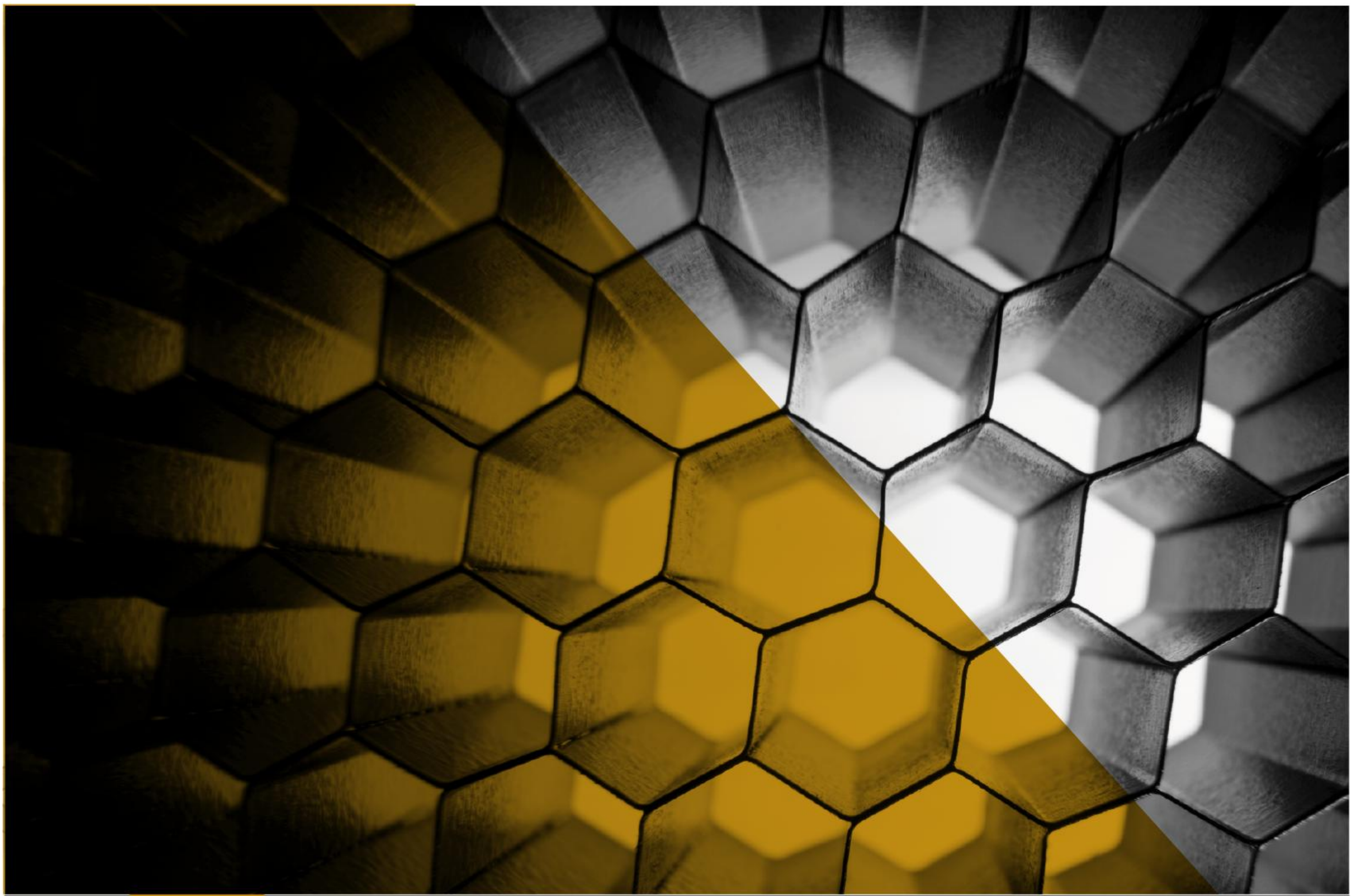


Trade Repository
Business Requirements and Technical Interface Specifications

2025/08/29

strate

Table of Contents

1. Document information

1.1 Version control

Version	Date	Authors	Summary of changes
0.1	2025-02-28	Ganesh Varadarajan, Robert Henwood	Initial draft
0.2	2025-03-12	Ganesh Varadarajan, Robert Henwood, Leroy Oosthuyzen, Jaco Greyling	Added reference section, usage guidelines, architecture diagrams, message schemas, consolidated terminology
1.0	2025-04-01	Ganesh Varadarajan, Robert Henwood, Leroy Oosthuyzen, Jaco Greyling	Final version for market distribution
2.0	2025-08-01	Robert Henwood, Leroy Oosthuyzen, Jaco Greyling	Version 2 for market distribution – various updates based on TR Working group discussions, including but not limited to updated role definitions/classifications, updated transactional reference data reporting standard fields (supporting documentation), updated onboarding reference data, consolidated relevant terminology, clarification of UTI generation methodology, inclusion of outstanding items, inclusion of Digital Regulatory Reporting (DRR) and Common Domain Model (CDM) adoption, exclusion of position-level reporting.
3.0	2025-08-29	Robert Henwood, Leroy Oosthuyzen, Jaco Greyling	Version 3 for market distribution – various updates based on TR Working group discussions, including but not limited to updated roles definitions/classifications, revised reporting deadlines/SLAs, inclusion of UTI sharing timelines/SLAs, inclusion of allegement file flow to facilitate UTI sharing, clarification on the provision of daily reconciliation reports i.e. end of day position files.

1.2 Approvals

Name	Role	Approval status	Date
Farzana Khan	Executive - Strate	Approved	15-09-2025 | 15:17 SAST
Beverley Van Niekerk	Business Manager - Strate	Approved Beverley Van Niekerk	15-09-2025 | 08:42 SAST
OTC Derivatives Providers / Entities Responsible for Reporting	Reporting obligation to the TR	60% approval required, per the TR Working Group Terms of Reference.	Approved at TRWG meeting held on 9 September 2025
[FSCA Representative- as a member of the TR Working Group]	Regulatory Oversight		16-09-2025 | 08:01 SAST

1.3 References

Ref no	Document	Version	Date	Published by
1	Financial Markets Act (Act No. 19 of 2012)	As amended	2012	Republic of South Africa
2	Conduct Standard for reporting obligations in respect of transactions in over-the-counter derivatives (FMA Conduct Standard 3 of 2018)	1.0	2018	Financial Sector Conduct Authority
3a 3b	ISDA EMIR Reporting Industry Best Practices Matrix March 2020 https://www.isda.org/a/qpwgE/EMIR-Refit_Field-requirement-interpretations_042424.xlsx	1.0	March 2020 April 2024	International Swaps and Derivatives Association

Ref no	Document	Version	Date	Published by
4	ISO20022 MDR Part2 FITRR TradeRepositoryReporting	1.0	May 2024	ISO
5	EMIR Refit - Outgoing Messages - FINAL	V1.1.0	November 2023	ESMA
6	EMIR Refit - Incoming Messages - FINAL	V1.1.0	November 2023	ESMA
7	ESMA Guidelines For Reporting Under EMIR – Final Report	V1.0.0	14 December 2022	ESMA
8	CDE Technical Guidance - Harmonisation of critical OTC derivatives data elements (other than UTI and UPI)	1.0	April 2018	CPMI-IOSCO

2. Introduction

2.1 Background and regulatory context

The Global Financial Crisis (GFC) in 2008 exposed significant weaknesses in the over-the-counter (OTC) derivatives markets. The lack of transparency in this market segment misled regulators and market participants about risks and risk concentrations, hampering regulatory interventions and eroding market confidence globally.

In response, the G20 leaders, including South Africa, agreed upon reforms aimed at increasing transparency and reducing systemic risks by mandating that:

- All OTC derivative contracts must be reported to a Trade Repository (TR)
- Standardised OTC derivative contracts should be centrally cleared and traded on exchanges, where appropriate
- Non-centrally cleared contracts should be subject to higher capital and minimum margin requirements

South Africa, as a G20 member, has implemented higher capital and margin requirements for non-centrally cleared derivatives and is currently assessing a central clearing mandate. However, a gap remained regarding the centralised reporting of OTC derivatives.

In November 2024, Strate was licensed by the Financial Sector Conduct Authority (FSCA), with concurrence from the Prudential Authority (PA), to operate South Africa's first trade repository and provide regulators and market participants with data-led insights.

2.2 Purpose of the document

This document serves as a combined authoritative reference, integrating both Business Requirements Specification (BRS) and Technical Interface Specifications, aimed primarily at business and technical implementation teams who will be interacting with the TR. Its primary objectives include:

- Providing comprehensive guidance on connecting with, submitting data to and receiving feedback from the TR
- Ensuring effective, consistent and accurate reporting of OTC derivatives transactions throughout their lifecycle
- Supporting regulatory compliance with the Financial Markets Act (Act No. 19 of 2012) and FMA Conduct Standard 3 of 2018 (CS3)
- Leveraging ISO 20022 messaging standards adopted in EMIR REFIT to minimise implementation costs and ensure alignment with international reporting standards

2.3 Definitions and terminology

Key terms and their equivalents between the South African market and international (ISO) standards are provided below. These definitions ensure clarity and standardisation:

South African term	Definition	ISO/International equivalent
OTC Derivatives Provider (ODP) – ***see Note 1 below***	Refers to a person or entity licensed by the FSCA in terms of the FMA who, as a regular feature of its business and transacting as principal: (a) originates, issues, or sells OTC derivatives; or (b) makes a market in OTC derivatives	Entity Responsible for Reporting (ERR)
Central Counterparty (CCP)	a clearing house that interposes itself between counterparties to transactions in securities, becoming a buyer to every seller and the seller to every buyer and thereby ensuring the performance of open contracts	Entity Responsible for Reporting (ERR)
Delegated Reporting Party – ***see Note 2 below***	Entity that has been delegated to submit transaction reports to the Trade Repository	Report Submitting Entity (RSE)
Financial Markets Act (FMA)	Primary legislation governing financial markets legislation	European Market Infrastructure Regulation (EMIR)
FMA Conduct Standard 3 (CS3)	Conduct Standard for reporting obligations in respect of transactions in over-the-counter derivatives	Regulatory Technical Standards (RTS) and

		Implementation Technical Standards (ITS)
FSCA	Financial Sector Conduct Authority, market conduct regulator established in terms of the Financial Sector Regulation Act of 2017	National Competent Authority (NCA)
Prudential Authority (PA)	Responsible for prudential supervision, established in terms of the Financial Sector Regulation Act of 2017	Prudential Supervisor
SARB	South African Reserve Bank, responsible for monetary policy and financial stability as outlined in terms of the Financial Sector Regulation Act of 2017	Central Bank
Legal Entity Identifier (LEI)	Refers to a 20 character, alpha-numeric code that uniquely identifies the counterparties to the financial transactions; the international standard of which is outlined in ISO 17442:2012 Financial Services	Same
Unique Transaction Identifier (UTI)	Identifier for unambiguous transaction identification.	Same
Unique Product Identifier (UPI)	Identifier for standardised product classification.	Same
Authorities	Collectively refers to the FSCA and PA	
TR Working Group (TRWG)	A working group that is chaired by Strate and includes members comprising the Authorities and a business and technical representative from each ODP. The output of TRWG will be the finalisation of the TR Business Requirements and Technical Interface Specifications which will be supported by the Authorities	
SA Reporting requirements and specifications	The proposed TR reporting requirements, based on the ISO standard and modified for the SA market. This is a living document that is collectively defined and agreed with the TRWG, and may be updated as required	

Note 1: The ODP, or CCP where applicable, will hereafter be referred to as the Entity Responsible for Reporting, which will be abbreviated to ERR

Note 2: The Delegated Reporting Party will hereafter be referred to as the Report Submitting Entity, which will be abbreviated to RSE

3. Trade Repository overview

3.1 Role and responsibilities

The TR operated by Strate serves as a centralised registry for all OTC derivatives contracts in South Africa. Its core functions include:

- **Centralised data collection:** Aggregating transaction data from market participants, ensuring transparency and integrity
- **Validation and storage:** Conducting comprehensive validation checks, securely storing data to maintain accurate and reliable electronic records of OTC derivatives transactions

- **Distribution and feedback:** Providing regulators and participants with data-led insights, enabling regulatory oversight and enhanced market transparency

3.2 TR ecosystem participants and roles

The TR ecosystem involves distinct participant types and clearly defined roles and responsibilities.

