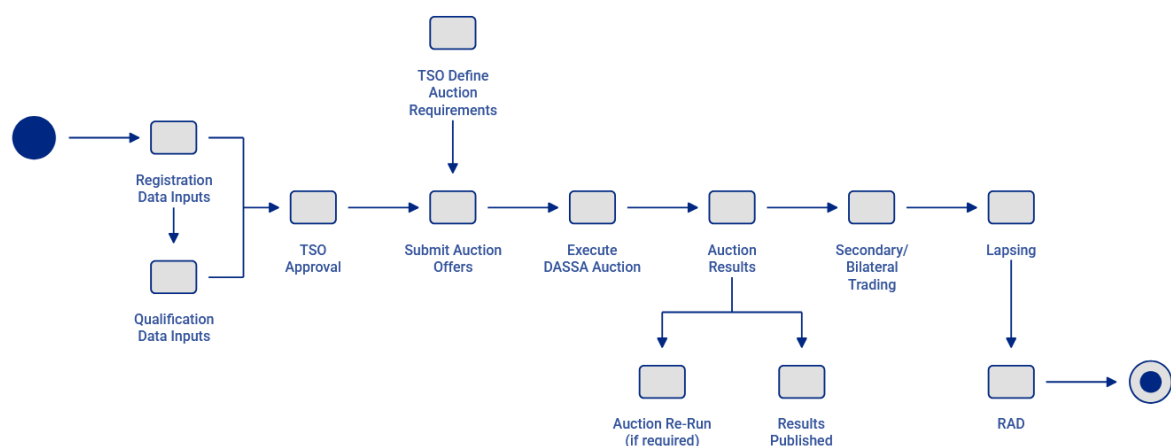


Figure 1 - Overview of FASS Platform Processes

Note, the figure above is intended to illustrate the relationship between the main FASS processes. It does not indicate that every process occurs as part of a single sequential workflow or that every Service Provider will undertake each activity on every Trading Day.

6.1.1 FASS Functional Modules

The FASS Platform supports the full participant lifecycle through five core functional modules, as set out in sections 6.1.2 to 6.1.6. Together, these modules enable Service Providers to register and qualify for participation, participate in the Day-Ahead System Services Auction (DASSA), manage post-auction positions and fulfil ongoing obligations. While these modules are closely related and interdependent, they represent distinct business processes and may be used at different stages of a participant's engagement with the FASS Platform.

6.1.2 Registration and Qualification

The Registration and Qualification module supports the onboarding of Service Providers and their units to the FASS arrangements. It enables the registration of a Party, the creation and management of units, and the submission of the information required to demonstrate eligibility to provide System Services. Registration and qualification applications are reviewed by the TSOs before the relevant Party or unit is approved to participate in applicable FASS processes.

6.1.3 DASSA Procurement

The DASSA Procurement module supports the daily procurement of System Services through the Day-Ahead System Services Auction (DASSA). The TSOs define the auction requirements, including the required volumes for each applicable combination of System Service Product, Zone, Quality Category and Trading Period¹. Eligible Service Providers may submit offers for System Service Product for which a Unit is qualified during the applicable auction gate window.

Following the submission of offers by Service Providers, the FASS Platform evaluates and executes the auction, determining the auction outcomes for each Trading Period. Once approved, the resulting auction outcomes are published and made available to subsequent FASS processes.

The principal output of the DASSA process is a set of Confirmed DASSA Orders, which establish the successful service volumes and associated obligations for participating Service Providers by Unit, System Service Product, Zone, Quality Category and Trading Period.

6.1.4 Secondary and Bilateral Trading

The Secondary and Bilateral Trading module enables Service Providers to manage DASSA obligations after the auction. Through Secondary Trading, Service Providers can submit Buy or Sell Orders, which are periodically matched in batches; Bilateral Trades agreed outside the FASS Platform can also be reported and are generally matched once both counterparties have submitted the trade. All trades are subject to business and technical validations. The Order Book records trade orders and their status, with Service Providers able to view an anonymised Active Order Book as well as their own orders through the private My Orders view. Successfully matched trades result in the relevant DASSA obligations being updated.

6.1.5 Lapsing

The Lapsing module supports the management of circumstances in which a Service Provider is unable to fulfil a System Services obligation. It facilitates the submission of Self-Lapsing notifications by Service Providers and supports the associated TSO processes used to assess and manage delivery obligations under the FASS arrangements.

¹ DASSA requirements, offers and results are defined using a combination of these market parameters. For example, a requirement or auction outcome may relate to *POR Up, Zone NI, Quality Category 1 (Dynamic)* and a specific half-hour Trading Period. Together, these parameters provide the level of detail required to define auction requirements, participant offers and resulting obligations.

6.1.6 Residual Availability Determination (RAD)

The Residual Availability Determination (RAD) module supports the identification and procurement of additional System Services volumes where system requirements are not fully satisfied through confirmed DASSA positions. The system facilitates the submission of offers by Service Providers and the processes determine the residual requirement and RAD orders required to maintain system security and operational needs.

6.2 Service Provider Interactions

Service Providers can interact with the FASS Platform through either the web-based graphical user interface (GUI) or, for supported activities, through system-to-system integration using the FASS Application Programming Interface (API). The web-based user interface is intended for individual users accessing FASS through a supported browser (refer to section 7.1.1 Browser and Device Support). The API enables a Service Provider's information system to exchange supported data directly with the FASS Platform through an API client.

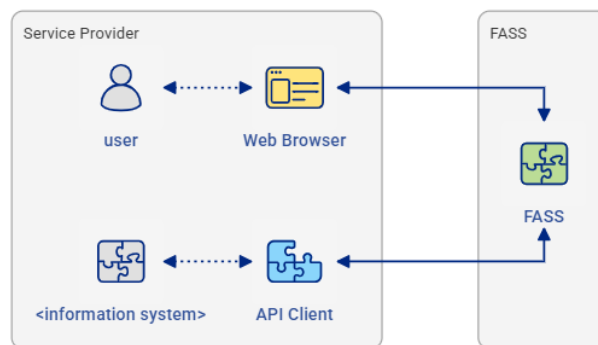


Figure 2 - Service Provider Interactions

6.2.1 Web-Based Graphical User Interface (GUI)

The web-based graphical user interface provides authorised users with access to the principal participant-facing functions of the FASS Platform. Via the user interface, Service Providers can complete registration and qualification activities, submit DASSA offers, access auction results, participate in Secondary Trading activities, submit lapsing notifications and access RAD-related functionality where applicable.

Figure 3 highlights the principal FASS activities that are supported through the web-based graphical user interface.

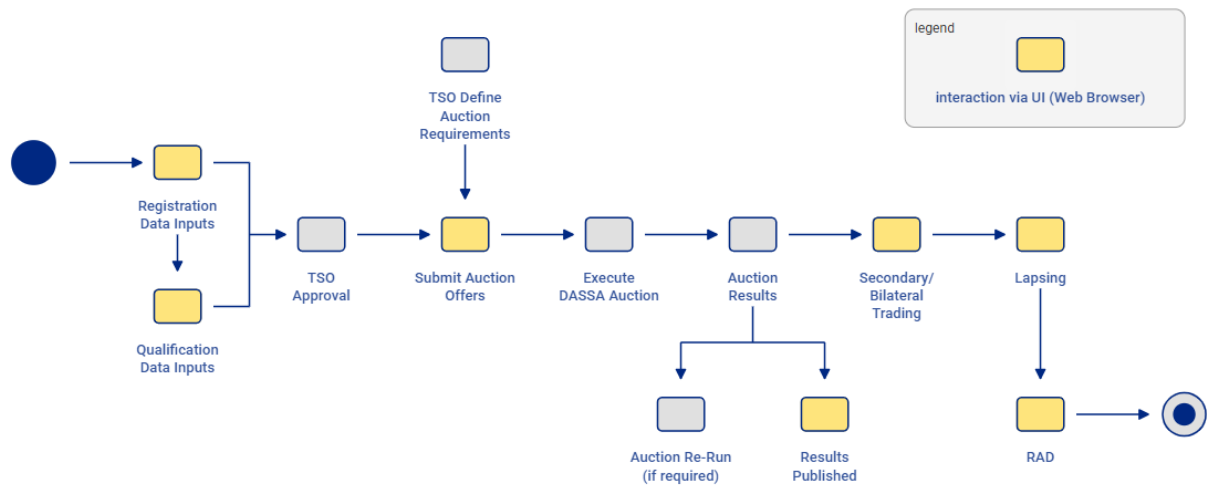


Figure 3 - Service Provider GUI interactions mapped to the process overview

6.2.2 Application Programming Interface (API)

The FASS API provides system-to-system interaction between a Service Provider's information systems and the FASS Platform. This enables supported data exchanges to be completed automatically without requiring manual interaction through the user interface.

API functionality is primarily intended for operational activities following registration and qualification. Registration and qualification activities are completed through the web-based user interface while day-to-day trading activities can use either the GUI or API.

Figure 4 highlights the principal FASS activities for which API interaction is supported.

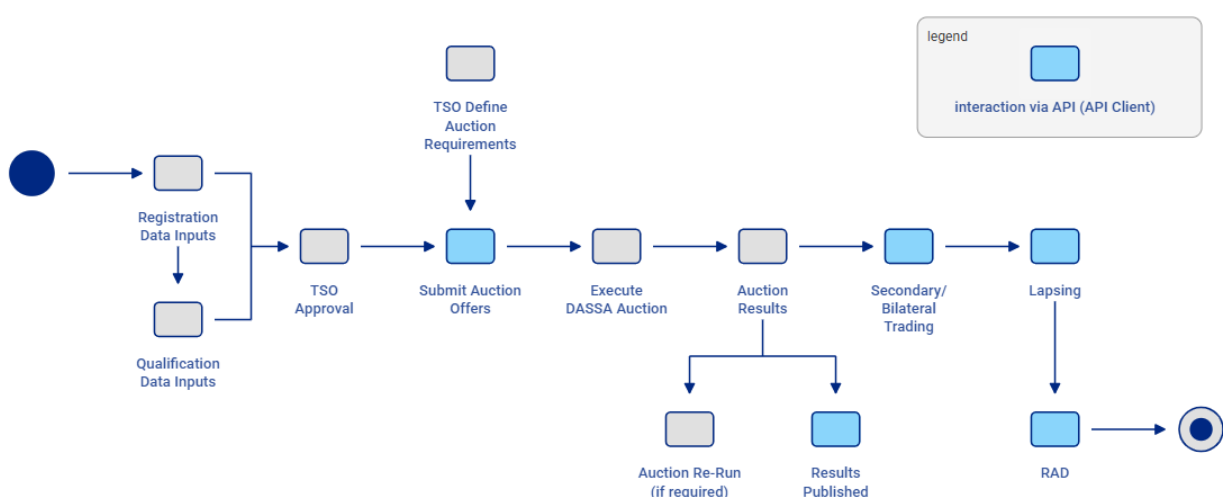


Figure 4 - Service Provider API interactions mapped to the process overview

The following chapters provide more detailed information on specific aspects of the FASS Platform. Chapter 7 describes the general system requirements and common platform functionality. Chapter 8 explains user account management, roles and access permissions. Detailed operational guidance for Registration and Qualification, DASSA Procurement, Secondary Trading, Lapsing and RAD processes is provided in Chapter 9, while Chapter 10 describes the available API functionality and integration requirements.

7. Generic Features and System Requirements

7.1 General System Requirements

7.1.1 Browser and Device Support

The supported browsers are:

Browser	Supported Versions
Chrome	latest 3 major versions
Chrome for Android	latest 3 major versions
Firefox	latest 3 major versions
Firefox for Android	latest 3 major versions
Microsoft Edge	latest 3 major versions
Opera	latest 3 major versions
Safari	latest 2 major versions
Safari for iOS	latest 2 major versions
Samsung Internet Browser	latest 2 major versions

In the browser, JavaScript must be enabled for the platform functionality to work correctly.

Some browser extensions may interact with the application and cause unexpected behaviour. Such extensions should be uninstalled or at least disabled.

The user interface in browser works on both desktops and mobile devices. It is designed to adapt to the display size and orientation. However, usage of some user interface elements, like tables, may be inconvenient on small displays.

7.1.2 Other requirements

The application requires stable internet connection.

- User interface runs in browser and uses HTTPS protocol on port 443.
- API is accessible via HTTPS protocol on port 443.7
- Email notifications from the platform are used to support registration and qualification processes, especially interaction notifications regarding 'Request for Information', and user management interactions
- **Details to be provided on the email address(es) that will be used for communication from the FASS Platform.**

Please note that internet filtering services may prevent the system from functioning properly.

7.2 Security Considerations

Both the GUI and API utilise the HTTPS protocol. That means that data is encrypted during transport.

Security sensitive data, like passwords, secrets, access keys etc. are hashed before they are stored. Hashing is a one-way encryption, the data cannot be decrypted, not even by the system.

Users, when accessing the system via the GUI, are required to authenticate. Multi-factor authentication is required. Access to the individual use cases must be authorised through appropriate user role assignments.

API Clients use API Key and OAuth 2.0 Client Credentials Flow for authentication and authorization.

7.3 Generic Features

7.3.1 Filtering Behaviour

Filters help users narrow down the data displayed on screen. Each filter field includes a small clear button, allowing the user to remove a selection at any time. Each filter bar includes also a button for opening filter options in a modal window.

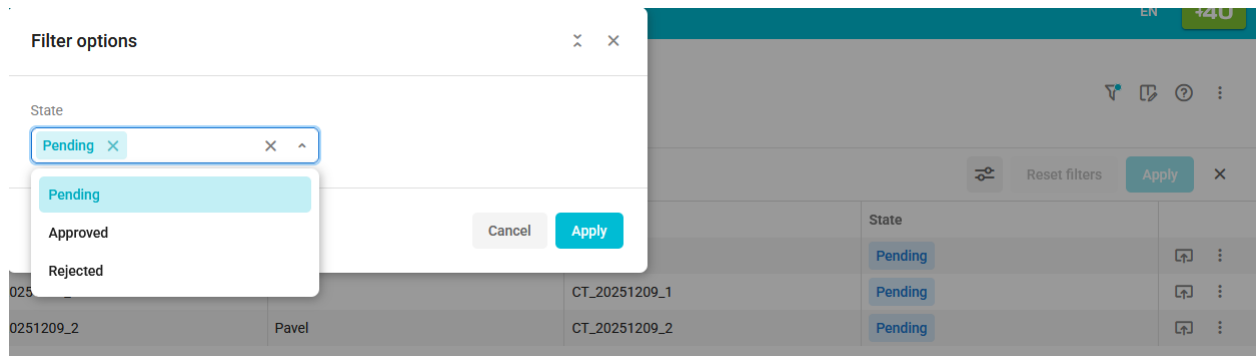


Figure 5 - Opening filters in a modal window

Party Authorised User Registrations

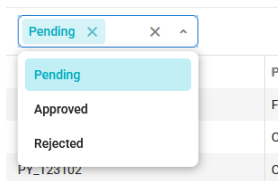


Figure 6 - Using filter bar

If a filter field has only one available option, the system will automatically select it for the user. In this case, the field becomes temporarily disabled (but remains visible) until more options become available. When new options appear, the field is cleared again so the user can make a new choice.

If a user selects a filter that later becomes incompatible with another choice, the system will automatically remove the invalid selection and display a warning message explaining what happened.

Users do not need to manually confirm their filter choices. As soon as all mandatory fields are filled in, the system automatically updates the data. Every change to a filter refreshes the results immediately.

Mandatory filters are marked with an asterisk (*). Some fields may be mandatory only under specific conditions; this is explained in the field's description.

7.3.2 Sorting Behaviour

Sorting controls how items are arranged in lists and tables. Whenever a user opens a page with a list, the system uses a predefined default order—for example, A to Z for text, or earliest to latest for dates.

When filters are applied, the list is always filtered first and sorted afterwards, so the sorting applies only to the filtered results.

Users can change the sorting by clicking a column header. Each click switches the order:

- First click: ascending
- Second click: descending
- Third click: sorting removed



 **Figure 7 - Sorting options**

The sorting direction is shown with arrows: upward for ascending and downward for descending. If no arrow is shown, the column is not used for sorting.

Some lists support multi-level sorting. This means the system orders the data by one column first (primary sorting) and then organises items with the same value by another column (secondary sorting). This can be applied to more than 2 columns (tertiary and more).

If the list contains many records, it may be split into pages, with up to 1000 items per page. Sorting always applies only to the page the user is currently viewing.

Sorting preferences are not saved. When the user leaves or refreshes the page, the list returns to its default sorting.

7.3.3 On-screen reporting (Excel export)

Unless stated otherwise, every screen which displays a data table natively supports data export to Excel. This can be triggered using a button located in the top-left corner of each relevant table.

The exported Excel file reflects the user's current view, including any limitations introduced by active filters (what you see is what you get).

The data is immediately downloaded via the user's browser into the default downloads folder in the user's OS, provided the local computer settings allow it.

Supported formats:

- XLSX

7.3.4 Time Zone and daylight-saving time

The following rules define how time is handled within the FASS system. These are generally valid unless otherwise specified for a particular data flow, screen or report.

- Internally, the FASS system operates in UTC (no daylight-savings time changes apply)
- All APIs for System Service Providers use UTC.
- All reports accessed via API are returned in UTC.
- Manual File uploads initiated via the GUI by a user use UTC.
- The GUI displays date and time values in **Greenwich Mean Time** (GMT, equivalent to UTC+0) during the winter period and switches to **British Summer Time** (BST, equivalent to UTC+1) during the summer period. This does not affect stored or exchanged data.
 - On-screen reports that follow the structure of the GUI are displayed in the same time zone as the GUI.

The **Trading Day** in the market is defined from 23:00 on D-1 to 23:00 on D (local time, i.e. GMT/BST), which aligns with the Central European Time (CET/CEST) calendar day. As a result, the UTC data are provided as follows:

- 23:00 D-1 – 23:00 D during wintertime
- 23:00 D-1 – 22:00 D during short clock change day
- 22:00 D-1 – 22:00 D during summertime
- 22:00 D-1 – 23:00 D during long clock change day

In the GUI the system automatically applies the daylight-savings time effects. These transitions occur twice per year:

- Start of summer time: On the last Sunday in March, clocks move forward by one hour at 01:00 local time. At this point, 01:00 becomes 02:00, resulting in a 23-hour day (commonly referred to as the "short day").
- End of summer time: On the last Sunday in October, clocks move back by one hour at 02:00 local time. At this point, 02:00 becomes 01:00 again, resulting in a 25-hour day (commonly referred to as the "long day").

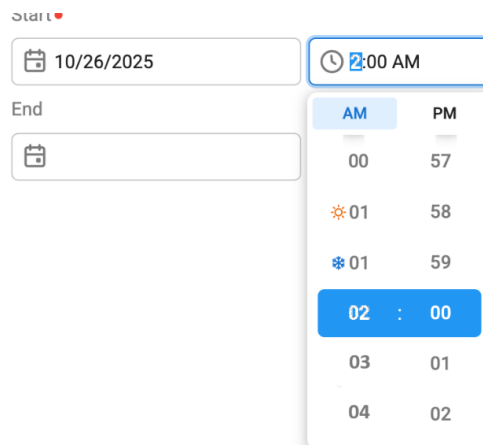
All data is stored in UTC to ensure consistency across systems and avoid ambiguity during daylight savings time transitions. When presented to users, timestamps are always displayed in the local (Belfast) time zone.

- On the short day (daylight savings starting in March), the local clock skips directly from 00:00 to 02:00. The hour 01:00 is not displayed in the user interface.
- On the long day (daylight savings ending in October), the local clock shows 01:00 twice: once in summer time (BST) and once in winter time (GMT). In this case, both 01:00 values are displayed, each accompanied by a visual indicator – a sun icon ☀ for summer time and a snowflake icon ❄ for winter time – to clearly distinguish between them.

This approach ensures that the system remains internally consistent while still presenting time information in a way that is both accurate and user-friendly.

Local time display vs. UTC storage during the clock-change day:

UTC Time	Local Time (March BST start)	Local Time (October BST end)
00:00	00:00 (GMT)	01:00 (BST) ☀
01:00	not displayed	01:00 (GMT) ❄
02:00	02:00 (BST)	02:00 (GMT)
03:00	03:00 (BST)	03:00 (GMT)



 **Figure 8: GGS Date-Time Picker Example During Long Day**

7.3.5 Quantity and Prices Format

Throughout the FASS system, in general,

- all quantity values in MW are stored and displayed with 3 decimal places
- all volume values in MWh are stored and displayed with 3 decimal places
- all price values in EUR/GBP are stored and displayed with 2 decimal places
- exchange rate values are stored and displayed with 4 decimal places

7.3.6 Landing Page

The landing page contains the options to log in, or to register to the system as a Party Authorised User. It can be accessed with any supported web browser by any internet user on following url:

- Production environment: Links to be provided in a future version
- Test/sandbox environment: Links to be provided in a future version

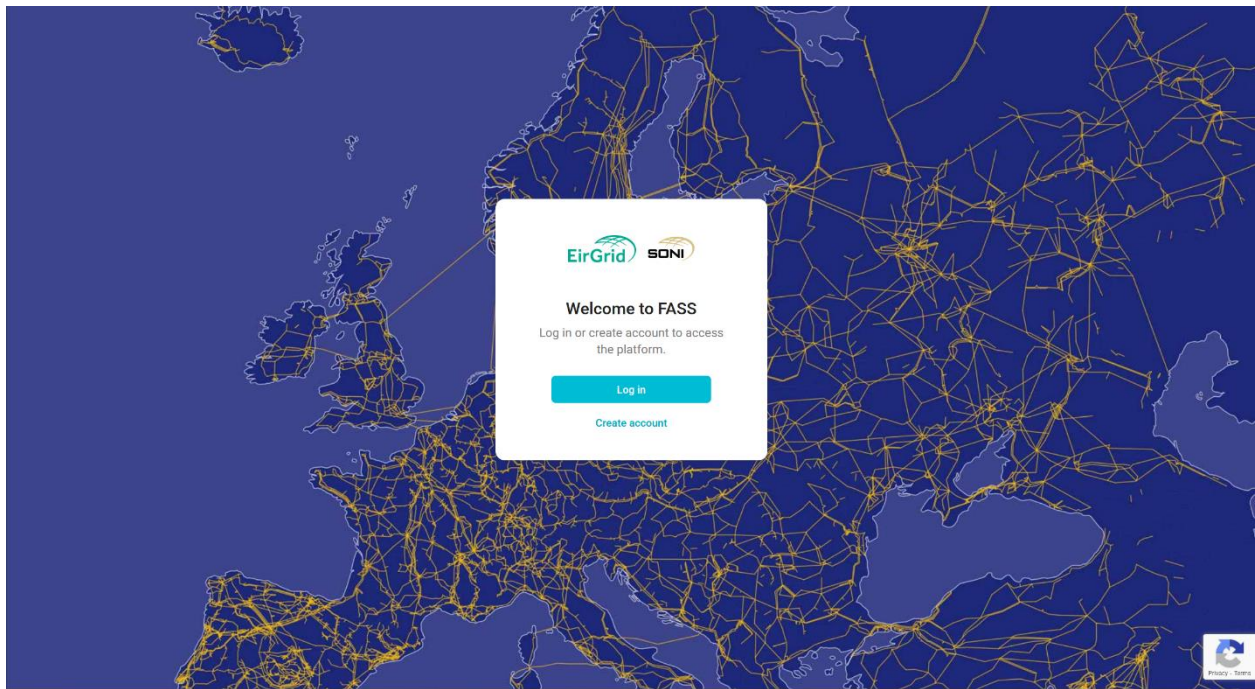


 Figure 9 - Landing page

7.3.7 Menu navigation

Once logged in, the User can navigate the platform using the menu on the left side of the screen. The available screens depend on the User role (Party Authorised User, Service Provider Operator, Service Provider Approver). Each chapter in step-by-step guides states which user roles can access the given use case.

