Over the Counter Channel Application (OTCnet)
Introduction and Usage of ISIM in OTCnet

July 2018

ISIM Overview

What is ISIM?

▸ ISIM stands for IBM Security Identity Manager. It is a user provisioning and role management system used for managing users across multiple Fiscal Service applications

What does ISIM do?

▸ ISIM provides the capability for security administrators to create and modify Fiscal Service user identities and to assign and modify user roles for specific Fiscal Service applications. ISIM is customized to support the requirements of specific Fiscal Service applications. OTCnet is one of the applications supported by ISIM

▸ For OTCnet, ISIM is used to create and modify OTCnet users and to manage each user's role or roles within the OTCnet application

▸ Users created using ISIM are provided with an Fiscal Service-wide, Single-Sign-On identity and can be assigned (if authorized) to other Fiscal Service applications that support Fiscal Service Single-Sign-On

Who uses ISIM in OTCnet?

▸ OTCnet employs a "distributed user management process" where each Federal Agency manages its own OTCnet users. Specifically, ISIM is used by an agency's OTCnet security administrators to manage its OTCnet users

▸ Each agency participating in OTCnet must have a minimum of two OTCnet security administrators at the highest level (department level) as defined in OTCnet. This is necessary in order to allow for the request/approval process workflow, which is described later in this document. The OTCnet agency adoption team will assist new agencies in setting up their two security administrators

ISIM Roles and Responsibilities

What is a Primary Local Security Administrator (PLSA)?

▸ Each agency can designate one and only one user as a PLSA. During the process of on-boarding an agency to OTCnet, a PLSA for the agency is designated and created

▸ The responsibility of the PLSA is to manage OTCnet access for users in their agency. Depending on the needs of an agency, the role of managing user access can also be delegated to one or more Local Security Administrators (LSAs). A PLSA can create additional Local Security Administrators (LSAs) as needed

What is a Local Security Administrator (LSA)?

▸ An LSA has the same responsibilities as a PLSA, that is, to manage OTCnet access for users in their agency

What are the primary differences between an LSA and a PLSA?

▸ Multiple LSAs can exist for an agency. Only one PLSA can exist for an agency

▸ An LSA cannot create another LSA; LSAs can only create and manage users who are not security administrators. Only the PLSA can create additional LSAs for their agency

▸ An LSA can exist at lower levels in a agency's hierarchy (e.g. department level or lower). A PLSA can only exist at the highest level of an agency

▸ LSA users can only manage users belonging to their own access group or to access groups at lower levels within the same organizational hierarchy to which they belong

ISIM Example PLSA and LSA Users within an Agency

Level 0

Department (top) Level

PLSA   LSA
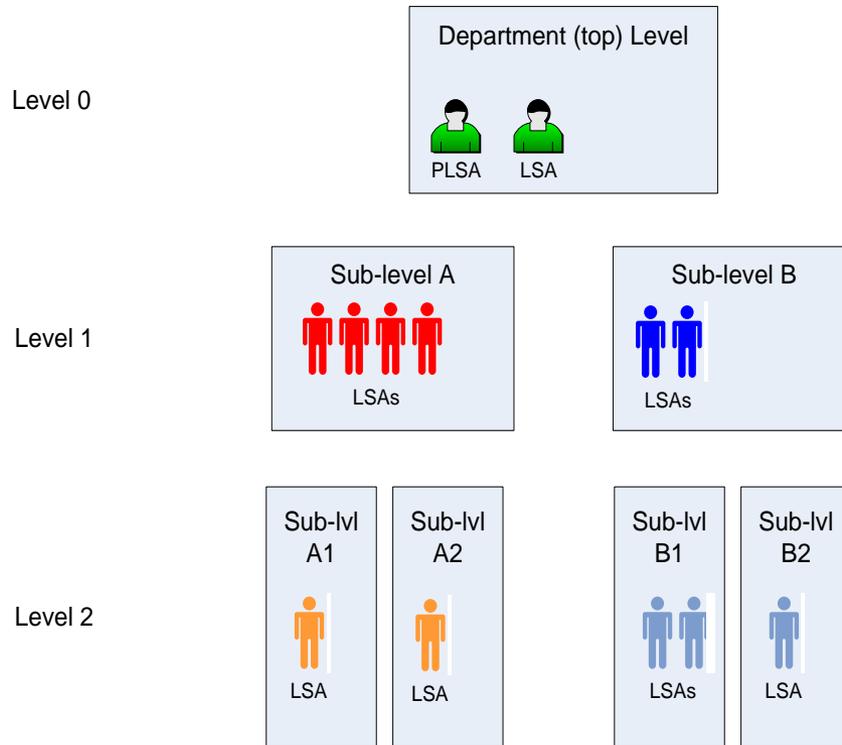
At the highest level of an agency, a PLSA and at least one LSA must exist