Participants and roles:

1. **Entity Responsible for Reporting (ERR):**
   - Licensed entities (ODP) providing OTC derivatives services in South Africa
   - CCP, where applicable
   - Primarily legally responsible for meeting reporting obligations directly, via a CCP or via delegation to a Report Submitting Entity (RSE)

2. **Report Submitting Entity (RSE):**
   - Entities responsible for submitting transactions to the Trade Repository , when delegated by the ERR
   - Is a delegated third party

3. **Non-Reporting Counterparty**
   - Entities that are counterparties to the ERR, who are not themselves designated as reporting parties.
   - These entities have no legal reporting duty (obligation) under Conduct Standard 3 (CS3) of 2018

4. **Authorities:**
   - **FSCA:** Enhancing and supporting the efficiency and integrity of financial markets
   - **Prudential Authority (PA):** Prudential supervision of institutions

Note: Please refer to 'Market Participants and roles' in section 5 for additional detail

3.3 Reporting obligations

Who must report?

- Entities responsible for reporting (ERR)
- Report submitting entities (RSE)

What must be reported?

- New trades and trade-level lifecycle events
- Daily valuation and margin updates

When to report?

- The TR will cater for a real-time reporting capability
- Minimum requirement, according to CS3, of End-of-Day (EOD) reporting by close of business (deemed to be 00:00 Coordinated Universal Time - UTC) T+1 following the trading day
- ERR/RSE's will therefore be able to report at any time between execution and EOD T+1

4. Global standards adoption

The South African TR adopts the ISO 20022 message standard for OTC derivatives reporting, aligning with global best practices while accommodating local market requirements.

4.1 Rationale for ISO 20022 adoption

The adoption of ISO 20022 as the messaging standard for South African OTC derivatives reporting provides several key advantages:

- **Global standardisation**: ISO 20022 is the internationally recognised standard for financial messaging, facilitating interoperability between global market infrastructures
- **Rich data model**: The standard provides a comprehensive data model capable of supporting the complex requirements of derivatives reporting
- **Forward compatibility**: ISO 20022's extensible design allows for future enhancements without disrupting existing implementations
- **Regulatory alignment**: Major jurisdictions worldwide are adopting ISO 20022 for regulatory reporting, facilitating cross-border reporting
- **Implementation efficiency**: Market participants operating across multiple jurisdictions can leverage existing ISO 20022 implementations

4.2 ISO 20022 message components

The South African TR implementation uses the 'auth' (Authorities) message set developed specifically for regulatory reporting:

- **Domain**: Securities
- **Business Area**: Authorities
- **Message Set**: Financial Instruments and Transactions Regulatory Reporting

Each ISO 20022 message consists of the following components:

1. **Business Application Header (BAH)**: Contains addressing and routing information (head.001.001.01)
2. **Message content**: Contains the business payload specific to each message type
3. **Supplementary data**: Optional component for additional information not captured in the structured fields

The messages utilise a standardised hierarchical structure:

- **Message building blocks**: Main sections of the message
- **Message components**: Reusable groups of related data elements
- **Data elements**: Individual fields containing specific information

4.3 XML implementation

The TR implementation uses XML syntax for ISO 20022 messages with the following characteristics:

- Messages are defined using XML Schema Definition (XSD) files
- Strict validation against published schemas is required
- XML namespaces are used to identify different message versions
- Character encoding must be UTF-8

4.4 EMIR REFIT alignment

The South African TR implementation strategically aligns with EMIR REFIT principles while accommodating local market requirements. This alignment offers substantial benefits for market participants while ensuring local regulatory needs are met.

4.4.1 Key alignments with EMIR REFIT

The South African implementation maintains alignment with EMIR REFIT in the following key areas:

- **Message structures**: Adoption of the same ISO 20022 message formats (auth.030, auth.107, etc.)
- **Lifecycle reporting**: Implementation of the same action types (New, Modify, Correct, etc.) and event types (Trade, Clearing, Exercise, etc.)
- **Field definitions**: Consistent field definitions and formats
- **Validation approach**: Similar technical and business validation methodology
- **Reconciliation process**: Adoption of the same reconciliation principles and tolerances

4.4.2 Implementation benefits

This strategic alignment with EMIR REFIT provides several benefits for South African market participants:

- **Reduced implementation costs**: Market participants with existing EMIR REFIT-compliant systems can leverage those investments and reporting mechanisms
- **Global compatibility**: Facilitates cross-border reporting for multinational entities and will enable the South African TR to share and receive data from global TRs in response to data harvesting requirements for developing a term-rate
- **Market certainty**: Provides a clear, well-established standard for implementation
- **Future-proof design**: Benefits from ongoing global standards development and enhancements

4.4.3 South Africa-specific adaptations – the SA Reporting requirements and specifications

While maintaining alignment with global standards, the South African implementation includes certain modifications and exclusions to address local requirements. Current exclusions are indicated below, but the SA Reporting requirements and specifications (annexure) will be the living document containing all modifications and updates, as collectively agreed with the TR Working Group.

Fields to be excluded / removed from the SA Reporting requirements and specifications:

1.7	Clearing threshold of counterparty 1	Indicates whether the counterparty exceeds clearing thresholds triggering mandatory clearing obligations.

1.13	Clearing threshold of counterparty 2	Indicates the second party's clearing obligation status for regulatory compliance.
2.4	Subsequent position UTI	References the resulting position when trades are incorporated into netting sets.
2.2	Report tracking number	Provides venue-specific tracking for exchange-traded derivatives.
2.7	ISIN	Provides standardized instrument identification for listed derivatives.

4.5 Digital Regulatory Reporting (DRR) and Common Domain Model (CDM) adoption

The South African TR will implement ISDA's Digital Regulatory Reporting (DRR) solution and the FINOS-managed Common Domain Model (CDM) to standardize and automate regulatory reporting processes. Once finalised, the South African OTC derivatives reporting requirements will be distributed as executable code through the DRR framework, as an option for participants who choose to adopt it.

4.5.1 Rationale for DRR/CDM adoption

Building upon our ISO 20022 implementation, the adoption of DRR and CDM will provide additional benefits:

- **Code-based standards**: Converting regulatory rules into executable code ensures consistent interpretation and implementation across all market participants
- **Enhanced accuracy**: Automated rule interpretation reduces manual errors and inconsistencies in regulatory reporting
- **Global interoperability**: Alignment with the growing global ecosystem of financial institutions adopting these open-source standards
- **Operational efficiency**: Streamlined reporting processes through automated data transformation and validation
- **Future innovation**: Access to ongoing developments in the global open-source financial technology community

4.5.2 Implementation approach

The South African TR will:

- Implement DRR/CDM alongside the ISO 20022 messaging standard to provide market participants with code-based regulatory specifications
- Distribute the finalised SA Reporting requirements and specifications as executable code through the DRR framework
- Collaborate with ISDA and FINOS communities to ensure alignment with global best practices
- Support market participants in adopting the DRR/CDM framework for their reporting implementations
- Maintain comprehensive documentation and support resources for the code-based regulations

This initiative positions South Africa at the forefront of regulatory technology adoption, joining leading global financial market infrastructures in embracing open-source, standardized solutions for regulatory reporting.

4.6 Global identifier standards

The South African TR implements three key global identifier standards: Legal Entity Identifier (LEI), Unique Transaction Identifier (UTI) and Unique Product Identifier (UPI). These standards are essential for the unambiguous identification of entities, transactions and products in the OTC derivatives market.

The three identifier standards are interconnected within the reporting framework:

- LEIs are used to identify parties, and in the generation of UTIs
- UTIs link related transactions (e.g. during clearing, compression, or allocation)
- UPIs categorise transactions for risk analysis and aggregation
- Together, these identifiers enable consistent tracking and analysis of OTC derivatives exposures

4.6.1 Legal Entity Identifier (LEI)

The Legal Entity Identifier (LEI) is a 20-character, alphanumeric code based on the ISO 17442 standard developed by the International Organization for Standardization (ISO). The LEI serves the primary purpose of clearly and uniquely identifying legal entities participating in both local and international financial transactions.

LEI usage in reporting:

- Identification of reporting counterparties
- Identification of other counterparties
- Identification of beneficiaries, brokers, clearing members and central counterparties
- Reference for generating UTIs

4.6.1.1 LEI requirements

When reporting OTC derivative transactions to the TR, the ERR and/or RSE should consider the following:

- The LEI is a mandatory identifier for all ERRs and their counterparts, except for the reporting of counterparties that are natural persons
- The LEI must be valid in accordance with the Global Legal Entity Identifier Foundation (GLEIF) database
- LEIs are issued by authorised Local Operating Units (LOUs) of the GLEIF. Strate is an authorised LOU and can support the application for a new LEI or the renewal of an LEI. *This service operates independently of the TR.*
- Valid LEIs assist the TR in conducting effective due diligence and KYC verification during the onboarding processes
- LEIs support compliance with regulatory requirements in alignment with global best practice

4.6.1.2 LEI structure

An LEI consists of 20 characters with the following structure:

- Characters 1-4: Prefix identifying the Local Operating Unit (LOU) that issued the LEI
- Characters 5-18: Entity-specific part, assigned by the LOU
- Characters 19-20: Check digits calculated according to the ISO 17442 standard

4.6.1.3 LEI for natural persons

Natural persons are not eligible for LEIs. For reporting transactions involving natural persons:

- Client codes should be used following the format specified in the CDE Technical Guidance
- The format is "LEI of Reporting Counterparty + Identifier of Individuals" where the identifier is the person's South African ID number or passport number for foreign nationals
  Maximum length is 72 characters

4.6.2 Unique Transaction Identifier (UTI)

The Unique Transaction Identifier (UTI) is a reference code of up to 52 characters that uniquely identifies individual OTC derivatives transactions, enabling consistent trade identification across market participants and jurisdictions. Primarily, a UTI helps to ensure the consistent aggregation of OTC derivatives transactions by minimising the likelihood that the same transaction will be counted more than once.

Implementation requirements:

- UTIs must be generated according to the ISO 23897:2020 standard
- UTIs must be unique across the entire global derivatives market
- Once assigned, a UTI must remain unchanged throughout the life of the transaction
- UTIs must be shared between counterparties to ensure consistent reporting

UTI structure:

- Maximum length of 52 characters
- Composed of the generating entity's LEI (20 characters) followed by a unique transaction identifier
- The South African TR proposes specific components detailed below as part of its UTI generation service, should parties opt for this UTI generation service.