7.3.8 Notifications

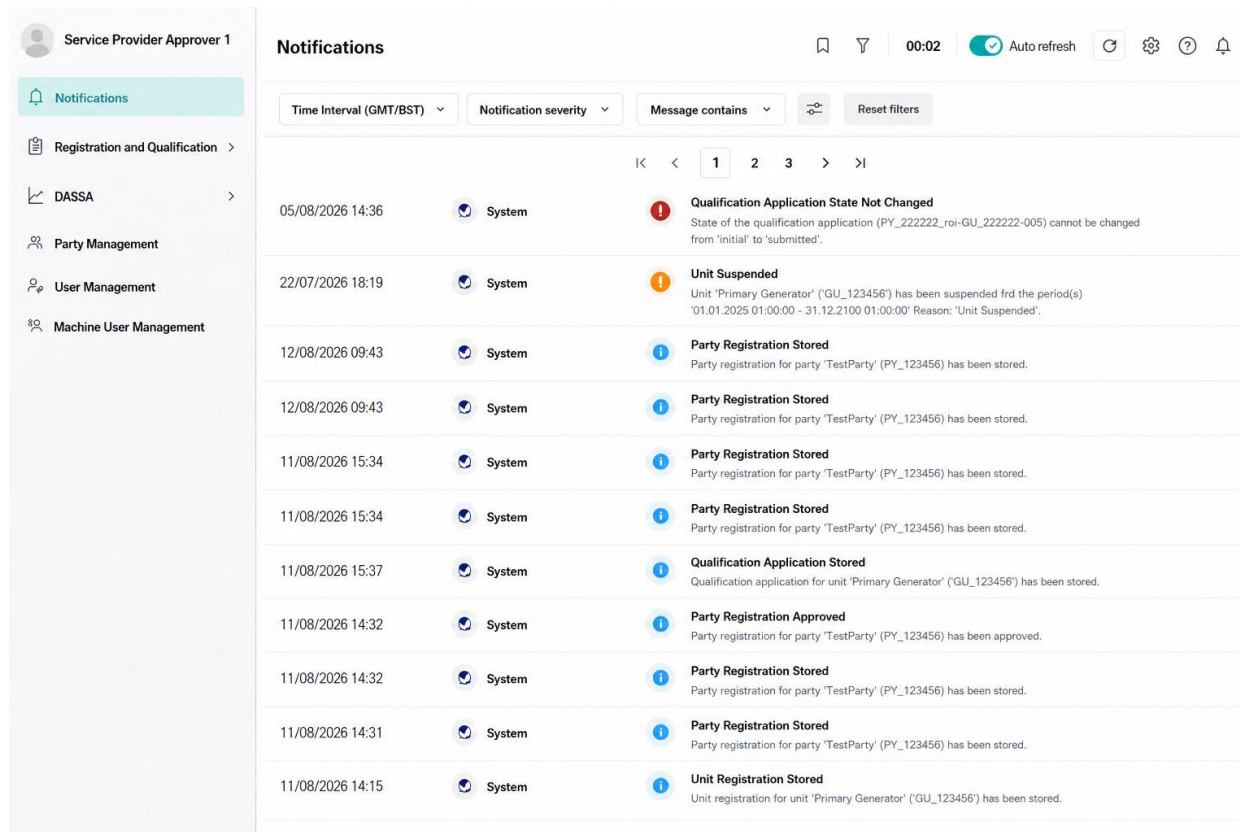
The system is monitoring business activities and sends corresponding notifications to the users. Most actions have a notification tied to them, e.g. receiving of input data, submission of dataflows, editing values via system screens, etc. When a notification is generated, it is made available to each authorised user separately. Notifications do not require any action to be taken; they serve only for information purposes.

Notifications have an associated severity which will be Information, Warning or Error. Error notification usually appears when an invalid file is uploaded (see also chapter Message upload) or in other severe system issues. Warning is an important notification about an alternative but expected business scenario, and information is merely a confirmation of successfully executed action / use case.

The notifications can be filtered by selecting:

- Time Interval
- Severity
- Message content

The notification page refreshes automatically unless the function is turned off by the switch in the top right corner of the screen. Other functions of the screen include (from left to right) management of user filtering presets, manual reload, setting of number of notifications per screen page and refresh interval.



Service Provider Approver 1

Notifications

Time Interval (GMT/BST) Notification severity Message contains 00:02 Auto refresh

Time Interval (GMT/BST) Notification severity Message contains Reset filters

1 2 3

05/08/2026 14:36	System	Qualification Application State Not Changed State of the qualification application (PY_222222_roi-GU_222222-005) cannot be changed from 'initial' to 'submitted'.
22/07/2026 18:19	System	Unit Suspended Unit 'Primary Generator' ('GU_123456') has been suspended for the period(s) '01.01.2025 01:00:00 - 31.12.2100 01:00:00' Reason: 'Unit Suspended'.
12/08/2026 09:43	System	Party Registration Stored Party registration for party 'TestParty' (PY_123456) has been stored.
12/08/2026 09:43	System	Party Registration Stored Party registration for party 'TestParty' (PY_123456) has been stored.
11/08/2026 15:34	System	Party Registration Stored Party registration for party 'TestParty' (PY_123456) has been stored.
11/08/2026 15:34	System	Party Registration Stored Party registration for party 'TestParty' (PY_123456) has been stored.
11/08/2026 15:37	System	Qualification Application Stored Qualification application for unit 'Primary Generator' ('GU_123456') has been stored.
11/08/2026 14:32	System	Party Registration Approved Party registration for party 'TestParty' (PY_123456) has been approved.
11/08/2026 14:32	System	Party Registration Stored Party registration for party 'TestParty' (PY_123456) has been stored.
11/08/2026 14:31	System	Party Registration Stored Party registration for party 'TestParty' (PY_123456) has been stored.
11/08/2026 14:15	System	Unit Registration Stored Unit registration for unit 'Primary Generator' ('GU_123456') has been stored.

Figure 10 – Warning, Error and Info Notification

Specific notification details for Manual File Upload are to be included in a future document version.

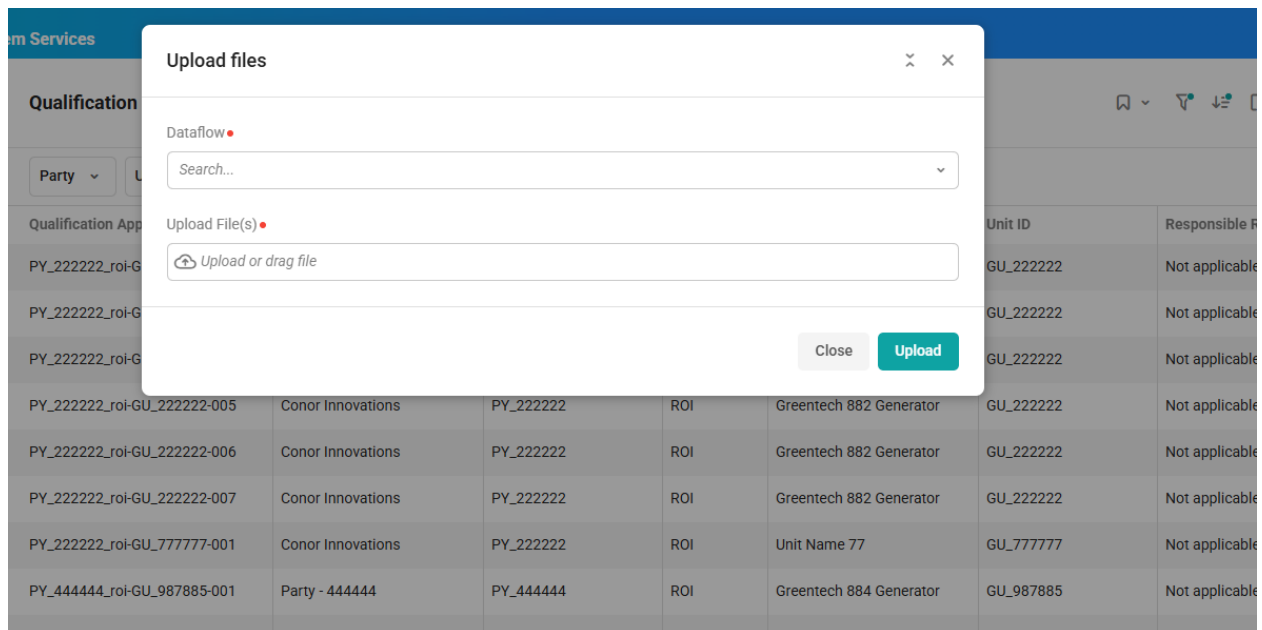
7.3.9 Manual File Upload

The Manual File Upload screen is available from the system menu. It allows user to submit data by uploading a file which will be processed in the same way as a file/payload submission via the API.

The manual file upload can also serve as a backup for some interfaces when the Service Provider's system cannot deliver data via the API. The JSON structure must match the API format, so existing API payloads or files can be reused. Uploaded data is validated, processed, and stored in the same way as API-delivered data, with the same audit and notification behaviour.

How to use it:

- The user selects a Data Flow Type that matches the data to be submitted:
 - DASSA Offers
 - Forecast Capability
 - RAD Offers
- The user selects or drops a .JSON file into the upload area (or browses for a file).
- The user clicks Upload.



 **Figure 11 - Manual File Upload Form**

The file upload is processed in phases:

1. Upload for processing: The system displays a confirmation on the screen if successfully uploaded or an appropriate warning/error.
2. Background processing of content: The file is then processed in the background using the same rules and validations as an API submission.
3. Review via Notifications: To review the background processing outcome, the user opens the Notifications screen (via the link in the success message or from the menu). The notification may include a downloadable response with validation details. After successful processing, the uploaded values can be viewed and, where applicable, amended on the related overview screens (for example, DASSA Offers Overview).

Limitations

Only JSON files are supported for Manual File Upload.

The upload screen confirms that the file was received; it does not show the final validation or processing result. That information is available on the Notifications screen.

Processing is asynchronous — meaning that results are not shown immediately on the upload screen.

If upload fails (for example, due to a connection problem), the user should retry or contact support if the issue continues.

8. User Account Management

This chapter describes how Service Provider users are registered, managed, and authenticated in FASS. For the full registration and qualification process, refer to the Step-by-step guide (9.1 Registration and Qualification).

Each user in FASS is assigned to a Party (the Service Provider organisation). A Service Provider user cannot exist without a Party assignment.

User management for Service Providers is performed by authorised users within the organisation — the Party Authorised User (PAU). The PAU can create and manage user accounts for their own Party only.

A user can be added by more than one Party and will have access to each in accordance with the user roles configured by the relevant PAU. This is illustrated in Figure 12 with 'User 4' having access to Party A with the Service Provider Operator user role and access to Party B with the Service Provider Approver user role. Note that the User Account Lifecycle (refer to section 8.3.5 User Account Lifecycle (non-Machine Users)) needs to be considered separately by each Party, e.g. each Party needs to Terminate the user to have them fully locked-out of the system.

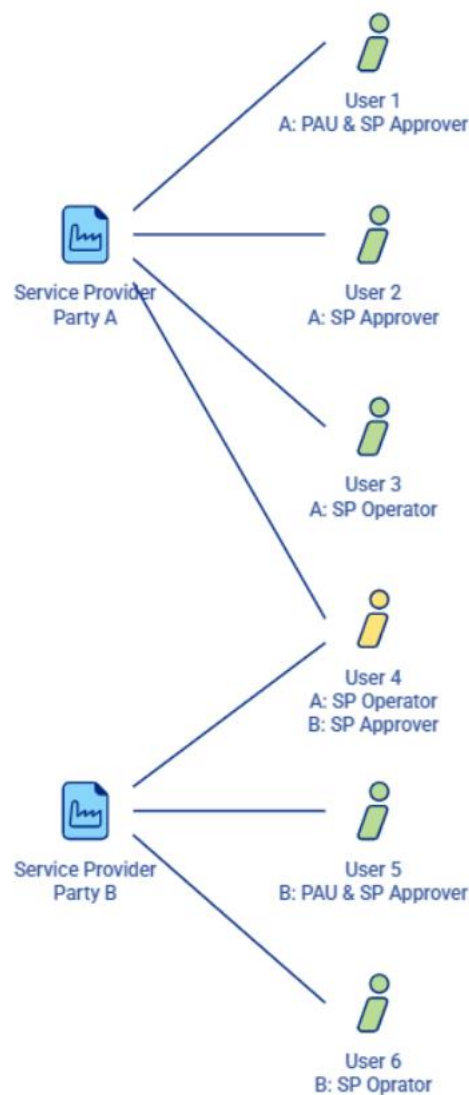


Figure 12 - A User configured for multi-Party access

8.1 Service Provider User Roles

FASS supports several Service Provider roles. Each user role defines what the user can view or do within their Party. Role permissions are not inherited between user roles. A user can be assigned one or more user roles.

The following table describes the list of Service Provider User roles used in the system:

User Role	Description
Party Authorised User (PAU)	Manages users within the Party; can create, and disable accounts
Service Provider Approver	Approves submissions related to Party, Unit, and processes registrations and qualifications within the respective Party
Service Provider Operator	Enters data, uploads documents within the respective Party
Service Provider Reader	View-only access within own Party; no actions allowed
Service Provider Machine User	Representation of Service Provider's IT system to interact via API to deliver/retrieve data

8.2 Registration

The management of users is split into two categories – User management and Party management.

In order to ensure proper access rights management, Users are always created with an assignment to a Party. There cannot be a User without any Party assigned.

The Registration and Qualification process is described in detail in the related Step-by-step guide.

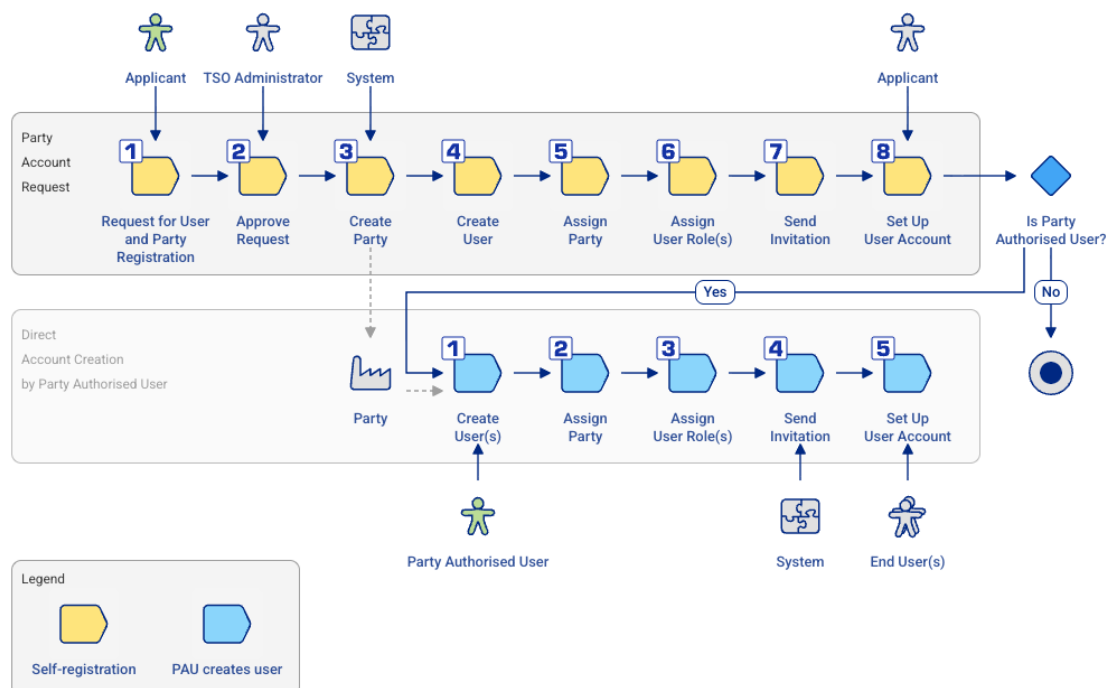


Figure 13 - Business diagram

8.2.1 Party Authorised User Registration

The first user of a Service Provider organisation is registered as part of the Party registration and qualification process. The organisation's responsible person follows the Step-by-step guide (refer to 9.1.6 Party Authorised User Registration) to complete the Party Authorised User registration. Upon approval, the initial Party Authorised User account is created and receives an email to complete registration.

8.2.2 User Registration by Party Authorised User

Once a PAU account is active, the PAU creates additional user accounts for colleagues within the same Party through the Users screen (accessible from the system menu). The specific steps are provided in the Step-by-step guide (refer to 9.1.7 User Creation by PAU).

8.2.3 User Management by Party Authorised User

This section of the document will be extended in a future document version with more detailed processes and screen-shots.

The PAU manages users through the Users screen in the system menu. From this screen, the PAU can:

- Display the list of users belonging to their Party
- View user details
- Create new users
- Update user account information and roles (for active users)
- Reset a user's password (the system sends a reset link to the user's email)
- Reset a user's multi-factor authentication (the user must re-enrol on next login)
- Suspend, reactivate, or terminate user accounts

Available actions depend on the current state of the user account (see section [User Account Lifecycle](#)).

The PAU can also manage the Service Provider Machine User for their Party — view the Client ID and generate a new Client Secret for API integration. When a new Client Secret is generated, the previous secret is invalidated immediately. The Client Secret is shown only at the moment of generation and cannot be retrieved later.

8.3 Log-in and Log-out

Service Provider users log in using their email address as the username, a password, and a one-time authentication code (multi-factor authentication).

To log out, the user selects the log out option from the top-right navigator. The system also logs the user out automatically after a period of inactivity (session lifetime is configured at system level, typically 12 hours). Before automatic logout, the system may display a session expiry warning so the user can extend the session or log out explicitly. Unsaved form data may be lost if the session expires.

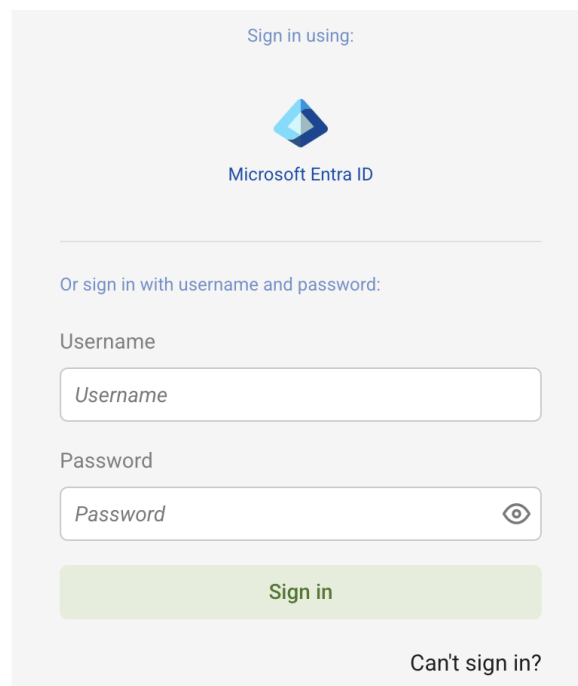
The system does not support switching between accounts. To use a different account, the user must log out and log in again with the other account's credentials or use a separate browser profile.

If the user does not yet have credentials, they should contact their Party Authorised User to create an account. If no PAU exists yet, the organisation's responsible person should follow the Party Authorised User registration process described in section [Party Authorised User Registration](#).

8.3.1 First login procedure

Once you have your access credentials, login using the following steps:

1. Open the FASS address in a web browser.
2. Click the Login button on the Landing page.
3. Enter the email address (username) and the temporary password from the invitation email.
4. Set a new permanent password that meets the FASS password policy (see section [Password Policy](#)).
5. Configure multi-factor authentication by synchronising an authenticator application with the system (see section [Multi-Factor Authentication](#)). This step is mandatory and cannot be skipped.
6. Enter the verification code from the authenticator application to complete login.
7. The Notifications screen is displayed. The user can navigate the platform using the menu.



