TARGET Instant Payment Settlement

Access Rights Management

TIPS Contact Group #8

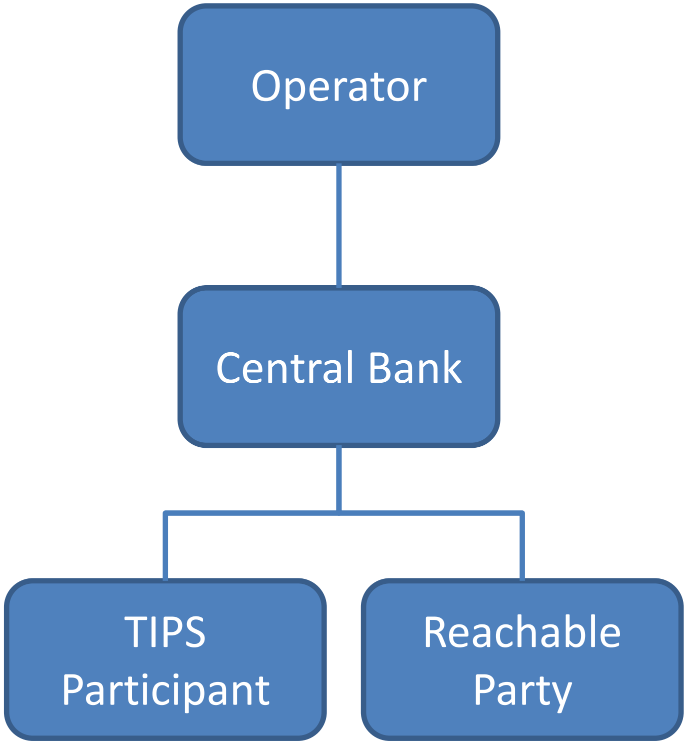
BANCA D'ITALIA EUROSISTEMA
BANCO DE ESPAÑA Eurosistema
BANQUE DE FRANCE EUROSYSTÈME
DEUTSCHE BUNDESBANK EUROSYSTEM

Frankfurt am Main, 04.07.2018

Access rights configuration in CRDM^TIPS

To ensure a smooth integration within the T2-T2S Consolidation framework, the access rights model of TIPS is being designed as a subset of the T2S access rights model.

Access rights are set up within **CRDM**.

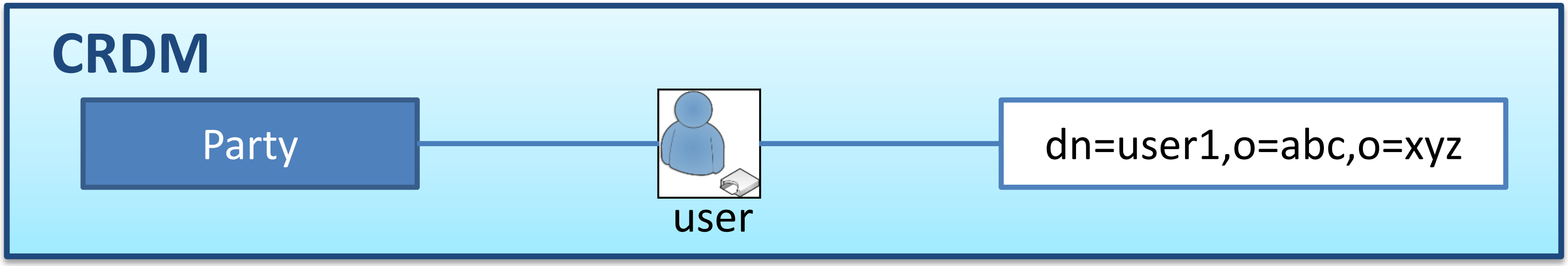


- The party model is based on a **hierarchical structure** (very similar to the cash branch of the T2S hierarchical party tree).
- Each piece of information belongs to one **system entity** (i.e. CB).
- Functions are granted **following the hierarchical party model** (e.g. by CBs to TIPS participants of their communities).

