Entitlement and Usage Control Requirements for Euronext Market Data

EMDA-Aligned Specification

EURONEXT

Table of contents

1. PURPOSE 3
2. DEFINITION OF AN ENTITLEMENT AND USAGE CONTROL FRAMEWORK 3
3. CONTROL CONCEPTS 3
4. CORE ENTITLEMENT MODEL 3
   - 4.1 ACCESS ID 3
   - 4.2 ALLOWED CONCURRENT INSTANCES 4
   - 4.3 INFORMATION PRODUCT 4
5. ACCESS CONTROL AND ENFORCEMENT 4
   - 5.1 DEFAULT DENY 4
   - 5.2 RESTRICTION BY PRODUCT AND INSTANCES 4
   - 5.3 RESTRICTION BY USAGE TYPE 4
   - 5.4 PREVENTION OF ACCESS ID SHARING 4
6. INSTANCE-, DEVICE-, AND WORKLOAD-LEVEL CONTROL 5
   - 6.1 PRINCIPLE 5
   - 6.2 DEFINITION OF AN INSTANCE 5
   - 6.3 INSTANCE IDENTIFICATION AND ATTRIBUTION 5
   - 6.4 INSTANCE COUNT ENFORCEMENT 6
   - 6.5 TELEMETRY-BASED CONTROL MODELS 6
7. ENTITLEMENT LIFECYCLE MANAGEMENT 7
8. RECORD-KEEPING AND AUDITABILITY 7
9. SECURITY AND INFRASTRUCTURE CONTROLS 7
10. SCOPE OF RESPONSIBILITY 8
11. PUBLIC DISPLAY EXCEPTION 8
12. ALIGNMENT WITH INDUSTRY-STANDARD ENTITLEMENT AND USAGE-CONTROL FRAMEWORKS 8
13. SUMMARY 9

1. Purpose

This document describes the functional, technical, and control requirements for an entitlement and usage control framework used to control access to, use of, and redistribution of Euronext market data in accordance with the Euronext market data agreement (EMDA) and related policies.

The objective of the entitlement and usage control framework is to ensure that market data is only accessed and used by authorised parties, strictly within the contractual scope, and that such access is fully auditable.

2. Definition of an Entitlement and Usage Control Framework

An entitlement and usage control framework is a technical control framework, system, or combination of systems through which access IDs, users, devices, applications, systems, workloads, or other technical identities are authorised to access and use Information, and through which such access and use is controlled, measured, recorded, and made auditable.

The framework must enforce entitlements and usage controls technically, and not solely through procedural or contractual controls.

3. Control Concepts

Compliance may be achieved through a traditional entitlement system, a cloud-native control framework, telemetry-based controls, or a combination of these. The relevant control framework must address three separate but related control objectives:

Entitlement control: determining which access IDs, users, devices, applications, systems, or workloads are authorised to access Information.

Concurrency control: determining and, where applicable, limiting the number of simultaneous authorised instances, sessions, workloads, or execution contexts capable of accessing or using Information.

Usage measurement: recording actual access to and use of information over time, including sufficient evidence to determine peak concurrent usage by information product and reportable Unit.

The contracting party must ensure that all concurrent usage is attributable, measurable, controllable, and auditable, irrespective of the technical architecture used.

4. Core Entitlement Model

The entitlement and usage control framework must operate using the following logical entities:

4.1 ACCESS ID

A unique identifier representing a user, device, application, or system through which information is accessed.

4.2 ALLOWED CONCURRENT INSTANCES

(sometimes referred to in industry systems as user access positions or maxcount)

A setting, policy, or control parameter that determines the number of permitted simultaneous instances, sessions, workloads, or execution contexts associated with an access ID or equivalent technical identity. This setting needs to be tracked over time (and kept on file for at least 5 years) in such a way that the number of potential instances capable of interacting with the information remains auditable.