Sign in using:


Microsoft Entra ID

Or sign in with username and password:

Username

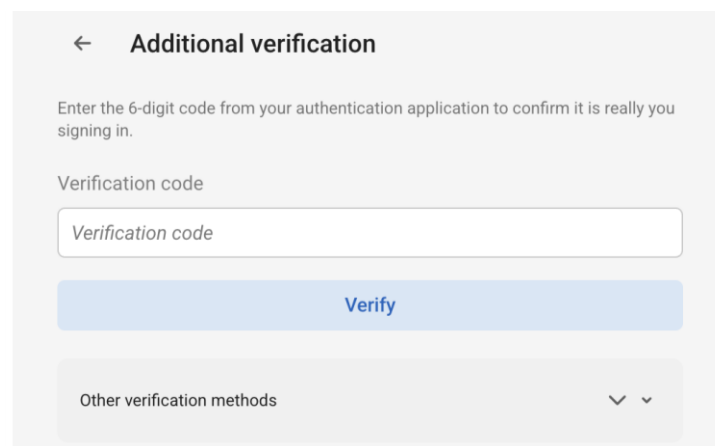
Password

Sign in

Can't sign in?

 **Figure 14 - Login Window - Username and password**



← **Additional verification**

Enter the 6-digit code from your authentication application to confirm it is really you signing in.

Verification code

Verify

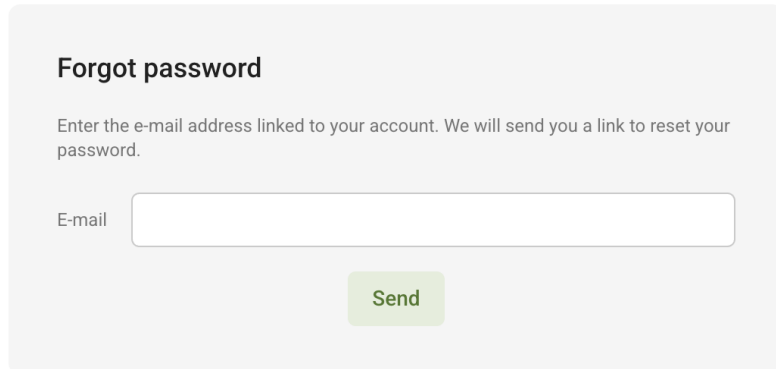
Other verification methods  

 **Figure 15 - Login window - Multifactor authentication**

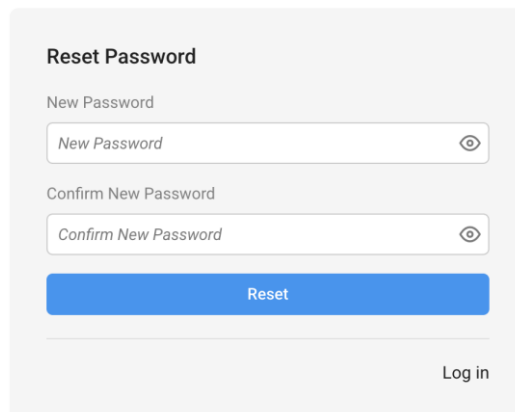
8.3.2 Forgotten Password

If the user forgets their password, they can request a reset by clicking the dedicated link on the login screen (e.g. "Can't sign in?"). The user enters the email address associated with their account and submits the form. The system sends an email with a link to set a new password.

Password recovery does not remove or disable multi-factor authentication. After resetting the password, the user must still authenticate with the second factor at login.



 *Figure 16 - Forgotten login information window*



 *Figure 17 - Reset Password*

8.3.3 Password Policy

Passwords must meet the following requirements:

- At least 8 characters long
- At least one uppercase letter, one lowercase letter, one number, and one symbol
- Changed at least every 45 days (the user is prompted to change an expired password at next login)
- Not changed more than once within 24 hours of the last change

After 5 failed login attempts, the user account is temporarily locked. The lock duration and the number of permitted attempts are configured at system level.

8.3.4 Multi-Factor Authentication

Multi-factor authentication (MFA) is required to access any part of FASS beyond the login screen. The user must provide a username, password, and a one-time code from an authenticator application.

The one-time code is generated by an RFC 6238 compliant authenticator application, typically installed on a mobile device. Microsoft Authenticator is recommended.

MFA must be configured immediately after the first successful login. Enrolment cannot be skipped.

To set up MFA, the user opens Advanced Security Options, enables two-step verification, scans the displayed QR code with the authenticator app, and activates the "Always use two-step verification" option.

The user can also generate backup codes as an alternative second factor when the primary authenticator is unavailable. Each backup code can be used only once. Backup codes should be stored securely.

If backup codes are exhausted or lost, the user must re-enrol MFA or contact their Party Authorised User to reset second-factor authentication.

A user can Remove or Renew MFA using the control buttons at the Advance Security Options screen.

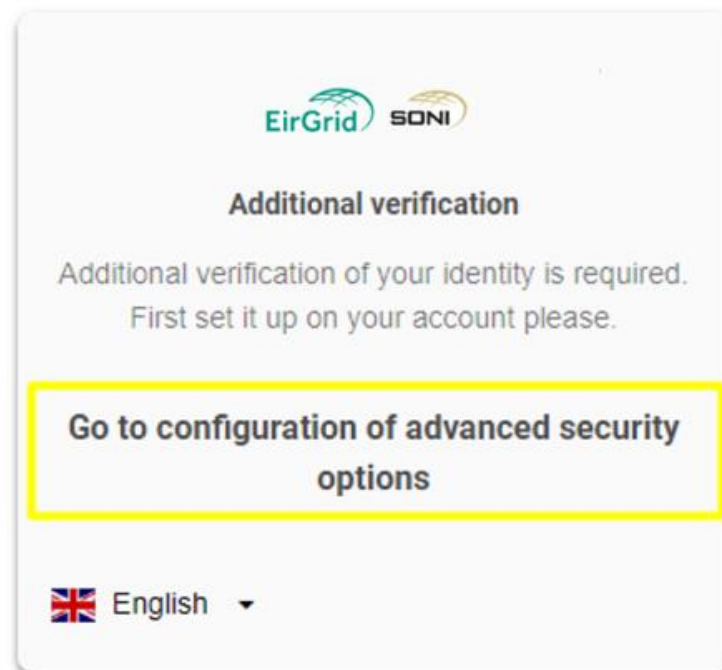


 Figure 18 - MFA setup required

Advanced Security Options

① This page allows you to set up and manage additional authentication methods providing better protection of your identity and allowing you to access applications requiring higher level of security.

Authentication Application

② This section allows you to setup authenticator application providing verification codes, such as Microsoft Authenticator or Google Authenticator (available for Android or iOS).

Device	Connected	Last verification
 Authenticator Enable	—	—

Backup codes

③ This section allows you to generate backup verification codes that let you verify your identity when you cannot use your authentication application.

Code	Connected	Last verification
 Backup codes Enable	—	—

Always Use Additional Verification

④ By enabling this option you will be asked for two-step verification with every login.

Always use two-step verification ☒

 Figure 19 - Advanced Security Options screen - enable authenticator

Add Device

1 Authorization

2 Confirmation

3 QR Code

You are about to enable two-step verification with authentication application. To continue, first verify that it's you. Please enter your username and password.

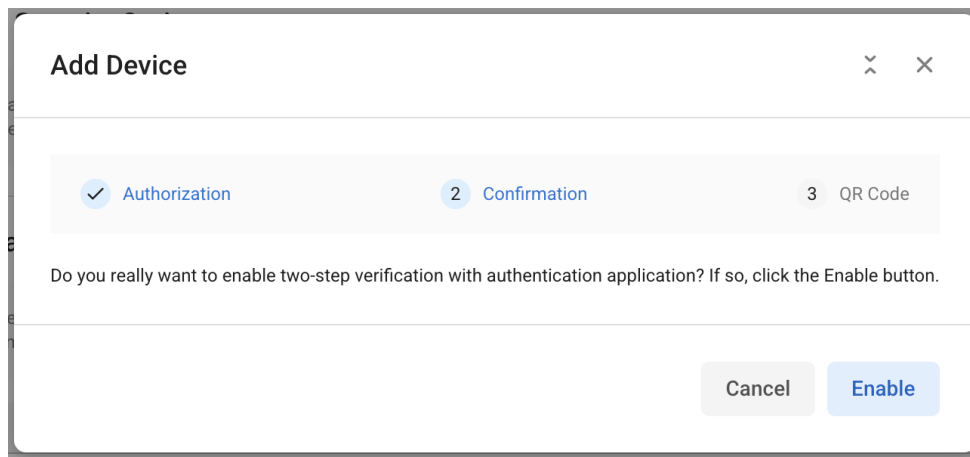
Username ●

Password ●

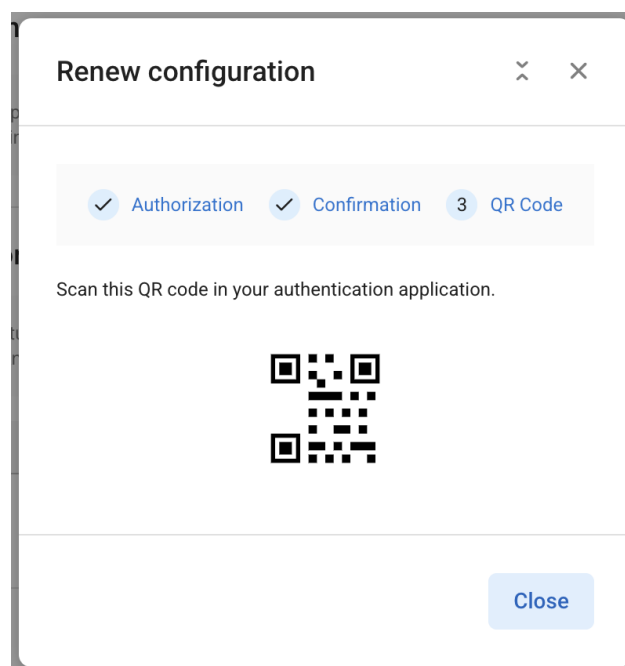
Cancel

Next

 Figure 20 - Add device - authorisation



 *Figure 21: Add device – confirmation*



 *Figure 22: Add device – QR code*

The user can close the modal window. On the *Advanced Security Options* screen, the device is displayed as connected.

8.3.4.1 Remove MFA

The MFA settings section showing the connected Authenticator device with its connection date and last verification. A user uses the delete icon (trash) to start the removal process.

Authentication Application

🔍 This section allows you to setup authenticator application providing verification codes, such as [Microsoft Authenticator](#) or [Google Authenticator](#) (available for [Android](#) or [iOS](#)).

Device	Connected	Last verification	
 Authenticator QR Code	September 22, 2023 12:32 pm	June 9, 2026 03:18 pm	 

 **Figure 23: Authentication Application Overview**

Clicking the Delete icon opens a confirmation dialog asking the user to verify their identity before the removal is performed. In the first step, the user is required to enter their password and click Next to proceed.

Remove device

1 Authorization

2 Confirmation

You are about to remove two-step verification with authentication application.

To continue, first verify that it's you. Please enter your credentials.

Password*



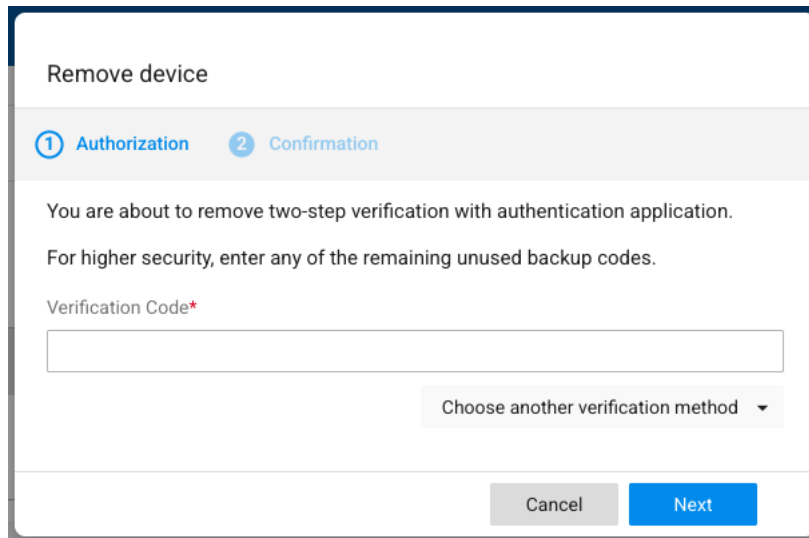
Choose another verification method

Cancel

Next

 **Figure 24: Remove device – Authorization - Password**

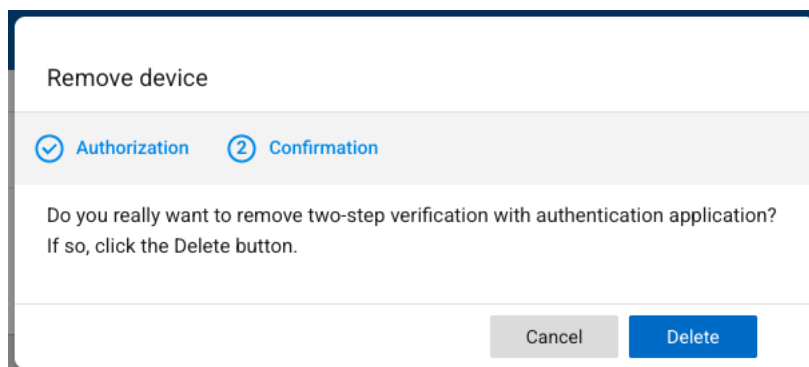
In the next step, the user is required to enter one of their remaining unused backup codes as an additional verification before the removal can proceed. After entering the code, the user clicks Next to continue.



The screenshot shows a dialog box titled "Remove device". At the top, there are two steps: "1 Authorization" (active) and "2 Confirmation". The main text reads: "You are about to remove two-step verification with authentication application. For higher security, enter any of the remaining unused backup codes." Below this is a label "Verification Code*" followed by a text input field. To the right of the input field is a dropdown menu labeled "Choose another verification method". At the bottom right are two buttons: "Cancel" and "Next".

 *Figure 25: Remove device – Authorization - Backup codes*

After successful identity verification, the user is presented with a final confirmation step asking whether they really want to remove the two-step verification. The user clicks Delete to confirm the removal or Cancel to abort the process.



The screenshot shows the same "Remove device" dialog box, but now in the "2 Confirmation" step. The "1 Authorization" step is marked with a checkmark. The main text reads: "Do you really want to remove two-step verification with authentication application? If so, click the Delete button." At the bottom right are two buttons: "Cancel" and "Delete".

 *Figure 26: Remove device - Confirmation*

8.3.4.2 Renew MFA

The user clicks the Renew icon (circular arrow) to start the re-enrolment process.

Authentication Application

ⓘ This section allows you to setup authenticator application providing verification codes, such as [Microsoft Authenticator](#) or [Google Authenticator](#) (available for [Android](#) or [iOS](#)).

Device	Connected	Last verification	
 Authenticator QR Code	September 22, 2023 12:32 pm	June 9, 2026 03:18 pm	 

 **Figure 27: Authentication Application Overview**

Clicking the Renew icon opens a confirmation dialog informing the user that a new configuration for two-step verification is about to be generated. In the first step, the user is required to enter their password and click Next to proceed.

Renew configuration

1 Authorization

2 Confirmation

3 QR Code

You are about to generate new configuration for two-step verification with authentication application.

To continue, first verify that it's you. Please enter your credentials.

Password*

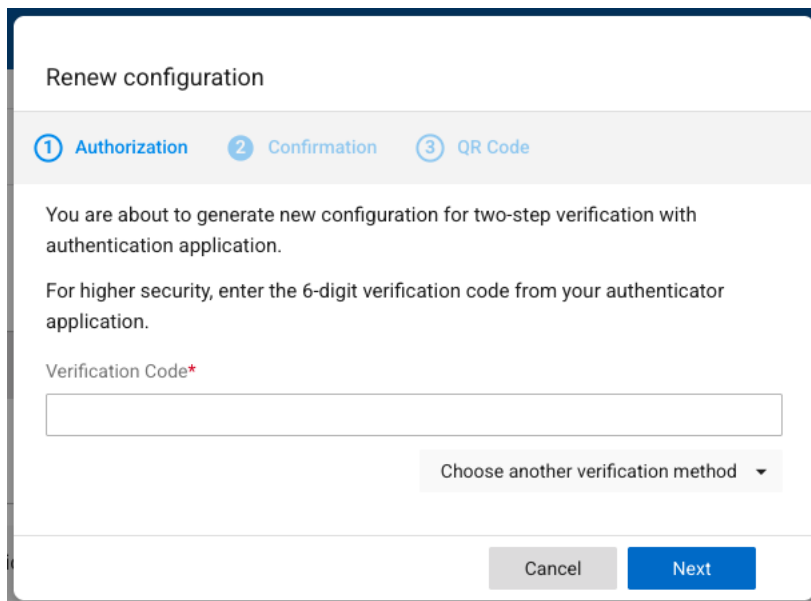
Choose another verification method

Cancel

Next

 **Figure 28: Renew configuration - Authorization - Password**

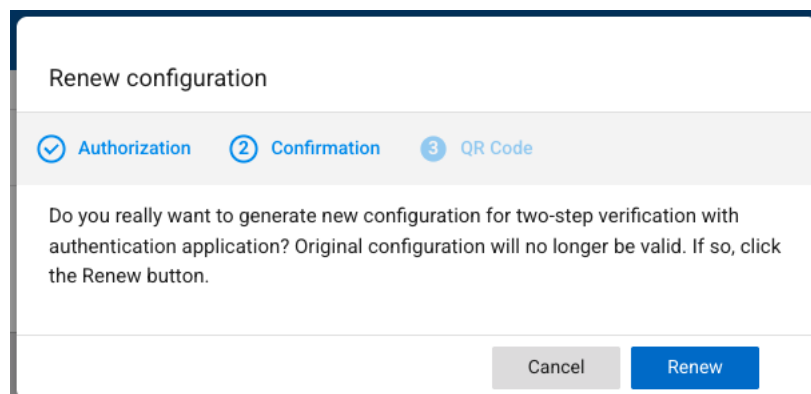
In the next step, the user is required to enter the 6-digit verification code from the currently registered authenticator to confirm identity before renewal (not to add a new device). After entering the code, the user clicks Next to continue.



The screenshot shows a dialog box titled "Renew configuration". At the top, there are three steps: "1 Authorization" (active), "2 Confirmation", and "3 QR Code". The main text reads: "You are about to generate new configuration for two-step verification with authentication application. For higher security, enter the 6-digit verification code from your authenticator application." Below this is a label "Verification Code*" followed by a text input field. To the right of the input field is a dropdown menu labeled "Choose another verification method". At the bottom right are two buttons: "Cancel" and "Next".

 **Figure 29: Renew configuration - Authorization - Verification**

After successful identity verification, the user is presented with a final confirmation step informing them that the original configuration will no longer be valid after renewal. The user clicks Renew to confirm the re-enrolment or Cancel to abort the process.



The screenshot shows the same "Renew configuration" dialog box, but now at the "2 Confirmation" step. The "Authorization" step is marked with a checkmark. The main text reads: "Do you really want to generate new configuration for two-step verification with authentication application? Original configuration will no longer be valid. If so, click the Renew button." At the bottom right are two buttons: "Cancel" and "Renew".

 **Figure 30: Renew Configuration - Confirmation**

8.3.5 User Account Lifecycle (non-Machine Users)

Each user account progresses through defined states:

- Created — The account exists in the system but no invitation has been sent yet.
- Invited — An invitation email has been sent. The user has not yet completed registration.
- Expired — The invitation link has expired without the user completing registration. The PAU must issue a new invitation.
- Active — The user has completed registration and can log in according to their assigned roles. This is the normal operational state.
- Suspended — The account is deactivated. The user cannot log in. The PAU can reactivate the account.

- **Terminated** — The account is permanently deactivated and cannot be reactivated. Active sessions are revoked.
- **Deleted** — The identity record is permanently removed from the system. This state is reached from Terminated or automatically from Expired for unverified accounts.

9. Step-By-Step Guides

9.1 Registration and Qualification

9.1.1 Introduction

9.1.1.1 Purpose of this guide

This guide explains how Service Providers can use the FASS platform to complete Registration and Qualification. Registration and Qualification covers the process by which capabilities required for Service Providers to participate in the DASSA and other trading arrangements are verified, and by which Service Providers are registered as participants by the TSOs.

As a Service Provider, you can use the Registration and Qualification module to:

- Initiate your organisation's registration as a Party by requesting a Party Authorised User (first user only)
- Create and manage user accounts for your Party
- Submit and maintain Party Registration applications
- Submit and maintain Unit Registration applications for your assets
- Submit Qualification Applications so your Units can qualify for System Service Products
- View the status of registrations and applications, respond to Requests for Information (RFI), and manage supporting documents

This guide provides step-by-step instructions for each of these activities.

9.1.1.2 Who can use the Registration and Qualification module

The following Service Provider roles have access to the Registration and Qualification module:

Role	Access
Service Provider Reader	Read-only access to Party, Unit, and Qualification data relating to own Party; can download attachments
Service Provider Operator	Read access plus the ability to create and edit registration/application drafts and submit them for internal approval within own Party (approval by Service Provider Approver)
Service Provider Approver	Read access plus the ability to create, edit, submit registrations/applications to TSO, respond to TSO update requests, withdraw applications, and raise RFIs to TSO within own Party
Party Authorised User (PAU)	Manages user accounts within own Party (see section User Creation by PAU)

Party Authorised User Registration (self-registration of the first user) is available to public users from the Landing Page and is described in section Party Authorised User Registration.