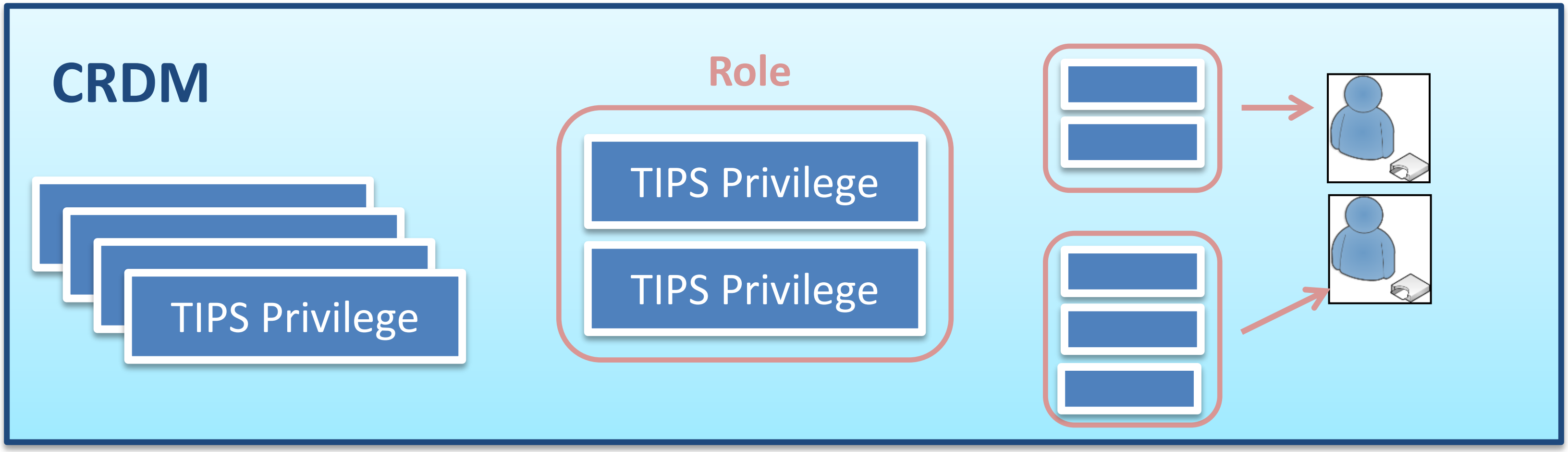
Access rights in CRDM^{TIPS}

- Access rights are based on a **RBAC** (Role-Based Access Control) model.
- Access rights management is **decentralized** (following the hierarchical party model).
- Privileges are granted to roles (they can not be granted directly to users or parties, differently from T2S). Roles are then granted to parties and users.
- Access rights granularity is **function-based and object-based** (i.e. account/CMB-based).
- The **data scope** is determined by the hierarchical party model. The data scope **cannot be altered** (differently from T2S).

TIPS Distinguished Names



- The capability to trigger a specific TIPS user function is granted by means of the related **Privilege** (stored within the **CRDM**).
- **CRDM** offers the possibility to group different Privileges into **Roles**.
- Roles are then granted to **users** identified by specific Distinguished Names (DNs)



TIPS Access Rights check

TIPS authorises the sender of a given request only if the related DN fulfils both of the following conditions:

1. **The DN has the relevant privilege(s) required to submit the request**
   - In other words, the DN submitting the request to TIPS must be linked to a User that has been granted the relevant privilege.
2. **The DN is authorised to submit the request on the requested business object(s)**
   - This condition depends on the business object itself on which a request is being performed
     - *For instance, in an Instant Payment transaction, the object is represented by the TIPS Account being debited; in an Account balance and status query, the object is the TIPS Account being queried*
   - TIPS applies specific business logic, which differs depending on the type of request, to determine whether a certain DN is authorised to act on a certain object.
   - If a certain DN is authorised to exercise a type of request (related to a specific Privilege) on a specific object, that object is said to be within the DN's **data scope** for that Privilege.

New privileges for CRDM^{TIPS}

The **CRDM access rights model** is based on the reuse of data and functional aspects from the T2S access rights management model.

Privileges to access functions related to **both CRDM and TIPS** will be stored in the CRDM database and assigned to the relevant Parties, Users and Roles through the CRDM functionalities.

The go-live of TIPS introduces two new privilege categories in the CRDM^{TIPS} context:

- **Privileges to handle new reference data objects within CRDM**

These new reference data objects are required for the set up of TIPS reference data, although some of them (e.g. Party-Service Link) are not strictly related to TIPS and may be used for the set up of data related to other services as well.

- **Privileges to grant access to specific TIPS functionalities**

These new privileges are assigned in CRDM (like all others) but they are strictly related to TIPS functionalities (e.g. instructing Instant Payments) and have no relevance for any function outside of TIPS.