4.3 INFORMATION PRODUCT

A defined Euronext market data product (e.g. real-time cash equities, derivatives, indices).

5. Access Control and Enforcement

The entitlement and usage control framework must technically enforce the following controls:

5.1 DEFAULT DENY

Access to information must be denied unless an explicit entitlement exists.

5.2 RESTRICTION BY PRODUCT AND INSTANCES

The system must limit and control:

- the number of access IDs,
- the number of allowed concurrent authorised execution contexts or sessions associated with an access ID,
- the permitted identity types, roles, usage rights, and access scopes associated with access IDs.

5.3 RESTRICTION BY USAGE TYPE

The system must control the permitted type of access and/or use of Information (e.g. display, non-display, redistribution) in line with contractual rights.

5.4 PREVENTION OF ACCESS ID SHARING

The system must implement authentication mechanisms (e.g. credentials, certificates, tokens) to ensure that only the registered user, client, or device can use a given access ID.

6. Instance-, Device-, and workload-Level Control

6.1 PRINCIPLE

Where the applicable usage type is device-based, control must extend beyond the access ID level to the technical instances, devices, workloads, sessions, or execution contexts through which Information is accessed or used.

An access ID alone is not sufficient to evidence compliant device-based usage unless the associated concurrent technical usage is also identifiable, measurable, controllable, and auditable.

6.2 DEFINITION OF AN INSTANCE

An instance is any uniquely identifiable technical execution context through which information is accessed or used, including but not limited to:

- Physical servers
- Virtual machines
- Cloud instances
- Containers
- Application processes
- Other automated systems or endpoints

Each concurrently active instance that accesses, receives, processes, distributes, or otherwise uses information constitutes a device where the device unit of count applies.

6.3 INSTANCE IDENTIFICATION AND ATTRIBUTION

The control framework must support identification and attribution of instances, devices, workloads, sessions, or execution contexts accessing information.

This may be achieved through explicit pre-registration, runtime workload identity, orchestration metadata, telemetry, API gateway records, IAM controls, or equivalent technical mechanisms.

The control framework must ensure that each relevant technical access point can be linked to:

- an access ID or equivalent technical identity;
- the entitled information product(s);
- the applicable reportable unit;
- the permitted usage type;
- the relevant time period of access.

Where explicit pre-registration is not technically appropriate, the contracting party must be able to demonstrate through telemetry and associated control records that access was limited to authorised technical contexts and that peak concurrent usage can be evidenced.

6.4 INSTANCE COUNT ENFORCEMENT

The control framework must technically control and evidence the maximum permitted concurrent usage in line with the entitled device count.

This includes:

- maintaining records of the allowed number of concurrent instances, devices, workloads, sessions, or execution contexts per information product;
- technically enforcing, constraining, limiting, throttling, blocking, revoking, or otherwise controlling access in line with the applicable entitlement limits;
- generating alerts, remediation actions, or equivalent control responses where entitlement limits are exceeded or at risk of being exceeded;
- producing reliable and auditable evidence of actual and peak concurrent usage during the relevant reporting period;
- retaining sufficient historical records to demonstrate both permitted and actual usage over time.

The implemented controls must ensure that concurrent usage cannot materially exceed the applicable entitlement limits without detection, attribution, and evidential recording.

Post-factum reconciliation alone is not sufficient unless supported by reliable technical controls and tamper-resistant telemetry capable of evidencing actual and permitted usage.

6.5 TELEMETRY-BASED CONTROL MODELS

Where a traditional entitlement system based on explicit Instance pre-registration is not technically appropriate (for example in cloud-native, elastic, containerised, or serverless environments), the contracting party may implement an alternative telemetry-based control framework, provided that such framework delivers equivalent control, auditability, and evidential capability.