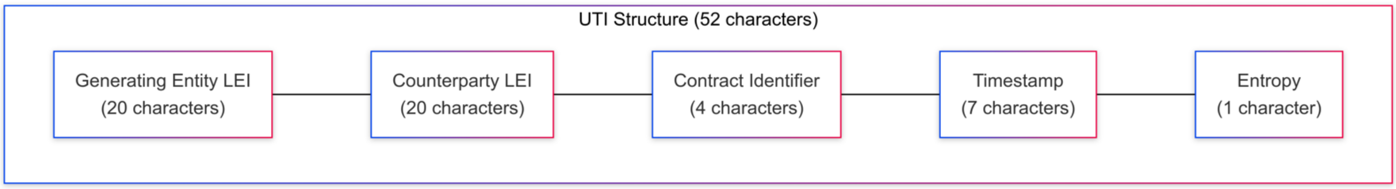
4.6.2.1 UTI generation service (optional)

The South African TR will provide an optional UTI generation service:

1. ERR/RSE can request a UTI from the TR system via REST API
2. The TR generates the UTI according to the proposed structure
3. The ERR/RSE provides the generated UTI to the counterparty
4. Both ERR, for dual-sided reporting, must use the same UTI

This service is optional. ERR/RSE may generate UTIs themselves, provided they follow the ISO 23897:2020 structure and uniqueness requirements.

4.6.2.2 Proposed UTI structure for the South African TR's UTI generation service



For market participants who opt to generate a UTI via the TR, the TR will adhere to this proposed UTI structure which aims to allow for independent UTI generation without requiring a central system, while minimising the risk of duplicates and conforming to the ISO guidelines for length and content:

Component	**Length**	**Description**
LEI A	20 alphanumeric	LEI of Party A (generating entity)
LEI B	20 alphanumeric	LEI of Party B (counterparty)
Asset type	2 alphanumeric	Code identifying the asset class
Instrument type	2 alphanumeric	Code identifying the instrument type
Millisecond timestamp	7 alphanumeric	Base 36 encoded millisecond timestamp (see section 13.6)
Entropy character	1 alphanumeric	Random character to ensure millisecond uniqueness

Asset type codes:

- IR: Interest Rate
- FX: Foreign Exchange
- CR: Credit
- EQ: Equity
- CO: Commodity

Instrument type codes:

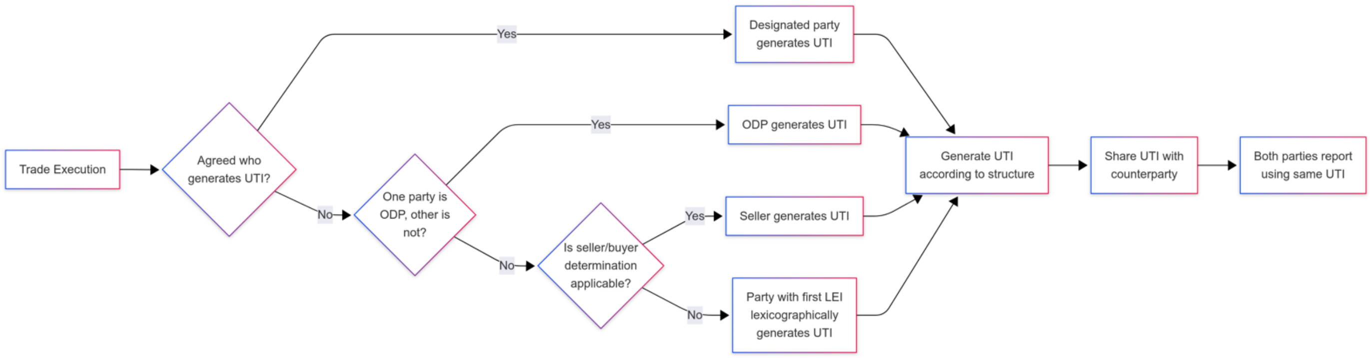
- SW: Swap
- FR: Forward Rate Agreement
- FW: Forward
- OP: Option
- DS: Default Swap
- CD: Financial Contract for Difference

- FU: Future
- SB: Spreadbet
- ST: Swaption

Example UTIs:

- 213800ZBWY3BU3UUMA42549300RH5FFHO48FXT69IRSWWGK7WGD8
- 213800ZBWY3BU3UUMA42549300RH5FFHO48FXT69FXFWRMP7C6BW
- 213800ZBWY3BU3UUMA42549300RH5FFHO48FXT69CRDSMP8C6ZAC

4.6.2.3 UTI generation responsibility



The responsibility for generating the UTI shall be determined according to the following hierarchy:

1. If specified in a contractual agreement between the counterparties, the designated party shall generate the UTI
2. If one counterparty is an ERR and the other is not, the ERR shall generate the UTI
3. If no agreement exists, the seller shall generate the UTI
4. If seller/buyer determination is not applicable, the counterparty with the first LEI in lexicographical order shall generate the UTI

The generating counterparty must communicate the Unique Transaction Identifier (UTI) to the receiving counterparty by 10:00 a.m. Coordinated Universal Time (UTC) on the working day following the date of the derivative's conclusion (T+1)

In case the generating party fails to generate or communicate the UTI in due time, which is 10:00 am UTC on T+1, in order to meet the reporting deadline, the receiving party should contact the generating party and enquire about the process instead of reporting using an UTI generated on its own.

4.6.3 Unique Product Identifier (UPI)

The Unique Product Identifier (UPI) is a 12-character code that uniquely identifies OTC derivative products based on their characteristics, facilitating consistent product classification across the market. UPIs must conform to the ISO 4914:2021 standard. Each UPI code is mapped to a set of reference data elements to describe the product (e.g. asset class, instrument type, underlier etc.) The combination of the UPI code, UPI reference data and the process of assigning a UPI code to a particular set of reference data represent the UPI System.

4.6.3.1 Structure of the UPI

1. **Character length**: Consist of 12 alphanumeric characters
2. **The first two-character prefix “QZ”**
3. **Nine alphanumeric characters** (upper case A-Z and 0-9 only, excluding the vowel characters (A, E, I, O, U) and the character Y) without separators or special characters
4. **One alphanumeric check character** (A-Z and 0-9 only, excluding the vowel characters (A, E, I, O, U) and the character Y)

4.6.3.2 Global OTC derivatives product list

The Derivatives Service Bureau (DSB), which was founded by Association of National Numbering Agency (ANNA), maintains the global OTC derivatives product list. In 2019, the Financial Stability Board (FSB) designated the DSB as both the service provider for the UPI system for OTC derivatives and the operator of the UPI reference data library. The UPI is used for identifying OTC derivative products in transaction reporting data and to helps to assess systemic risk and detect market abuse.

4.6.3.3 Proposed UPI operating model

The TR platform will validate the existence of the UPI at the time of trade reporting and validation of the trade attribute with the UPI attributes, to ensure that the correct UPI has been reported by the ERR and/or RSE.

The TR will:

- Check for UPI existence against the DSB reference data
- Validate that the reported UPI is consistent with the reported trade attributes
- Notify reporting entities of any inconsistencies between UPI and trade attributes
- Maintain a local cache of UPI reference data for validation purposes

5. Market participants and roles

5.1 Entities Responsible for Reporting - ERR

Regulated entities that conduct regulated activities in OTC derivatives within the South African market, as defined under the FMA.

Note: This role will include Central Counterparties (CCPs), as and when applicable

5.1.1 Definition and licensing requirements

ERRs are market participants who originate, issue, sell or make a market in OTC derivatives as a regular business activity. They are subject to specific licensing requirements under the FMA and must comply with the reporting obligations set out in FMA Conduct Standard 3.

An ERR can be categorised as:

- **Bank**: Financial institutions with banking licences
- **Non-bank**: Other financial entities licensed to provide OTC derivatives services
- **Resident**: South African-based entities
- **Non-resident**: Foreign entities authorised to operate in the South African market
- **CCP**: Central Counterparty

Note 1: All ERRs must obtain and maintain a valid license to operate in the South African OTC derivatives market

5.1.2 Reporting obligations and responsibilities

ERRs assume primary reporting obligations under the FMA and Conduct Standard 3. These obligations include:

- Reporting of all OTC derivative transactions to the Trade Repository
- Ensuring the completeness, accuracy and timeliness of reported data
- Reporting within T+1 of the transaction execution
- Providing ongoing updates throughout the lifecycle of each transaction
- Reporting daily valuations and collateral information
- Maintaining systems and processes to support accurate reporting
- Correcting any identified errors or omissions in reporting

The ERR can fulfil these obligations directly or delegate the reporting function to a third-party entity (RSE), though the legal responsibility remains with the ERR.

5.1.3 Delegation of reporting responsibilities to a Report Submitting Entity - RSE

The ERR may choose to delegate the reporting function to a third-party, the Report Submitting Entity (RSE), through a formal delegation agreement. Key aspects of this delegation include:

- The ERR must establish a formal agreement with the RSE defining roles and responsibilities
- There is no licencing requirement for an RSE
- The ERR retains legal responsibility for reporting obligation and compliance, even when delegated
- The RSE must have the necessary systems, processes and expertise to ensure the submission of transactions to the Trade Repository
- Both parties must establish procedures for data transmission, validation and error resolution
- The agreement should include provisions for business continuity and contingency arrangements

5.2 Report Submitting Entities - RSE

RSEs are entities responsible for the submission of transaction reporting in accordance to TR requirements , when delegated by the ERR.

5.2.1 Definition and role

RSEs assume the responsibility for ensuring that OTC derivatives transactions are reported to the TR on behalf of an ERR. An RSE can be:

- A third-party entity designated by an ERR to submit transaction reports to the TR
- An entity providing reporting services to multiple ERR

The ERR is accountable for ensuring that all required transaction data is submitted to the TR in accordance with regulatory requirements, regardless of whether this reporting obligation has been delegated.

5.2.2 Technical requirements

The RSE must meet specific technical requirements to effectively perform their role:

- Implement one or more of the approved connectivity methods (IBM MQ, Kafka, SFTP, etc.)
- Develop systems capable of generating ISO 20022 compliant messages
- Establish processes for message validation and error handling
- Implement security measures in accordance with TR requirements
- Maintain business continuity arrangements for reporting functions
- Have technical staff capable of troubleshooting reporting issues

6. Onboarding

6.1 Reference data requirements: ERR and/or RSE

The following reference data must be provided to TR as part of the onboarding process:

Field name	**Field description**	**Mandatory/Optional /Conditional**	**Remarks**
Name	Name of the entity	Mandatory	
Type of entity	Type of participant	Mandatory	Valid values: ERR, RSE
Type of ERR	Type of the ERR	Conditional	Valid values: Bank, Non-bank, CCP
Resident/Non-resident indicator	Resident/Non-resident indicator of the entity	Mandatory	Valid values: R – Resident, N – Non-resident
LEI	Legal Entity Identifier of the entity	Mandatory	LEI must be in active status. If LEI is not available, please contact https://www.lei-strate.co.za/ to obtain new LEI or renew LEI
Company registration number	Company registration number allocated by CIPC	Conditional	RSA specific

Field name	Field description	Mandatory/Optional /Conditional	Remarks
SARS income tax number	Income tax number allocated by SARS	Conditional	RSA specific
VAT number	VAT number allocated by SARS	Conditional	RSA specific
Address details	Address of the entity	Mandatory	
Contact details	Contact details of the entity	Mandatory	
LEI of the RSE (if different to the ERR)	Reporting party appointed/delegated by the ERR	Conditional	Can be its own reporting party or an existing RSE
Method of communication	Method of communication to the TR system	Mandatory	[MQ, Kafka, API, SFTP, Portal]
Sector code	Sector code that ERR belongs to	Mandatory	Please refer to Appendix for sector code mapping details
UTI generation methodology	Detail based on the methodology, if any, used for the creation of UTIs	Mandatory	Will allow the TR to ascertain existing UTI methodologies used by market participants
Regulatory-licensed reporting market segment(s) of ERR	Indication of the market segment(s) for which reporting is to be expected	Mandatory	Commodity, Credit, Foreign Exchange, Equity, Interest Rate. (Some, or all of these, may be reported directly by the ERR whilst others may be delegated)
LOA	Letter of Authority	Conditional	The ERR must establish a formal agreement with the RSE defining roles and responsibilities

Note: Relevant onboarding pack will be distributed once finalised

6.2 Onboarding process

1. ERR and/or RSE to submit onboarding forms to Strate via Strate’s client portal.
2. TR onboarding team at Strate to verify all documents submitted. If all documents are in order, the ERR and/or RSE will be created in the TR platform with relevant security credentials.
3. Relevant endpoints, key stores and network security configurations will be created by the TR.
4. TR onboarding team to notify the ERR and/or RSE of the relevant credentials and security configurations.
5. ERR and/or RSE to test and confirm send/receive success for relevant message channel.

