SWIFT's Solution for ESMIG U2A Setup Guide

Step-by-Step

07 November 2022

Significant Changes

The following table lists the main changes in this publication of the document but does not include general edits and minor updates.

New and updated information	Location
Inclusion of ECMS information in the PAC file example	8. Prepare End User's Workstation - Browser

In addition to the installation information contained in release letters, see 7. Install ESMIG U2A SWIFT Login Application.

This document is updated on a regular basis. Please always use the latest version (link).

Contents

Introduction

This presentation describes all the steps necessary to access the ESMIG services in User-to-Application (U2A) mode. The ESMIG U2A flow is a browser-based solution based on the requirements imposed by the Eurosystem owning the service. The WebAccess method used to access other web services available through the SWIFT network was not adequate based on these requirements.

Connection to ESMIG U2A

End users connect to the ESMIG U2A services over SWIFT's secure IP network (MV-SIPN).

Connectivity to MV-SIPN is provided by an Alliance Connect VPN connectivity. Only Alliance Connect options with leased lines are allowed.

Alliance Cloud users can connect to ESMIG U2A using their current connection, where both MV-SIPN and Internet are allowed.

End user authentication

End users are authenticated by a personal certificate (SWIFTNet PKI certificate), stored either on a personal token or stored on an HSM box. As for any other SWIFTNet certificate, the SWIFTNet security officers can manage the personal token certificates and personal HSM certificates through the SWIFTNet Online Operations Manager.

ESMIG U2A SWIFT Login Application

The ESMIG U2A SWIFT Login Application is a software provided by SWIFT. It authenticates the end user before accessing the ESMIG U2A services. The application runs in the background and has an associated icon in the Windows notification area.

The latest release of the ESMIG U2A SWIFT Login Application supports both personal token and personal certificates stored on an HSM box. Since release 2.0 any Java dependencies have been removed and a proxy has been included. This proxy is referred to as “ESMIG proxy” in this document.

Notes

- **This document is based on ESMIG U2A SWIFT Login Application 2.0 and higher**. Previous versions of the documentation covering the initial solution to access ESMIG U2A (for example, using a Java proxy and the SWIFT Login Application 1.0) is available on the Knowledge Base article 5024862.
- The solutions that rely on a Java proxy do not support access to the ECMS service and will be phased out in November 2023.
- The usage of the ESMIG U2A SWIFT Login Application 2.0 and higher is **mandatory** for **Alliance Cloud** customers connecting to ESMIG U2A through the **Internet** (and so, **not** through MV-SIPN).
- A **personal HSM certificate** requires the ESMIG U2A SWIFT Login Application to be installed on the host running the end user’s browser, and **release 7.5 (or above)** of **SWIFTNet Link** and **Alliance Gateway.**
- A **personal token** requires Personal Token Software to be installed on the end user’s PC.
- As of release 2.0, the ESMIG U2A SWIFT Login Application came with **new URLs** to access the ESMIG and TIPS services – see 11. Access ESMIG U2A – URLs.

ESMIG U2A SWIFT Login Application

For customers setting up the U2A flow for the first time

The adoption of the ESMIG U2A SWIFT Login Application 2.x should be the preferred approach to access the ESMIG U2A platform.

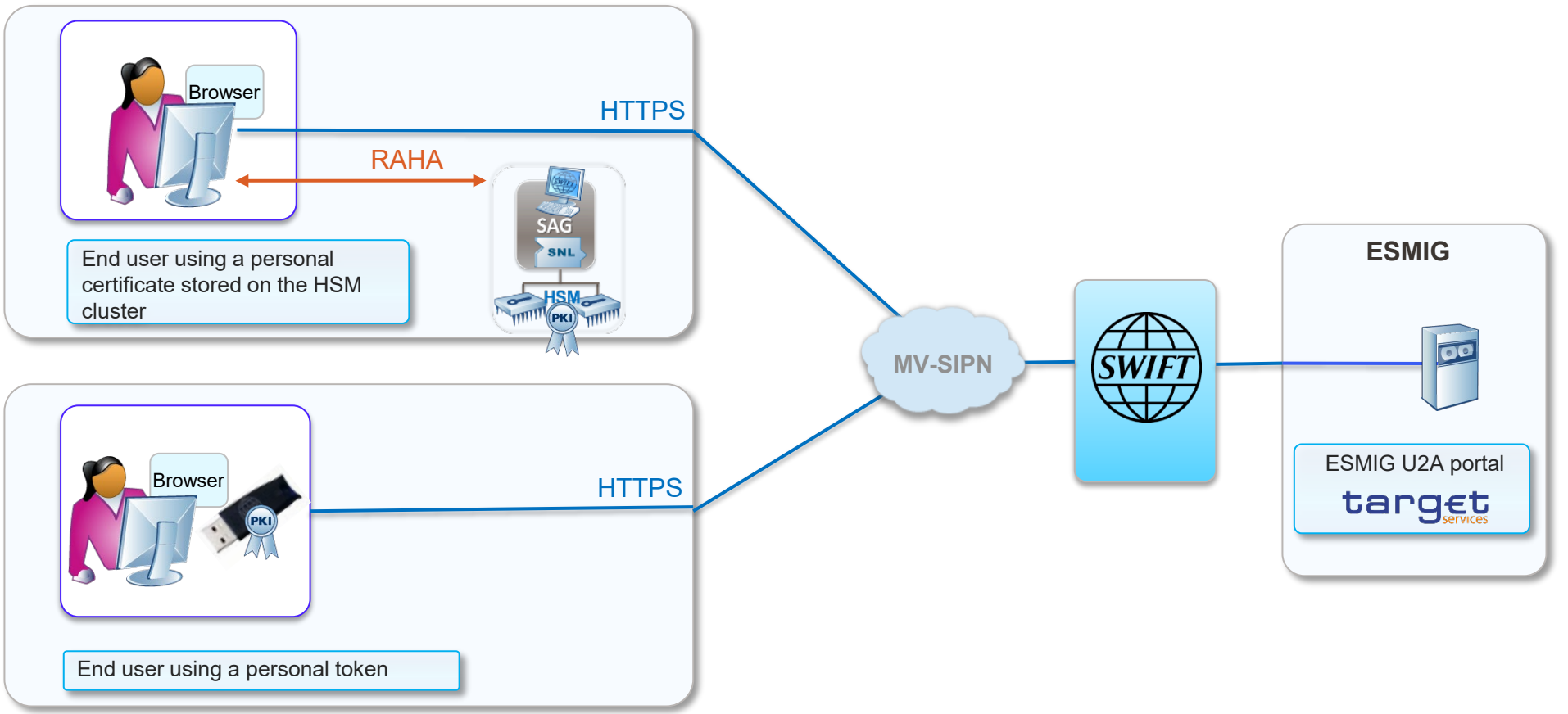
For customers already accessing TIPS and/or ESMIG U2A with an automatically downloaded Java proxy

Solutions that use a downloaded Java proxy will be phased out in November 2023. These solutions do not support access to the ECMS U2A services (none of the environments). For more information see Knowledge Base article 5024862.