Level 1

Sub-level A

LSAs

Sub-level B

LSAs

Multiple LSAs can exist at lower levels of an agency

Level 2

Sub-lvl A1

LSA

Sub-lvl A2

LSA

Sub-lvl B1

LSAs

Sub-lvl B2

LSA

Each of the red LSAs can only create and modify OTCnet users within the following access groups:

• Sub-level A

• Sub-lvl A1

• Sub-lvl A2
The orange LSA belonging to **Sub-lvl A1** can only create and modify OTCnet users within **Sub-lvl A1**

ISIM Roles and Responsibilities (con't)

Why is it necessary to have two security administrators at the highest level?

▸ Fiscal Service requires all application-specific user management actions to be approved by an authorized user. ISIM implements an electronic approval process to address this requirement for OTCnet

▸ To support this requirement, an agency must have at least one user who can submit a user management request and at least one user who can approve the request. As a result, it is required for each agency to have two security administrators at the highest level (a PLSA and an LSA)

▸ The PLSA can act as an approver for a request submitted by the LSA and the LSA can act as an approver for a request submitted by a PLSA

▸ The ISIM Request Approval Process for OTCnet is discussed in detail later in this document
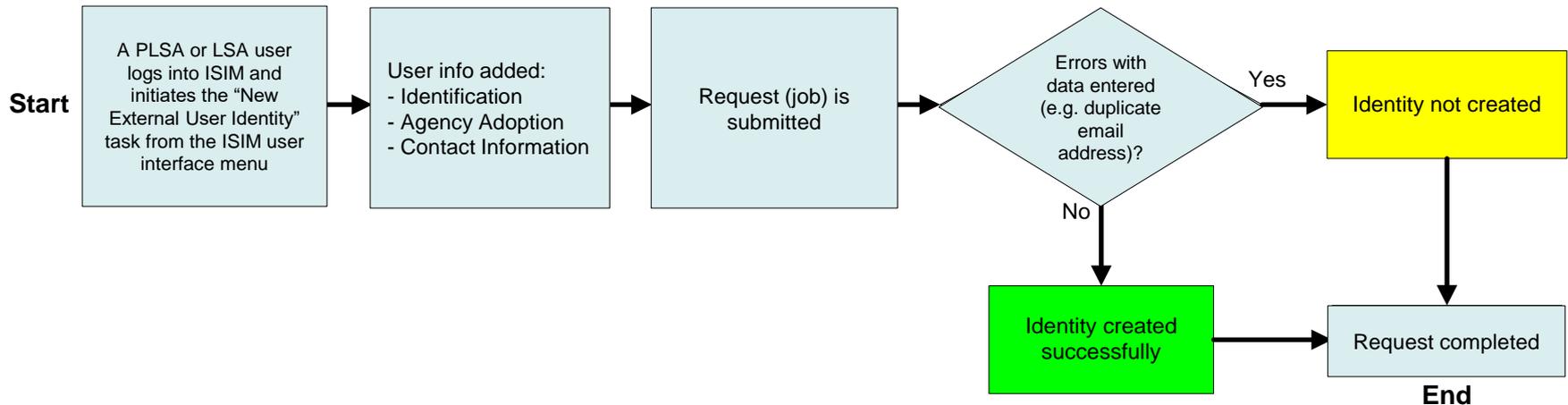
ISIM Tasks

The specific ISIM tasks performed by an OTCnet security administrator (PLSA or LSA) include the following:

- Creation of a new external user identity

- Modification of an existing external user identity

- Resetting the password for an existing external user identity

- Creation of a new OTCnet account for an external user identity

- Modification of an existing OTCnet account for an external user identity

- ISIM Request Approval Process for OTCnet

The above tasks are not necessarily specified in order of execution, as different scenarios require the execution of different tasks.

ISIM Creation of a New External User Identity

▶ Creation of a new external user identity is necessary if the user does not have an existing Fiscal Service Single-Sign-On identity. If a user was (formerly) an active TGAnet user, the user already has an Fiscal Service Single-Sign-On identity and the creation of a new identity is not required

▶ To create a new external user identity, the PLSA or LSA logs into ISIM and performs the task. The process workflow is as follows:

Start

A PLSA or LSA user logs into ISIM and initiates the "New External User Identity" task from the ISIM user interface menu → User info added:
- Identification
- Agency Adoption
- Contact Information → Request (job) is submitted → Errors with data entered (e.g. duplicate email address)?