New privileges for CRDM^{TIPS}

Parties that wish to connect to TIPS will therefore require three categories of privileges:

1. **Existing T2S privileges** to activate the corresponding functions in CRDM
   - *e.g. Create Party, Update Limit.*

2. **New CRDM privileges** to activate reference data management functions for new CRDM^{TIPS} objects
   - *e.g. Create Authorised Account User, Party Service Link Query.*
   - *The proposed approach is to adjust the already existing T2S default Roles for CBs to include these privileges.*

3. **New TIPS privileges** to activate specific TIPS functions
   - *e.g. Instruct Instant Payment, Adjust CMB Limit.*
   - *The proposed approach is to create a new default Role for CBs including these privileges.*

Update of T2S Roles

"National Service Desk (NCB)" Role – new privileges

Role: National Service Desk (NCB)		
Create Message Subscription Rule	Delete Message Subscription Rule	Update Message Subscription Rule
Create Message Subscription Rule Set	Delete Message Subscription Rule Set	Update Message Subscription Rule Set
Create Technical Address Network Service Link	Delete Technical Address Network Service Link	Data Migration Tool access
Create Party	Delete Party	Update Party
Create Report Configuration	Delete Report Configuration	Update Report Configuration
Create Limit	Delete Limit	Update Limit
Create T2S Dedicated Cash Account	Delete T2S Dedicated Cash Account	Update T2S Dedicated Cash Account
T2S Dedicated Cash Account Audit Trail Query	T2S Dedicated Cash Account Reference Data Query	T2S Dedicated Cash Account List Query
Market-specific Restriction Type Rule Detail Query	Market-specific Restriction List Query	Market-specific Restriction Type Rule Parameter Details Query
Market-specific Restriction Type Rule Set List Query	Limit Query	
Create Party-Service Link	Delete Party-Service Link	Update Party-Service Link
Create Authorised Account User	Delete Authorised Account User	Update Authorised Account User
Create DN-BIC Routing	Delete DN-BIC Routing	Update DN-BIC Routing

Update of T2S Roles

“Reading Role” Role – new privileges

Role: Reading Role		
T2S System User Query	T2S System User Link Query	Certificate Query
Data Changes of a Business Object Details Query	Data Changes of a Business Object List Query	Privilege Query
Message Subscription Rule List Query	Message Subscription Rule Set Details Query	Message Subscription Rule Set List Query
T2S BIC Query	Technical Address Network Service Link Details Query	Network Service List query
Party Audit Trail Query	Party List Query	Party Reference Data Query
Report Configuration Details Query	Report Configuration List Query	Country Query
Currency Query	Residual Static Data Audit Trail Query	System Entity Query
Queued Data Changes Query	Trouble Management System Access	Role List Query
Party-Service Link List Query	Party-Service Link Query	Authorised Account User Query
Service List Query	Service Query	DN-BIC Routing Query

Update of T2S Roles

New Role: “TIPS NCB Settlement Manager”

Role: TIPS NCB Settlement Manager
Modify All Blocking Status
Modify CMB Blocking Status
Adjust CMB Limit
Query All
Query as Reachable Party
Instruct Liquidity Transfer
Instruct Instant Payment

Responsible Actors

The Access Rights setup process will follow the blueprint already in place for T2S.

- The CRDM Operator will set up Central Bank parties and the related Party Administrator Users, as well as grant the relevant default Roles.

- The Central Bank Party Administrator will set up Payment Bank parties, the related Party Administrator Users and the relevant Role grants.

- Central Banks have the option to create their own Roles and propagate them selectively to Payment Banks.

- Central Banks will also set up links between their Payment Banks and TIPS in the form of Party Service Links, which also define the TIPS participation type (i.e. as TIPS Participant or Reachable Party).

- Central Bank and Payment Bank Party Administrators will set up their own business users, link them to the relevant DN and set up the correct access rights, in the form of Role/Privilege grants and possibly authorisations to instruct on a specific TIPS Account or CMB.