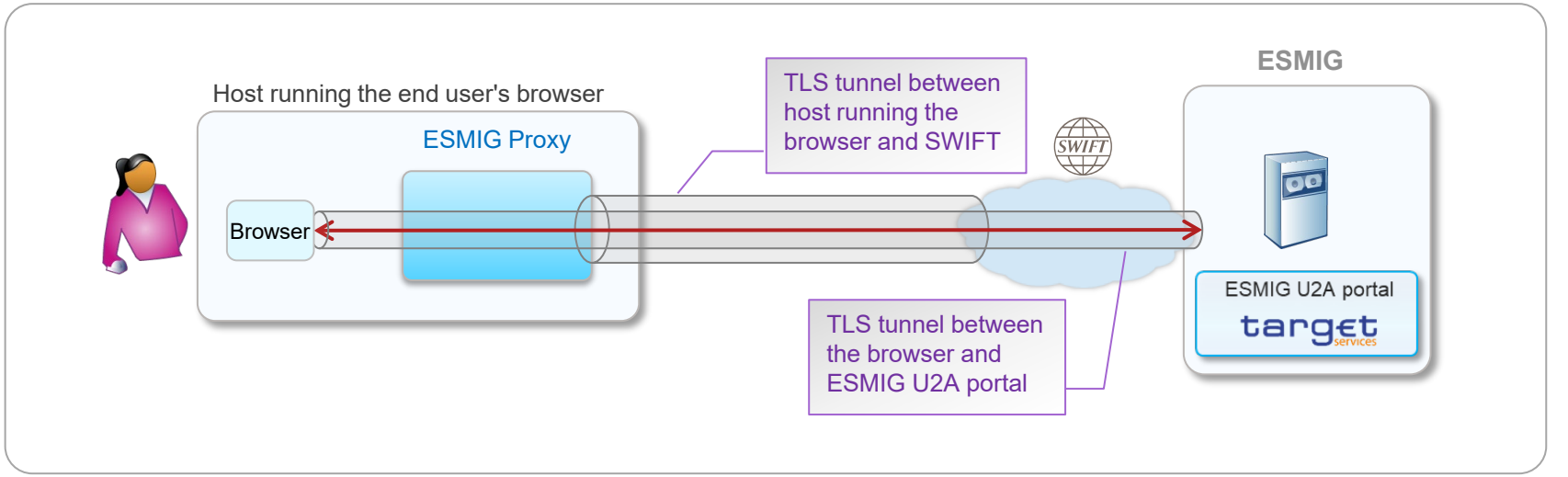
For all customers, the adoption of the ESMIG U2A SWIFT Login Application 2.x remains the preferred approach to access the ESMIG U2A platform.

Connection to ESMIG U2A

HSM-based certificate versus personal token certificate

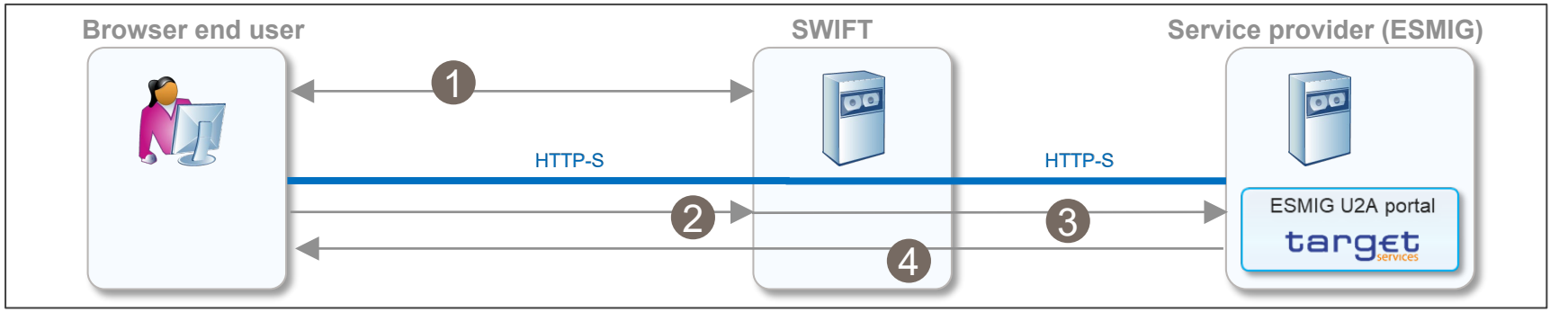


ESMIG U2A – Technical Overview



- A TLS tunnel is established with SWIFT to allow the CUG (Closed User Group) checks. Before establishing the connection with the ESMIG U2A web server, SWIFT verifies that the Distinguished Name of the personal certificate is part of the provisioned CUG.
- Subsequently, an end-to-end TLS tunnel is set up between the user's browser and the ESMIG U2A portal.

Connection Steps – High Level



End users authenticated by a personal HSM certificate or a personal token must first log in to the ESMIG U2A SWIFT Login Application*. See 11. Access ESMIG U2A.

1. User enters the ESMIG URL (see 11. Access ESMIG U2A - URLs) and reaches SWIFT.
2. SWIFT verifies that the DN of the certificate is allowed to access the ESMIG service (CUG).
3. SWIFT forwards the connection request to ESMIG.
4. TLS handshake from ESMIG (user enters the token password or Session PIN) and the end-to-end HTTP-S session is established.

*The ESMIG U2A SWIFT Login Application is provided by SWIFT and must be installed on the host running the end user's browser.

Contents

Preparation

- Familiarise yourself with ESMIG U2A documentation. See the SWIFT`s Solution for ESMIG Service Description for information about the features and functions of SWIFT's Solution for ESMIG. More general information on ESMIG is available at the SWIFT's Solution for ESMIG Support Page on swift.com.