9.1.2 Getting Started

9.1.2.1 Accessing the Registration and Qualification module

The Registration and Qualification module is accessed from the FASS system menu. The main screens available to Service Providers are:

Screen	Purpose
Party Registrations	View the list of Party Registration applications and open details or create a new registration
Unit Registrations	View the list of Unit Registration applications and open details or create a new registration
Qualification Applications	View the list of Qualification Applications and open details or create a new application
System Services Register	View the System Services Register - read-only catalogue of qualified units and their capacities per qualified System Service Product

9.1.2.2 Role permissions summary

Activity	Service Provider Reader	Service Provider Operator	Service Provider Approver	Party Authorised User (PAU)
View Party / Unit / Qualification lists and details	Yes	Yes	Yes	No
Download attachments	Yes	Yes	Yes	No
Create registration/application draft	No	Yes	Yes	No
Edit registration/application (state Initial)	No	Yes	Yes	No
Submit for Internal Approval	No	Yes	No	No
Submit to TSO	No	No	Yes	No
Edit after internal submission (Pending Updates)	No	No	Yes	No
Withdraw registration/application (not yet final)	No	No	Yes	No
Raise RFI to TSO	No	No	Yes	No
Respond to RFI (when assigned as solver)	No	Yes	Yes	No
Create user accounts (PAU)	No	No	No	Yes

9.1.2.3 Key concepts and terminology

Term	Description
Party	Your organisation as registered in FASS (Party ID & Jurisdiction)
Unit	Generation, demand, and other Service Provider assets belonging to your Party

Term	Description
System Service Product	A specific system service for which a Unit may be qualified (e.g. POR Up, POR Down)
Party Registration	Process by which your Party is registered to participate in the FASS
Unit Registration	Process by which a Unit belonging to your Party is registered in FASS
Qualification Application	Application to qualify a Unit for one or more System Service Products
Responsible Role	Indicates which actor is expected to act next on a registration/application (derived from its state)
Request for Information (RFI)	A task raised on a registration/application to request or provide additional information; does not change the registration state
Qualification Pack	TSO-published requirements that a Qualification Application must comply with
System Services Code	Code that Party Registration applicants must acknowledge compliance with

9.1.3 The Registration and Qualification Process — Service Provider View

9.1.3.1 End-to-end timeline

As a Service Provider, your organisation typically progresses through the following sequence:

- Party Authorised User Registration — the first user self-registers and, upon TSO approval, receives Party Authorised User and Service Provider Approver roles
- User account creation — the Party Authorised User creates accounts for colleagues (Service Provider Operator, Service Provider Reader, Service Provider Approver, and Party Authorised User roles as needed)
- Party Registration — your Party submits and obtains TSO approval of its registration application
- Unit Registration — you register one or more Units belonging to your Party
 - Once the Party Registration has started you can start a Unit Registration in parallel
 - Party Registration must complete before the Unit Registration can complete
- Qualification Application — you apply to qualify each Unit for the required System Service Products
 - Once the Unit Registration has started you can start a Qualification Application in parallel
 - Unit Registration must complete before the Qualification Application can complete
- TSO review and approval — the relevant TSO reviews each submission, and you may be asked to respond to any Requests for Information or update requests
- Active participation — once Party, Unit, and Qualification are approved, your Units appear in the System Services Register and you may participate in FASS

9.1.3.2 Registration and application business states

Party Registration, Unit Registration, and Qualification Application each progress through defined business states. The table below explains what each state means for your work:

State	What it means for you
Initial	Draft created. Service Provider Operator or Approver can edit. Operator may submit for internal approval.

State	What it means for you
In Progress	Submitted for internal approval. Service Provider Approver must review and submit to TSO. Operator can view only.
Submitted	Submitted to TSO. Service Provider users can view only unless TSO requests updates.
Complete	TSO Operator has confirmed completeness. Awaiting TSO Approver review.
In Review	TSO Approver is reviewing the submission.
In Testing	Qualification Application only: TSO has initiated technical testing. Service Provider Approver must submit testing evidence.
Pending Updates	TSO has requested updates. Service Provider Approver must edit and re-submit.
On Hold	TSO has put the submission on hold. Service Provider Approver must respond by the deadline or the submission may be withdrawn.
Approved	Final state — registration/application approved. Party or Unit becomes Active; qualified products are recorded in the System Services Register.
Rejected	Final state — TSO rejected the submission. You may submit a new application.
Withdrawn	Final state — submission was withdrawn (by Service Provider Approver or automatically after On Hold deadline). You may submit a new application.

9.1.3.3 Notifications you receive

The system sends notifications and emails to authorised users in your Party for key events, including submission for internal approval, submission to TSO, requests for updates, approval, rejection, withdrawal, and RFI activity. Notifications are available in the platform and relevant events also trigger email messages.

9.1.3.4 List and detail screens

Each registration type has a list screen (Party Registrations, Unit Registrations, Qualification Applications) accessible from the system menu. Use filters to narrow results by state and category (Active / Finalised). Your Party is pre-selected and cannot be changed, unless you have access to more than one Party. Click Detail on a row to open the registration/application detail, where you can view submitted data, manage attachments via the file manager, and access the RFI task list. Service Provider Operator and Approver can create new registrations from the list screen; Update is available from the More Options menu when the state allows editing for your role. Service Provider Reader can only view the existing documents of their Party.

9.1.4 Request for Information

In the following chapters (Party Registration, Unit Registration, Qualification Application), users may raise a Request for Information (RFI) to ask for additional information needed to process the registration/application.

An RFI is not assigned to a specific user, but rather to a User role within a Party or organisation. That means that any user with the assigned role can see the RFI and react to it.

The RFI is visible as a task (i.e. “activity”) in the detail of the registration/application (Menu navigation -> Registration and Qualification -> [select according to type of registration/application] -> Detail). It is also visible in the User’s task list. Task list is available under the button in the top right corner of the screen, where in the case that an RFI is present, will show a notification icon with the number of open RFIs (see below).

Each user assigned to the Role and Party also receives an email with the relevant information and a link to the related registration.

Party Registration Detail

Address Line 1	Not provided
Address Line 2	Not provided
Address Line 3	Not provided
Country	Not provided
County	Not provided
Eircode/Postcode	Not provided
Telephone	Not provided
E-mail	Not provided
Legal Status	Not provided
System Services Code Confirmed	No

Health & Safety, Environment, and Employment Details

Occupational Health and Safety Confirmed	No
Environmental Management Confirmed	No
Employment and Equality Legislation Confirmed	No
Modern Slavery Act Confirmed	No
Standard Procedures Applied	No

Activity List

- ✓ Revision of provided information
Please, fix the address and provide insurance details
14/08/2026 23:59
TSO Admin 2 → Solver(s) ▾

[Raise an RFI](#)

Figure 31 - Detail of registration with RFI section

Party Registration

✓ Revision of provided information

Overview | History & Comments | Solvers

14/08/2026 23:59

Please, fix the address and provide insurance details

TSO Admin 2
↓
Sawyer Tom

☒ Solved
☐ Comment only
☐ Accepted
☒ Solved
☐ Warning
☐ Not solved
☐ Problem

I added the required information. [Set State](#)

[Submit to TSO](#) [Withdraw](#)

Activity List

[Raise an RFI](#)

Figure 32 - Service Provider reacting to RFI

Depending on the content of the request, the User should react to the task accordingly (e.g., submit additional documents and confirm, that the task is completed).

Users can add comments or change states of the tasks by opening the activity list in the detail of the registration/application and interacting with the form. The RFI is resolved once the submitter of the RFI marks it as complete.

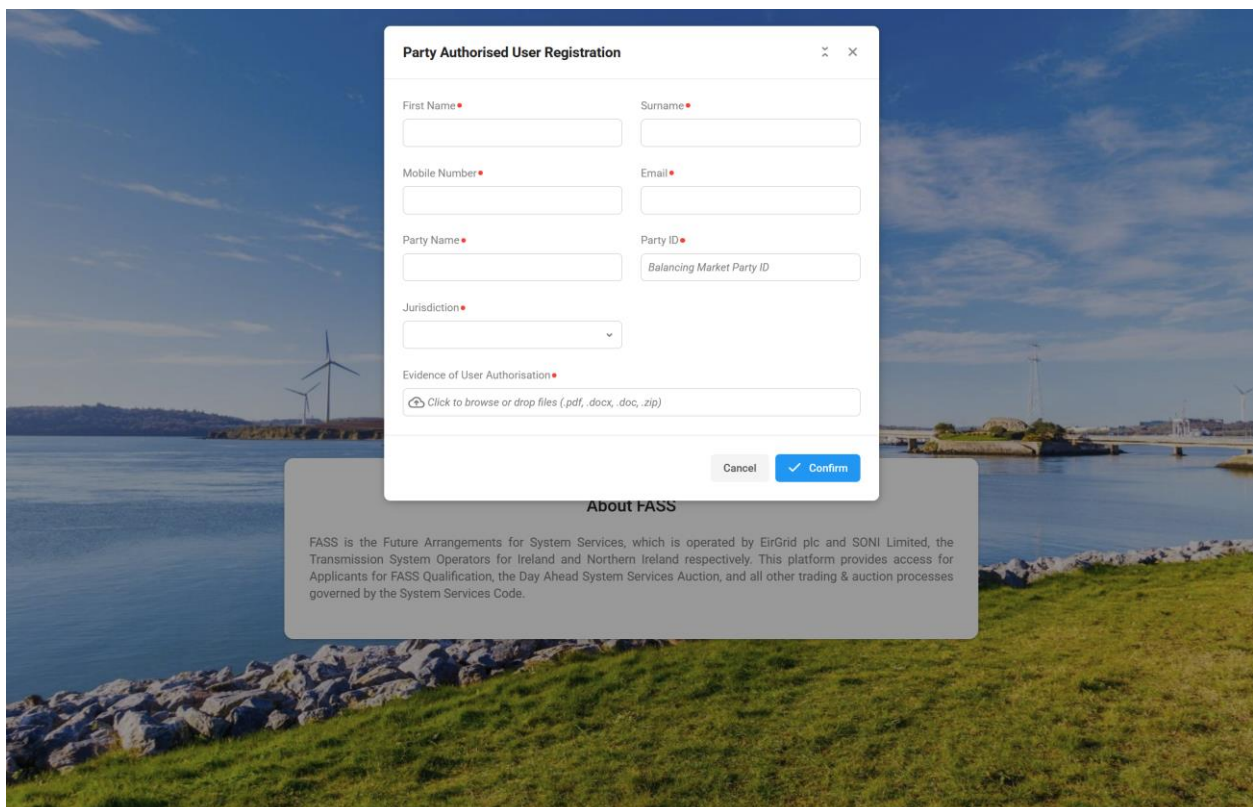
Who can raise and respond to RFIs:

Raised by	Addressed to	Visible to Service Provider
TSO	Service Provider Operator, Service Provider Approver	Yes — solvers respond; Operator may also view RFIs raised by Approver to TSO
Service Provider Approver	TSO	Yes — Operator can view as interested party

9.1.5 Managing Attachments (File Manager)

File Manager functionality to be added in a future document version

9.1.6 Party Authorised User Registration



 **Figure 33 - Party Authorised User Registration**

Authorised roles: Public

The first user of a particular Party can self-register in the system as the Party Authorised User. This process is designed to create the Party in the system (if it does not exist yet), create the User account, and upon approval by TSO, assign the Party Authorised User and Service Provider Approver roles to that user account (see chapter 8.1 Service Provider User Roles).

As part of the Party Authorised User Registration, Party-related basic information is required as the assignment of a User to a Party is necessary for access rights setup. Registered Party Authorised User may create other user accounts within the relating Party directly in the system. Therefore, only the first user needs to self-register via this form and all other users of the Party must be created by this user as described in chapter User Creation by PAU.

How to access:

1. Open web browser.
2. Enter the FASS address into your browser address bar (see address above in chapter Landing Page).
 1. Web browser displays Login screen.
3. Click on "Create account".
4. Fill out the form as described below.
5. Confirm form and check the success notification pop-up.

Form description (required fields are marked with * symbol):

- First Name *
- Surname *
- Mobile Number *
- Email *
- Party Name *
- Party ID * - Balancing Market Party ID PY_6digits, e.g.: PY_123456
- Jurisdiction * - Select one of NI (Northern Ireland) or ROI (Republic of Ireland)
- Evidence of User Authorisation * - upload file with .pdf, .docx, .doc, or .zip format
- Cancel – returns User to previous step
- Confirm – sends the data to be approved or rejected by the TSO. If any error occurs, the User is notified and can correct the invalid data

Common issues:

- Party Authorised User registration cannot be submitted for an already registered Party with the same Party ID and Jurisdiction (as those are created as part of Party Authorised User registration)

Expected Outcome:

In both cases of approval or rejection by the TSO Approver, the applicant is informed about the result by an email sent to the provided email address. There are multiple possible outcomes:

1. PAU Registration has been accepted, new user account – user gets an invitation email to finish their user registration (reset password and setup MFA) along with an approval information email.
2. PAU Registration has been accepted, existing user account – user gets an approval information email and after logging in via their existing credentials, they are additionally granted access to the new party.
3. PAU Registration has been rejected – user is informed about the reason for rejection in the email.

9.1.7 User Creation by PAU

Authorised roles: Party Authorised User (PAU)

Once a PAU account is active, the PAU creates additional user accounts for colleagues within the same Party through the Users screen (accessible from the system menu). Each user must have their own email address; multiple users within the same Party cannot share an email address.

When creating a new user, the PAU must provide at least a unique email address and assign one or more roles.

After the user record is saved, the system sends an automatic invitation email.

The new user must confirm the invitation to complete registration.

The invitation link is valid for a limited period (**typically 14 days**). If the link expires before registration is completed, the PAU must issue a new invitation.

If the invitation email cannot be delivered, the PAU can resolve this by correcting the email address and creating a new user account if necessary.

Steps:

1. Open the Users screen from the system menu.
2. Click Create New User (or equivalent action button).
3. Enter the user's email address (must be unique within the Party), name, and surname.
4. Assign one or more Service Provider roles (e.g. Service Provider Operator, Service Provider Reader, Service Provider Approver).
5. Save the user record.
6. The system sends an invitation email to the new user.

Expected outcome: A new user account is created in state Invited. The new user receives an invitation email to complete registration.

9.1.8 Party Registration

Authorised roles: Service Provider Operator, Service Provider Approver

This use case is intended for Service Providers and enables authorised users to submit an application for Party registration. The applicants can submit the form only for their own Party assigned to them.

The entry form also serves as an update form. The User can save the form and return to it later without losing data, until the registration is submitted to the TSO.

How to access:

1. Open the system in your web browser.
2. Click on "Party Registrations" in the system menu navigation.
3. Click on "Create New Registration" button located above the list of registrations on the right side.
4. Fill out the form as described below.
 1. You can save data by the "Save Draft and Close" button, and return to the form later.
5. Confirm form and check the success notification pop-up.

9.1.8.1 Party Registration process — Service Provider view

1. Service Provider Operator or Approver creates the application (optionally saving a draft in state Initial).
2. Service Provider Operator submits for internal approval (state In Progress) — the form becomes read-only for the Operator.
3. Service Provider Approver reviews, may edit, and submits to TSO (state Submitted) – Service Provider users can no longer edit unless the TSO requests an update.
4. TSO reviews the submission. Service Provider users can view progress and respond to RFIs.
5. If TSO requests updates (state Pending Updates), the Service Provider Approver edits and re-submits.
6. Upon TSO approval (state Approved), the Party becomes Active and Unit Registrations for that Party may be approved by TSO.

7. Only one Party Registration per Party can be in progress at a time. A new registration may be submitted after Rejected or Withdrawn.

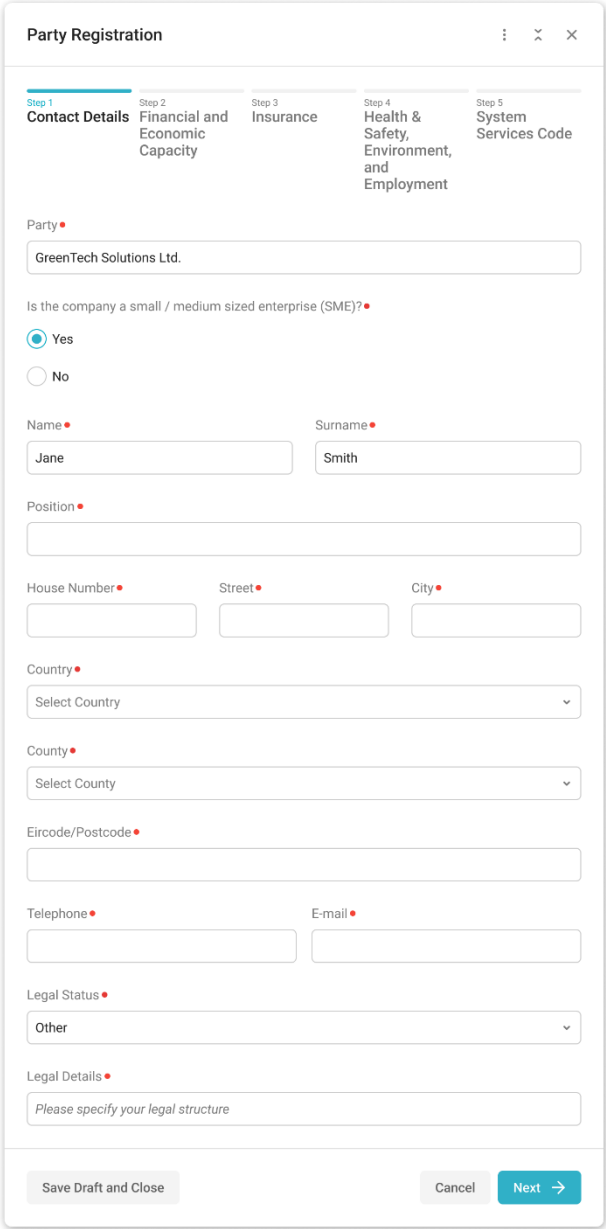
The form consists of the following parts:

- **Step 1: Contact Details**
- **Step 2: Financial and Economic Capacity Declaration**
- **Step 3: Insurance**
- **Step 4: Health & Safety, Environment, and Employment**
- **Step 5: System Services Code**
- **Action Buttons**

9.1.8.2 Submitting Party Registration

Form Step 1: Contact Details

The first step of the form consists of general identifying information related to the party registered.



Party Registration

Step 1: Contact Details | Step 2: Financial and Economic Capacity | Step 3: Insurance | Step 4: Health & Safety, Environment, and Employment | Step 5: System Services Code

Party *
GreenTech Solutions Ltd.

Is the company a small / medium sized enterprise (SME)? *
☒ Yes
☐ No

Name *
Jane

Surname *
Smith

Position *

House Number *

Street *

City *

Country *
Select Country

County *
Select County

Eircode/Postcode *

Telephone *

E-mail *

Legal Status *
Other

Legal Details *
Please specify your legal structure

Save Draft and Close | Cancel | Next →

Form description (required fields are marked with * symbol):

- Party * - is prefilled by User's assigned Party and cannot be changed (unless the user has multiple Party assignments)
- SME * - small / medium sized enterprise (SME)
- Name *
- Surname *
- Position *
- House Number *
- Street *
- City *
- Country *
- County *
- Eircode/Postcode *
- Telephone *
- E-mail *
- Legal Status * - Company / Partnership / Sole Trader / Other
- Legal Details * - Mandatory text field. Displayed only if "Other" option is selected in Legal Status field.

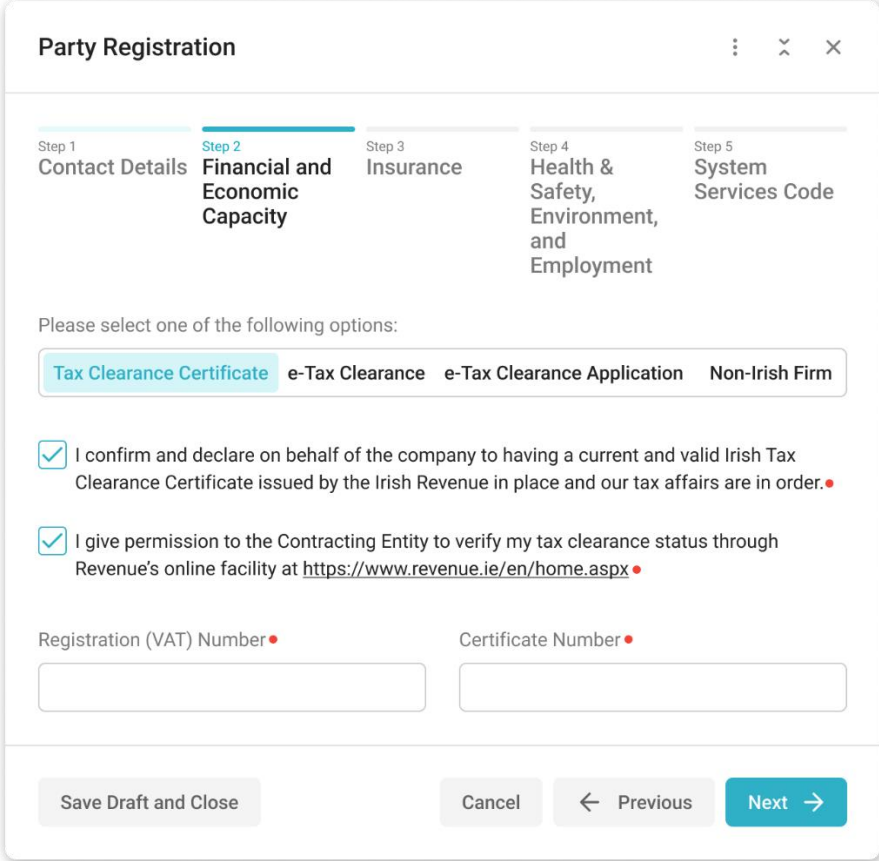
 Figure 34 - Party registration step 1

Form Step 2: Financial and Economic Capacity Declaration

This step is not displayed if Party jurisdiction is selected as Northern Ireland.

The User must fill in one of the following options first. Depending on the option selected, the declaration form will look different.