Yes → Identity not created

No → Identity created successfully → Request completed
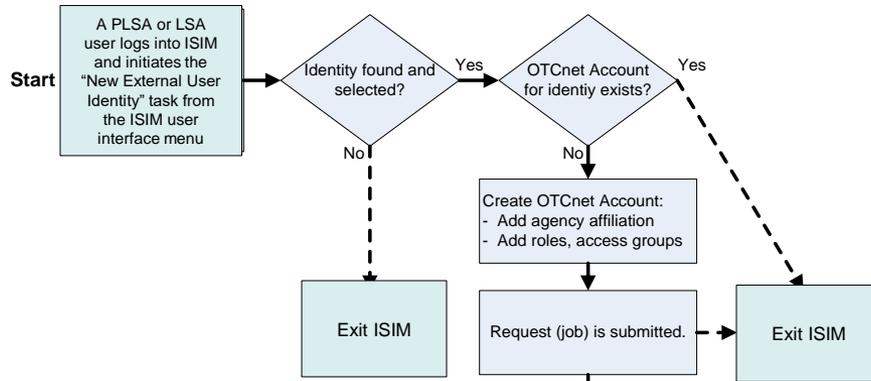
Identity not created → Request completed

End

▶ Note that this task does not incorporate the ISIM request approval process for OTCnet; creation of an external user identity does not require approval from another security administrator

▶ For a detailed, step-by-step instructions on how to create an external user identity, please refer to the printable job aid for managing user accounts
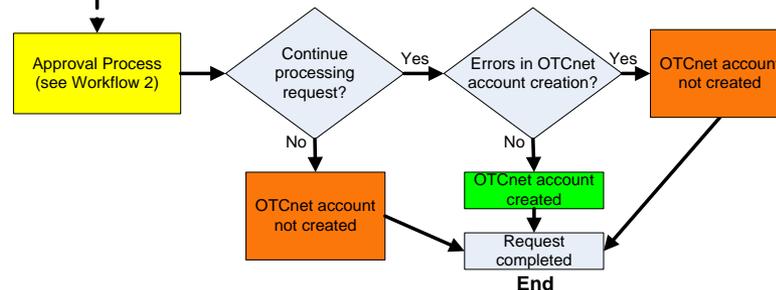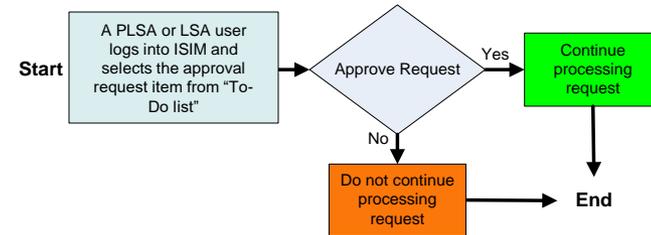
ISIM Creation of a New OTCnet Account for an External User Identity

▸ To allow a user access to OTCnet, an OTCnet account must be created and roles and agency access groups must be assigned to the account. The user identity for which the OTCnet account is created must already exist. The process workflows are shown as follows:

Workflow 1 (Requestor)

Start → A PLSA or LSA user logs into ISIM and initiates the "New External User Identity" task from the ISIM user interface menu → Identity found and selected?

- No → Exit ISIM
- Yes → OTCnet Account for identiy exists?
  - Yes → Exit ISIM
  - No → Create OTCnet Account:
    - Add agency affiliation
    - Add roles, access groups
    → Request (job) is submitted. → Exit ISIM

Request (job) is submitted → Approval Process (see Workflow 2) → Continue processing request?
- No → OTCnet account not created → Request completed (End)
- Yes → Errors in OTCnet account creation?
  - Yes → OTCnet account not created → Request completed
  - No → OTCnet account created → Request completed (End)

Workflow 2 (Approver)

Start → A PLSA or LSA user logs into ISIM and selects the approval request item from "To-Do list" → Approve Request
- Yes → Continue processing request → End
- No → Do not continue processing request → End

▸ This task incorporates the ISIM request approval process for OTCnet; creation of an OTCnet account requires approval from another security administrator. This is denoted in workflow 2 and the yellow process box in workflow 1

▸ For detailed, step-by-step instructions on how to create an OTCnet account, please refer to the printable job aid for managing user accounts

ISIM Roles

▸ OTCnet roles can be assigned during the OTCnet account creation/modification process. The OTCnet roles available to be assigned are shown in the following table:

Role Name	Role Description	Assignable By	Applicable For
Accounting Specialist (AccSpec)	The agency user in this role is an expert on the organizational structure, reporting needs and accounting rules for their agency. This role will establish and maintain the organizational foundation, accounting data and accounting relationships at the highest level of the agency in OTCnet.	Agency PLSA, LSA	Deposit Processing
Agency Manager	The agency user in this role can view/download CIRA and view reports.	Agency PLSA, LSA	Check Processing
View Report	This role is created to accommodate the need to users to have need to access to agency reports other than the Agency Manager role.	Agency PLSA, LSA	Check Processing
CIRA Viewer	The agency user in this role can only perform view location, view CIRA records and download CSV. This is the check processing role with the lowest level of access.	Agency PLSA, LSA	Check Processing
Deposit Approver	The agency user in this role will approve the deposit report and submit the information to the TGA financial institution.	Agency PLSA, LSA	Deposit Processing
Deposit Confirmer	The financial institution user in this role will verify the submitted deposit ticket, reject the deposit ticket if necessary, forward the information to the Treasury, and create adjustments, as necessary.	Financial Institution PLSA, LSA	Deposit Processing
Deposit Preparer	The agency user in this role prepares the deposit ticket and supporting information for transmission to the TGA financial institution.	Agency PLSA, LSA	Deposit Processing

ISIM Roles (con't)

Role Name	Role Description	Assignable By	Applicable For
FI Viewer	The financial institution user in this role will only be able to search / view deposit and adjustments, view Financial Institution information and produce reports from it.	Financial Institution PLSA, LSA	Deposit Processing
FRB Confirmer	The FRB user in this role will verify the submitted deposit ticket, reject the deposit ticket if necessary, forward the information to the Treasury, and create adjustments, as necessary.	Financial Institution PLSA, LSA	Deposit Processing
FRB Viewer	The FRB user in this role will only be able to search / view deposit and adjustments, view FRB information and produce reports from it.	Financial Institution PLSA, LSA	Deposit Processing
FPA Viewer	The FPA user in this role will only be able to search / view deposit and adjustments, and produce reports from it.	Agency PLSA, LSA	Deposit Processing
Local Accounting Specialist (AcSpecLocal)	The agency user in this role is an expert on the organizational structure, reporting needs and accounting rules for their depositing endpoint and its lower level endpoints. This role will establish and maintain the organizational structure, accounting code mappings to individual endpoints and the processing options that one or more lower level endpoints will use in OTCnet.	Agency PLSA, LSA	Deposit Processing
Agency Local Security Administrator (LSA)	The agency user in this role will maintain user access to an organization, including assigning/removing user roles and assigning/removing organization hierarchy access. (Approver, same capability of Agency PLSA).	Agency PLSA	All
Financial Institution Local Security Administrator (LSA)	The financial institution/federal reserve bank user in this role will maintain user access to an organization, including assigning/removing user roles and assigning/removing organization hierarchy access. (Approver, same capability of FI PLSA).	Financial Institution PLSA	All

ISIM Roles (con't)

Role Name	Role Description	Assignable By	Applicable For
MVD Editor	The agency user in this role can create, update and read verification records. This role can also download CSV formatted reports.	Agency PLSA, LSA	Check Processing
MVD Viewer	The agency user in this role can read CIRA records in addition to read verification records and read block record containing only ABA permissions. This role also has the permission to download CSV formatted reports.	Agency PLSA, LSA	Check Processing
Check Capture Lead Operator	Check Capture Lead Operator – The agency user in this role will have the ability to scan checks into a batch, close a batch, balance check amounts and entering batch control values during batch closing. However, Cashers are not allowed to accept duplicates, make MICR corrections, authorized the use of out-of-date LVD or accept checks with poor quality.	Agency PLSA, LSA	Check Processing, Check Capture
Check Capture Administrator	The agency user in this role has the capability to define and modify the check capture sites. For example, they will be able to setup the location policy and location group. This user will also configure the Check Capture functions and perform upgrades of the application. This user will have the permission to download user profiles for the site as well. Lastly, the user in this role will have the permission to download software or firmware to the terminal using the Download Check Capture application permission.	Agency PLSA, LSA	Check Processing, Check Capture
Check Capture Operator	The agency user in this role can perform only very minimal Check Capture activities.	Agency PLSA, LSA	Check Capture
Check Capture Supervisor	The agency user in this role is the most powerful user on the Check Capture site. The user can perform all the functions on the Check Capture including accept duplicates, make MICR corrections, authorize the use of out-of-date LVD, accept checks with poor quality.	Agency PLSA, LSA	Check Processing, Check Capture

ISIM Roles (con't)