Such telemetry-based frameworks must be capable of:

- uniquely identifying technical workloads, execution contexts, or runtime instances accessing Information;
- associating such workloads with authorised access IDs, information products, and permitted usage types;
- measuring and evidencing concurrent active usage over time;
- enforcing or otherwise technically constraining access in line with contracted entitlement limits;
- retaining tamper-resistant historical records for a minimum of five (5) years;
- producing auditable electronic records demonstrating actual and permitted usage levels.

Examples of acceptable telemetry identifiers may include:
instance IDs, workload IDs, pod UIDs, container IDs, cloud instance identifiers, orchestration metadata, API client identities, or equivalent technical runtime identifiers.

The contracting party remains responsible for demonstrating that the telemetry-based framework provides control and evidential capabilities equivalent in outcome to those of a traditional entitlement system.

7. Entitlement Lifecycle Management

The entitlement and usage control framework must support full lifecycle management for each access ID and instance, including:

- Activation and deactivation of entitlements;
- Association of access IDs and instances with information products;
- Allowed instance fluctuations over time must be captured and kept for at least 5 years;
- Definition of entitlement start and end dates;
- Revocation where required (e.g. contract termination, audit findings).

At any point in time, it must be possible to determine exactly which information products an access ID and its associated instances were entitled to use.

8. Record-Keeping and Auditability

The entitlement and usage control framework must be capable of producing complete, continuous, and authentic entitlement and usage control records, including:

- Access ID
- Instance / device identifier (where applicable)
- Information product(s)
- Allowed instances over time
- Entitlement start and end dates

Key requirements:

- Entitlement records must be retained for a minimum of five (5) years;
- Records must be protected against unauthorised alteration;
- The system must be capable of generating electronic data files providing complete entitlement and usage histories for audit and compliance purposes.

Records must be time-sequenced and sufficiently protected to evidence integrity and prevent retrospective manipulation.

9. Security and Infrastructure Controls

The entitlement and usage control framework must operate within a secure technical environment, including:

- Up-to-date physical and logical security controls;
- Network security (e.g. firewalls);
- Restricted access to entitlement administration functions;
- Protection against unauthorised external access;
- Identity and workload authentication controls.

The entitlement and usage control framework must form part of the contracting party's broader security architecture.

10. Scope of Responsibility

The contracting party remains fully responsible for:

- All access IDs and instances under its control;
- Usage by affiliates, employees, contractors, and third parties;
- Any downstream access facilitated through its systems.

Responsibility applies irrespective of whether access is direct or indirect, manual or automated.

11. Public Display Exception

Where Information is publicly displayed strictly in accordance with the EMDA public display policy, such display is not required to be controlled via an entitlement and usage control framework.

All other uses remain subject to entitlement control.

12. Alignment with Industry-standard Entitlement and Usage-control Frameworks

While EMDA does not mandate a specific technology, architecture, vendor, or deployment model, the required control capabilities are consistent with established market-data entitlement and usage-control frameworks, including both traditional entitlement platforms (e.g. LSEG DACS) and modern cloud-native control architectures.

Acceptable implementations may include, but are not limited to:

- Centralised entitlement administration systems;
- Identity and access management (IAM) frameworks;
- API gateway and token-based access controls;
- Workload identity and orchestration controls;
- Telemetry-based monitoring and enforcement frameworks;
- Instance- and workload-level registration and control mechanisms;

- Product-specific, usage-specific, and time-bound entitlement controls;
- Historical audit logging and evidential record retention.

Any custom-built, cloud-native, or telemetry-based implementation must therefore provide capabilities equivalent in outcome and evidential quality to those of established entitlement systems.

13. Summary

An entitlement and usage control framework is considered EMDA-compliant only where it:

- Technically controls, measures, and evidences authorised access and usage by access ID and reportable unit;
- Identifies, controls, measures, and evidences the number of permitted concurrent technical instances, devices, workloads, sessions, or execution contexts where the device unit of count applies;
- Prevents unauthorised use and access ID sharing;
- Maintains complete, tamper-resistant entitlement records for at least five years;
- Supports audit and compliance verification at any time.

euronext.com