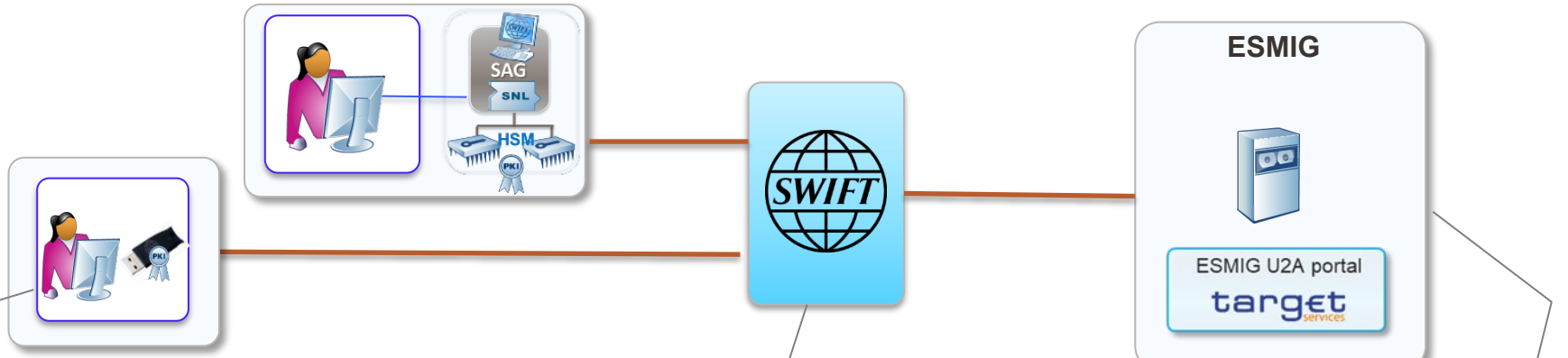
- To access the ESMIG U2A portal, you need a connection to SWIFT through a VPN box. The minimum bandwidth is 256 Kbps. In case of several concurrent users, the minimum recommended bandwidth is 512 Kbps. Alliance Cloud users can connect to ESMIG U2A using their current connection, where both MV-SIPN and Internet are allowed.

- Multi-factor authentication is a mandatory control type of the Customer Security Programme (CSP). A personal token can provide 2-factor authentication when it respects the PIN Code policy described in Knowledge Base article 5021567. For end users using a personal certificate stored on HSM (personal HSM certificate), multi-factor authentication can be provided at:
  - Operator PC login
  - Operator access to jump server
  - Login as a virtual SWIFTNet user on Alliance Gateway, linked to a multi-factor authentication type such as Lightweight Directory Access Protocol (LDAP) or Remote Authentication Dial-In User Service (RADIUS), if configured with multi-factor authentication on the server side.

  For more information about multi-factor authentication, see SWIFT Customer Security Controls Framework and Alliance Security Guidance.

- This guide does not cover instructions for installing and configuring software provided by the Eurosystem, such as the Ascertia GoSign desktop application. Please refer to the ECB website for those instructions.

ESMIG U2A - End User Registration



End users are identified by the DN (distinguished name) of the certificate stored on the personal token or HSM box.

```
cn=firstname-lastname,o=bbbbccll,o=swift
```

End users register with SWIFT to enable access to ESMIG U2A using an e-order page on www.swift.com
The configuration order form proposes by default BIC8 with wildcard.

```
*,o=bbbbccll,o=swift
```

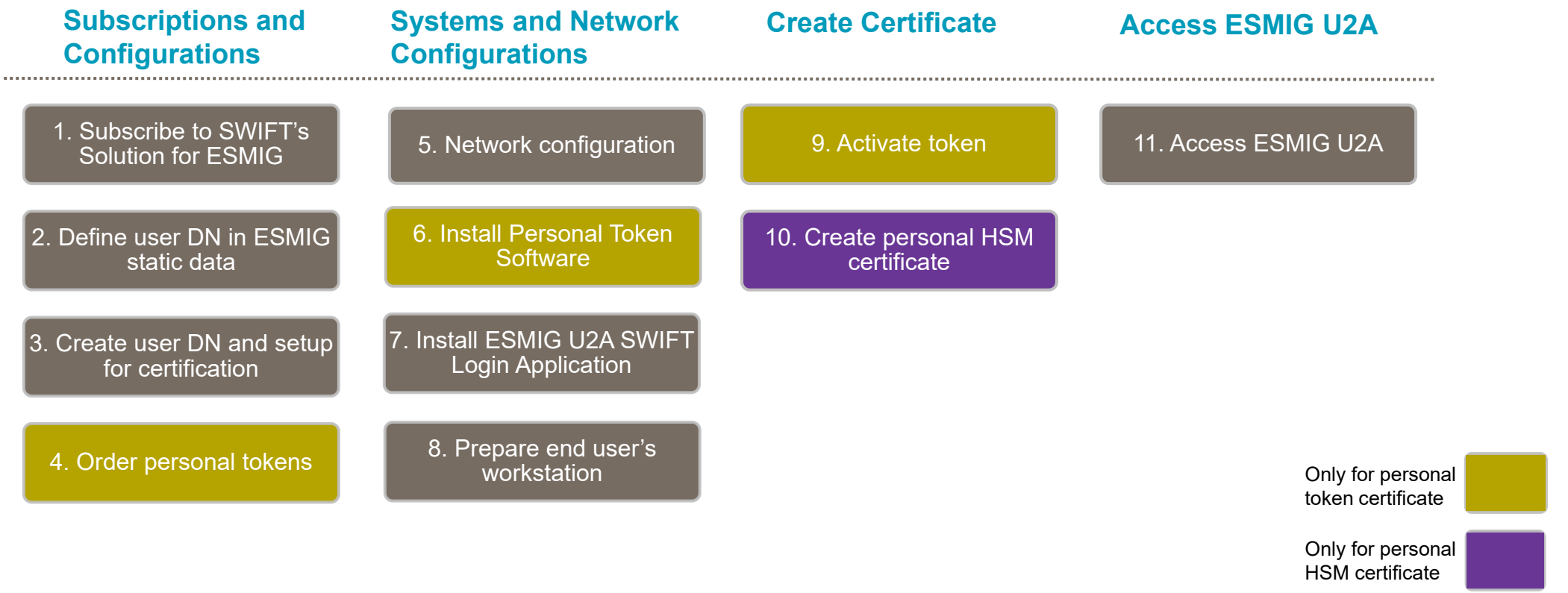
SWIFT performs the provisioning of the Closed User Group (CUG).

End users (ESMIG participants) register their user DNs in ESMIG static data.
The static data forms are made available to the participants by their respective Central Banks.
The association between DNs and ESMIG participants is maintained in ESMIG static data.