Option 1: Tax Clearance Certificate



Party Registration

Step 1 Contact Details **Step 2 Financial and Economic Capacity** Step 3 Insurance Step 4 Health & Safety, Environment, and Employment Step 5 System Services Code

Please select one of the following options:

Tax Clearance Certificate e-Tax Clearance e-Tax Clearance Application Non-Irish Firm

☒ I confirm and declare on behalf of the company to having a current and valid Irish Tax Clearance Certificate issued by the Irish Revenue in place and our tax affairs are in order. •

☒ I give permission to the Contracting Entity to verify my tax clearance status through Revenue's online facility at <https://www.revenue.ie/en/home.aspx> •

Registration (VAT) Number • Certificate Number •

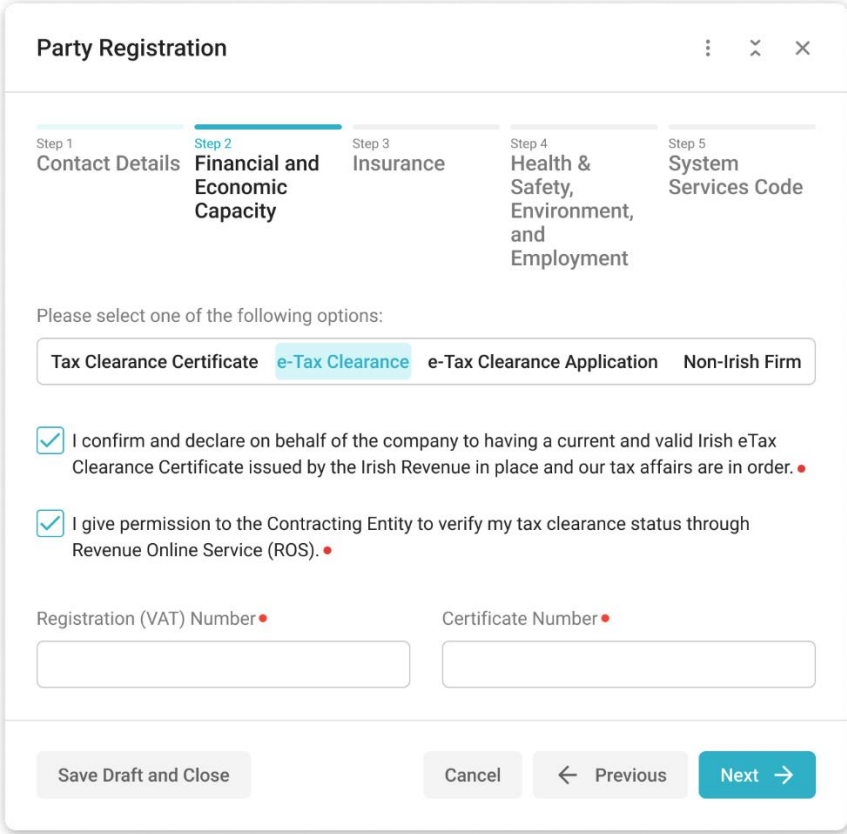
Save Draft and Close Cancel ← Previous Next →

 **Figure 35 - Party registration step 2a**

Form description (required fields are marked with * symbol):

- Confirm Tax Clearance Declaration * - checkbox
- Confirm Online Verification * - checkbox
- Registration (VAT) Number *
- Certificate Number * - insert Tax Clearance Certificate number

Option 2: e-Tax Clearance



Party Registration

Step 1 Contact Details **Step 2 Financial and Economic Capacity** Step 3 Insurance Step 4 Health & Safety, Environment, and Employment Step 5 System Services Code

Please select one of the following options:

Tax Clearance Certificate **e-Tax Clearance** e-Tax Clearance Application Non-Irish Firm

☒ I confirm and declare on behalf of the company to having a current and valid Irish eTax Clearance Certificate issued by the Irish Revenue in place and our tax affairs are in order. •

☒ I give permission to the Contracting Entity to verify my tax clearance status through Revenue Online Service (ROS). •

Registration (VAT) Number • Certificate Number •

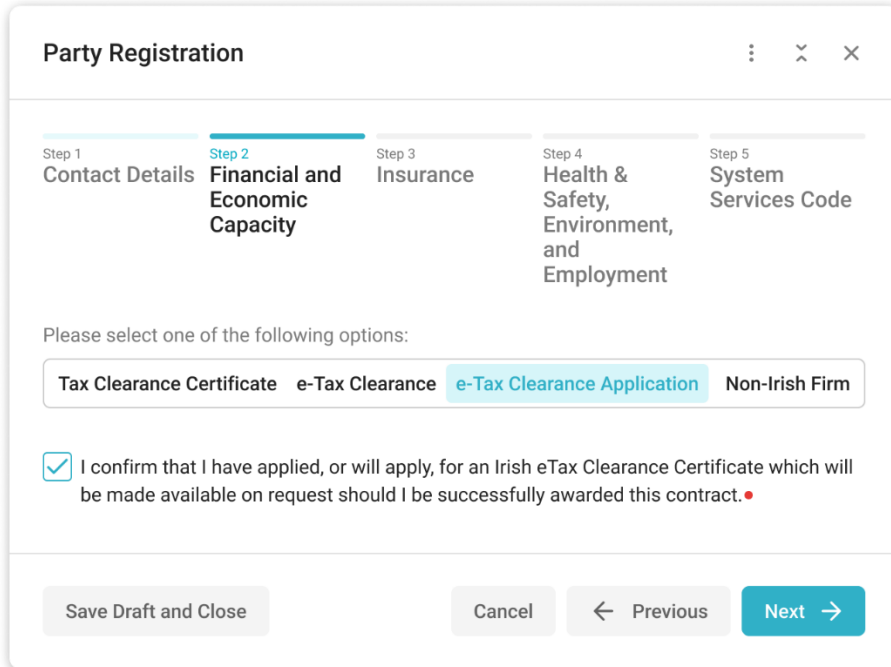
Save Draft and Close Cancel ← Previous Next →

 **Figure 36 - Party registration step 2b**

Form description (required fields are marked with * symbol):

- Confirm Tax Clearance Declaration * - checkbox
- Confirm Online Verification * - checkbox
- Registration (VAT) Number *
- Certificate Number * - insert e-Tax Clearance Certificate number
- The Contracting Entity is SONI for Jurisdiction Northern Ireland and EirGrid for Jurisdiction Republic of Ireland

Option 3: e-Tax Clearance Application



Party Registration

Step 1 Contact Details **Step 2 Financial and Economic Capacity** Step 3 Insurance Step 4 Health & Safety, Environment, and Employment Step 5 System Services Code

Please select one of the following options:

Tax Clearance Certificate e-Tax Clearance **e-Tax Clearance Application** Non-Irish Firm

☒ I confirm that I have applied, or will apply, for an Irish eTax Clearance Certificate which will be made available on request should I be successfully awarded this contract. •

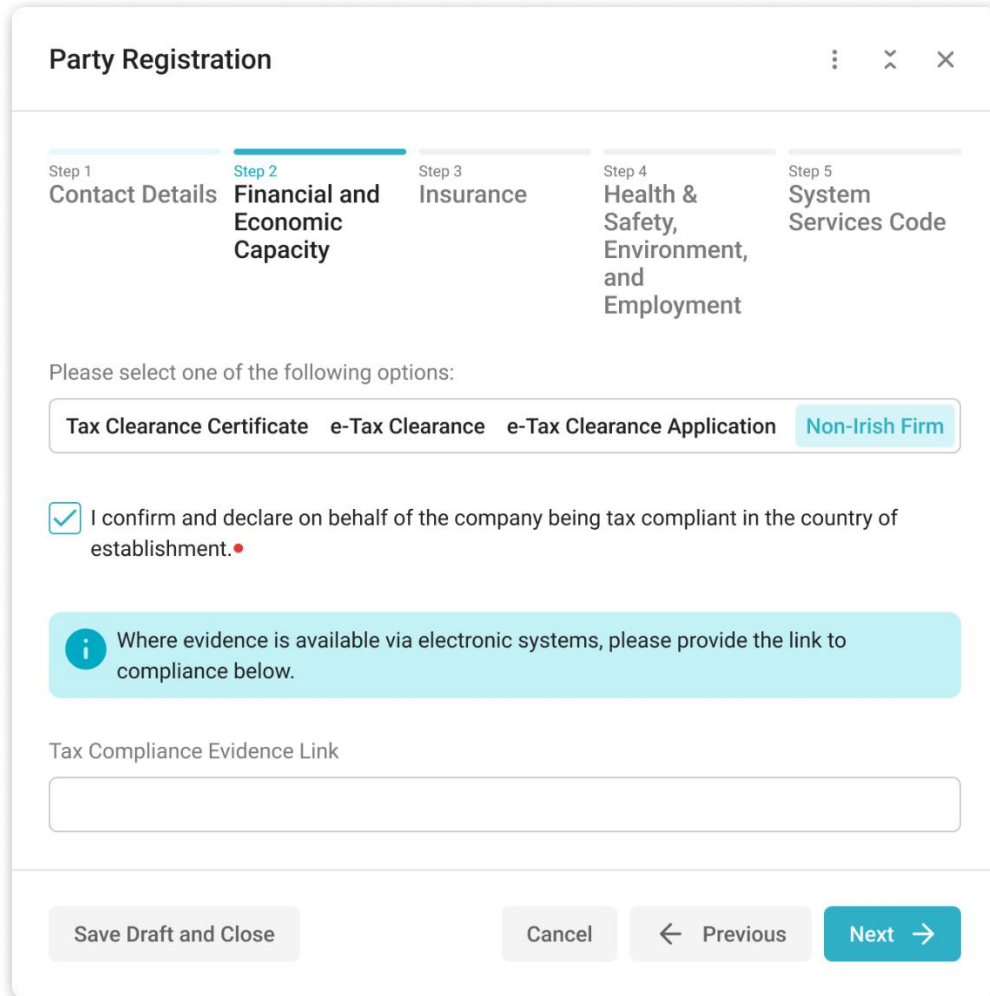
Save Draft and Close Cancel Previous Next

Figure 37 - Party registration step 2c

Form description (required fields are marked with * symbol):

- Confirm Tax Clearance Declaration * - checkbox

Option 4: Non-Irish Firm



Party Registration

Step 1 Contact Details **Step 2 Financial and Economic Capacity** Step 3 Insurance Step 4 Health & Safety, Environment, and Employment Step 5 System Services Code

Please select one of the following options:

Tax Clearance Certificate e-Tax Clearance e-Tax Clearance Application **Non-Irish Firm**

☒ I confirm and declare on behalf of the company being tax compliant in the country of establishment. •

i Where evidence is available via electronic systems, please provide the link to compliance below.

Tax Compliance Evidence Link

Save Draft and Close Cancel < Previous Next >

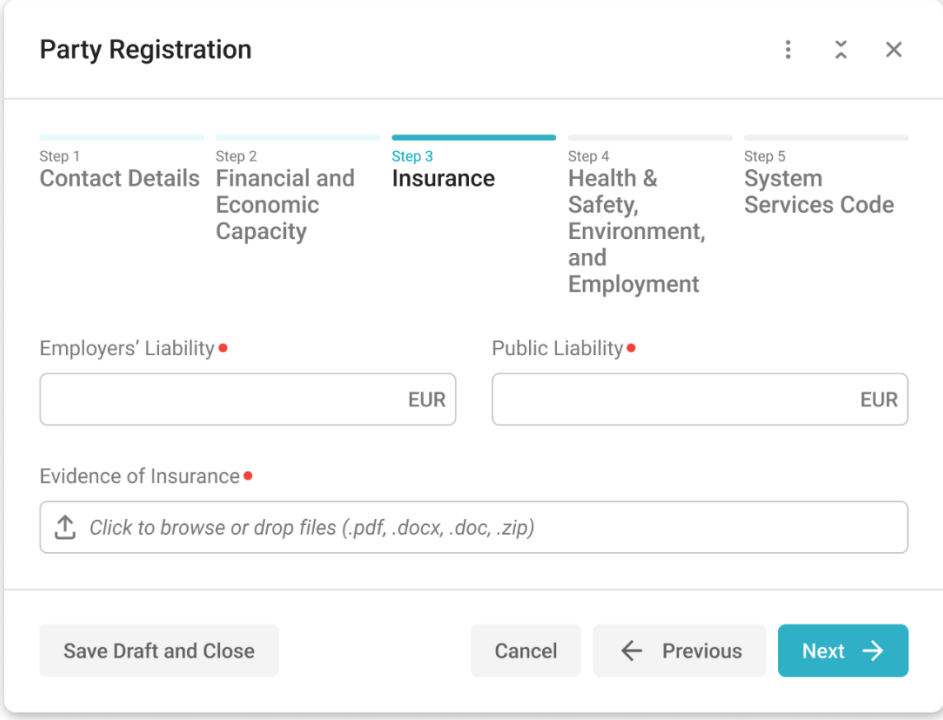
 *Figure 38 - Party registration step 2d*

Form description (required fields are marked with * - checkbox):

- Confirm Tax Clearance Declaration * - checkbox
- Tax Compliance Evidence Link
 - User shall insert a link to a webpage where evidence is available via electronic systems.

Form Step 3: Insurance

This section requires information on the Party insurance in a specified amount including evidence.



Party Registration

Step 1 Contact Details Step 2 Financial and Economic Capacity **Step 3 Insurance** Step 4 Health & Safety, Environment, and Employment Step 5 System Services Code

Employers' Liability * Public Liability *

EUR EUR

Evidence of Insurance *

Click to browse or drop files (.pdf, .docx, .doc, .zip)

Save Draft and Close Cancel Previous Next

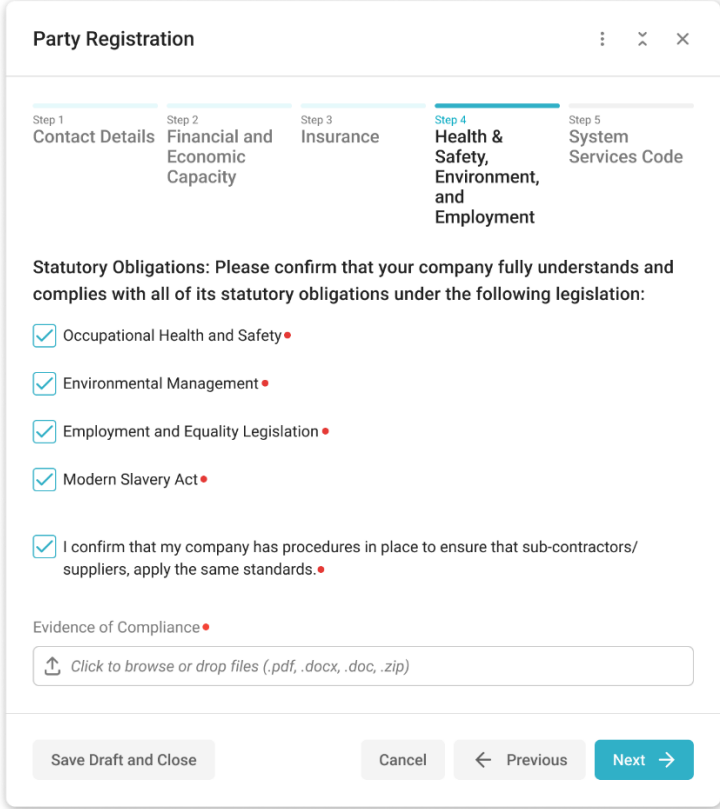
 **Figure 39 - Party registration step 3**

Form description (required fields are marked with * symbol):

- Employers' Liability [*referenceCurrency*] * - in GBP or EUR based on the jurisdiction.
- Public Liability [*referenceCurrency*] * - in GBP or EUR based on the jurisdiction.
- Evidence of Insurance * - .pdf, .docx, .doc, .zip attachment
 - This field is **required** for new registration, for update this field is **optional**

Form Step 4: Health & Safety, Environment, and Employment

This section requires user to comply with all of its statutory obligations under legislation.



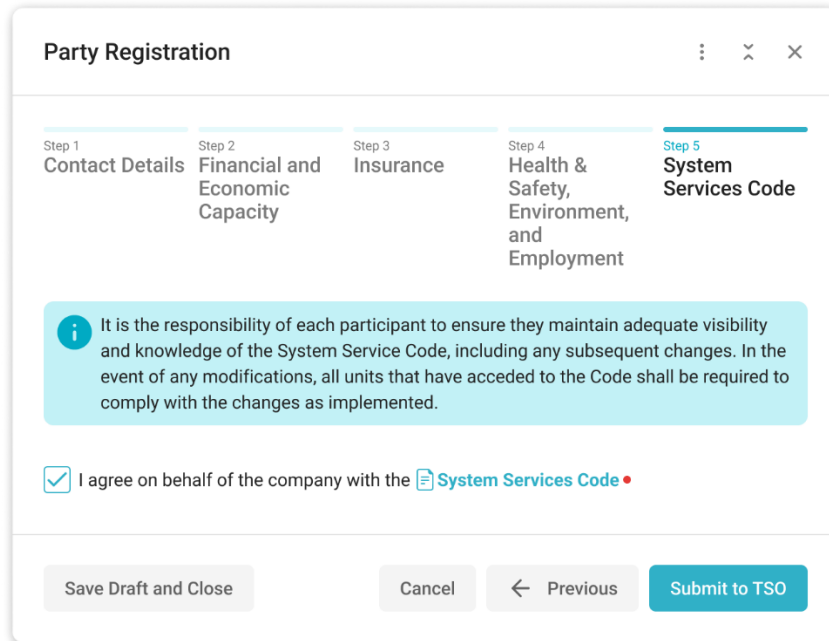
 **Figure 40 - Party registration step 4**

Form description (required fields are marked with * symbol):

- Occupational Health and Safety * - checkbox
- Environmental Management * - checkbox
- Employment and Equality Legislation * - checkbox
- Modern Slavery Act * - checkbox
- Confirm Standard Procedures * - checkbox
- Evidence of Compliance * - upload file with .pdf, .docx, .doc, or .zip format

Form Step 5: System Services Code

This part of the form only needs the user to confirm the System Services Code, which is linked in the text for quick navigation to the content of the System Services Code.



 **Figure 41 - Party registration step 5**

Form Action Buttons

The User can interact with the form in the following ways:

- Cancel – cancels the form without saving
- Previous – navigate to the previous step
- Next – navigate to the next step
- Save Draft and Close – saves data and closes the form. The User may return to the draft later and continue working on the registration
- Submit for Internal Approval – only displayed to Service Provider Operator. Moves the registration to the Service Provider Approver, who can review the data, adjust it and then submit it to the TSO.
- Submit to TSO – only displayed to Service Provider Approver. Submits the registration to TSO, which means that the Service Provider roles cannot make changes anymore, unless the TSO requests an update.

The results of the form submission are sent as a notification to the User's email.

9.1.9 Unit Registration

Authorised roles: Service Provider Operator, Service Provider Approver

This use case is intended for Service Providers and enables authorised users to submit an application for Unit registration. Multiple Unit(s) can be registered for one Party. The applicants can submit the form only for their own Party assigned to them in User Management.

The entry form also serves as an update form. The User can save the form and return to it later without losing data, until the registration is submitted to the TSO.

How to access:

1. Open the system in your web browser.
2. Click on "Unit Registrations" in the system menu navigation.
3. Click on "Create New Registration" button located above the list of registrations on the right side.
4. Fill out the form as described below.
 1. You can save data by the "Save Draft and Close" button, and return to the form later.
5. Confirm form and check the success notification pop-up.
 1. Depending on the User Role, the Confirm button acts differently:
 1. For Service Provider Operator, it is "Submit for Internal Approval" which submits the form to be reviewed by the Approver of the Party. The Service Provider Operator cannot make changes anymore.
 1. For Service Provider Approver, it is "Submit to TSO" which submits the form to TSO for approval. The Service Provider roles cannot make changes anymore, unless the TSO requests an update.

Unit Registration

Party

GreenTech Solutions Ltd.

Unit ID

Unit Name

Site Name

☐

 I confirm that there is a corresponding registered unit in the Balancing Market (a prerequisite to register a unit for the DASSA).

Grid Coordinates of the Connection Point (Easting, Northing)

Metering Reference

Jurisdiction

Please provide the following documents as Unit Requirements Evidence below:

• Info box above the file upload area will display the text in bullets as follows plus a longer tooltip description where specified:

• Site Specific Wiring Certificate*

• Evidence of Minimum Capability*

• Proven Technology Confirmation*

• Connection Point Capability Confirmation*

• Final Operational Notification*

• Operational Certificate*

• ION Certificate*

• TSO-approved System Services Test Report

• Distribution Operator Notification

• Monitoring Equipment Evidence

Unit Requirements Evidence

Click to browse or drop files

Safe Draft and Close

Cancel

✓ Submit to TSO

 Figure 42 - Unit registration

9.1.9.1 Unit Registration process — Service Provider view

- Service Provider Operator or Approver creates the application (optionally saving a draft in state Initial).
- Service Provider Operator submits for internal approval (state In Progress) — the form becomes read-only for the Operator.
- Service Provider Approver reviews and submits to TSO (state Submitted) – Service Provider users can no longer edit unless the TSO requests an update.
- TSO reviews and approves once the relating Party Registration is approved.
- Multiple Unit Registrations may run in parallel for different Units. Only one Unit Registration per Unit can be in progress at a time.
- Upon approval (state Approved), the Unit becomes Active and may be qualified via Qualification Application.

9.1.9.2 Submitting Unit Registration

Form description (required fields are marked with * symbol):

- Party * - is prefilled by User's assigned Party and cannot be changed (unless the user has multiple Party assignments)
- Unit ID * - Balancing Market Unit ID, e.g.: GU_123456
- Unit Name *
- Site Name *
- Unit Registered in the Balancing Market * - checkbox to acknowledge
- Grid Coordinates of the Connection Point (Easting, Northing) * - two six-digit numeric values separated by a comma (e.g. 315904, 234671)
- Metering Reference *
- Jurisdiction * - set as the Party Jurisdiction
- Unit Requirements Evidence * - .pdf/.doc/.docx/.zip attachment
 - This field is **required** for new registration, for update, this field is **optional**
 - This field requires the uploading of several documents with the required ones marked by a * symbol:
 - Site Specific Wiring Certificate*
 - Evidence of Minimum Capability*
 - Proven Technology Confirmation*
 - Connection Point Capability Confirmation*
 - Final Operational Notification*
 - Operational Certificate*
 - ION Certificate*
 - TSO-approved System Services Test Report
 - Distribution Operator Notification
 - Monitoring Equipment Evidence
 - A brief description of each of the documents is available in the on-screen tooltip.
- Cancel – closes the form without saving data
- Save Draft and Close – saves data and closes the form

- Submit for Internal Approval – only displayed to Service Provider Operator. Moves the registration to the Service Provider Approver, who can review the data, adjust it and then submit it to the TSO.
- Submit to TSO – only displayed to Service Provider Approver. Submits the registration to the TSO, which means that the Service Provider roles cannot make changes anymore, unless TSO requests an update.

The results of the form submission are sent as a notification to the User's email.