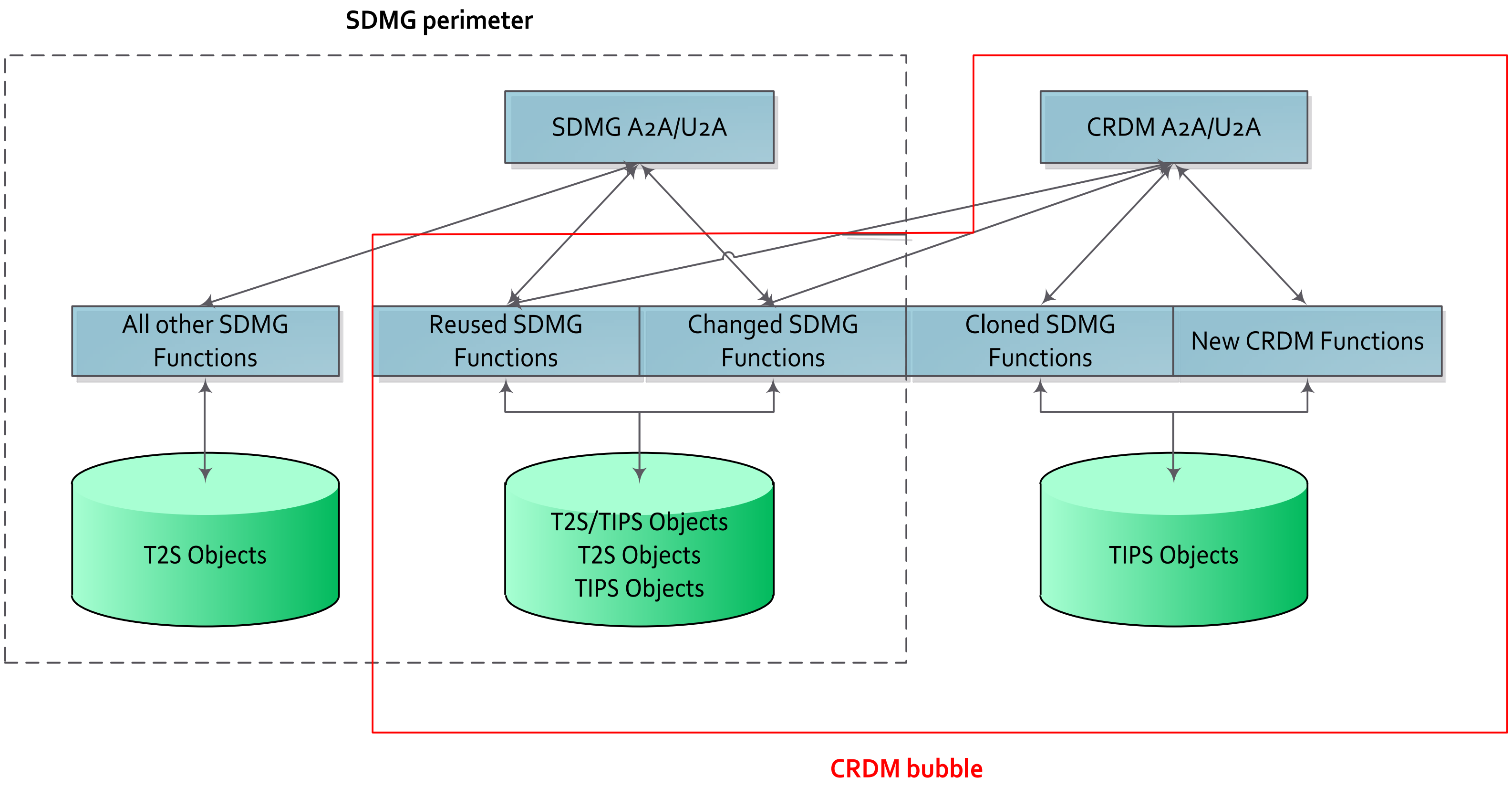
Q&A

Will data propagation to TIPS affect T2S operations?

- Data set up in CRDM will be propagated to TIPS on a daily basis.
- Changes made in CRDM will be available in TIPS only after each subsequent propagation.
- This will not cause any effect in T2S data or from an operational perspective.
- T2S static data management will continue working as it does today.

Will T2S Users see CRDM^{TIPS} data and vice versa? (1/2)

- CRDM and T2S data is stored in the same physical database.
- Visibility and segregation criteria are applied to prevent any impact to T2S functions and possible misuse of the new objects from T2S side.



Will T2S Users see CRDM^{TIPS} data and vice versa? (2/2)

- The actual visibility criteria depend on the specific objects. There are three main cases:

1. **Fully shared objects** where the same instances are relevant and used by both services (e.g. Parties, Users).

2. **Categorised shared objects** which are used in both services but each instance has a specific link to a single service (e.g. Cash Accounts, Limits). Specific attributes or properties determine the relationship between an object instance and its relevant service.

3. **Service-specific objects** which only have meaning for one service (e.g. Authorised Account User and DN-BIC Routing for CRDM-TIPS; Securities and CSD Account Links for T2S).

Q&A

Will T2S privileges grant access to CRDM^{TIPS} functions?

- As stated before, certain pre-existing privileges in T2S are used to activate functions that also exist in CRDM (e.g. Create Party, Create Report Configuration)

- These privileges can be granted to Users from both the CRDM and T2S interface.

- Data segregation is ensured by the normal access rights rules

  e.g. a User can only modify a Cash Account if it falls within their data scope

- In addition, certain types of shared data are not accessible through T2S due to the aforementioned visibility rules

  e.g. TIPS Accounts are completely invisible/not accessible from T2S;
  Report Configurations for TIPS Reports are completely invisible/not accessible from T2S