Contents

U2A Setup Steps – Overview

Note - Several of these steps can happen in parallel. The step numbers are just for reference to sections further on in this document.



Steps to be executed depending on the certificate class

End users can be authenticated by a certificate stored on a personal token or by a personal certificate stored on an HSM box. The choice is made by the SWIFTNet security officer when setting up the end user for certification (step 3).

As part of the end user's setup for certification, the security officer has to select the certificate class: Personal token or personal HSM.

The following steps must only be executed for end users authenticated by a personal token:

- 4. Order personal tokens
- 6. Install token software
- 9. Activate token

The following step must only be executed for end users authenticated by a personal HSM certificate:

- 10. Create personal HSM certificate

Alliance Cloud customers can only use **Personal Token.** The usage of HSM-based certificate is not an option in this case.

U2A Setup Steps – Roles and Related Documentation

Each step is detailed in the following pages.

Step	Responsible	Reference Documents
1. Subscribe to SWIFT's Solution for ESMIG	• ESMIG business owner (swift.com account)	Section "Ordering and Subscription" in the SWIFT`s Solution for ESMIG Service Description
2. Define user DN in ESMIG static data	• ESMIG business owner	ESMIG operator documentation
3. Create user DN and setup for certification	• SWIFTNet security officer	Section "Certificate Management" in the SWIFTNet Online Operations Manager - User Guide
4. Order personal tokens	• Token administrator	Boxes of 10 personal tokens can be ordered on swift.com in the ordering section
5. Network configuration	• Network administrator	• Knowledge Base article 5018711 • Section "Network Configuration in the SWIFT WebAccess Configuration and Troubleshooting Guide
6. Install Personal Token Software	• System administrator	See Personal Token Software Installation Guide

Only for personal token certificate

Only for personal HSM certificate

U2A Setup Steps – Roles and Related Documentation

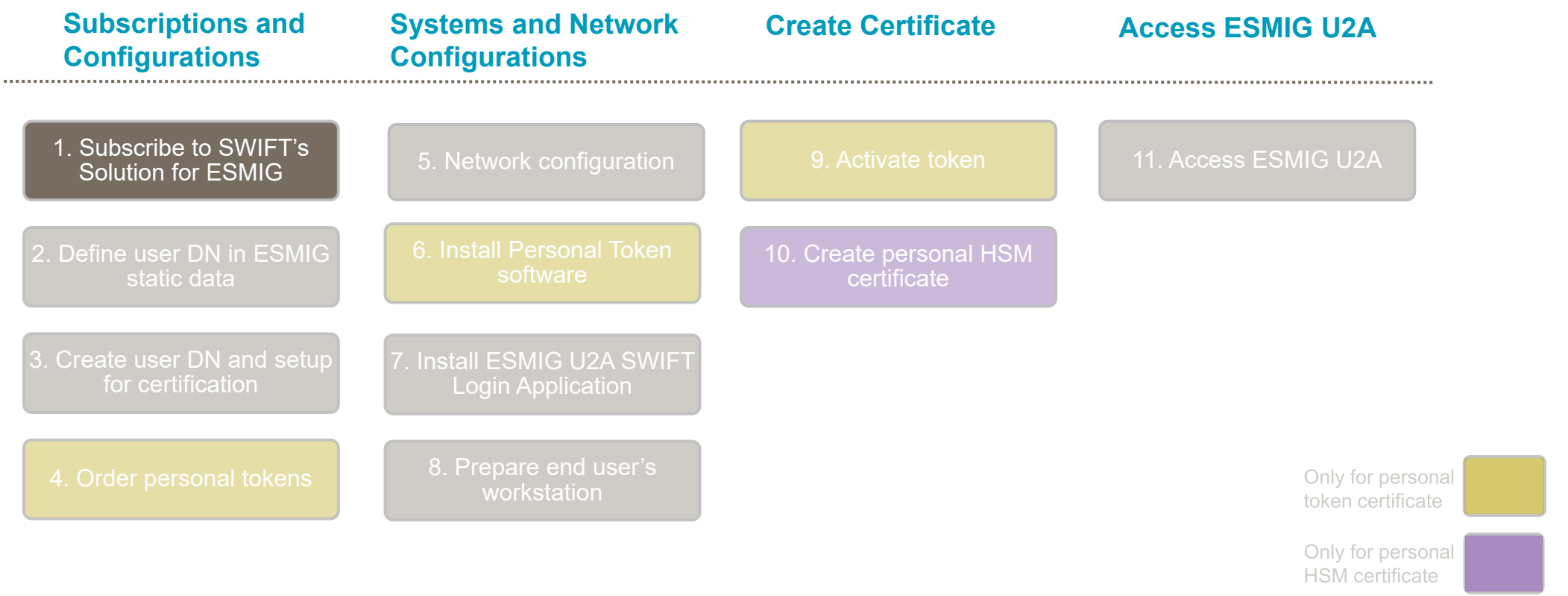
Each step is detailed in the following pages.

Step	Responsible	Reference Documents
7. Install ESMIG U2A SWIFT Login Application	• System administrator • Alliance Gateway administrator	Section “Application Interface” in the Alliance Gateway 7.5 Administration and Operations Guide
8. Prepare end user’s workstation	• System administrator • End user	Section “SWIFT CA Certificate ” in the SWIFT WebAccess Configuration and Troubleshooting Guide
9. Activate token	• End user	SWIFT Certificate Centre - Portal User Guide
10. Create personal HSM certificate	• SWIFTNet Security Officer • Alliance Gateway administrator • End user	Section “SWIFTNet Certificates” and “SWIFTNet Users” in the Alliance Gateway 7.5 Administration and Operations Guide
11. Access ESMIG U2A	• End user	Appendix A in the SWIFT`s Solution for ESMIG Service Description

Only for personal token certificate

Only for personal HSM certificate

1. Subscribe to SWIFT’s Solution for ESMIG



1. Subscribe to SWIFT’s Solution for ESMIG

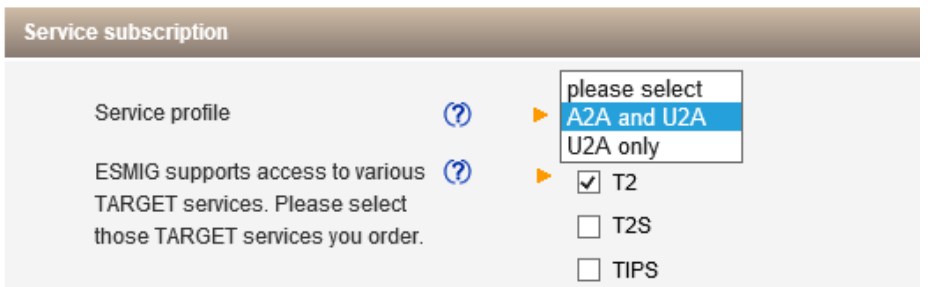
This step contains 2 parts. Both actions are performed through the use of the relevant subscription e-form, available at www.swift.com.