6.3 User access management

As part of the onboarding process, each entity must establish appropriate user access management:

1. **Administrator setup**:
   - At least one administrator is required per entity
   - Administrator is responsible for managing user access
   - Administrator credentials are provided during onboarding

2. **User group configuration**:
   - ‘Admin’ group: Authorised to assign or edit user access
   - ‘Edit’ group: Authorised to submit and modify reports
   - ‘Read/view’ group: Authorised to view but not modify data

3. **User provisioning**:
   - Administrators create and manage user accounts
   - Assign appropriate access levels based on responsibilities
   - Implement principle of least privilege for access rights

Through this structured onboarding process, the TR ensures that all market participants are properly authorised, technically prepared and operationally ready to fulfil their reporting obligations.

Note: Relevant onboarding pack will be distributed once finalised

6.4 Testing and certification

Following the initial onboarding, market participants must complete a testing and certification process before being authorised to submit production data:

1. **Technical connectivity testing**:
   - Establish connectivity through chosen channel (IBM MQ, SFTP, etc.)
   - Validate basic message transmission and receipt
   - Test authentication and security mechanisms

2. **Message validation testing**:
   - Submit test messages covering all required scenarios
   - Validate message formats and content
   - Test error handling and correction processes

3. **End-to-end process testing**:

- Validate complete reporting workflows
- Test lifecycle event reporting
- Verify reporting timeliness and completeness

4. **Certification**:
   - Complete formal certification test cases
   - Receive approval from TR for production reporting
   - Sign production access agreements

7. Message types, specifications and flows

7.1 Message types and usage

The South African TR will implement the ISO 20022 'Authorities' Business Area message set as published by ESMA and generated by SWIFT MyStandards for derivative transaction reporting. These messages provide a comprehensive framework for all reporting activities and more detail can be found here:

Source – Message Usage Guidelines

Message Set - Financial Instruments and Transactions Regulatory Reporting (Trade Repository Reporting)

https://www.iso20022.org/iso-20022-message-definitions?search=financial%20instruments%20and%20transactions%20regulatory%20reporting

For further details on the use of these messages, refer to the ISO 20022 Financial Instruments and Transactions Regulatory Reporting (Trade Repository Reporting) Message Definition Report Part 1, provided as part of the above message set.'

Message ID	Name	Purpose	Senders	Recipients	Usage Guideline (SWIFT - MyStandards)
auth.029.001.04	Derivatives Trade Report Query	Request trade data from TR	ERR, RSE, Authorities	TR	https://www2.swift.com/mystandards/#/mp/mx/_ZF_MIHltEe6cZfzZFKLwyg/_tM-vkHltEe6cZfzZFKLwyg!content
auth.030.001.03	Derivatives Trade Report	Report trade activity	ERR, RSE	TR	https://www2.swift.com/mystandards/#/mp/mx/_ZF_MIHltEe6cZfzZFKLwyg/_v596QXltEe6cZfzZFKLwyg!content

Message ID	Name	Purpose	Senders	Recipients	Usage Guideline (SWIFT - MyStandards)
auth.031.001.01	Financial Instrument Reporting Status Advice	Provide status of submitted reports	TR	ERR, RSE, Authorities	https://www2.swift.com/mystandards/#/mp/mx/_ZF_MIHltEe6cZfzZFKLwyg/_yyu3IXltEe6cZfzZFKLwyg!content
auth.091.001.02	Derivatives Trade Reconciliation Statistical Report	Report reconciliation statistics	TR	ERR, RSE, Authorities	https://www2.swift.com/mystandards/#/mp/mx/_dTj_0HltEe6cZfzZFKLwyg/_Pe6uwXluEe6cZfzZFKLwyg!content
auth.092.001.04	Derivatives Trade Rejection Statistical Report	Report submission rejections	TR	ERR, RSE, Authorities	https://www2.swift.com/mystandards/#/mp/mx/_dTj_0HltEe6cZfzZFKLwyg/_CshaVXluEe6cZfzZFKLwyg!content
auth.106.001.01	Derivatives Trade Warnings Report	Report data quality warnings	TR	ERR, RSE, Authorities	https://www2.swift.com/mystandards/#/mp/mx/_dTj_0HltEe6cZfzZFKLwyg/_Fak8BXluEe6cZfzZFKLwyg!content
auth.107.001.01	Derivatives Trade State Report	Provide current trade state	TR	ERR, RSE, Authorities	https://www2.swift.com/mystandards/#/mp/mx/_dTj_0HltEe6cZfzZFKLwyg/_Fak8CXluEe6cZfzZFKLwyg!content
auth.108.001.01	Derivatives Trade Margin Data Report	Report margin activity	ERR, RSE	TR	https://www2.swift.com/mystandards/#/mp/mx/_ZF_MIHltEe6cZfzZFKLwyg/_v596RXltEe6cZfzZFKLwyg!content

Message ID	Name	Purpose	Senders	Recipients	Usage Guideline (SWIFT - MyStandards)
auth.109.001.01	Derivatives Trade Margin Data Transaction State Report	Provide current margin state	TR	ERR, RSE, Authorities	https://www2.swift.com/mystandards/#/mp/mx/_dTj_0HltEe6cZfzZFKLwyg/_Fak8EXluEe6cZfzZFKLwyg!content

7.2 Message relationships and sequences

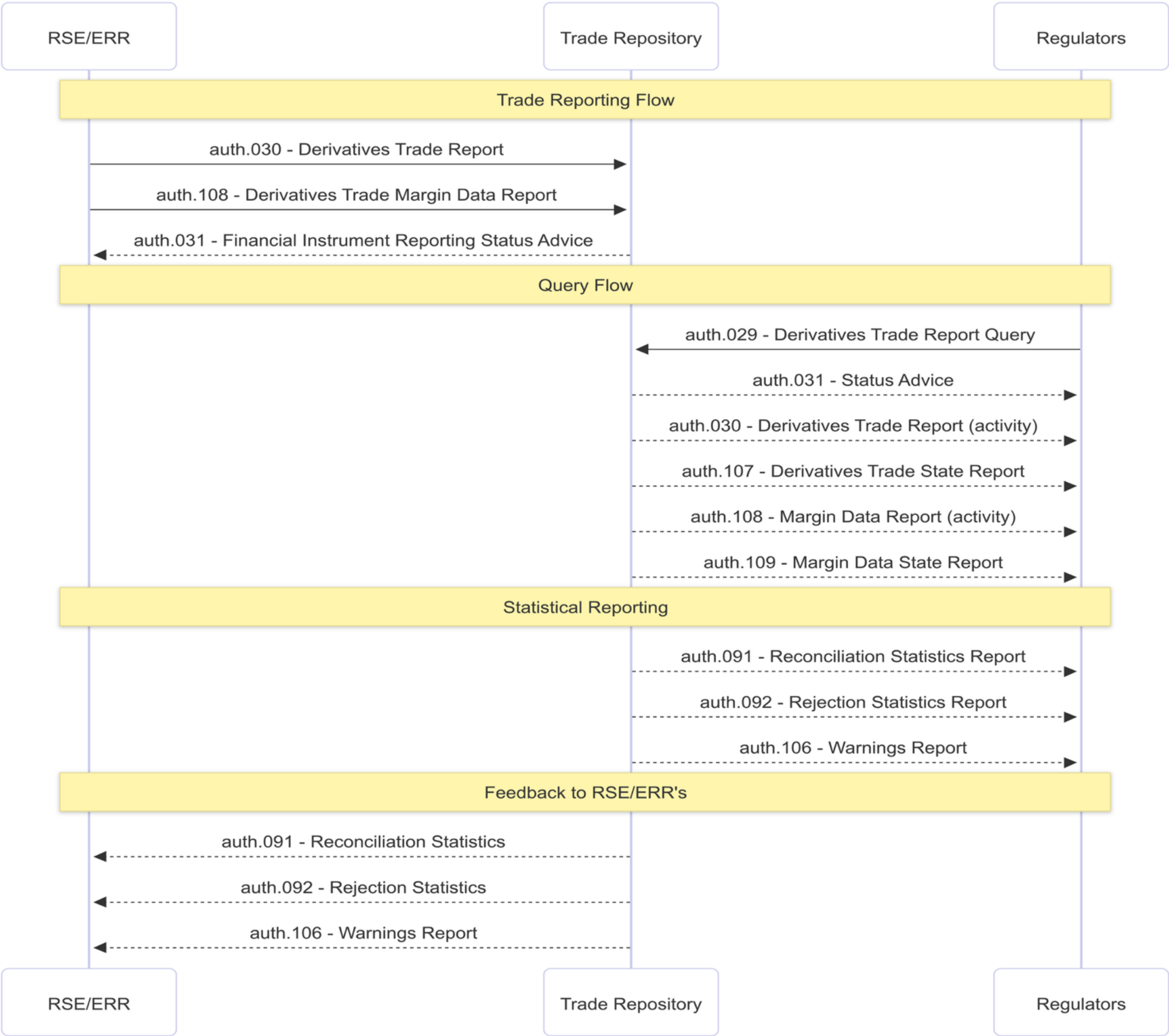
Messages in the TR ecosystem follow specific relationship patterns:

Reporting flow:
- ERR and/or RSE submits trade data via auth.030
- ERR and/or RSE submits margin data via auth.108
- TR acknowledges via auth.031
- TR provides feedback via auth.091/092/106

Query flow:
- Authority, ERR and/or RSE submits query via auth.029
- TR acknowledges via auth.031
- TR responds with requested data via appropriate message

Lifecycle relationships:
- auth.030 reports lifecycle events
- auth.107 provides current state derived from auth.030 events
- auth.108 reports margin updates
- auth.109 provides current margin state derived from auth.108 updates

Statistical relationships:
- auth.091 provides reconciliation statistics
- auth.092 provides rejection statistics
- auth.106 provides data quality warnings



All messages use the Business Application Header (BAH) for consistent addressing and identification.