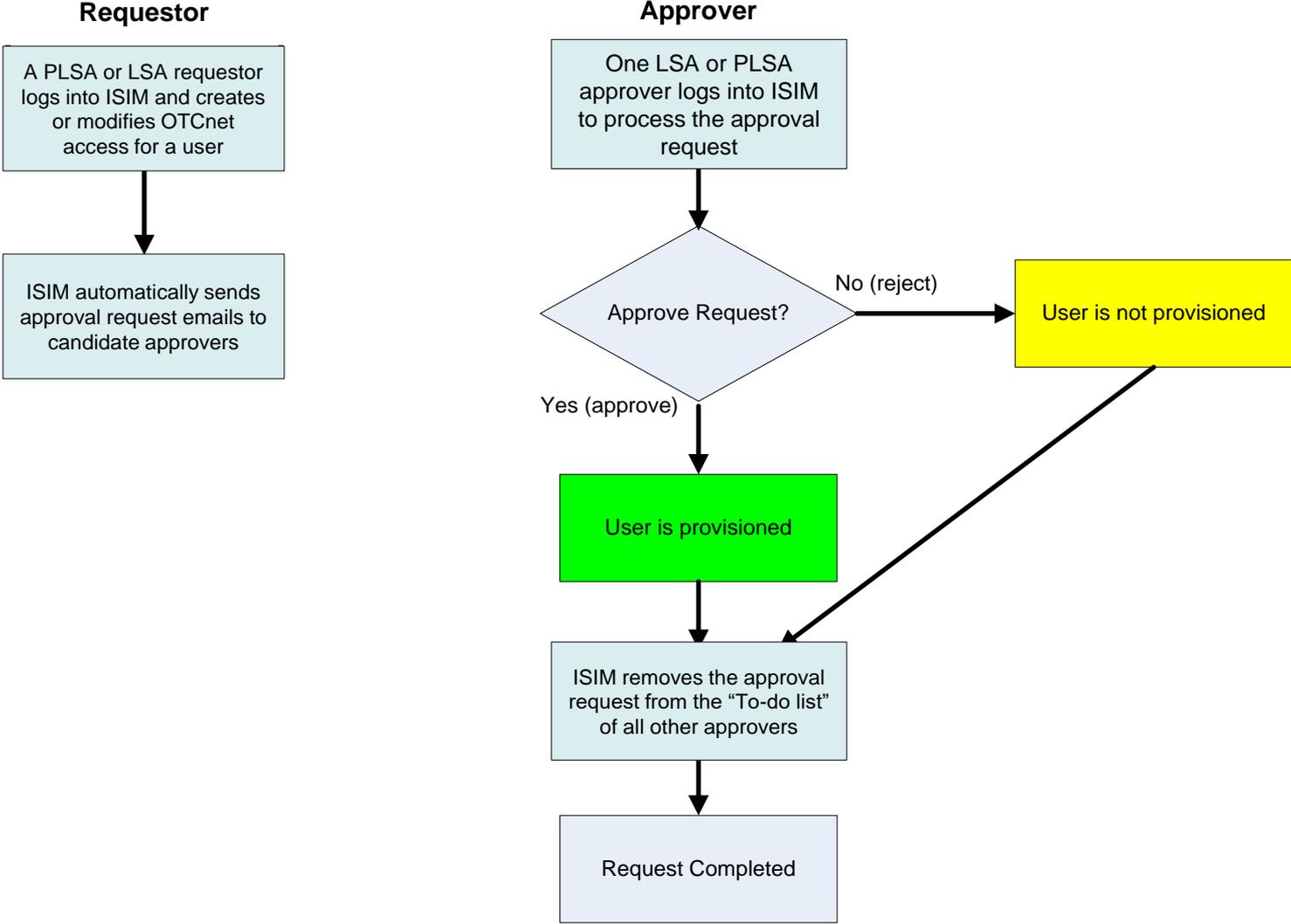| Role Name	Role Description	Assignable By	Applicable For
Batch Approver	The user assigned this role permission will have the ability to approve a batch either prior to batch upload (from Offline) or when a batch is uploaded/submitted to OTCnet but not yet approved. This permission is granted especially when, in offline mode, a user has configured the terminal to upload a batch upon Batch Close. An example of this permission applies to a Check Capture Operator: though a terminal may be configured to upload upon close, an Operator is able to close a batch but does not inherently have Upload permissions, therefore the user's permissions will override the terminal configuration, and the batch will not be automatically uploaded. Providing this permission along with Batch Uploader allows for the Check Capture Operator to auto-upload the batch upon close. This role should be granted in limited cases at sites where there is a need for the Operator to perform this function without a Supervisor present.	Agency PLSA, LSA	Check Processing, Check Capture
Batch Uploader	The Offline user assigned this role permission will have the ability to upload a batch from Offline OTCnet to the online database; this user has no other permissions, and therefore should typically be granted to a Check Capture Operator and Lead Operator. This permission is granted especially when, in offline mode, a user has configured the terminal to upload a batch upon Batch Close. An example of this permission applies to a Check Capture Operator: though a terminal may be configured to upload upon close, an Operator is able to close a batch but does not inherently have Upload permissions, therefore the user's permissions will override the terminal configuration, and the batch will not be automatically uploaded. Providing this permission along with Batch Approver allows for the Check Capture Operator to auto-upload the batch upon close. This role should be granted in limited cases at sites where there is a need for the Operator to perform this function without a Supervisor present.	Agency PLSA, LSA	Check Processing, Check Capture