- **Subscribe to SWIFT’s Solution for ESMIG** (**1 e-form**). This step creates the contract with SWIFT. It applies to test and production services and for all Target services such as T2, TIPS and T2S.

- **Configure your access to ESMIG** (**multiple e-forms**). This step registers the DNs that will have access to the ESMIG U2A services. There is a separated configuration form for each services (T2, T2S and TIPS) and environment. This leads to the provisioning of the relevant CUG (closed user group).

1. Subscribe to SWIFT’s Solution for ESMIG - Subscription

Subscribe to SWIFT’s Solution for ESMIG, through the ordering page on swift.com.



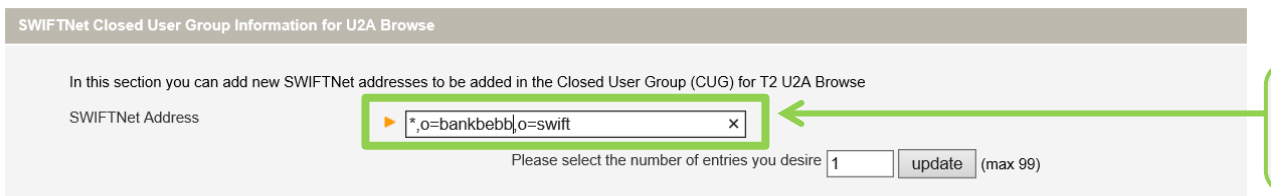
Select “A2A and U2A” or “U2A only”

1. Subscribe to SWIFT’s Solution for ESMIG - Configuration

Configure SWIFT’s Solution for ESMIG, through the configuration page on swift.com. Each service (T2, T2S, TIPS) requires a separate configuration form.

Allow ~2 weeks for the approval and provisioning to happen. You can choose your preferred implementation date in the e-order.

Closed User Group information (by default, any DN under BIC8)



The default allows any browse user (DN) under your BIC8

2. Define User DN in ESMIG Static Data

Subscriptions and Configurations	Systems and Network Configurations	Create Certificate	Access ESMIG U2A
1. Subscribe to SWIFT's Solution for ESMIG	5. Network configuration	9. Activate token	11. Access ESMIG U2A
2. Define user DN in ESMIG static data	6. Install Personal Token Software	10. Create personal HSM certificate	
3. Create user DN and setup for certification	7. Install ESMIG U2A SWIFT Login Application		
4. Order personal tokens	8. Prepare end user's workstation		

Only for personal token certificate

Only for personal HSM certificate

2. Define User DN in ESMIG Static Data

Register with ESMIG and configure the DN(s) in the ESMIG static data. The static data forms are made available by your Central Bank.

- The DN(s) must match the user DN(s) registered in the ESMIG configuration form on swift.com. The DN in the ESMIG configuration form can contain a wildcard.

- The DN(s) must match the DN(s) of the end users accessing the ESMIG U2A portal. An end user is identified by the DN of its certificate (on a personal token or HSM box).

3. Create User DN and Setup for Certification

Subscriptions and Configurations	Systems and Network Configurations	Create Certificate	Access ESMIG U2A
1. Subscribe to SWIFT's Solution for ESMIG	5. Network configuration	9. Activate token	11. Access ESMIG U2A
2. Define user DN in ESMIG static data	6. Install Personal Token Software	10. Create personal HSM certificate	
3. Create user DN and setup for certification	7. Install ESMIG U2A SWIFT Login Application		
4. Order personal tokens	8. Prepare end user's workstation		

Only for personal token certificate

Only for personal HSM certificate

Overview Certificate Generation

3. Create DN and setup for certification

Security officer(s)

Using SWIFTNet Online Operations Manager (O2M):

- Create user (DN) **for personal identity** in PKI tree
- Set up certificate for certification. Select certificate class "personal token“ or “personal HSM”

Provide activation secrets to end user:

- Personal token: provide certificate activation code, token, and default token password to end user
- Personal HSM certificate: provide reference number to the Alliance Gateway administrator and the authorisation code to the end user

8. Activate Token

End user

Using SWIFT Certificate Centre:

- Activate personal token

9. Create Personal HSM Certificate

Alliance Gateway administrator

End user

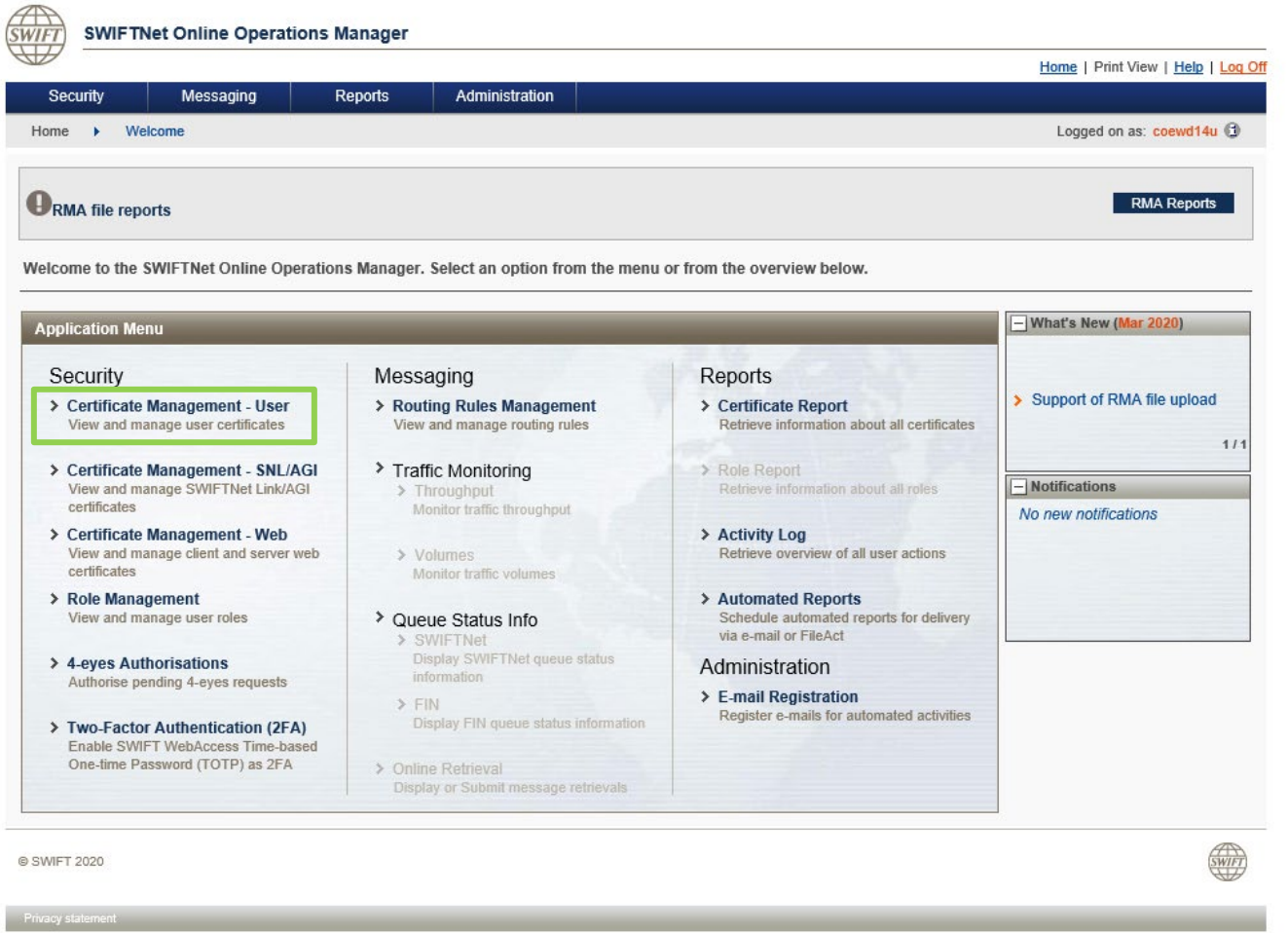
Using the Alliance Gateway Configuration application:

- Create draft certificate
- Define password

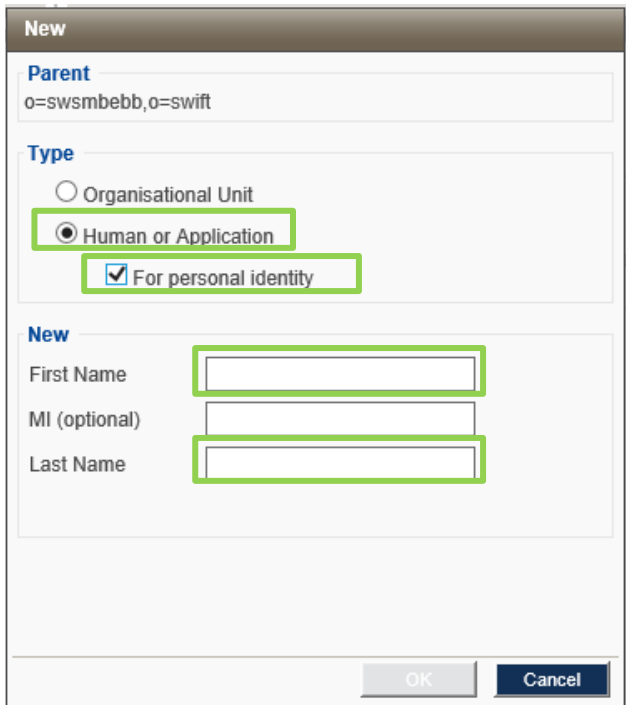
- The Policy ID for personal HSM certificates is 1.3.21.6.3.10.200.5. The Policy ID for personal token certificates is 1.3.21.6.3.10.200.2
- Access to the ESMIG U2A portal does not require an RBAC role.
- The certificates used today for accessing the TARGET2 WebAccess service cannot be used for accessing the ESMIG U2A portal. These certificates are either Business or Lite certificates and cannot be recovered as a personal token or personal HSM certificate. In case these certificates are only used for accessing the TARGET2 WebAccess service, then they can be disabled after the go-live of ESMIG T2 or can be re-used for other business flows.
- The personal tokens used today for accessing the T2S or TIPS U2A services can be used to access the ESMIG U2A portal.
- During the set-up for recovery, security officers will be able to change the certificate type between personal token and personal HSM certificates.

3. Create User DN

O2M – logged in as security officer



3. Create User DN



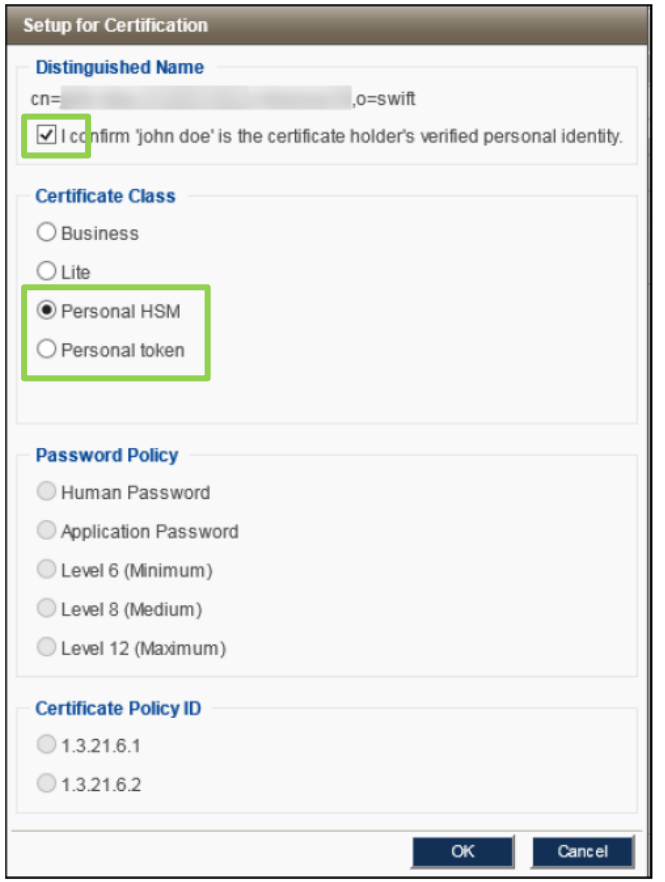
Select the BIC Organisational Unit for which you want to create the new DN and click “New”.