7.3 Message exchange pattern

Message flows between participants and the TR follow specific patterns:

Inbound messages (to TR)
- auth.029: Query messages from authorities and authorised ERR and/or RSE
- auth.030: Derivative trade activity reports from ERR and/or RSE
- auth.108: Margin update reports from ERR and/or RSE

Outbound messages (from TR)

- auth.031: Status advice messages confirming processing status
- auth.030: Trade activity data in response to queries
- auth.107: Trade state data in response to queries
- auth.108: Margin activity data in response to queries
- auth.109: Margin state data in response to queries
- auth.091: Reconciliation statistics reports
- auth.092: Rejection statistical reports
- auth.106: Warning reports for potential data quality issues

Message sequencing rules:

1. Every auth.030 and auth.108 submission must receive an auth.031 response
2. Action type sequencing for auth.030 must follow logical progression:
    - "New" must precede any other action type for a given UTI
    - "Error" terminates the sequence for a UTI unless followed by "Revive"
    - "Revive" can only follow "Error" or erroneous "Terminate"
    - "Terminate" ends the active lifecycle for a UTI

The submission/response pattern follows a synchronous-asynchronous hybrid model:

1. **Submission (asynchronous)**:
    - ERR/RSE submit trade reports (auth.030) and margin data reports (auth.108) to the TR via their preferred method

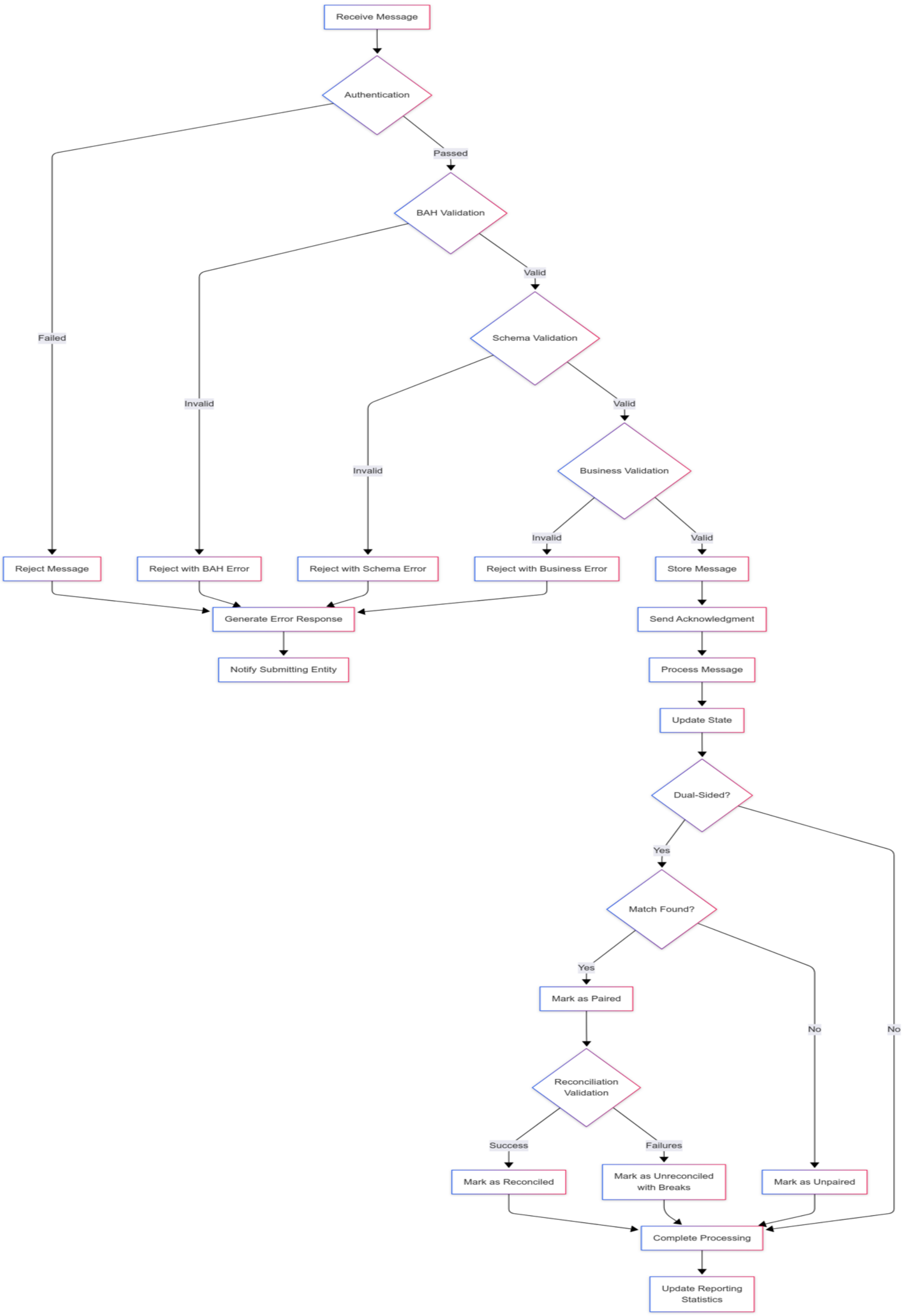
2. **Validation and acknowledgment:**
    - The TR performs initial technical validation upon receipt
    - Acknowledgment of receipt and validation report is returned via the auth.031 message

3. **Processing and response (asynchronous)**:
    - Successfully processed reports are incorporated into the repository
    - Detailed trade state report can be requested and returned via auth.107 message
    - Reporting entities can receive recurring reports at their chosen frequency or ad-hoc via an auth.029 message

7.4 Message processing flow

The TR implements a structured message processing flow to ensure consistent handling of all submissions.

7.4.1 Inbound processing flow



The inbound processing flow consists of the following steps:

1. **Receipt**: Message received via preferred channel (e.g. Kafka)
    - Message timestamped upon arrival
    - Assigned unique processing identifier
    - Initial logging of receipt

2. **Authentication**: Verification of sender credentials
    - Validate digital certificates or API keys
    - Check IP restrictions and access rights
    - Confirm sender authorisation for message type
    - Validate message signature (HMAC)

3. **BAH validation**: Verification of Business Application Header
    - Validate format and required fields
    - Check addressing information
    - Verify message references

4. **Syntax validation**: XML schema validation
    - Validate against published XSD schemas
    - Check namespace declarations
    - Verify field formats and constraints

5. **Business validation**: Field-level and cross-field business rules
    - Apply field validations specific to message type
    - Check cross-field dependencies and relationships
    - Validate reference data (e.g. LEIs, UTIs)

6. **Persistence**: Storage of validated message
    - Store complete message content
    - Index for retrieval and processing
    - Update audit trails and logs

7. **Status notification**: Confirmation or rejection notice to sender
    - Send auth.031 message with processing status
    - Include detailed error information if rejected
    - Provide unique reference for successful submissions

8. **Reconciliation**: Trade-to-Trade and System-to-System Confirmation
    - Match reports from both counterparties on dual-sided reports
    - Compare field values with defined tolerances
    - Identify and record reconciliation breaks

9. **State update**: Incorporation into trade/margin state
    - Update trade/margin state database
    - Apply lifecycle events to existing records
    - Maintain historical state information

7.4.2 Outbound processing flow

The outbound flow handles queries and data requests:

1. **Query receipt**: Processing of auth.029 query message
    - Validate query parameters
    - Check access rights for requested data
    - Prioritise based on query type and source

2. **Access validation**: Verification of data access rights
    - Check regulatory mandates for authorities
    - Validate ERR access to own data
    - Apply data access restrictions

3. **Query execution**: Retrieval of requested data
    - Execute database queries
    - Apply filters and date ranges
    - Aggregate data as required

4. **Response formatting**: Creation of appropriate response message
    - Format data according to message specification
    - Apply pagination for large result sets
    - Include metadata and reference information

5. **Response delivery**: Transmission via appropriate channel
    - Send response through same channel as request
    - Apply compression for large responses
    - Ensure secure transmission

7.4.3 Error handling flow

When validation or processing errors occur, the system follows a structured approach:

1. **Error detection**: Identification of validation failures
    - Capture specific error condition
    - Record context information
    - Preserve original message content

2. **Classification**: Categorisation by error type and severity
    - Technical errors (syntax, format)
    - Business errors (content, rules)
    - System errors (processing, availability)

3. **Logging**: Recording of error details for analysis
    - Store error code and description
    - Record message identifier and timestamp
    - Maintain error statistics

4. **Notification**: Communication to affected party
    - Generate auth.031 with error details
    - Include resolution guidance
    - Provide reference information

5. **Remediation guidance**: Information on corrective actions
    - Specific guidance based on error type
    - Reference to relevant rules or requirements
    - Suggested resolution approach

6. **Recovery**: Automatic or manual processes as appropriate
    - Retry processing where applicable
    - Roll back partial processing
    - Maintain system integrity

7.5 Business Application Header (BAH)

The Business Application Header (BAH), conforming to the ISO 20022 standard head.001.001.01, is a mandatory component for all messages exchanged with the TR. It functions as a digital envelope, providing essential metadata for routing, identification, processing and security.

7.5.1 BAH Structure (head.001.001.01)

The 13 elements of the BAH can be understood through the following logical groups:

Core identification and routing elements:

These elements define the message's origin, destination, unique identity and content type.

- **From:** Identifies the sending messaging endpoint (typically the LEI of the sender) that created the message. This might differ from the transport layer sender address.
- **To:** Identifies the designated recipient messaging endpoint (typically the TR's LEI) that will process the message. This might differ from the transport layer recipient address.
- **Business Message Identifier (BizMsgIdr):** A unique identifier assigned by the sender to this specific message instance (e.g. following the format LEI-YYYYMMDD-SEQUENCE). Crucial for tracking and duplicate prevention.
- **Message Definition Identifier (MsgDefIdr):** Specifies the precise ISO 20022 message type and version contained in the payload (e.g. auth.030.001.04), enabling the receiver to interpret the content correctly.
- **Business Service:** Optionally specifies the agreed service context or level under which the message is exchanged (e.g. E&I).

Context and control flag elements:
These provide metadata about the message's creation context and special handling instructions.

- **Creation Date (CreDt):** The date and time (normalised to UTC with 'Z' annotation) when the BAH (and effectively the message) was created by the sender.
- **Copy Duplicate:** A flag indicating whether the message is a copy, a duplicate or a copy of a duplicate of a previously sent message.
- **Possible Duplicate:** A flag indicating the message *might* be a duplicate, often used during resends after potential transmission issues. It instructs the receiver to check if the original was processed, ensuring idempotent behaviour (processing the same logical message only once).
- **Priority:** An optional field indicating the relative processing precedence of this message compared to others.

Linking and security elements:
These elements connect the message to related messages and contribute to its integrity and authenticity.

- **Related:** Specifies the BAH information (like the BizMsgIdr) of a previous message to which this current message relates. This is used for replies (e.g. auth.031 status advice related to an auth.030 submission), cancellations or amendments.
- **Signature:** Contains the digital signature of the business message, allowing the receiver to verify the sender's identity and message integrity.
- **Cross Element Complex Rule: RelatedPresentWhenCopyDupl:** A rule within the standard stating that if the 'Copy Duplicate' flag is used, the 'Related' element *must* also be present and correctly reference the original message being duplicated.

Technical element:

- **Character Set:** Specifies the character encoding (e.g. UTF-8) used for the text-based elements within the business message payload.

These elements collectively provide the necessary framework for the TR system to manage the flow of reporting data efficiently and securely.

7.5.2 South African requirements

- **From/To**: Must use valid LEIs registered in GLEIF database
- **BusinessMessageIdentifier**: Must follow format: `<LEI>-<YYYYMMDD>-<SEQUENCE>`
- **MessageDefinitionIdentifier**: Must match the message schema version in use
- **CreationDate**: Must be in UTC format with "Z" timezone indicator

7.5.3 Validation rules

- BAH must be well-formed XML compliant with head.001.001.01 schema
- All mandatory fields must be populated
- BusinessMessageIdentifier must be unique for sender/receiver combination
- CreationDate must not be in the future
- MessageDefinitionIdentifier must match actual message content

7.6 Trade Affirmation and UTI Sharing (ODP-to-ODP)

The TR will support pre-reporting trade affirmation and UTI sharing for trades where **both** counterparties are licensed ODPs. The workflow below enables ODPs to surface trades to each other and coordinate UTIs to improve pairing/matching and overall data quality.

The system will provide each ODP with a dedicated inbound stream of trades where it is **Counterparty 2**, so it can (a) consume or confirm the **UTI**, and (b) optionally use the payload to seed its own reporting pipelines and validations.

When an ERR/RSE submits a trade to the TR, the TR creates an **allegement** event and routes a copy to the **ODP identified by the LEI captured in the Counterparty 2 field** via that ODP's chosen connection method.