9.1.10 Qualification Application

Authorised roles: Service Provider Operator, Service Provider Approver

This use case is intended for Service Providers and enables authorised users to submit an application for qualification of their Unit(s). The applicants can submit the form only for their own Party assigned to them in the User Management. Each Unit may qualify for one or more System Service Product(s) within one application.

The entry form also serves as an update form. The User can save the form and return to it later without losing data, until the qualification application is submitted to the TSO.

How to access:

1. Open the system in your web browser.
2. Click on "Qualification Applications" in the system menu navigation.
3. Click on "Create New Application" button located above the list of qualification applications on the right side.
4. Fill out the form as described below.
 1. You can save data by the "Save Draft and Close" button, and return to the form later.
5. Confirm form and check the success notification pop-up.
 1. Depending on the User Role, the Confirm button acts differently:
 1. For Service Provider Operator, it is "Submit for Internal Approval" which submits the form to be reviewed by the Approver of the Party. The form becomes read-only for the Operator
 2. For Service Provider Approver, it is "Submit to TSO" which submits the form to TSO for approval. Service Provider users can no longer edit unless the TSO requests an update.

9.1.10.1 Qualification Application process — Service Provider view

- Service Provider Operator or Approver creates the application (optionally saving a draft in state Initial).
- Service Provider Operator submits for internal approval (state In Progress).
- Service Provider Approver reviews and submits to TSO (state Submitted).
- TSO reviews; may request updates (Pending Updates), initiate testing (In Testing), or approve/reject.
- During In Testing, the Service Provider Approver submits testing evidence as attachments.
- Upon approval, TSO selects which System Service Products are qualified; others are rejected. Qualified products are recorded in the System Services Register.
- Only one ongoing Qualification Application per Party, Unit, and System Service Product combination. Multiple parallel applications are allowed for different product sets.
- Re-qualification for an already qualified product updates the System Services Register (e.g. eligible capacity).

The form consists of the following parts:

- **Step 1: Qualification Application**
 - **Section 1 - General Party and Unit Information**
 - **Section 2 - Technology Type Details**
 - **Section 3 - Operating Mode Details**
 - **Section 4 - Eligible Capacity per System Service Product**
- **Step 2: Reserve Characteristics Parameters**
- **Step 3: Qualification Pack**
- **Form Action Buttons**

Form Qualification Application

Figure 43 - Qualification application step 1

Section 1 - General Party and Unit Information

Form description (required fields are marked with * symbol):

- Party * - is prefilled by User's assigned Party and cannot be changed (unless the user has multiple Party assignments).
- Unit * - list of available Units of the Party. Cannot be edited if this form is being used for an update of existing details.

Section 2 - Technology Type Details

Form description (required fields are marked with * symbol):

- Technology Type *
 - One Technology Type is displayed as default, displayed as "Primary Technology Type" (next added item is named "Secondary Technology Type" and next one "Tertiary Technology Type")
 - For each Technology Type, the user specifies the Technology Type(from the select box) – there can only be only one of each Technology Type across Primary, Secondary, Tertiary
 - User may select a maximum of three "Technology Type"(s), and at least one
- Add Technology Type select box
- Remove Technology Type – removes the last Technology Type

Section 3 - Operating Mode Details

Form description (required fields are marked with * symbol):

- For units with multiple operating modes, the set of applicable operating modes need to be selected:
 - Combined Cycle Mode and Open Cycle Mode
 - Emulated Inertia Mode and non-EI mode

Section 4 - Eligible Capacity per System Service Product

Form description (required fields are marked with * symbol):

- System Service Products * - the products supported by the system are displayed, such as POR Up and POR Down. Users should mark in the corresponding checkbox to add each product to the qualification.
- Eligible Capacity [MW] * - Mandatory value for each checked item from the "System Service Products"

Form Step 2: Reserve Characteristics Parameters (per Technology Type, and if applicable Operating Mode)

This step is displayed based on the number of Technology Types as selected in Section 2: Technology Type Details and Operating Modes in Section 3: Operating Mode Details :

- Separate tabs for each selected Technology Type, and if applicable Operating Mode, combination are displayed

Form description for each tab (required fields are marked with * symbol):

- This is where the respective reserve capability curve is defined
- System Service Product (column header) - one for each item from the selected "System Service Products" from Step 1
- Rows of coefficients for specification - RMX, GMN, R0, R1, R2, DELTA1, DELTA2, DELTA3, BETA
 - User must fill in values of coefficients for each applicable one, the non-applicable remain with default value 0.

Qualification Application

Qualification Application

Primary Technology Type

Biomass - Combined Cycle Mode

Primary Technology Type

Biomass - Emulated Inertia Mode

Secondary Technology Type

Distillate - Combined Cycle Mode

Secondary Technology Type

Distillate - Emulated Inertia Mode

Qualification Pack

Reserve characteristic parameters on Primary Technology Type - Biomass - Combined Cycle Mode

System Service Product	FFR1D	FFR2U	PORU	SORU
RMX	0	0	0	0
GMN	0	0	0	0
R0	0	0	0	0
R1	0	0	0	0
R2	0	0	0	0
DELTA1	0	0	0	0
DELTA2	0	0	0	0
DELTA3	0	0	0	0
BETA	0	0	0	0

Save Draft and Close

Cancel

Previous

Next

 Figure 44 - Qualification application step 2

Form Step 3: Qualification Pack

Form description (required fields are marked with * symbol):

- Please confirm the Qualification Pack * - User confirms that qualification application is in accordance with the latest published Qualification Pack published on the website of the TSO which is linked in the text for quick navigation to the website.

Form Action Buttons

The User can interact with the form in the following ways:

- Cancel – cancels the form without saving
- Previous – navigate to the previous step
- Next – navigate to the next step
- Save Draft and Close – saves data and closes the form. User may return to the draft later and continue working on the qualification application
- Submit for Internal Approval – only displayed to the Service Provider Operator. Moves the registration to the Service Provider Approver, who can review the data, adjust it and then submit it to the TSO.
- Submit to TSO – only displayed to the Service Provider Approver. Submits the registration to the TSO, which means that the Service Provider roles cannot make changes anymore, unless TSO requests an update.

The results of the form submission are sent as a notification to the User's email

9.2 DASSA Procurement

9.2.1 Introduction

9.2.1.1 Purpose of this guide

This guide explains how Service Providers use the FASS platform to participate in the **DASSA** (Day-Ahead System Services Auction) module.

As a Service Provider, you can use the DASSA module to:

- View DASSA auctions and the Auction Information Pack
- Submit and maintain DASSA offers for your Units during the DASSA offer gate window
- Submit forecast capability data for your Units
- View published DASSA results
- View confirmed DASSA orders for your Units

This guide provides step-by-step instructions for each of these activities.

9.2.1.2 Key concepts and terminology

Term	Description
Trading Day	• The calendar day for which the DASSA auction is held
Trading Period	• A time interval within the Trading Day (currently 30 minutes)
Party	• Your organisation as registered in FASS (Party ID & Jurisdiction)
Unit	• Generation, demand, and other Service Provider assets belonging to your Party
System Service Product	• A specific system service for which a Unit may be qualified (e.g. POR Up, POR Down)
Zone	• A geographic or jurisdictional area associated with an auction requirement
Quality Category	• A quality classification applied to an auction requirement
Auction requirement combination	• A unique combination of System Service Product, Zone, and Quality Category defined for an auction
DASSA offers gate	• The time window during which offers can be submitted; the gate opens and closes automatically at scheduled times
Offer segment	• One price-quantity pair within an offer; up to 10 segments can be submitted per trading period
Divisibility	• Indicates whether an offered quantity may be partially accepted during evaluation, or must be fully accepted
Offers gate	• The time window during which DASSA offers can be submitted
Auction Information Pack	• The published package of auction parameters made available before offers submission
Confirmed DASSA Order	• The primary output of a completed DASSA auction, assigning cleared volume to your Unit
Public results	• Aggregated auction outcomes visible to all participants, including clearing prices and volume insufficiency if applicable
Private results	• Party-specific cleared volumes and prices for your Units
Forecast Capability	• Expected delivery capacity communicated by a Service Provider to the TSO

Forecast Period	For submission of Forecast Capability – the time interval for which DASSA Order data is available and ending 1 hour before the start of the Trading Period
Insufficiency volume	Volume by which cleared quantity falls short of the minimum requirement
Transaction ID	Unique identifier assigned to each successful offer submission

9.2.1.3 Who can use the DASSA module

Two Service Provider roles have access to the DASSA module:

Role	Access
Service Provider Reader	Read-only access to data relating to your own Party
Service Provider Operator	Read access plus the ability to submit and update DASSA offers and forecast capability for your own Party

9.2.1.4 Prerequisites for participation

Before you can participate in DASSA, the following must be in place:

- Your **Party** is registered and approved/active in FASS
- Your **Units** are registered and approved/active

Your Units are **qualified** for the relevant System Service Products with effective dates that include the Trading Day (as recorded in the System Services Register)

- Neither your Party nor your Units are **suspended** from DASSA provision
- You can only view and manage data relating to **your own Party**

Only Parties with registered Units that have successfully qualified for System Service Products may participate in DASSA.

9.2.2 Getting Started

9.2.2.1 Accessing the DASSA module

The DASSA module is accessed from the FASS system menu. The main screens available to Service Providers are:

Screen	Purpose
DASSA Auctions	View the list of DASSA auctions and open auction details
DASSA Offers Overview	View, enter, and update DASSA offers (also reachable from a specific auction). Data entry and update is only possible when the applicable gate window is open
Forecast Capability Overview	View, enter, and update forecast capability values. Data entry and update is only possible when the applicable forecast capability window is open
DASSA Orders	- View confirmed DASSA orders after results are published - Updates to DASSA orders including Secondary Trades, Bilateral Trades, and Lapsing will be available also.
DASSA Results	View published auction results (also reachable from a specific auction)

9.2.2.2 Role permissions summary

Activity	Service Provider Reader	Service Provider Operator
----------	-------------------------	---------------------------

View DASSA auctions	• Yes	• Yes
View Auction Information Pack	• Yes	• Yes
View DASSA offers	• Yes (own Party)	• Yes (own Party)
Enter/update DASSA offers	• No	• Yes (when offers gate is open)
Copy previous DASSA offers	• No	• Yes (when offers gate is open)

9.2.3 The DASSA Process — Service Provider View

9.2.3.1 End-to-end timeline (Happy Day Scenario)

As a Service Provider, your involvement in the daily DASSA cycle follows this sequence:

1. **Before D-19 Auction Created** — auction parameters become available; you can review the auction definition
2. **D-19 Offers gate opens** — you can begin submitting offers
3. **You may submit offers** — enter or update offers for your qualified Units and System Service Products
4. **D-1 10:00 Auction Information Pack published** — auction parameters become available; you can review the auction definition
5. **You may submit offers** — enter or update offers for your qualified Units and System Service Products
6. **D-1 15:30 Offers gate closes** — no further offer submissions or changes are accepted
7. **By D-1 16:00 Evaluation and approval** — the auction is evaluated and results are approved (no action required from you)
8. **From D-1 16:00 Final results published** — confirmed results and DASSA orders become available
9. **From D-1 16:00** You can submit **forecast capability** data for the relevant Forecast Period

9.2.3.2 DASSA auction business states

Each DASSA auction progresses through business states. The table below explains what each state means for your work:

State	What it means for you
Scheduled	• The auction is being prepared. • You can submit offers once the offers gate is open.
Requirements Specified	• Auction parameters including volume requirements are set. Awaiting publication of the Auction Information Pack.
Published	• The Auction Information Pack is available. • You can continue to submit offers until the offers gate closes.
Evaluated	• The auction has been evaluated. Awaiting final results publication.
Final Results Published	• Confirmed results and DASSA orders are available for viewing.
Cancelled	• The auction has been cancelled. Any offers you submitted are no longer valid. You may need to submit new offers on a replacement auction.
Failed	• DASSA fallback has been initiated. No valid DASSA results exist for this Trading Day.

9.2.3.3 Timing and gates

Auction Information Pack

The Auction Information Pack is published at a scheduled time once the auction has been configured and volume requirements specified. After publication, it is available in the FASS platform (GUI and API). The pack includes the auction identifier, timeframe, minimum requirement values, valuation parameters, price caps and floors, offer limits, and other parameters you need to prepare your offers.

Offers gate

You can submit or update DASSA offers, via the GUI or API, only while the **offers gate is open**. The gate opens and closes automatically at the times defined for each auction. When the gate is open, a green **Gate Open** badge is displayed on the DASSA Offers Overview screen and on the auction list.

Offers are accepted only when:

- The auction is in an active state (not cancelled), **and**
- The current time is within the gate window (gate opening time ≤ now < gate closure time)

Results publication

Confirmed DASSA results and orders become available once the auction reaches the **Final Results Published** state, at the configured results publication time.

9.2.3.4 Notifications you receive

The system makes notifications available to Service Provider Operators within your Party for the following events:

Event	Notification summary
DASSA offers stored	Offers for a Unit and System Service Product have been stored, with a transaction ID
DASSA offers copied	Offers from the previous trading day have been copied for a Unit; lists any products with no data to copy
DASSA offers store failed	Offer submission failed for a Unit/System Service Product or Party
DASSA offers copy failed	Copy Previous operation failed for a Unit

Forecast capability updates do not generate notifications; success or failure is shown as an on-screen message upon submission.

9.2.4 Viewing DASSA Auctions

9.2.4.1 Opening the DASSA Auctions list

Purpose: View all DASSA auctions and navigate to auction details, offers, or results.

Preconditions: You are logged in with a Service Provider Reader or Service Provider Operator role.

Steps:

1. Open the **DASSA Auctions** screen from the system menu.
 2. The system displays the DASSA Auctions list. If no auctions match your filters, the list is empty.
 3. Use the **Filter** section to narrow the list:
 - Select a **Business State** (filters marked with a red star are mandatory)
 - Set any additional filter criteria as needed
 4. Click **Apply Filters** to load matching auctions, or **Reset Filters** to restore defaults.
 5. Review the auction table. For each auction you can see:
 - Trading Day
 - Business State (with a green **Gate Open for Offers Entering** label when the offers gate is currently open)
 - Other auction summary information
- Click the **Detail** button on a row to open the **DASSA Auction Detail** screen.

Expected outcome: The auction list displays auctions matching your filter criteria.

9.2.4.2 Viewing auction detail

Purpose: Review the parameters and configuration of a specific DASSA auction.

Preconditions: At least one DASSA auction exists.

Steps:

1. From the DASSA Auctions list, click **Detail** on the desired auction row.
2. The **DASSA Auction Detail** screen opens, showing the **Auction Parameters** tab with information such as:
 - Trading Day
 - Business State (with a green **Gate Open for Offers Submission** label when the gate is open)
 - Minimum Offer Quantity Step [MW]
 - Minimum Offer Price Step (per MW)
 - Offer Price Floor and Offer Price Cap (switchable between EUR and GBP using the currency toggle button)
 - Other auction parameters relevant to your offer preparation
3. Review the parameters you need for offer submission.

Expected outcome: You can read the auction parameters needed to prepare valid offers.

9.2.4.3 Navigating to related screens

From the DASSA Auctions list or DASSA Auction Detail screen, use the action menu to navigate to related screens:

Action	When available	Description
DASSA Offers	• Auction is active (not cancelled)	• Opens the DASSA Offers Overview for this auction
DASSA Results	• Auction is in Final Results Published state	• Opens the DASSA Results screen for this auction

To open DASSA Offers:

On the DASSA Auctions list, click the **More Options** icon (drop-down) on the auction row and select **DASSA Offers**.

— or —

On the DASSA Auction Detail screen, click **DASSA Offers**.

To open DASSA Results:

On the DASSA Auctions list, click the **More Options** icon and select **DASSA Results**.

— or —

On the DASSA Auction Detail screen, click **DASSA Results**.

Expected outcome: You are taken to the DASSA Offers Overview or DASSA Results screen for the selected auction.

9.2.4.4 Understanding the Auction Information Pack

The **Auction Information Pack** is published when the auction reaches the **Published** business state. It contains the finalised auction information, including:

- Auction identifier and timeframe
- Minimum requirement values per auction requirement combination (Product + Zone + Quality Category + Trading Period)
- Valuation parameters

Price caps and floors (Bid Price Cap/Floor)

- Offer limits and other auction constraints

Accessing the pack in the GUI

The auction parameters and published information are available on the **DASSA Auction Detail** screen once the auction has been published.

Accessing the pack via API

Refer to section 10.6.3 DASSA Auction Information Pack (to Service Provider) for details on API retrieval of the Auction Information Pack.

9.2.5 Submitting DASSA Offers

9.2.5.1 Overview

DASSA offers are price-quantity bids that can be submitted for Units during the offers gate window. Key points:

- **Who can submit:** Service Provider Operator (Service Provider Reader can view only)
- **When:** Only while the offers gate is open and the auction is in an active state
- **Scope:** Your own Party only; only Units qualified for System Service Products defined in the auction
- **Structure:** One offer per Unit, System Service Product, and Trading Period, with up to **10 segments** (price-quantity pairs) each
- **Currency:** Offers are entered in EUR or GBP depending on your Party's jurisdiction
- **Divisibility:** Each segment has a divisibility flag indicating whether partial acceptance is allowed
- **Versioning:** Each successful submission replaces the previous version for the same auction, Unit, System Service Product, and Trading Period. A unique **transaction ID** is assigned to each submission
- **Cancelling an offer:** Offers cannot be deleted. To cancel, submit **zero values** for the offer (via screen: use **Remove Offer**; via API or file upload: submit zero quantities). Zero-quantity offers are disregarded during DASSA auction evaluation
- **Channels:** Screen, file upload (see Manual File Upload chapter), or API

The DASSA Offers Overview screen remains available in read-only mode even when the gate is closed.

9.2.5.2 Viewing DASSA offers

Purpose: Review submitted offers for your Units.

Preconditions: A DASSA auction exists. You have access to at least one Unit under your Party.

Steps:

1. Open the **DASSA Offers Overview** screen:
 - From the system menu, or
 - From a DASSA auction via **DASSA Offers** (see Section 9.2.4.3)
2. The screen opens in **read-only** mode, showing auction summary information including Business State and gate times (Gate Opening Time and Gate Closure Time in GMT/BST). A green **Gate Open** badge appears when the gate is currently open.
3. To select which Party and Unit to view, click the **More Options** drop-down and select **Party and Unit**:
 - **Party** — pre-selected to your Party (mandatory)
 - **Unit** — select the Unit to display (mandatory)
 - Click **Confirm** to reload the screen
4. If your Party or Unit is suspended, a red **Suspended** badge is displayed next to the respective field.
5. Review the tabs across the top of the screen — one tab per **System Service Product** defined in the auction for which the selected Unit is qualified.

6. If the Unit is not qualified for any product in the auction, the message *"The selected unit is currently not qualified for any system service product defined in the DASSA auction."* is displayed.
7. For each tab, review the time series table showing offer data per Trading Period and Segment:
 - Offered **Quantity** [MW]
 - Offered **Price** (in EUR or GBP per MW, based on your jurisdiction)
 - **Divisibility** flag

Expected outcome: You can view all submitted offer data for the selected Unit and System Service Product.

9.2.5.3 Entering offers via the GUI

Purpose: Enter or update DASSA offers for a specific Unit and System Service Product.

Preconditions:

- You are logged in as **Service Provider Operator**
- The offers gate is open
- The auction is in an active state (not cancelled, finalised)
- Your Party and Unit are not suspended
- The Unit is qualified for the selected System Service Product

Steps:

1. Open the **DASSA Offers Overview** screen and select the desired **Party** and **Unit** (see Section 9.2.5.2).
2. Click the tab for the **System Service Product** you want to update.
3. Click **Update** to enter **on-screen edit mode** for the current tab only.
 - Only the currently displayed table (Unit + System Service Product combination) becomes editable

Other tabs remain read-only; multiple users can edit different tabs simultaneously

4. Enter or modify offer data for each Trading Period:
 - For each segment (1–10), enter **Offered Quantity** [MW], **Offered Price**, and set the **Divisibility** flag
 - You may add or remove segments within the 10-segment limit
5. To remove an entire offer for this Unit and System Service Product, click **Remove Offer**:
 - A warning is displayed; the removal takes effect only after you save

On save, all segments for the trading day are cleared for this combination

6. Click **Save Changes** to submit.
 - The system validates your input (formal and business rules)
 - The system verifies that offers are not being modified by another user, to prevent concurrent updates and data inconsistency.
 - On success, the message *"DASSA offers stored."* is displayed
 - Edit mode closes and the screen returns to read-only overview
7. To discard changes without saving, click **Cancel** (or navigate away — you will be prompted to confirm if unsaved changes exist).

Navigating between tabs in edit mode:

If you switch tabs while in edit mode, a confirmation dialog appears:

- **Leave without saving** — discards changes and opens the selected tab
- **Stay** — returns to the current tab

Expected outcome: Your offers are stored and a notification is sent to Service Provider Operators in your Party. A transaction ID is recorded.

Common errors:

Message	Cause
<i>DASSA offers gate is not yet open.</i>	Gate opening time has not been reached
<i>DASSA offers gate is already closed.</i>	Gate closure time has passed
<i>DASSA offers storing failed.</i>	Validation or technical error — see Section 9.2.5.7
<i>DASSA offers are currently being modified by another user. Therefore, the submission is locked for modifications to avoid possible discrepancies.</i>	Another user holds the edit lock

9.2.5.4 Copy Previous offers

Purpose: Copy offer values from the previous trading day's DASSA auction for the currently displayed Unit.

Preconditions:

- You are logged in as **Service Provider Operator**
- The offers gate is open
- A DASSA auction existed on the previous trading day and was not cancelled
- The Unit is qualified for at least one System Service Product in the current auction

Steps:

- Open the **DASSA Offers Overview** screen and select the desired **Party** and **Unit**.
- Click the **More Options** drop-down and select **Copy Previous Offers**.
- A confirmation dialog appears:
Do you want to copy the DASSA offer values from the DASSA auction from the previous trading day for this unit? It will overwrite any stored values for all system service products.
- Click **Copy Values** to proceed, or **Cancel** to abort.
- The system copies offers from the previous trading day for all qualified System Service Products that match products in the current auction. Values are stored immediately (not just pre-filled).
- On success, the message "DASSA offers copied." is displayed.
- If some products had no data in the previous auction, a notification lists the affected System Service Products. You can amend copied values by opening edit mode on each tab (see Section 9.2.5.3).