ISIM Request Approval Process for OTCnet

▸ Once an OTCnet account has been created in ISIM, a request for approval is automatically created by ISIM. As mentioned earlier, the request must be approved by an authorized user, using ISIM

▸ As mentioned in slide 5, an agency must have at least one user who can submit an OTCnet account creation or modification request and at least one user who can approve the request in order to support the request approval process. As a result, it is required for each agency to have two security administrators at the highest level (a PLSA and an LSA)

▸ The PLSA can act as an approver for a request submitted by the LSA and the LSA can act as an approver for a request submitted by a PLSA

▸ Additional LSAs at the same or lower levels can be created to allow for additional requestors and approvers

Scope of the ISIM Request Approval Process for OTCnet

The ISIM Request Approval Process only applies when provisioning OTCnet access (e.g. creating or modifying an OTCnet account) and not when managing user identities

▸ The ISIM Request Approval Process **does not** apply for the following tasks:

- Creation of a new external user identity

- Modification of an existing external user identity

- Resetting the password for an existing external user identity

▸ The ISIM Request Approval Process **does** apply for the following tasks:

- Creation of a new OTCnet account for an external user identity

- Modification of an existing OTCnet account for an external user identity

ISIM Request Approval Process Workflow

Requestor

A PLSA or LSA requestor logs into ISIM and creates or modifies OTCnet access for a user

↓

ISIM automatically sends approval request emails to candidate approvers

Approver

One LSA or PLSA approver logs into ISIM to process the approval request

↓

Approve Request?

No (reject) → User is not provisioned

Yes (approve) ↓

User is provisioned

↓

ISIM removes the approval request from the "To-do list" of all other approvers

↓

Request Completed

ISIM Approval Process

What determines if a security administrator is a requestor or approver?

▸ All LSAs and the PLSA are potential requestors and potential approvers. If a PLSA or LSA initiates an OTCnet account creation or modification task in ISIM, the action triggers a request and the PLSA or LSA automatically becomes the requestor

▸ The approver(s) for a request are determined by the location of the requestor in the agency's organizational hierarchy. The approvers are any LSA or PLSA users that exist in the same or higher access group as the requestor and within the same hierarchy branch as the requestor

▸ To ensure efficient operation, ISIM limits the number of approvers to a maximum of 12. ISIM automatically selects the approvers for each request, eliminating the need for agencies to designate specific approvers. If there are more than 12 LSAs, who are potential approvers within the hierarchy of the requestor, ISIM will automatically choose the 12 approvers. This offers convenience by eliminating the need for agencies to manually limit the number of approvers

▸ All approvers receive email notifications from ISIM, alerting them that a request requires their approval

ISIM Approval Process

What happens when a request is approved or rejected?

▸ Only one of the approvers needs to approve or reject a particular request. Once an approver logs into ISIM and approves or rejects the request from their "To-do list", the request is completed and is no longer available for the other approvers to approve or reject

▸ Examples 1 and 2 on the next two slides illustrate example request creation and approval processes

– Example 1 shows an OTCnet user at an intermediate level (Access Group B) being provisioned by a requestor residing at the highest level (Access Group A) of the agency.

