

CMTAT

# Incorporating ICMA Bond Data Taxonomy in CMTAT

Proposal to include ICMA Fields and Tamper-Proof Methodology  
in CMTA's upcoming debt standard

November 2024

**cmta.**

# Tokenization of debt instruments – challenges linked to data uniformity



## **Challenges of tokenized debt instruments:**

- **No uniform terms:** Debt instruments have characteristics that vary from issuance to issuance, and there is typically no central register of debt instruments
- **Smart contract link:** If a debt instrument is tokenized, identifying to what instrument the token relates may be challenging if the smart contract does not include sufficient information
- **Difficulties in automation:** The lack of standardization in information found in smart contracts for debt securities makes straight-through processing (STP) and automated workflows considerably more challenging.



## **Business need:**

- **Standardization:** Introducing a standard governing what information should appear in the smart contract to be used when tokenizing debt instruments
- **Leverage existing taxonomy:** Taxonomies are complex, to the extent possible, CMTA's standards should seek to leverage established initiatives in the field, rather than developing its own taxonomy.



## **Solution :**

- Integrating the **ICMA Bond Data Taxonomy (BDT)** in CMTA's debt standard, with corresponding adjustments to the CMTAT framework
- The BDT provides unified language to describe common bond features, thereby reducing errors, enhancing the reliability in financial transactions and fostering interoperability
  - ICMA has already updated the BDT to include fields that are specific to tokenized fixed income securities

# BDT fields – Third party control option

## Third party control concept

By default, from a CMTAT perspective, all BDT fields would be populated and updated (as the case may be) by the issuer or by a third party services provider appointed by the issuer for this purpose.

It would however be possible to designate certain fields as controlled by a third party, such that a third party would have the ability to populate them.

Field Name	Issuer/Third Party Controlled	Purpose
Issue Date	Issuer	Lifecycle Tracking
Price Feed	Issuer	Real-Time Valuation
Proceeds	Issuer	Audit and Reporting
Issuer Rating Value	Third Party	Rating

As an example, the issuer may decide that the rating score is populated by a third party, e.g. a rating agency

## CMTAT implementation

- Giving third party access to certain functions is **purely optional**
- To give such access, the issuer would rely on the CMTAT authorization module (which is also used e.g. to authorize a third party to whitelist addresses)
- Prior to deciding that a field can be controlled by a third party, issuers would need to consider whether relevant third parties are technically equipped to fulfil their role

# BDT fields – Tamper-proofing

BDT fields can be added to CMTAT-compliant smart contracts in clear text, but it is proposed to also allow adding these fields in hashed format, to ensure data authenticity and prevent tampering. In terms of implementation, it is possible to have a single hash for all BDT fields, or to hash fields individually or smaller groups, to then create a Merkle tree. The two options are discussed below

## Single hash of BDT fields

- **Method:** Creates a single hash of the bond data taxonomy, stored on-chain.
- **Pros:** Simple, efficient, and easy to implement.
- **Cons:** Requires full data visibility, potentially compromising confidentiality.

## Merkle tree hashing for BDT fields

- **Method:** Each data field is hashed individually, forming a Merkle tree for cryptographic security.
- **Pros:** Allows selective verification, enhancing confidentiality and security.
- **Cons:** More complex but offers greater data integrity.

Proposal and specific recommendations to be discussed within CMTA's Tech and Corporate committees.