Expected outcome: Offers from the previous trading day are stored for the selected Unit. You can review and amend them in edit mode.

Common errors:

Message	Cause
<i>DASSA offers gate is not yet open. / DASSA offers gate is already closed.</i>	Gate is not open
<i>DASSA auction for the previous trading day does not exist or has been cancelled.</i>	No valid previous auction
<i>No matching DASSA offers for previous trading day have been found.</i>	Previous auction exists but has no matching offers
<i>Unit ... is not qualified for any system service product defined in the DASSA auction.</i>	Unit has no eligible products
<i>Party ... is suspended from DASSA participation. / Unit ... is suspended from DASSA participation.</i>	Suspension active
<i>DASSA offers copying for unit ... has failed ...</i>	Validation failure during copy

9.2.5.5 Submitting offers via file upload

To submit DASSA offers in bulk via file upload, refer to the **Manual File Upload** chapter of this user guide.

The uploaded file uses the same format and validations as API submission. Offers may be submitted for one Party in one jurisdiction per submission.

9.2.5.6 Submitting offers via API

Refer to section 10.6.1 DASSA Offers for details on API submission of DASSA offers.

Note: To cancel an offer via API or file upload, submit a single PQ pair with a zero quantity value for the offer. It is not possible to remove an offer entirely — only to zero out the quantities.

9.2.5.7 Validation rules and common errors

The system validates all offer submissions against business rules and auction parameters. The following errors may be displayed:

Gate and auction state

Error message	Description
<i>DASSA offers gate is not yet open.</i>	Submission attempted before gate opening time
<i>DASSA offers gate is already closed.</i>	Submission attempted after gate closure time

Party and authorisation

Error message	Description
<i>Party ... is not valid.</i>	Party record not found
<i>Party ... is not effective.</i>	Party is outside its effective date range
<i>Party ... is suspended from DASSA provision.</i>	Party is suspended
<i>User is not authorised to submit DASSA offers for party ...</i>	You are not assigned to this Party
<i>DASSA offers are submitted for multiple parties. The offers may be submitted only for one party in one jurisdiction at a time.</i>	Bulk submission contains multiple Parties

Unit

Error message	Description
<i>DASSA offers are submitted for a unit that is not valid.</i>	Unit record not found
<i>Unit ... is not effective.</i>	Unit is outside its effective date range
<i>Unit ... is suspended from DASSA provision.</i>	Unit is suspended
<i>User is not authorised to submit DASSA offers for the unit The unit is not assigned to party ...</i>	Unit does not belong to your Party
<i>Unit ... is not qualified for system service product ...</i>	Unit lacks qualification for the product

Offer content

Error message	Description
<i>Offered quantity for unit ... exceeds unit's eligible capacity (... MW) for system service product ...</i>	Total quantity across segments exceeds eligible capacity
<i>Offered quantity for unit ... exceeds maximum eligible capacity (... MW) for system service product For system service products with hierarchy, unit's eligible capacity must be treated as cumulative.</i>	Hierarchy constraint violated
<i>Offered quantity is not submitted in accordance with the DASSA Auction definition. Minimum offer quantity step is ... MW.</i>	Quantity step between segments is too small
<i>Offered price is not submitted in accordance with the DASSA auction definition. Minimum offer price step is .../MW.</i>	Price step between segments is too small
<i>Offered price is not between the DASSA offer price floor (.../MWh) and offer price cap (.../MWh).</i>	Price is outside allowed range
<i>Combinations of unit, system service product and segment are not unique. Only one offer can be submitted for a unit and system service product for up to 10 segments (P-Q pairs).</i>	Duplicate segment numbers submitted

Concurrency

Error message	Description
<i>DASSA offers are currently being modified by another user. Therefore, the submission is locked for modifications to avoid possible discrepancies.</i>	Another submission is in progress

When multiple validations fail, error messages are aggregated and displayed at the top of the form. Individual cells that fail validation are highlighted with a red callout.

9.2.6 Submitting Forecast Capability

9.2.6.1 Overview

Forecast capability data communicates your expected delivery capacity to the TSO for your Units and System Service Products.

Key points:

- **Who can submit:** Service Provider Operator (Service Provider Reader can view only)
- **When:** Within the forecast capability entry window (see Section 9.2.6.3)
- **Scope:** Your own Party and Units only; qualified System Service Products only
- **Independence:** Forecast capability submission is independent of the DASSA auction lifecycle
- **Versioning:** All submission versions are retained with the latest successful submission taking precedence; timestamps are recorded in the audit log
- **Cancelling values:** Forecast capability values cannot be deleted — submit **zero** to clear a value
- **Channels:** Screen, file upload (see Manual File Upload chapter), or API

Entry window rules

Forecast capability values can be entered only within the gate window defined by system configuration:

- An **offset** (e.g. one hour from the current time, rounded up to the nearest Trading Period) determines the earliest Trading Period you can modify
- A **time specification** (e.g. 11:00 GMT/BST) determines how far into the future you can enter values:
- If the current time is **before** the configured time: values can be entered from the gate opening until the **end of the current trading day**
- If the current time is **after** the configured time: values can be entered from the gate opening until the **end of the next trading day**

Example:

- Current time: 09:10 (GMT/BST), resolution 30 minutes → values can be entered from 10:30 until end of current trading day
- Current time: 16:40 (GMT/BST), resolution 30 minutes → values can be entered from 18:00 until end of next trading day

9.2.6.2 Viewing forecast capability

Purpose: Review submitted forecast capability values for your Units.

Preconditions: You are logged in with a Service Provider Reader or Service Provider Operator role.

Steps:

1. Open the **Forecast Capability Overview** screen from the system menu.
2. Set the **Filter** parameters:
 - **Time Interval** — select the period to display (mandatory; defaults from current time plus the configured offset, rounded up to the nearest Trading Period)
 - **Party** — pre-selected to your Party (mandatory)
 - **Unit** — select the Unit to display (mandatory; only non-suspended Units are listed)
3. Click **Apply Filters**.
4. Review the time series table showing **Forecast Capability [MW]** per System Service Product tab (one tab per qualified product for the selected Unit and time interval).
5. If the Unit is not qualified for any product in the selected interval, the message *"The selected unit is currently not qualified for any system service product for the selected time interval."* is displayed.

Expected outcome: Forecast capability values are displayed for the selected Party, Unit, and time interval.

9.2.6.3 Entering forecast capability via the screen

Purpose: Enter or update forecast capability values for a Unit.

Preconditions:

- You are logged in as **Service Provider Operator**
- Your Party and Unit are not suspended
- The time interval you want to modify is within the allowed entry window

Steps:

1. Open the **Forecast Capability Overview** screen and set the **Filter** to the desired Party, Unit, and Time Interval (see Section 9.2.6.2).
2. Click **Update** to enter **on-screen edit mode**.
 - If some Trading Periods in the interval are past the gate closure (not yet editable), a warning block is displayed:

The gate for forecast capability modifications is closed for Trading Periods until [time] (GMT/BST). Only Trading Periods where the gate is open for modifications will be updated.

3. Enter or modify **Forecast Capability [MW]** values in the editable cells (only Trading Periods where the gate is open are editable).
4. Click **Save Changes**.
 - The system validates your input
 - On success: "*Forecast Capability updated.*" is displayed (or a note if only part of the interval was updated due to gate closure timing)
 - Edit mode closes
5. To discard changes, click **Cancel**.

Expected outcome: Forecast capability values are stored for the editable Trading Periods in the selected interval.

Common errors:

Message	Cause
<i>No data found.</i>	No forecast capability data exists for the selected filters
<i>Forecast Capability update failed.</i>	Validation or technical error
<i>Forecast capability values are currently being modified by another user. Therefore, the submission is locked for modifications to avoid possible discrepancies.</i>	Concurrent edit lock
<i>The gate for forecast capability modifications is already closed for Trading Periods until [time] (GMT/BST).</i>	Attempted to submit values for Trading Periods past the gate
<i>The gate for forecast capability modifications is open only for Trading Periods until [time] (GMT/BST). Trading Periods past the gate closure cannot be updated at the moment.</i>	Submitted interval extends beyond allowed window

9.2.6.4 Submitting forecast capability via file upload

To submit forecast capability in bulk via file upload, refer to the **Manual File Upload** chapter of this user guide.

9.2.6.5 Submitting forecast capability via API

Refer to section 10.6.2 Forecast Capability for details on API submission of forecast capability.

9.2.6.6 Validation rules and common errors

Party and authorisation

Error message	Description
<i>Party does not exist.</i>	Party not found in submission
<i>Party ... is not valid. / Party ... is not effective.</i>	Party validation failed
<i>Party ... is suspended.</i>	Party is suspended
<i>User is not authorised to submit forecast capability values for party ...</i>	Not assigned to this Party

<i>Forecast capability values are submitted for multiple parties. The values may be submitted only for one party in one jurisdiction at a time.</i>	Multiple Parties in one submission
---	--

Unit

Error message	Description
<i>Unit ... is not effective.</i>	Unit outside effective date range
<i>Unit ... is suspended from DASSA provision.</i>	Unit is suspended
<i>User is not authorised to submit forecast capability values for the unit The unit is not assigned to party ...</i>	Unit does not belong to your Party
<i>Unit ... is not qualified for system service product ...</i>	Unit lacks qualification

Data format

Error message	Description
<i>Forecast Capability must be a non-negative number with up to 3 decimal places.</i>	Invalid value format
<i>Combination of parameters Unit and System Service Product are not unique. Duplication found.</i>	Duplicate combinations in submission
<i>Forecasts intervals are not consistent with the resolution ...</i>	Time interval does not match configured resolution
<i>Forecasts time intervals are not consistent with the declared time interval.</i>	Trading periods do not match document time interval
<i>Forecasts time intervals overlap</i>	Overlapping time intervals in submission

9.2.7 Viewing DASSA Results

9.2.7.1 When results are available

DASSA results are available when the auction reaches the **Final Results Published** business state. At this point:

- Confirmed DASSA orders are generated
- Public results can be viewed in the GUI
- Public and private results can be retrieved via API (when available)

9.2.7.2 Viewing public results in the GUI

Purpose: Review published DASSA auction results.

Preconditions: The auction is in **Final Results Published** state.

Steps:

- Open the **DASSA Results** screen:
 - From a DASSA auction via **DASSA Results**, or
 - From the DASSA Auctions list **More Options** menu
- The screen opens as a read-only overview for the selected auction.
- In the **Filter** section, select an **auction requirement combination** (System Service Product, Zone, and Quality Category). Filters marked with a red star are mandatory.
- Review the **DASSA Results** table for the selected combination, showing aggregated data per Trading Period:
 - Clearing prices

- Volume requirements
- Aggregated cleared volume
- Insufficiency volume

5. Change the filter selection to view results for other auction requirement combinations.

Expected outcome: Published public results are displayed for the selected auction requirement combination.

If results are not yet available:

The message *"No data found. DASSA results are not published for this DASSA auction."* is displayed.

9.2.7.3 Retrieving public results via API

Refer to section 10.6.5 Publish DASSA Results - Public (to Service Provider) for details on API retrieval of public DASSA results.

Public results contain aggregated data per System Service Product, Zone, and Quality Category for each Trading Period: clearing prices, volume requirements, aggregated cleared volume, and insufficiency volume.

9.2.7.4 Retrieving private (party-specific) results via API

Refer to section 10.6.4 Publish DASSA Results - Private (to Service Provider) for details on API retrieval of private DASSA results (per Unit, clearing prices and cleared volume for your Party).

Private results contain data specific to your Party: per Unit, System Service Product, Zone, Quality Category, and Trading Period — clearing prices and cleared volume.

9.2.8 Viewing DASSA Orders

9.2.8.1 Overview

Confirmed DASSA Orders are the primary output of a completed DASSA auction. They represent the cleared volume assigned to your Units after results publication.

As a Service Provider, you can view only orders relating to your own Party.

9.2.8.2 Viewing the DASSA Orders list

Purpose: Find and review confirmed DASSA orders for your Units.

Preconditions: DASSA results have been published (orders exist for the Trading Day).

Steps:

1. Open the **DASSA Orders** screen from the system menu.
2. Set the **Filter** parameters:
 - **Date interval** — select the Trading Day range (orders are filtered by Trading Day within this interval)
 - **Party** — pre-selected to your Party
 - **Unit** — optionally filter by Unit
 - **System Service Product, Zone, Quality Category** — optionally narrow the results
 - **Advanced filter** — additional filtering options (e.g. to find orders with associated self-lapsing notifications)
3. Click **Apply Filters** (filters marked with a red star are mandatory).
4. Review the orders table, showing for each order:
 - Party
 - Unit
 - System Service Product, Zone, Quality Category

- Trading Period
 - Cleared volume and related data
5. If no orders match your filters, the message *"No data found."* is displayed.
 6. Click the **Detail** button on a row to open the **DASSA Order Detail** screen.

Expected outcome: A list of confirmed DASSA orders for your Party is displayed.

9.2.8.3 Viewing order detail

Purpose: Review the full details of a specific confirmed DASSA order.

Preconditions: At least one DASSA order exists.

Steps:

1. From the DASSA Orders list, click **Detail** on the desired order row.
2. The **DASSA Order Detail** screen opens, showing:
 - **Auction Parameters** section: Party, Unit, System Service Product, Zone, Quality Category, Trading Period, and related order parameters
 - **Time series data** for the order (cleared volume and related values)
3. Review the order details.

Expected outcome: Full order detail is displayed for the selected confirmed DASSA order.

9.2.8.4 Retrieving DASSA Orders via API

Details on retrieving DASSA Order details via the API will be available in a future document version.

9.2.9 Special Situations and Impacts on Service Providers

9.2.9.1 Auction cancellation

A DASSA auction may be cancelled before the offers gate closes.

Impact on you:

- Any offers you submitted for the cancelled auction remain **viewable** but are **no longer valid** and will not be used in evaluation
- If a **replacement auction** is created for the same Trading Day, you must submit **new offers** for that auction
- If no replacement auction is created by the configured deadline, **DASSA fallback** is triggered for the Trading Day

9.2.9.2 DASSA fallback (auction state Failed)

DASSA fallback occurs when no valid DASSA results can be produced for a Trading Day. This may happen when:

- An auction is cancelled and no replacement is created in time
- An auction is cancelled after a defined deadline
- Results are not approved by the configured deadline
- No DASSA auction was created for the Trading Day

Impact on you:

- The auction moves to the **Failed** business state
- **No valid DASSA results** exist for the affected Trading Day
- **No confirmed DASSA orders** are generated
- Downstream processes (secondary trading, bilateral trading, lapsing) do not occur for the affected Trading Day

9.2.9.3 Suspended Party or Unit

If your Party or a Unit is suspended from DASSA provision:

You **cannot submit** DASSA offers

- A red **Suspended** badge is displayed on the DASSA Offers Overview screen

Error messages you may see:

- *Party ... is suspended from DASSA provision.*
- *Unit ... is suspended from DASSA provision.*

9.2.9.4 Concurrent editing in the GUI

DASSA offers

- Edit mode applies to **one tab** (one Unit + System Service Product combination) at a time
- Multiple users from your Party can edit **different tabs** simultaneously
- If another user is submitting offers, you may see: *"DASSA offers are currently being modified by another user. Therefore, the submission is locked for modifications to avoid possible discrepancies."*
- Wait and retry, or coordinate with colleagues to avoid conflicting edits on the same tab

Forecast capability

- An edit lock is activated while forecast capability values are being saved
- If another user is submitting, you may see: *"Forecast capability values are currently being modified by another user. Therefore, the submission is locked for modifications to avoid possible discrepancies."*

9.2.10 Reference

9.2.10.1 Screen quick-reference

Screen	Menu path	Primary use
DASSA Auctions	• System menu → DASSA Auctions	• Browse auctions, open detail, navigate to offers/results
DASSA Auction Detail	• Detail button on auction row	• Review auction parameters
DASSA Offers Overview	• System menu or from auction → DASSA Offers	• View and submit offers
Forecast Capability Overview	• System menu → Forecast Capability	• View and submit forecast capability
DASSA Results	• From auction → DASSA Results	• View published public results
DASSA Orders	• System menu → DASSA Orders	• View confirmed orders
DASSA Order Detail	• Detail button on order row	• Review order detail

9.3 Secondary Trading

Details to be added in a future document version

9.4 Lapsing

Details to be added in a future document version

9.5 Residual Availability Determination (RAD)

Details to be added in a future document version

10. API Guide

10.1 API Overview

The API provides Service Provider the possibility to integrate their information systems into FASS. The key features of the API are:

- It exposes HTTP (REST/JSON) endpoints, specifically HTTPS on port 443 is used.
- It utilises API Key and OAuth 2.0 Client Credentials Flow for authentication and authorization.
- It provides OpenAPI Description (OAD) as a technical documentation of the endpoints, that conforms to the OpenAPI Specification (OAS).
- The OpenAPI Descriptions (incl. JSON examples) will be shared in a ZIP file initially. Later they will be published on the web site. The current structure of the ZIP file looks as follows:



10.2 Reliability And Operations

10.2.1 API Versioning

The API is designed to be backward compatible and if there are use cases in the future where this is not possible the deprecation policy will be followed. New functionality may result in a new API endpoint being necessary and an old end point being retired.

10.2.2 Deprecation Policy

In the event an end point needs to be retired. The deprecation policy will give a sufficient notice period for the end point to be retired. The intention will be to give a minimum of 6 months' notice in the event an end point needs to be retired.

10.2.3 Rate Limit

A rate limit of 10 requests per second per IP address for production is defined as the limit. For test environments a lower limit of 2 requests per second is defined as the limit.

10.2.4 Idempotency

The combination of documentId and documentVersion uniquely identifies a document submission (refer to section 10.6). If a document is submitted more than once with the same documentId and documentVersion, only the first submission will be accepted. Subsequent submissions with the same version will be rejected.

10.2.5 Availability

The API service is hosted in Microsoft Azure and is designed to provide a resilient and highly available service, with appropriate fault-tolerance capabilities to support continuity of service in the event of component failures. However, planned outage windows will be required at times to support updates to the API.

10.2.6 Retry Behaviour

If a 5xx Server Error response is received, clients retry behaviour is recommended to use an exponential backoff strategy to avoid generating excessive traffic during service degradation or outages (e.g. backoff policy retrying a submission every 2, 4, 8, 16 etc. seconds). In such cases where the service is unavailable for an extended period, retrying approximately every 5 minutes is expected to be sufficient.

10.2.7 IP Whitelisting

IP whitelisting is not implemented for this API. Access is controlled through the authentication and authorisation mechanisms described in Section 10.5.

10.2.8 Response Timeout

If no response is received within 30 seconds, the request should be considered timed out. The participant may resubmit the request using the same documentId and documentVersion as described in Section 10.6. Where repeated timeouts occur, participants should apply either a fixed retry interval or an exponential backoff policy. A maximum retry interval of approximately 5 minutes is recommended. *Note: As described in Section 10.2.4, requests are idempotent. Resubmitting the same documentId and documentVersion will not result in duplicate processing.*

10.2.9 Trouble Shooting Logs

PLACEHOLDER: Approach to be defined for sharing trouble shooting logs

10.2.10 Pagination

Pagination is not currently supported, as no use cases have been identified that require this functionality. Should future requirements identify endpoints that return sufficiently large result sets, pagination can be implemented on an endpoint-by-endpoint basis.

10.3 Architecture and Vocabulary

The solution consists of several microservices implementing business logic. These are not directly exposed to external systems. There is a single microservice in front that provides the API for external systems. The microservice delegates the API requests to the appropriate microservices.

10.3.1 HTTP Request Methods

The API provides common RESTful operations (methods), with HTTP as the transfer protocol and JSON as the data transfer format (payload).

Following operations are supported:

- GET – retrieves a resource
- POST – creates or updates a resource
- Placeholder: PATCH is being assessed to check if this Method can be supported, possible this may be included in the next iteration. DELETE and PUT are likely to remain omitted.

Every method is defined by the following properties:

- URI path suffix defining which command it is
- URI query parameters
- The form of the request body
- The form of the response body
- List of possible errors.

These are specified as OpenAPI Descriptions.

10.3.2 HTTP Request Headers

The following table lists HTTP headers that must be sent when invoking any method, unless the method description specifies otherwise.

Header	Value
Content-Type	application/json Mandatory for requests that transfer content (have body).
Authorization	Bearer <token>
Accept	application/json Optional.
X-Request-ID	<UUID v4> Optional.

10.3.3 HTTP Response Headers

The following table lists HTTP headers that are expected to be received after invoking any method, unless the method description specifies otherwise.

Header	Value
Content-Type	application/json Mandatory for responses that transfer content (have body).
Content-Length	Length of the method body.

10.3.4 HTTP Status

Method invocations follow standard semantics of HTTP response statuses as briefly described here.

Note: The list of the HTTP statuses is not exhaustive and can be extended in the future. The description below is generic, and the more specific details are provided in the OpenAPI Description.

Status Group	Description
200	OK Method invocation was successful.
400	Bad Request The request sent by the client is not valid and cannot be processed. The request shouldn't be repeated until it is corrected. Typical cause is a failing business validation, e.g. when the request parameter contains negative number and positive number is required by a business rule.
401	Unauthorized Authentication failed. Missing or invalid authentication credentials or authentication token.
403	Forbidden Authorization failed. Insufficient permissions to the requested resource or action.
404	Not Found The resource does not exist.
422	Unprocessable Content Indicates that the server understood the content type of the request content, and the syntax of the request content was correct, but it was unable to process the contained instructions.
423	Locked Indicates that a resource is locked, meaning it can't be accessed.
429	The request cannot be processed because the permitted request rate has been exceeded. The rate limited is defined in 10.2.3.

Status Group	Description
5xx	Method invocation was unsuccessful because of an unexpected internal error. Such errors fall into two categories: - A temporary problem with, for example, a network connection during command execution. The command may succeed if repeated later. - A permanent problem with the command implementation (or corrupted data). The command will not succeed if repeated. If this is the case, please contact support and describe the problem.