Select type “Human or Application” and select the checkbox “For personal identity”.

This will provide extended name fields for the Firstname and Lastname. A middle initial is optional and may be used in case the combination of Firstname and Lastname is not unique within the organisation.

This name is used as the common name, which forms part of the DN. The following mandatory syntax for the DN will be automatically created : cn=**firstname-lastname**,o=bankbebb,o=swift

3. Create User DN – Setup for Certification



Once new SWIFTNet users are registered, they must be set up for certification. This procedure generates activation secrets that are required in the certification process.

Go to a Certificate Management page and click the User Certs tab.
In the tree view, double-click a node to open its details. Click Certify.

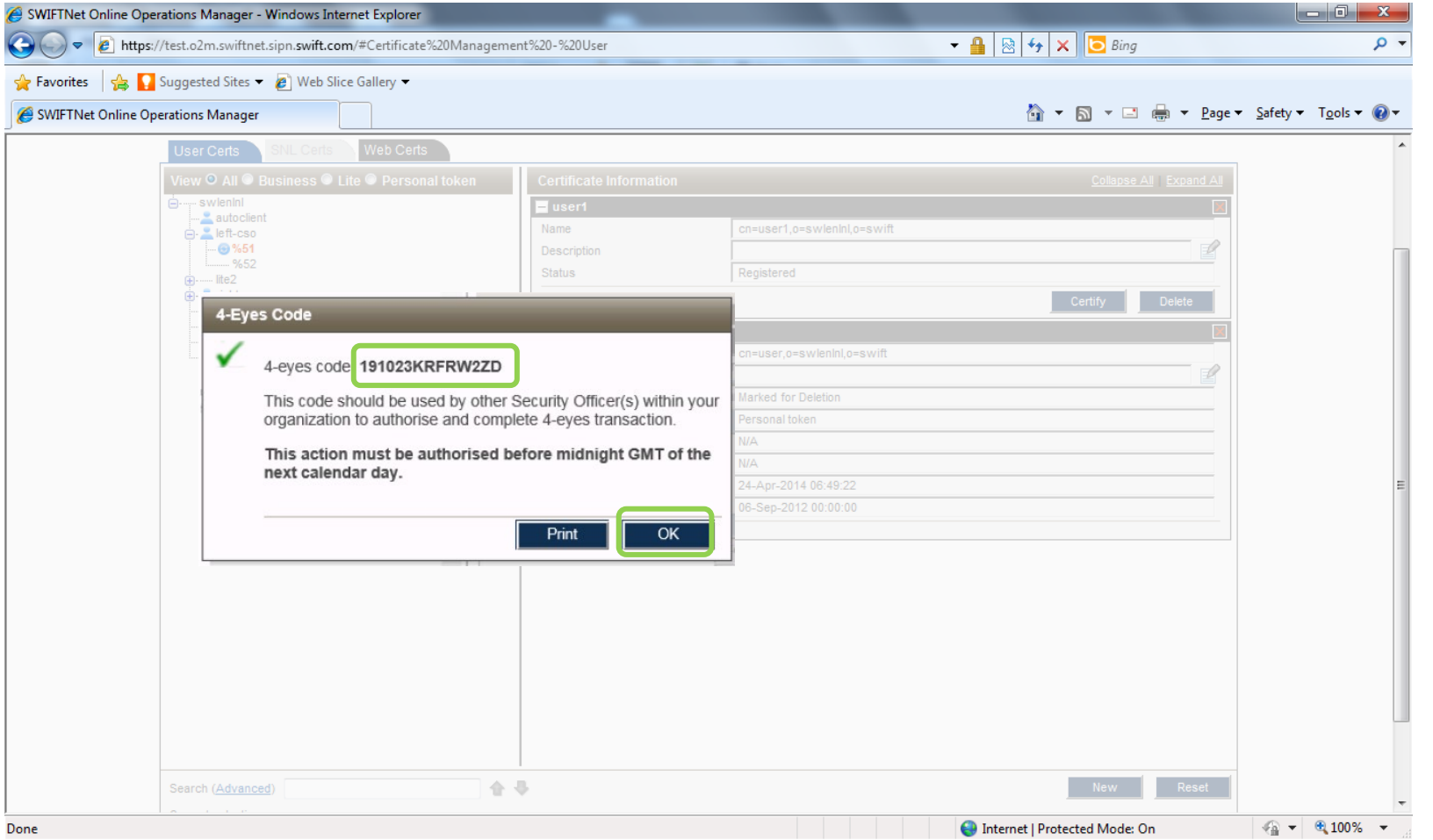
Select the checkbox in the Distinguished Name field "I confirm ...", indicating that the security officer has verified that the DN belongs to a real person and his/her identity has been verified.

Select either the **Personal token** or the **Personal HSM** certificate class.
A personal token certificate is stored on a USB device and a personal HSM certificate is stored on an HSM box.

For a personal token certificate, choose Password Policy from Level 6, Level 8, and Level 12. SWIFT recommends to select Level 12. No selection is available for personal HSM.