Trade affirmation inbound and outbound endpoints will be defined in the relevant onboarding instructions, depending on the ERR/RSE's chosen connection method.

8. Reporting workflows using ISO 20022 standards

This section details how to report derivative transactions and their lifecycle events to the South African TR using the adopted ISO 20022 message standards, aligned with the EMIR REFIT framework and modified for South Africa.

The primary messages are auth.030 (Derivatives Trade Report) for trade events and valuations and auth.108 (Derivatives Trade Margin Data Report) for collateral information.

Accurate reporting relies on correctly using Action Types and Event Types for each submission associated with a Unique Transaction Identifier (UTI).

8.1 Introduction to lifecycle reporting

Each report submitted to the TR describes either the creation of a derivative, a change to its state, or its ongoing status (like valuation or margin). The auth.030 message uses a combination of an **Action Type** (defining the report's purpose) and, where applicable, an **Event Type** (defining the business reason for the action) to precisely describe the reported event. Using the correct combination, as defined by the EMIR REFIT standard, is essential for maintaining an accurate lifecycle history for each UTI.

8.2 Core reporting actions - Action Types

These define the fundamental purpose of your report submission within the auth.030 message (unless noted otherwise). Ensure that you select the correct Action Type for each situation:

NEWT (New):

- **Purpose:** To report a derivative transaction (identified by its UTI) to the TR for the first time. This action establishes the initial record.
- **Usage:** Used when a new trade is executed and reportable. Must be the first action reported for any given UTI. Requires population of all relevant trade details.
- **Event Types:** Used with Event Types like TRAD (standard trade), CLRG (creation via clearing), EXER (creation via exercise), ALOC (allocation resulting in new trades), CORP (creation via corporate event), COMP (creation via compression/PTRR), NOVA (creation via step-in/novation).

MODI (Modify):

- **Purpose:** To report a modification to the terms or details of a previously reported, active derivative *that is not a correction of an error*.
- **Usage:** Captures changes agreed between counterparties or resulting from trade features (e.g. scheduled notional changes, option exercises amending terms, partial terminations reducing notional). The report should reflect the state of the trade *after* the modification. Requires population of fields relevant to the modification and potentially updated fields like valuation.
- **Event Types:** Used with Event Types like TRAD (renegotiation), COMP (modification via PTRR), ETRM (modification due to partial early termination), EXER (modification due to exercise), ALOC

(partial allocation), CREV (modification due to credit event), CORP (modification via corporate event), UPDT (transitional update).

CORR (Correct):

- **Purpose:** To correct errors in specific data fields of a *previously submitted and accepted* report. This is *only* for fixing reporting mistakes, not for reflecting new economic events or bilaterally agreed changes.
- **Usage:** Requires resubmitting the *entire original report* with the erroneous fields corrected. It references the specific report being corrected. Cannot be used to change key identifiers like UTI or Counterparty IDs after initial submission. Does not change the trade's economic state history, only the reported data for a past point in time.
- **Event Types:** No Event Type is used with CORR.

TERM (Terminate):

- **Purpose:** To report the termination (full) of an active derivative *before* its scheduled expiration date.
- **Usage:** Applied when a trade ceases to exist due to a specific event. Natural expiry at maturity date generally does not require a TERM report (the trade simply becomes inactive based on its maturity date). The final state before termination should be reported.
- **Event Types:** Used with Event Types like ETRM (bilateral early termination), CLRG (termination due to clearing), EXER (termination due to full exercise), ALOC (termination of block trade upon allocation), CREV (termination due to credit event), CORP (termination via corporate event), COMP (termination via compression/PTRR), NOVA (termination via step-in/novation.

VALU (Valuation):

- **Purpose:** To report the daily mark-to-market or mark-to-model valuation of an active derivative.
- **Usage:** Submitted daily using the auth.030 structure. Primarily involves populating valuation amount, currency, timestamp and type fields. Does not report changes to other trade terms.
- **Event Types:** No Event Type is used with VALU.

EROR (Error):

- **Purpose:** To cancel an *entire report* that was submitted erroneously. Use this *only* if the reported derivative (or specific report instance) should be disregarded entirely.
- **Usage:** Used for scenarios like reporting a trade that never existed, reporting a trade not subject to FSCA rules, or cancelling a duplicate submission. It invalidates the specific report identified. Cannot be used to correct field-level errors (use CORR for that).
- **Event Types:** No Event Type is used with EROR.

REVI (Revive):

- **Purpose:** To reinstate a derivative that was previously and *incorrectly* cancelled using Action Type 'EROR' or terminated using Action Type 'TERM'.
- **Usage:** Used to undo an erroneous cancellation or termination, making the trade active again in the TR. Can only follow an 'EROR' or a mistaken 'TERM' action for a given UTI.
- **Event Types:** No Event Type is used with REVI.

**Note: Margin/Collateral reporting uses Action Type MARU within the auth.108 message - see Section 8.6*.*

8.3 Contextual events - Event Types

These codes provide the business context for NEWT, MODI and TERM actions within the auth.030 message:

- **TRAD (Trade):** Standard trade event – used for initial execution (with NEWT) or subsequent renegotiation/modification not covered by other specific event types (with MODI).
- **NOVA (Step-in/Novation):** A change in one or both counterparties, legally replacing an existing party with a new one. Can result in NEWT (for the new trade leg involving the new party) and TERM (for the old trade leg being replaced).
- **COMP (PTRR/Compression):** A Post-Trade Risk Reduction event, such as portfolio compression, which may terminate existing trades (TERM/COMP) and potentially create new ones (NEWT/COMP).
- **ETRM (Early Termination):** Bilateral agreement to terminate a trade before its scheduled maturity, where no other specific event type applies (used with TERM or MODI for partial termination).
- **CLRG (Clearing):** Submission of a trade to a Central Counterparty (CCP). Typically results in the termination of the original alpha trade (TERM/CLRG) and the creation of new cleared trades (NEWT/CLRG).
- **EXER (Exercise):** Exercise of an option or swaption. Can result in modification of terms (MODI/EXER), termination (TERM/EXER) or creation of a new underlying trade (NEWT/EXER).
- **ALOC (Allocation):** Allocation of a block trade to multiple end clients/funds. Can result in new allocated trades (NEWT/ALOC) and potentially modification (MODI/ALOC) or termination (TERM/ALOC) of the original block trade.
- **CREV (Credit Event):** A credit event occurrence affecting a credit derivative, potentially leading to modification (MODI/CREV) or termination (TERM/CREV).
- **CORP (Corporate Event):** A corporate action on an underlying equity or entity affecting the derivative's terms, leading to modification (MODI/CORP) or termination (TERM/CORP).
- **UPDT (Update):** Primarily used during transitional periods to update outstanding derivatives to meet new reporting requirements (used with MODI).

8.4 Valid Action Type/Event Type combinations

It is critical to understand that **only specific combinations of Action Types and Event Types are valid**. For instance, Action Type VALU or CORR do not use an Event Type. Reporting an invalid combination will result in rejection.

Refer to Section 13.2 for the definitive matrix detailing all valid combinations as per the EMIR REFIT standard adopted by the South African TR. Ensure your reporting logic strictly adheres to this matrix.

8.5 Key workflow examples (conceptual)

- **New IRS involving two ERR:** ERR A sends NEWT/TRAD. ERR B sends NEWT/TRAD.
- **Daily valuation:** ERR A sends VALU. ERR B sends VALU.
- **Correction of notional:** ERR A discovers error in previous report, sends CORR (no Event Type) with corrected notional and all other data as it was in the corrected report.
- **Trade cleared:** ERR A (original alpha) sends TERM/CLRG. ERR A (new beta leg vs CCP) sends NEWT/CLRG.
- **Portfolio compression:** Original trades terminated via TERM/COMP. New resulting trade(s) reported via NEWT/COMP. Link via PTRR ID field.

8.6 Margin reporting workflow (auth.108)

Reporting of collateral (Initial Margin, Variation Margin, Excess Collateral) is handled separately using the **auth.108 Derivatives Trade Margin Data Report** message.

- **Action Type:** The primary Action Type within auth.108 is **MARU (Margin Update)**.
- **Frequency:** Submitted daily by ERR, or via delegation by RSE
- **Content:** Includes collateral portfolio codes, collateral amounts posted/received (pre/post haircut), currency, and relevant timestamps. Corrections to margin reports are typically submitted as another MARU report with the corrected values for the relevant date.

8.7 Dual-sided reporting considerations

For ERR-ERR trades, successful processing relies on consistency:

- **UTI:** Both ERR MUST use the exact same UTI.
- **Action/Event Types:** Both ERR should ideally report corresponding lifecycle events using the same valid Action Type/Event Type combination to ensure smooth pairing and reconciliation by the TR. Discrepancies may lead to reconciliation breaks requiring investigation.

9. Validation rules

The South African TR employs a multi-layered validation process upon message receipt to ensure data quality, integrity and compliance with regulatory requirements. This process aligns with the EMIR REFIT validation methodology and leverages the ISO 20022 message standards.

9.1 Validation process overview

All incoming messages undergo a sequential validation process:

1. **Technical validation:** Checks for basic message integrity, including schema compliance (XSD validation), correct Business Application Header (BAH) structure, message signature (HMAC) and authentication/authorisation of the ERR and/or RSE.

2. **Content validation:** Performs checks on the data content based on predefined rules. This includes:
   - **Field-level validations:** Examining individual field values against expected formats, data types and allowed value sets.
   - **Cross-field validations:** Ensuring logical consistency between related fields within the same message.
   - **Cross-message validations:** Verifying consistency across different messages related to the same derivative's lifecycle.

3. **Reconciliation validation (for dual-sided reporting):** Matching and comparing data submitted by both ERRs for the same UTI, applying defined tolerance levels. Reconciliation validations will only be applied to messages having successfully passed the technical and content validations.
   Validation outcomes:
   - **Acceptance:** The message passes all relevant validation checks and is processed.
   - **Warning:** The message passes validation but contains potential data quality issues or inconsistencies that require attention. The message is accepted and processed, but a warning is generated.

Feedback on validation outcomes is provided via specific response messages (see Section 9.3).

Detailed validation rules, including specific conditions and logic, are referenced from the EMIR REFIT framework and ISDA Best Practices documents and will be further detailed in Appendix 13.3.

9.2 Field-level validations

These validations check the syntax and semantics of individual data fields within a message:

- **Mandatory/conditional requirements:** Ensures all mandatory fields are populated. Conditional fields are checked based on the presence or value of other fields, action types or asset classes as specified in the rules. Referenced documents like the ISDA Best Practices provide detailed applicability matrices (M/C/O/-) for different action types.
- **Data type and format:** Verifies that field values conform to the defined data types (e.g. string, decimal, Boolean, date, code) and formats (e.g. ISO 8601 for dates/times, specific numeric precision, character limits, patterns).
- **Code list validation:** Ensures that values provided for coded fields match the permissible values defined in the relevant code lists (e.g. currency codes, country codes, action types, collateralisation categories).
- **LEI validation:** Checks the format (ISO 17442), validity and status (e.g. “Issued”, “Lapsed”) of Legal Entity Identifiers against the GLEIF database.

Common validation errors at this level include incorrect date formats, invalid LEIs, missing mandatory fields or use of unrecognised codes.

9.2.1 Cross-field validations

These rules check for logical consistency and dependencies between different fields within the same message:

Conditional dependencies: Validates fields required only under specific conditions. For example:
- Collateral portfolio code is mandatory only if Collateral portfolio is ‘Y’ (Yes).
- Termination date is checked against Maturity date and Execution timestamp if populated.
- Margin fields are conditional based on the Collateralisation status.