10.3.5 Common Method Properties

10.3.5.1 Request Body

For method which sends data the request body contains the data in the JSON format.

10.3.5.2 Response body

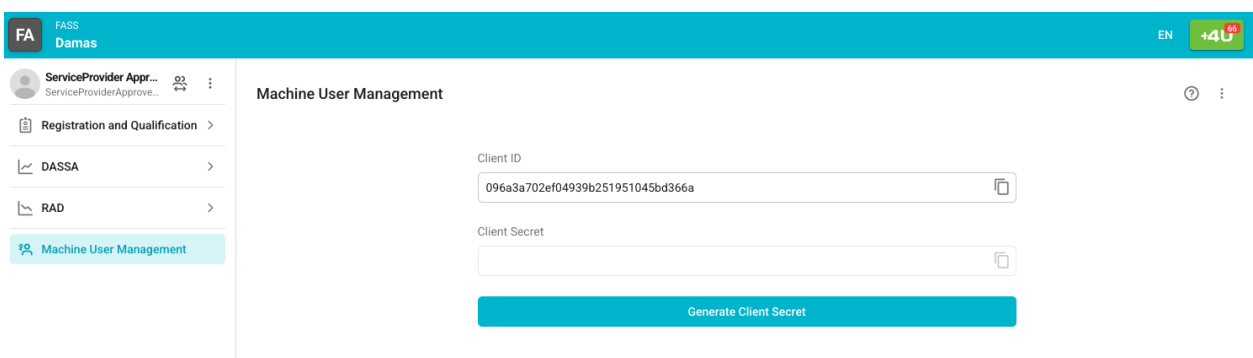
Except for methods providing binary data, the response body of a method is always a JSON document (more specifically, a JSON object).

All response body objects, no matter their overall structure, always contain a uuAppErrorMap attribute describing possible errors or warnings.

10.4 Machine User Management

Internally, the API Client is within FASS represented by a technical identity called Machine User. This identity is created automatically during the Registration and Qualification process. It is used for authentication and authorization of the API Client via OAuth 2.0 Client Credentials Flow.

The Client Credentials Flow uses Client ID and Client Secret as credentials for the authentication. These values are accessible to the Party Authorised User.



The screenshot shows the FASS Dams interface. On the left is a sidebar with navigation links: 'ServiceProvider Appr...', 'Registration and Qualification', 'DASSA', 'RAD', and 'Machine User Management' (which is highlighted). The main area is titled 'Machine User Management'. It contains two input fields: 'Client ID' with the value '096a3a702ef04939b251951045bd366a' and 'Client Secret' which is empty. Below these fields is a blue button labeled 'Generate Client Secret'. There are also icons for help and settings in the top right corner of the main area.

Figure 45: Machine User Management - Client Credentials

The Party Authorised User can

- Copy the Client ID
- Generate and copy the Client Secret. The Client Secret is shown only once at the time of generation. For security reasons, FASS has no direct access to this value and cannot display it again. The user is expected to copy it and keep it in a secure location.

Having the Client ID and Client Secret, the user should configure the API Client to use this credential for authentication via Client Credentials Flow.

10.5 Authentication and Authorisation

This section is a placeholder pending completion of the OAuth and Identity Management design.

The API security model will consist of two complementary mechanisms:

- API Key
- OAuth 2.0 Client Credentials Flow

Both mechanisms will be described in the following sections in the next iteration of the user guide. The diagram below illustrates the authentication and authorisation flow between the Service Provider and the FASS platform.

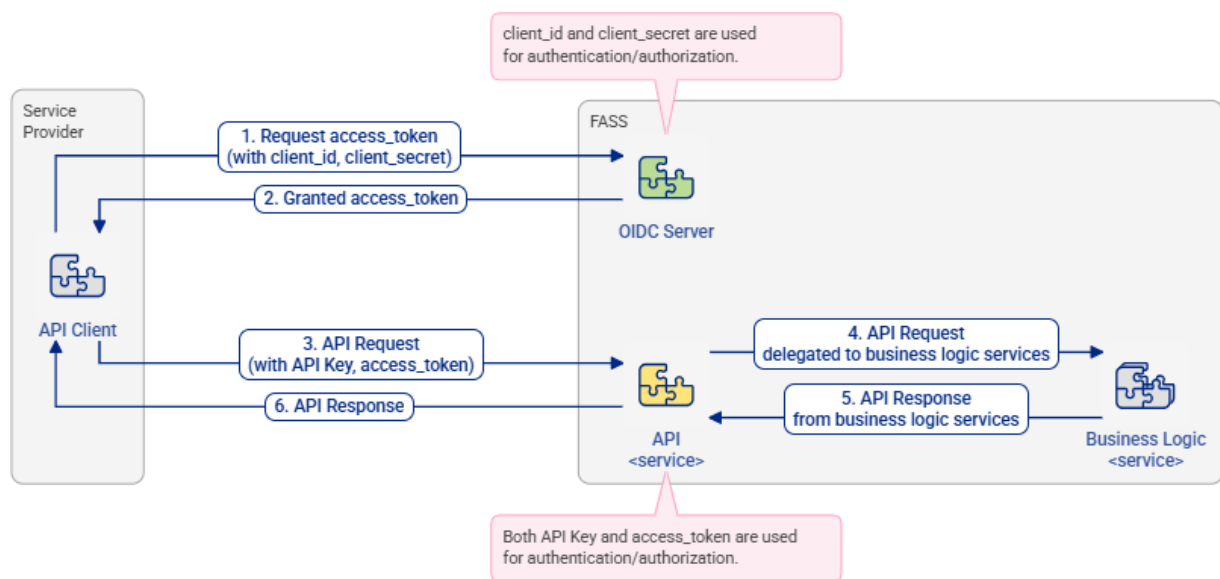


Figure 46: Overview of Authentication and Authorisation process steps

10.5.1 API Key

API Key Management – Placeholder: API consumers shall be issued an API key which must be included in re-quests as specified in the API documentation. Detailed requirements will be defined during solution design.

10.5.2 Client Credential Flow

The authentication and authorization follow the OAuth 2.0 Client Credentials Flow. All commands expect to receive a properly filled HTTP Authorization header with Bearer token. The token can be obtained by invoking oidc/grantToken endpoint on the OIDC Server (described below). The request to OIDC Server contains credentials (client_id, client_secret) assigned to Machine User, which represents the API Client identity. Response from the OIDC Server contains access_token which should be used in the HTTP Authorization header to authenticate the command invocation.

10.5.3 oidc/grantToken Request Description

10.5.3.1 Basic information

HTTP Method	POST
URL* Template	https://{uidentity-gateway}/uu-oidc-maing02/{awid}/oidc/grantToken

*Placeholder: URL's to be provided once available

10.5.3.2 HTTP request headers

Header	Value
Content-Type	application/json

10.5.3.3 Request body example

```
{
  "grant_type": "client_credentials",
  "scope": "openid Error! Hyperlink reference not valid.",
  "client_id": "4cfa9ade3e7148df835ee3c16ab9857f",
  "client_secret": "8$81F60m..."
}
```

10.5.3.4 Request body object description

Name	Description	Mandatory	Data type
grant_type	OAuth 2.0 grant type. Always client_credentials.	yes	string
scope	OAuth 2.0 scope. Always openid	yes	string
client_id	Machine user's credentials – client_id	yes	string
client_secret	Machine user's credentials – client_secret	yes	string

10.5.4 oidc/grantToken Response Description

10.5.4.1 Response body example

```
{
  "access_token": "at.ySPH5G5tjyh2-eEwtOGYP27Cg7-AnmQmVdTfAtbqR4k",
  "token_type": "Bearer",
  "expires_in": 1800,
  "uuAppErrorMap": {}
}
```

10.5.4.2 Response body object description

Name	Description	Data type
access_token	OAuth 2.0 access token.	string

token_type	OAuth 2.0 token type.	string
expires_in	Expiration interval (in seconds).	integer
uuAppErrorMap	Error description (if any)	object (see comment bellow)

The uuAppErrorMap contains information about all errors and warnings that occurred during the command's execution. It is a map of key-value pairs with key being an error code or a warning code. Usually there is one error and zero or more warnings.

If there is no error nor warning, the uuAppErrorMap is an empty object {}.

An example of uuAppErrorMap when grantToken is called with wrong credentials follows:

```
{
  "uuAppErrorMap": {
    "uu-oidc-main/grantToken/couldNotAuthenticate": {
      "id": "e33a3752c9b846b99fabcd509e174c",
      "timestamp": "2026-01-28T15:39:01.491Z",
      "type": "error",
      "message": "OidcClient could not be authenticated.",
      "cause": {
        "uu-oidc-main/authOidcClient/authenticate/notAuthenticated": {
          "id": "f960eb45d7784e33ae00989927cecbc9",
          "timestamp": "2026-01-28T15:39:01.486Z",
          "type": "error",
          "message": "Invalid OidcClient authentication.",
          "cause": {
            "uu-oidc-main/authAccessCodes/authenticateCredentials/notAuthenticated":
              {
                "id": "da4d5281d10f4c8b9420cc098b372e84",
                "timestamp": "2026-01-28T15:39:01.485Z",
                "type": "error",
                "message": "Invalid user authentication."
              }
            }
          }
        }
      }
    }
  },
  "error_description": "OidcClient could not be authenticated.",
  "error": "invalid_client"
}
```

10.6 API Endpoints

Documentation of the API endpoints uses OpenAPI.

Key information for all submissions:

- For a new submission, a new unique documentId must be set and the documentVersion must be set to 1. Refer to the specific API endpoint for the correct documentId format.
- When updating the document, the document (JSON) should use the same documentId and the documentVersion must be increased.

10.6.1 DASSA Offers

The OpenAPI Description is defined in 10.5.1-DASSA-Offers.yaml in the attached ZIP file.

10.6.1.1 Introduction

It is possible to submit DASSA offers as a JSON document identifying their party and jurisdiction, the trading day, and a list of units. For each unit and qualified system service product, the payload contains all trading periods of that trading day; each period holds up to 10 segments (price/quantity pairs with divisibility).

Submissions are sent via REST API POST or by uploading the same JSON structure manually. Offers can be created, updated, or effectively removed (by setting quantity to zero) using POST only — no DELETE method.

Prerequisites: Offers are accepted only when an active DASSA auction exists for the trading day, the gate is open for DASSA offers submission, the party/unit are valid, effective, and not suspended, and the unit is qualified for the system service products.

Data Flow Aspect	Description
Data Flow Name	> DASSA Offers
Source System	> Service Provider
Target System	> FASS
Trigger	> Ad-hoc – whenever the request is received by the system
Communication Channel	> REST API, POST method
Alternative Channel	> Manual upload of a JSON file
Format	> JSON (as request payload, not a file)
Acknowledgement	> JSON response containing a Transaction ID and HTTP 200 (OK)

10.6.1.2 Submission Rules

Key information on DASSA offers submission follows:

- The documentId is a mandatory field. The format is <source>_<target>_<message type>_YYYYMMDD where
 - Source system - SPR
 - Target system - SSP
 - Message type – short name for data flow name, DassaOffers
 Example: SPR_SSP_DassaOffers_20260101
- A submission may contain one or multiple units.
- Values may be submitted for one party in one jurisdiction per submission (identified by party ID + jurisdiction).
- A unit (or units) may contain one or multiple system service products for which the unit is qualified.
- For each product, the submission must cover all trading periods of the trading day (e.g. 48 periods at 30-minute resolution; actual count depends on the target resolution defined in the system configuration).
- Each trading period may contain up to 10 price/quantity pairs (segments), each with offered quantity, offered price, and divisibility flag.
 - Note: Price currency is derived from jurisdiction (EUR or GBP), reference currency is not sent explicitly in the payload.
- '0' is an acceptable value to indicate no submission for the combination of unit, product and segment in a trading period.
- After an initial submission:
 - Update: To update any previous submission, use the same combination of data elements to include any updated values.

- Note: Any number of segments can be submitted. The offers are always overridden for the given combination of unit and product in a trading period. E.g. if three segments are submitted in the first submission and only two segments are submitted in the next submission for the same combination of data elements, the original three segments are removed and the new two segments are stored.
- Note: Combination of data elements missing from a resubmission are not overridden — only submitted combinations are updated.
- Remove: To remove any previous offer, set the quantity to '0' in an update.
 - Note: Only one segment can be submitted with the zero value even if multiple segments have been previously submitted for the given combination of unit and product in a trading period.
- Uses the POST method to create, update, or delete an offer submission (explicit DELETE is not supported).

10.6.1.3 Example

An example JSON is provided containing two units, each of them submitting DASSA offers for two system service products. Various number of segments are submitted per trading periods.

The example can be found in 10.5.1-DASSA-Offers_example.json in the examples folder in the attached ZIP file.

10.6.2 Forecast Capability

The OpenAPI Description is defined in 10.5.2-Forecast-Capability.yaml in the attached ZIP file.

10.6.2.1 Introduction

It is possible to submit forecast capability as a JSON document identifying their party and jurisdiction, and a forecast period time interval. For each unit and qualified system service product, the payload contains forecast capability values for each trading period within that time interval. Values for trading periods past the gate closure are not editable. If such trading periods are included, the submission is rejected.

Submissions are sent via REST API POST or by uploading the same JSON structure manually. Forecasts can be created, updated, or effectively removed (by setting quantity to zero) using POST only — no DELETE method.

Prerequisites: Forecasts are accepted only when the gate is open for forecast capability submission, the party/unit are valid, effective, and the unit is qualified for the system service products.

Data Flow Aspect	Description
Data Flow Name	> Forecast Capability
Source System	> Service Provider
Target System	> FASS
Trigger	> Ad-hoc – whenever the request is received by the system
Communication Channel	> REST API, POST method
Alternative Channel	> Manual upload of a JSON file
Format	> JSON (as request payload, not a file)
Acknowledgement	> JSON response containing a Transaction ID and HTTP 200 (OK)

10.6.2.2 Submission Rules

Key information on forecast capability submission follows:

- The documentId is a mandatory field. The format is <source>_<target>_<message type>_YYYYMMDD where
 - Source system - SPR
 - Target system - SSP
 - Message type – short name for data flow name, ForecastCap
 Example: SPR_SSP_ForecastCap_20260101

- A submission may contain one or multiple units.
- Values may be submitted for one party in one jurisdiction per submission (identified by party ID + jurisdiction).
- A unit (or units) may contain one or multiple system service products for which the unit is qualified.
- For each product, the submission must cover all trading periods within a forecast period (e.g. 48 periods at 30-minute resolution for the whole trading day; actual count depends on the forecast period time interval and target resolution defined in the system configuration).
 - Note: Forecast period is from the next open hour to the end of the trading day or the next trading day based on the current time of the submission (if submitted before a specific time defined by the configuration, the forecast period end is equal to the end of the current trading day; else if submitted after the specific time defined by the configuration, the forecast period end is equal to the end of the next trading day).
- Each trading period contains forecast capability value.
- '0' is an acceptable value to indicate no capability for the combination of unit and product in a trading period.
- After an initial submission:
 - Update: To update any previous submission, use the same combination of data elements to include any updated values.
 - Note: Combination of data elements missing from a resubmission are not overridden — only submitted combinations are updated.
 - Remove: To remove any previous forecast capability, set the quantity to '0' in an update.
- Uses the POST method to create, update, or delete a forecast capability submission (explicit DELETE is not supported).

10.6.2.3 Example

An example JSON is provided containing two units, one of them submitting forecast capability values for two system service products and one of them submitting forecast capability values for one system service product.

The example can be found in 10.5.2-Forecast-Capability_example.json in the examples folder in the attached ZIP file.

10.6.3 DASSA Auction Information Pack (to Service Provider)

The OpenAPI Description is defined in 10.5.3-DASSA-Auction-Information-Pack-to-Service-Provider.yaml in the attached ZIP file.

10.6.3.1 Introduction

It is possible to retrieve the DASSA auction information pack via API request with the trading day in the URL.

FASS returns JSON response describing the published DASSA auction: one entry per auction requirement (i.e. per combination of system service product, zone, and quality category) in a list of products including the auction parameters, each with all trading periods of the trading day, containing the minimum requirement values.

Data is available only after the DASSA auction information pack has been published for that trading day.

Requests are sent via REST API GET.

Prerequisites: DASSA auction information pack data is available only when DASSA auction exists for the trading day, after the auction is published.

Data Flow Aspect	Description
Data Flow Name	> DASSA Auction Information Pack (to Service Provider)
Source System	> FASS
Target System	> Service Provider
Trigger	> Ad-hoc – whenever the request is received by the system

Communication Channel	> REST API, GET method
Format	> JSON (as response payload, not a file)

10.6.3.2 Response Description

Key information on DASSA Auction Information Pack response follows:

The response is returned for a specific trading day.

The response relates to one DASSA auction for that trading day.

Product list contains one item per auction requirement (i.e. each combination of System Service Product, Zone, and Quality Category).

For each auction requirement combination, the response includes auction parameters: valuation function coefficient, auction price caps and floors, offer price caps and floors, scarcity price, min price/quantity steps. Prices are reported in EUR and GBP (with exchange rate).

For each auction requirement combination, the response covers all trading periods of the trading day (e.g. 48 periods at 30-minute resolution; actual count depends on the target resolution defined in the system configuration) and includes minimum requirement values.

Uses the GET method; the response is JSON with HTTP 200 (OK).

10.6.3.3 Example

An example JSON is provided containing two auction requirement combinations.

The example can be found in 10.5.3-DASSA-Auction-Information-Pack-to-Service-Provider_example.json in the examples folder in the attached ZIP file.

10.6.4 Publish DASSA Results - Private (to Service Provider)

The OpenAPI Description is defined in 10.5.4-Publish-DASSA-Results-Private-to-Service-Provider.yaml in the attached ZIP file.

10.6.4.1 Introduction

It is possible to retrieve the Service Provider's DASSA results (awarded DASSA orders) via API request with the trading day in the URL. The party is determined from the API token (Service Provider Machine User).

FASS returns JSON response describing the DASSA results (own DASSA orders): one entry per unit in a list of units, per auction requirement (i.e. per combination of system service product, zone, and quality category) in a list of products, each with all trading periods of the trading day, containing the cleared quantity and clearing price.

If the party has no awarded DASSA orders, HTTP 200 is returned with an empty list of units.

Data is available only after the DASSA results have been published for that trading day.

Requests are sent via REST API GET.

Prerequisites: Final DASSA results data is available only when DASSA auction exists for the trading day, after the auction results are published.

Data Flow Aspect	Description
Data Flow Name	> Final DASSA Results (Private) (to Service Provider)
Source System	> FASS
Target System	> Service Provider
Trigger	> Ad-hoc – whenever the request is received by the system
Communication Channel	> REST API, GET method
Format	> JSON (as response payload, not a file)

10.6.4.2 Response Description

Key information on Final DASSA Results (Private) response follows:

The response is returned for a specific trading day.

The response relates to the authenticated Service Provider's party only (i.e. for a party identified by party ID and jurisdiction).

The response relates to one DASSA auction for that trading day and may contain one or multiple units with awarded DASSA orders.

- Note: An empty list of units may be returned in the response if the party has no awarded DASSA orders.

Product list contains one item per auction requirement (i.e. each combination of System Service Product, Zone, and Quality Category). Only auction requirement combinations of the awarded DASSA orders are included.

For each auction requirement combination, the response covers trading periods of the trading day where awarded DASSA orders exist, trading periods without data may be omitted (e.g. 48 periods at 30-minute resolution for the whole trading day; actual count depends on trading periods with awarded data and the target resolution defined in the system configuration) and includes cleared quantity and clearing price. Prices are reported in EUR and GBP.

Uses the GET method; the response is JSON with HTTP 200 (OK).

10.6.4.3 Example

An example JSON is provided containing two units, each having DASSA results (awarded DASSA orders) values for two auction requirement combinations.

The example can be found in 10.5.4-Publish-DASSA-Results-Private-to-Service-Provider_example.json in the examples folder in the attached ZIP file.

10.6.5 Publish DASSA Results - Public (to Service Provider)

The OpenAPI Description is defined in 10.5.5-Publish-DASSA-Results-Public-to-Service-Provider.yaml in the attached ZIP file.

10.6.5.1 Introduction

It is possible to retrieve public DASSA results via API request with the trading day in the URL. The response is not party-specific.

FASS returns JSON response describing the DASSA results: one entry per auction requirement (i.e. per combination of system service product, zone, and quality category) in a list of products, each with all trading periods of the trading day, containing the cleared quantity, clearing price, minimum requirement values, indication of the volume insufficiency and volume insufficiency values.

Data is available only after the DASSA results have been published for that trading day.

Requests are sent via REST API GET.

Prerequisites: Final DASSA results data is available only when DASSA auction exists for the trading day, after the auction results are published.

Data Flow Aspect	Description
Data Flow Name	> Final DASSA Results (Public) (to Service Provider)
Source System	> FASS
Target System	> Service Provider
Trigger	> Ad-hoc – whenever the request is received by the system
Communication Channel	> REST API, GET method
Format	> JSON (as response payload, not a file)

10.6.5.2 Response Description

Key information on Final DASSA Results (Public) response follows:

The response is returned for a specific trading day.

The response relates to one DASSA auction for that trading day.

- Data is not party-specific – the response contains aggregated results across all units.

Product list contains one item per auction requirement (i.e. each combination of System Service Product, Zone, and Quality Category). All auction requirement combinations as defined in the given DASSA auction are included.

For each auction requirement combination, the response covers all trading periods of the trading day (e.g. 48 periods at 30-minute resolution; actual count depends on the target resolution defined in the system configuration) and includes cleared quantity, clearing price, minimum requirement values, indication of the volume insufficiency and volume insufficiency values. Prices are reported in EUR and GBP.

Uses the GET method; the response is JSON with HTTP 200 (OK).

10.6.5.3 Example

An example JSON is provided containing two auction requirement combinations.

The example can be found in 10.5.5-Publish-DASSA-Results-Public-to-Service-Provider_example.json in the examples folder in the attached ZIP file.

API endpoint details for trading, lapsing, and RAD to be added in a future document version