– Example 2 shows an OTCnet user residing at the lowest level (Access Group E) being provisioned by a requestor residing in an intermediate level (Access Group B). Follow the steps in order (denoted in yellow) from each example to learn about the specific processes.
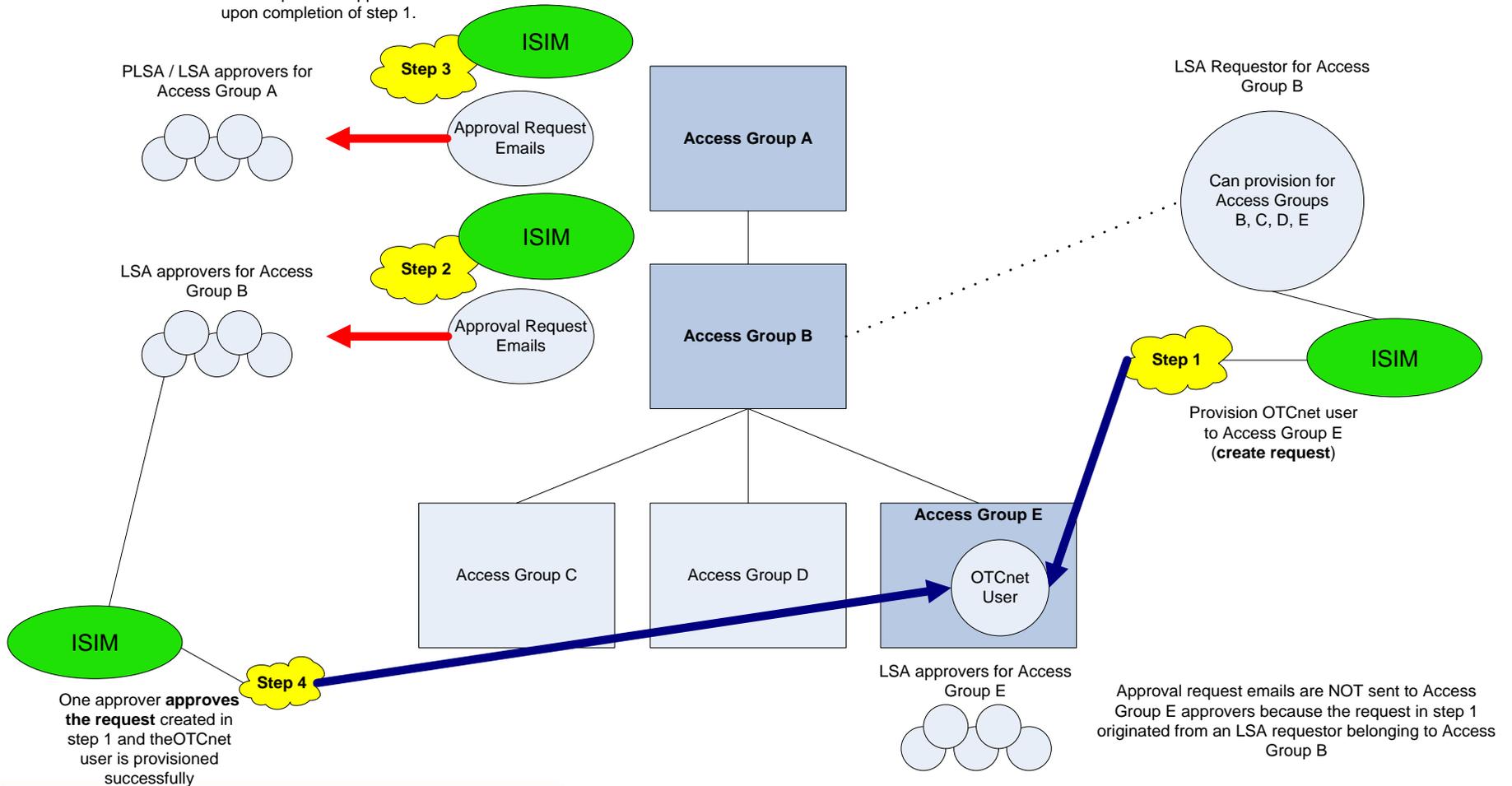
ISIM Creation and Approval Process Example