Logical relationships: Ensures fields align logically. For example:
- Dates must be sequential (e.g. Expiration date >= Effective date).
- Currency fields must be populated if corresponding amount fields have values (e.g. Currency of the value if Value of contract is populated).
- Attachment point must be less than Detachment point for tranched credit derivatives.

Product-specific validations: Rules specific to certain asset classes or product types are applied, based on fields like Asset class and Contract type. For example:
- Interest rate fields (e.g. fixed/floating rates, day counts) are validated for IR derivatives.
- Option fields (Option type, Strike price, Exercise style) are validated for options and swaptions.
- Credit derivative fields (Seniority, Reference entity, Tranche, attachment/detachment points) are validated for CR derivatives.

Refer to Appendix 13.3 for details on cross-field validation logic, guided by the EMIR REFIT rules.

9.2.2 Cross-message validations

These validations ensure consistency and logical progression across multiple related messages over the lifecycle of a derivative:

- **UTI consistency:** The UTI must remain unchanged throughout the lifecycle of a single derivative transaction. Linkages between related derivatives (e.g. post-clearing, allocation, PTRR) are validated using Prior UTI and PTRR ID fields.
- **Action type sequencing:** Submissions must follow the valid sequence of Action type values (e.g. 'NEWT' must be the first report, 'TERM' or 'EROR' generally prevent further modifications unless followed by 'REVI'). The Section 13.2 illustrates these state transitions.
- **Lifecycle event consistency:** The combination of Action type and Event type must be valid according to the defined matrix (e.g. 'NEWT' can be combined with 'TRAD', 'CLRG', 'EXER' etc.; 'VALU' requires no event type). See Section 13.2 for the valid combinations table.
- **Modification consistency:** When modifying ('MODI') or correcting ('CORR') a report, key identifying fields (like UTI, Counterparty IDs) generally cannot be changed. Changes must be consistent with the specified Event type.
- **Valuation/margin reporting:** Updates ('VALU', margin updates via auth.108) must reference an existing, active UTI.

9.3 Validation response handling

The TR communicates validation outcomes and processing status back to the submitter using specific ISO 20022 messages:

Status advice (auth.031): This is the primary feedback message, sent in response to auth.030 and auth.108 submissions. It indicates:

- Acknowledgement of receipt.
- Overall status: Accepted ('ACPT'), Partially Accepted ('PART', rarely used), Rejected ('RJCT').

Detailed validation results: If rejected ('RJCT'), it includes specific error codes and descriptions identifying the failed validation rules.

Warnings report (auth.106): Used to communicate potential data quality issues (warnings) that did not cause rejection. This includes issues like missing or outdated valuations/margins or abnormal values.

Rejection statistics report (auth.092): Provides aggregate and granular statistics on rejected submissions over a period, including rejection reasons.

Reconciliation statistics report (auth.091): Provides feedback on the reconciliation status of paired trades, highlighting breaks and inconsistencies.

Scheduled day-end and intraday reconciliation and trade status reports will be made available via the portal and response endpoints for the relevant connection method.

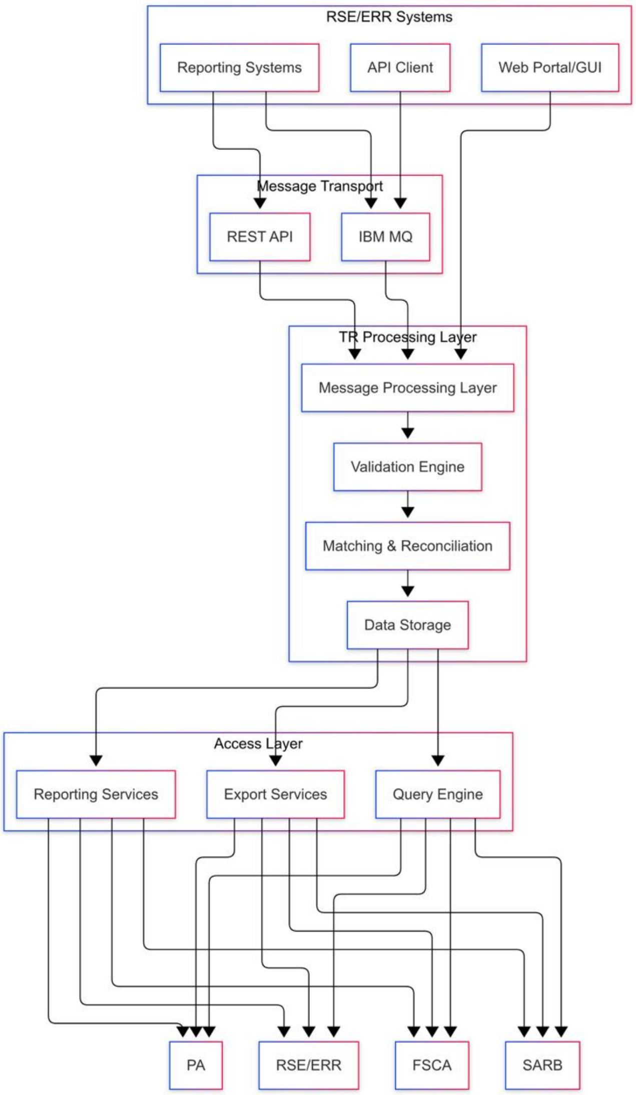
Reporting entities must monitor these response messages to confirm successful processing and to identify and remediate any reported errors or warnings promptly.

10. Technical architecture

10.1 System overview

The South African TR employs a robust hybrid architecture that combines on-premise and cloud components to ensure security, scalability and reliability.

10.1.1 Architectural framework



The South African TR system architecture consists of four main layers:

1. **Message ingestion layer**:
   - Receives incoming messages from market participants
   - Provides multiple connectivity options to accommodate different participant needs
   - Ensures secure, reliable message transmission

2. **Processing layer**:
    - Performs message validation and verification
    - Executes business logic and transaction matching
    - Processes lifecycle events and reconciliation

3. **Data persistence layer**:
    - Stores transaction and reference data
    - Maintains historical records and audit trails
    - Ensures data integrity and security

4. **Access layer**:
    - Provides controlled access to authorised parties
    - Generates reports and data extracts
    - Supports regulatory oversight and participant queries

10.2 Connectivity options

The ERR and/or RSE will be able to access the TR in one or more of the following ways:

10.2.1 Reporting system integration

Market participants can connect their reporting systems directly to the TR through the following channels:

1. **IBM MQ**:
    - Legacy message queuing protocol
    - Suitable for ODP's with existing MQ implementations

2. **Kafka Topics and Connectors**:
    - High-throughput, low-latency streaming protocol
    - Recommended for all new implementations
    - Offers robust integration with direct connectors to various source systems
    - Supports event-driven architectures

3. **SFTP**:
    - Secure File Transfer Protocol for file-based submission (ISO20022 XML format)
    - Daily batch processing of transaction reports
    - Suitable for low-volume participants

4. **REST API**:
    - Modern web-based interface using HTTPS protocol
    - Supports both individual message submission and small batch file uploads
    - Suitable for low-throughput machine-to-machine reporting

5. **SWIFT (Once Enabled)**:
    - Integration via the SWIFT network
    - Leverages existing SWIFT infrastructure
    - Global standard for financial messaging

- Suitable for both local and international participants

10.2.2 Portal access

For market participants who prefer direct interaction with the TR platform, a web-based portal will be available:

1. **Graphical User Interface (GUI) functionality**:
   - Browser-based user interface
   - Manual transaction reporting capabilities
   - Query and report access
   - User administration functions

2. **XML File Uploader**:
   - ISO20022 XML file format upload for single trade reporting
   - Validation and error reporting
   - Suitable for smaller participants or infrequent reporting

10.3 Security requirements

The South African TR mandates a multi-layered security model to ensure the confidentiality, integrity and availability of all reported data. All participants connecting to the TR via primary channels including IBM MQ, Kafka, REST APIs and SFTP must strictly adhere to these requirements.

10.3.1 Transport Layer Security (Secure Channel)

All communication channels connecting to the TR must be secured using Transport Layer Security (TLS) version 1.2 or higher. This establishes an encrypted tunnel for data transmission.

Connection establishment requires mutual TLS (mTLS). Both the participant's connecting system and the TR's endpoint will authenticate each other using valid digital certificates issued by the designated TR Certificate Authority. This verification occurs during the TLS handshake, ensuring both parties are authenticated before the secure channel is fully established. During onboarding, participants will receive specific instructions for obtaining and managing these certificates.

10.3.2 Network Layer Security (Firewall Access)

Connection attempts to the TR's endpoints (including MQ, Kafka, API, SFTP gateways) are restricted at the network firewall level. Participants must provide their specific, static, public IP addresses during onboarding for whitelisting. Only connections originating from these registered IP addresses will be permitted. Changes to static IPs will need to be communicated to the TR via the support desk **at least two weeks** prior to the change taking effect.

10.3.3 Authentication and authorisation

Multiple mechanisms ensure that only authorised entities and applications can access specific resources and perform actions. Participants will receive credentials for their chosen connection method during onboarding.

10.3.4 Message integrity and authenticity (HMAC)

To guarantee that submitted messages originate from the authenticated participant and have not been altered, all business messages must be digitally signed:

- **Message signing:** Each submitted business message payload must include an HMAC signature confirming the source and contents of the message.
- **Verification:** Upon receipt, the TR uses the HMAC signature to validate the authenticity of the message, verifying its origin and ensuring its content has not been tampered with.
- Details of the necessary keys and encryption standards will be shared during the onboarding process.

10.3.5 Supporting security practices

Effective security relies on participants maintaining robust internal practices:

- **Key management:** All credentials must be stored securely. The use of a Hardware Security Module (HSM) or equivalent secure vault technology is strongly recommended. Procedures must be in place for managing key lifecycles and for immediately reporting any suspected compromise.
- **Access monitoring and auditing:** Participants must maintain comprehensive, immutable audit logs of system access, credential usage and all interactions related to TR reporting.
- **Security assessments:** Participants may be required to provide attestations confirming compliance with these TR security requirements.
- **Incident response:** Participants must have documented procedures for responding to security incidents affecting their TR connectivity or data handling.

Compliance with this multi-layered security framework is mandatory. Specific technical parameters, key retrieval methods and operational details will be provided in detailed onboarding documentation and technical guides.

11. Proposed implementation timeline

The implementation of reporting to the South African TR will be determined by the Authorities based on updates to Conduct Standard 3 (CS3) and will follow a broad implementation across all market segments. The Authorities have advised that they intend to implement **mandatory** transaction reporting to the TR by **1 March 2027 at the earliest**.

11.1 Key milestones

Phase 1: Strate development and internal testing (Q3 2025 – Q2 2026)

- BRS and technical specifications sign-off: authorities and market consultation and sign-off on BRS and technical specifications
- Strate development: Core TR system development
- Potential early adopter development: Market development may commence for early adopters, potentially international ERR and RSE that are already compliant with EMIR reporting requirements
- Strate process documentation: Finalisation of operational processes and exception handling procedures
- Internal testing: Strate begins internal system testing

- Governance implementation: TR governance workplans executed

Market development and testing (to be determined)

- Market development: Market development commences (may be dependent on updated CS3)
- Testing expansion: Potential expansion from Strate internal testing to early adopter testing
- Governance delivery: Corporate governance framework implementation

Go-live preparation (to be determined in conjunction with the Authorities)

- Market testing: Mandatory market testing activities across all participants
- Governance completion: Completion of TR governance workplan
- Technical go-live: Strate technical go-live
- Onboarding preparation: Strate preparations for client onboarding into production

Production readiness and implementation (1 March 2027 onwards)

The onboarding of market participants will follow a structured approach to ensure orderly adoption.