Example 1: Request Creation and Approval Process (provisioning user to intermediate level by requestor at highest level)
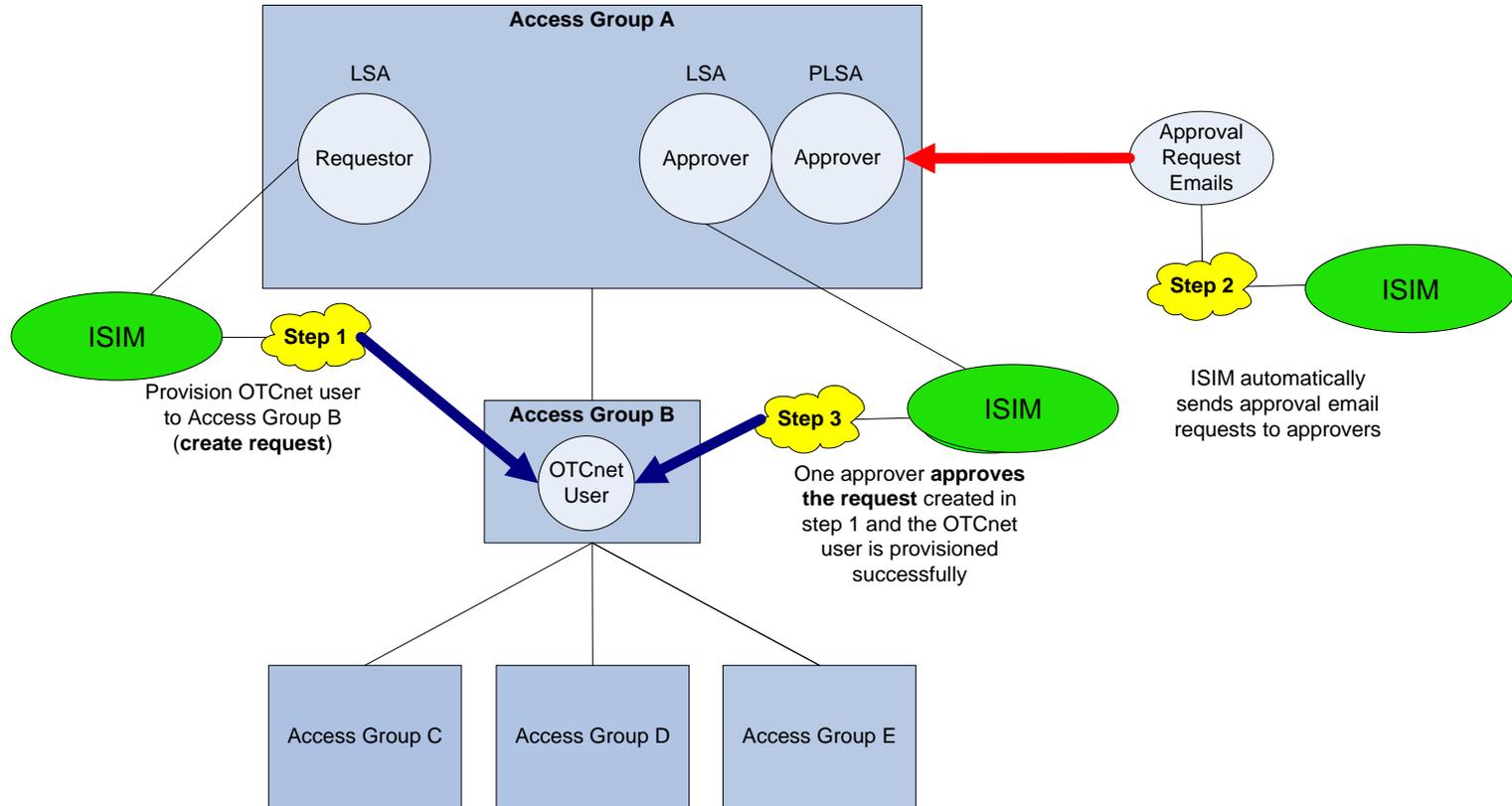
ISIM Creation and Approval Process Example

Example 2: Request Creation and Approval Process (provisioning user to lowest level by requestor at intermediate level)

For Steps 2 and 3, ITIM automatically sends approval email requests to approvers upon completion of step 1.

PLSA / LSA approvers for Access Group A

Step 3 — ISIM

Approval Request Emails

LSA Requestor for Access Group B

Can provision for Access Groups B, C, D, E

Access Group A

Step 2 — ISIM

LSA approvers for Access Group B

Approval Request Emails

Access Group B

Step 1 — ISIM

Provision OTCnet user to Access Group E (**create request**)

Access Group E

Access Group C

Access Group D

OTCnet User

ISIM

Step 4

One approver **approves the request** created in step 1 and theOTCnet user is provisioned successfully

LSA approvers for Access Group E

Approval request emails are NOT sent to Access Group E approvers because the request in step 1 originated from an LSA requestor belonging to Access Group B

ISIM Summary

▸ ISIM is used by OTCnet security administrators (PLSAs and LSAs) to create and modify users for their respective agencies

▸ To create or modify an OTCnet user, an OTCnet security administrator logs into ISIM and performs the following tasks:

  – Creates a new external identity (if necessary)

  – Creates or modifies an OTCnet account for an identity

▸ The creation or modification of OTCnet access for a user triggers a request approval process which requires an agency to maintain a minimum of two security administrators (either one can create a request and either one can approve requests created by the other)

▸ An agency's PLSA can create additional LSAs in order to delegate the task of creating users and approving requests to others

▸ An approver can only approve requests from another security administrator that exists in the same or lower level access group and in the same hierarchy branch of the approver's agency