11.2 Transitional arrangements – to be agreed with the TR Working Group

During the implementation period, the following transitional arrangements may be in place:

- **Relaxed validation:** Initial validation rules may be relaxed for historical trades to facilitate migration
- **Extended reporting windows:** Temporary extensions to reporting deadlines may be permitted during the early implementation phase
- **Enhanced support:** Dedicated technical support resources available during transitions

12. Summary of outstanding items

Item No.	Item	Status of issue	Comments
#1	Reporting of historical (open) OTC derivative transactions (initial migration strategy and transitional arrangements)	Open	Strategy to be defined in collaboration with the TR Working Group
#2	Onboarding pack	Open	Pack to be distributed once finalised
#3	Billing/Fee model	Open	To be determined based on data
#4	Implementation timeline	Open	To be determined by the Authorities

13. Appendices

13.1 Message schemas (XSD)

ISO provides message schemas for the complete set of auth messages here

13.2 Valid lifecycle event/action combinations

The following table defines the valid combinations of Action Types and Event Types for trade reporting at the *transaction level only*:

Action Type	Event Type	Applicability	Description
New	Trade	T	When a derivative with a new UTI is created for the first time through trade and not because of another prior event
New	Step-in	T	When a derivative with a new UTI is created for the first time due to a Step-in event
New	PTRR	T	When a derivative with a new UTI is created for the first time due to a Post-Trade Risk Reduction event
New	Clearing	T	When a derivative with a new UTI is created for the first time due to a Clearing event
New	Exercise	T	When a derivative with a new UTI is created for the first time due to an Exercise event
New	Allocation	T	When a derivative with a new UTI is created for the first time due to an Allocation event
New	Corporate Event	T	When a derivative with a new UTI is created for the first time due to a corporate action on the underlying equity
Modify	Trade	T	When a derivative with an existing UTI is modified due to renegotiation of the terms of the trade
Modify	Step-in	T	When a derivative with an existing UTI is modified due to a Step-in event

Action Type	Event Type	Applicability	Description
Modify	PTRR	T	When a derivative with an existing UTI is modified due to a PTRR event
Modify	Early termination	T	When a derivative with an existing UTI is modified due to an early termination agreed in advance or due to a partial termination
Modify	Exercise	T	When a derivative is amended due to the exercise of an option or swaption
Modify	Allocation	T	When a derivative with an existing UTI is partially allocated
Modify	Credit event	T	When a derivative with an existing UTI is modified due to a Credit event
Modify	Corporate Event	T	When a derivative with an existing UTI is modified due to a corporate action on the underlying equity
Modify	Update	T	When a derivative that is outstanding on the reporting start date is updated to conform with the amended reporting requirements
Correct	No event type required	T	When a derivative with an existing UTI is corrected due to an earlier submission of incorrect information
Terminate	Step-in	T	When a derivative with an existing UTI is terminated due to a Step-in event
Terminate	PTRR	T	When a derivative with an existing UTI is terminated due to a PTRR event
Terminate	Early termination	T	When a derivative with an existing UTI is terminated due to an early termination
Terminate	Clearing	T	When a derivative with an existing UTI is terminated due to a Clearing event

Action Type	Event Type	Applicability	Description
Terminate	Exercise	T	When a derivative with an existing UTI is terminated due to an Exercise event
Terminate	Allocation	T	When a derivative with an existing UTI is terminated due to an Allocation event
Terminate	Credit event	T	When a derivative with an existing UTI is terminated due to a Credit event
Terminate	Corporate Event	T	When a derivative with an existing UTI is terminated due to a corporate action on the underlying equity
Error	No event type required	T	When a derivative with an existing UTI is cancelled due to an earlier submission of incorrect information
Revive	No event type required	T	When a derivative that has been cancelled is reinstated due to an earlier submission of incorrect information
Valuation	No event type required	T	When data related to the valuation are submitted for a derivative with an existing UTI
Margin update	No event type required	T	When data related to the collateral are submitted for a derivative with an existing UTI

Legend: T = Transaction level

13.3 Validation rule references

ISDA provides a comprehensive validation rule reference here

13.4 Reference data tables

13.4.1 Sector codes

The below references the mapping between SARB sector codes published in August 2023 versus the EMIR sector codes.

ESMA Code	ESMA Description	SARB Code	SARB System	SARB Description

A	Agriculture, forestry and fishing	1	SIC	Agriculture, hunting, forestry and fishing
B	Mining and quarrying	2	SIC	Mining and quarrying
C	Manufacturing	3	SIC	Manufacturing
D	Electricity, gas, steam and air conditioning supply	41	SIC	Electricity, gas, steam and hot water supply
E	Water supply, sewerage, waste management and remediation	42	SIC	Collection, purification and distribution of water
F	Construction	5	SIC	Construction
G	Wholesale and retail trade, repair of motor vehicles	6	SIC	Wholesale and retail trade; repair of motor vehicles…
H	Transportation and storage	71	SIC	Land transport; transport via pipelines
I	Accommodation and food service activities	64	SIC	Catering and accommodation
J	Information and communication	75	SIC	Post and telecommunications
K	Financial and insurance activities	8	SIC	Financial intermediation, insurance, real-estate and business services
L	Real estate activities	84	SIC	Real-estate activities
M	Professional, scientific and technical activities	87	SIC	Research and development
N	Administrative and support service activities	85	SIC	Renting of machinery and equipment, without operator
O	Public administration and defence; compulsory social security	91	SIC	Public administration and defence activities
P	Education	92	SIC	Education
Q	Human health and social work activities	93	SIC	Health and social work
R	Arts, entertainment and recreation	96	SIC	Recreational, cultural and sporting activities
S	Other service activities	99	SIC	Other service activities
T	Activities of households as employers	01	SIC	Private households with employed persons

U	Activities of extraterritorial organizations and bodies	02	SIC	Extra-territorial organisations
AIFD	Alternative investment fund (AIF)	S124	Institutional	Non-money market fund investment funds
CDTI	Credit institution	S122	Institutional	Deposit-taking corporations (Banks)
CSDS	Central securities depository	S125	Institutional	Other financial intermediaries (specifically CCPs)
INUN	Insurance undertaking or reinsurance	S128	Institutional	Insurance corporations
INVF	Investment firm	S125	Institutional	Other financial intermediaries (investment banks, dealers)
ORPI	Institution for occupational retirement provision	S129	Institutional	Pension funds
UCIT	UCITS and management company	S124	Institutional	Non-money market funds

13.5 Base36 Encoding for UTI timestamps

13.5.1 Introduction to Base36 Encoding

Base36 encoding is a numeral system that uses 36 unique digits, consisting of the Arabic numerals 0-9 and the Latin letters A-Z. By using 36 distinct characters instead of the traditional 10 (decimal) or 16 (hexadecimal), base36 encoding allows for more compact representation of large numbers.

The digits in base36 have the following values:

- `0-9`: Represent values 0 through 9, as in decimal
- `A-Z`: Represent values 10 through 35

13.5.2 Why Base36 for UTI timestamps?

For UTI generation, base36 encoding offers several advantages:

- **Compactness**: Represents large millisecond values in fewer characters
- **Alphanumeric only**: Complies with UTI character restrictions
- **Case insensitivity**: Using uppercase letters only simplifies processing
- **Human readability**: More readable than binary or hexadecimal
- **Efficient storage**: Maximises the information contained in the allocated 7 characters

13.5.3 Encoding process for milliseconds since epoch

The process to encode milliseconds since epoch into a 7-character base36 string is as follows:

1. Calculate the milliseconds between the transaction timestamp and January 1, 1980 00:00:00 UTC
2. Convert this decimal (base10) value to base36
3. Pad with leading zeros if necessary to ensure a 7-character length

13.5.4 Mathematical conversion from decimal to base36

To convert a decimal number to base36:

1. Divide the number by 36
2. Record the remainder (0-35)
3. If the remainder is 0-9, use that digit
4. If the remainder is 10-35, use the corresponding letter (A-Z)
5. Take the quotient from step 1 and repeat until the quotient is 0
6. Reverse the sequence of remainders to get the base36 representation

13.5.5 Examples

Example 1: Converting recent date

Date: October 15, 2023 14:30:45.500 UTC

1. **Calculate milliseconds since epoch**:

   - Milliseconds between Jan 1, 1980, and Oct 15, 2023 14:30:45.500 = 1,381,845,845,500

2. **Convert to base36**:

   - 1,381,845,845,500 ÷ 36 = 38,384,606,819 remainder 32 → `W`
   - 38,384,606,819 ÷ 36 = 1,066,239,078 remainder 11 → `B`
   - 1,066,239,078 ÷ 36 = 29,617,752 remainder 6 → `6`
   - 29,617,752 ÷ 36 = 822,715 remainder 12 → `C`
   - 822,715 ÷ 36 = 22,853 remainder 7 → `7`

   - 22,853 ÷ 36 = 634 remainder 25 → `P`
   - 634 ÷ 36 = 17 remainder 22 → `M`
   - 17 ÷ 36 = 0 remainder 17 → `H`

3. **Result**: `HMP7C6BW`
4. **Apply 7-character limit**:
   - Take the rightmost 7 characters: `MP7C6BW`

Note: The actual value may vary slightly due to millisecond precision and exact calculation methods.

Example 2: Historical date

Date: June 15, 1995 09:45:30.250 UTC

1. **Calculate milliseconds since epoch**:

   - Milliseconds between Jan 1, 1980, and Jun 15, 1995 09:45:30.250 = 486,380,730,250

2. **Convert to base36**:

- 486,380,730,250 ÷ 36 = 13,510,575,840 remainder 10 → `A`
- 13,510,575,840 ÷ 36 = 375,293,773 remainder 12 → `C`
- 375,293,773 ÷ 36 = 10,424,827 remainder 1 → `1`
- 10,424,827 ÷ 36 = 289,578 remainder 19 → `J`
- 289,578 ÷ 36 = 8,043 remainder 30 → `U`
- 8,043 ÷ 36 = 223 remainder 15 → `F`
- 223 ÷ 36 = 6 remainder 7 → `7`
- 6 ÷ 36 = 0 remainder 6 → `6`

3. **Result**: `67FUJ1CA`
4. **Apply 7-character limit**:

- Take the rightmost 7 characters: `7FUJ1CA`

13.5.6 Decoding process

To decode a base36 timestamp back to a date:

1. Convert the base36 string to a decimal number
2. Add this number of milliseconds to the epoch (January 1, 1980 00:00:00 UTC)
3. The result is the original timestamp

Example decoding:

For base36 timestamp `MP7C6BW`:

1. **Convert to decimal**:

- M = 22 × 36^6 = 2,186,639,616
- P = 25 × 36^5 = 60,466,176
- 7 = 7 × 36^4 = 4,147,200
- C = 12 × 36^3 = 559,872
- 6 = 6 × 36^2 = 7,776
- B = 11 × 36^1 = 396
- W = 32 × 36^0 = 32
- Total: 2,251,821,068

2. **Add to epoch**:

- January 1, 1980 + 2,251,821,068 milliseconds = May 7, 1980 15:10:21.068

13.5.7 Edge cases and considerations

1. **Leading zeros**: Always pad the base36 representation to exactly 7 characters.
2. **Implementation precision**: Be aware of potential differences in millisecond calculation across systems.
3. **Time zone handling**: Always use UTC to avoid time zone complications.
4. **Date boundaries**: Take care at day/month/year boundaries when calculating milliseconds.

13.5.8 Implementation best practices

1. Use established libraries for date manipulation when available.
2. Implement comprehensive test cases covering various date ranges.
3. Include validation to ensure encoded timestamps are exactly 7 characters.
4. Establish a reference implementation to ensure consistency across systems.