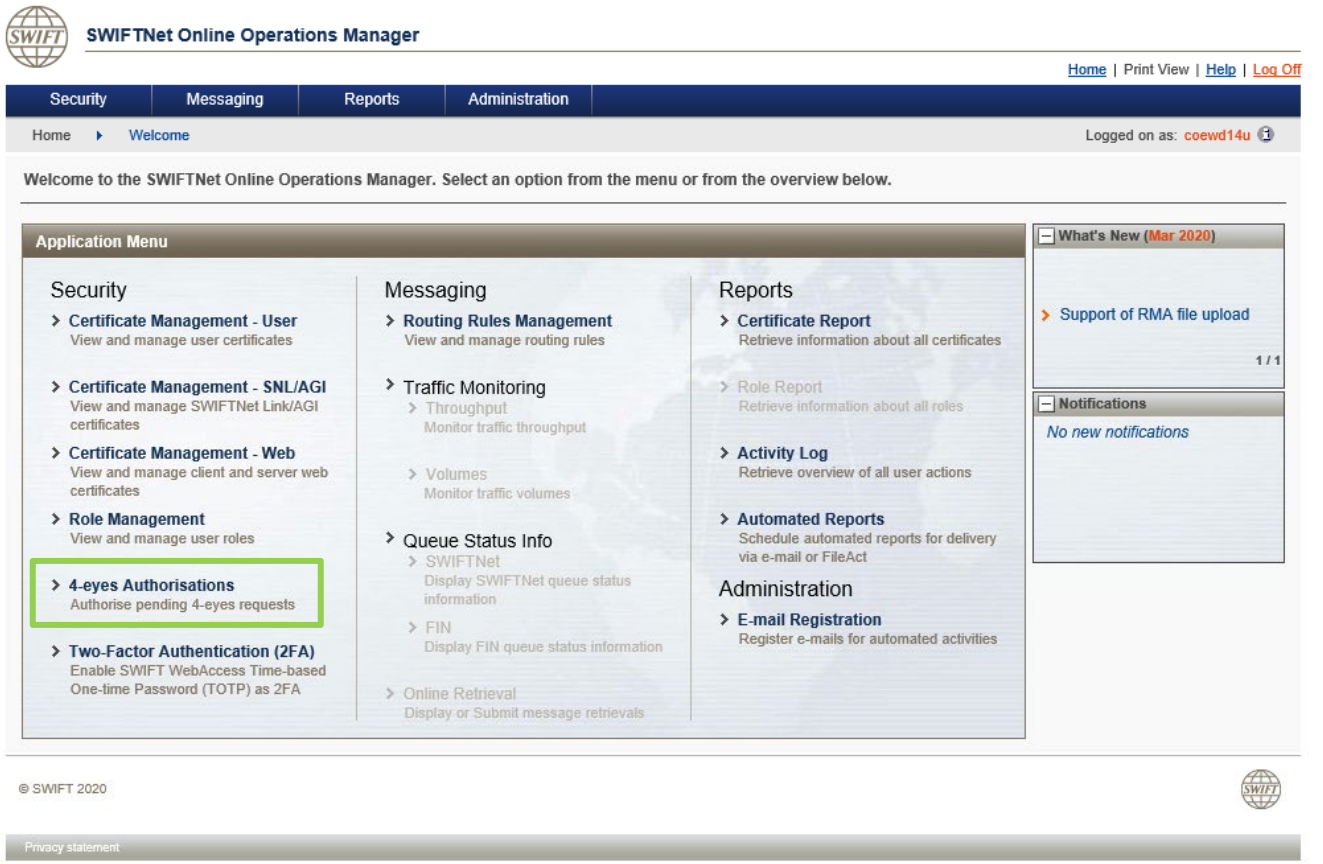
	Level 6	Level 8	Level 12
Minimum length	6	8	12
Complexity	• Maximum 2 repeating characters • Minimum n digits		• Maximum 2 repeating characters • Minimum 1 lower case, upper case, digit, symbol
Expiration	90 days	180 days	1 year

3. Create User DN – If 4-eyes is applicable



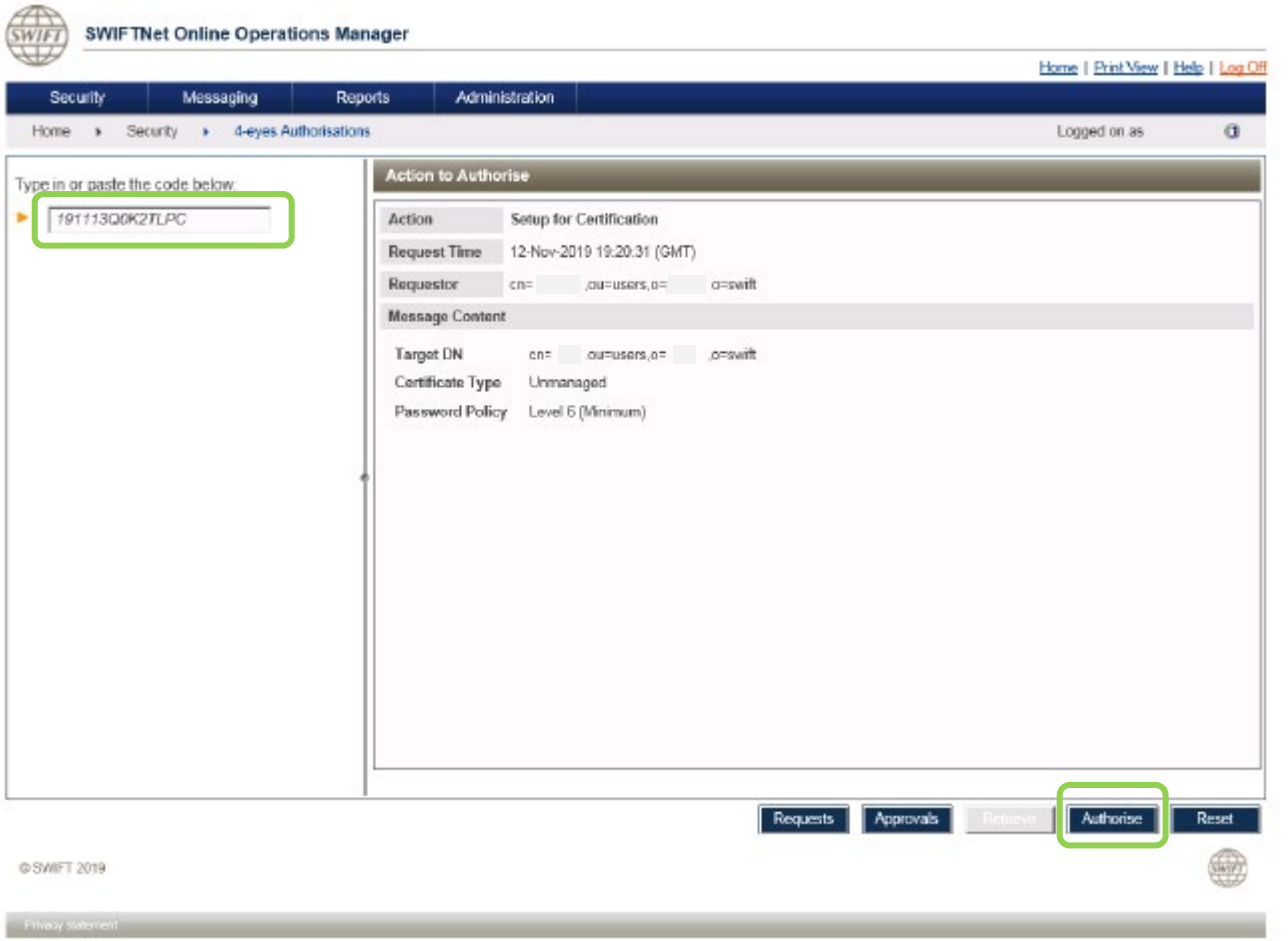
3. Create User DN – If 4-eyes is applicable

O2M - 2nd security officer

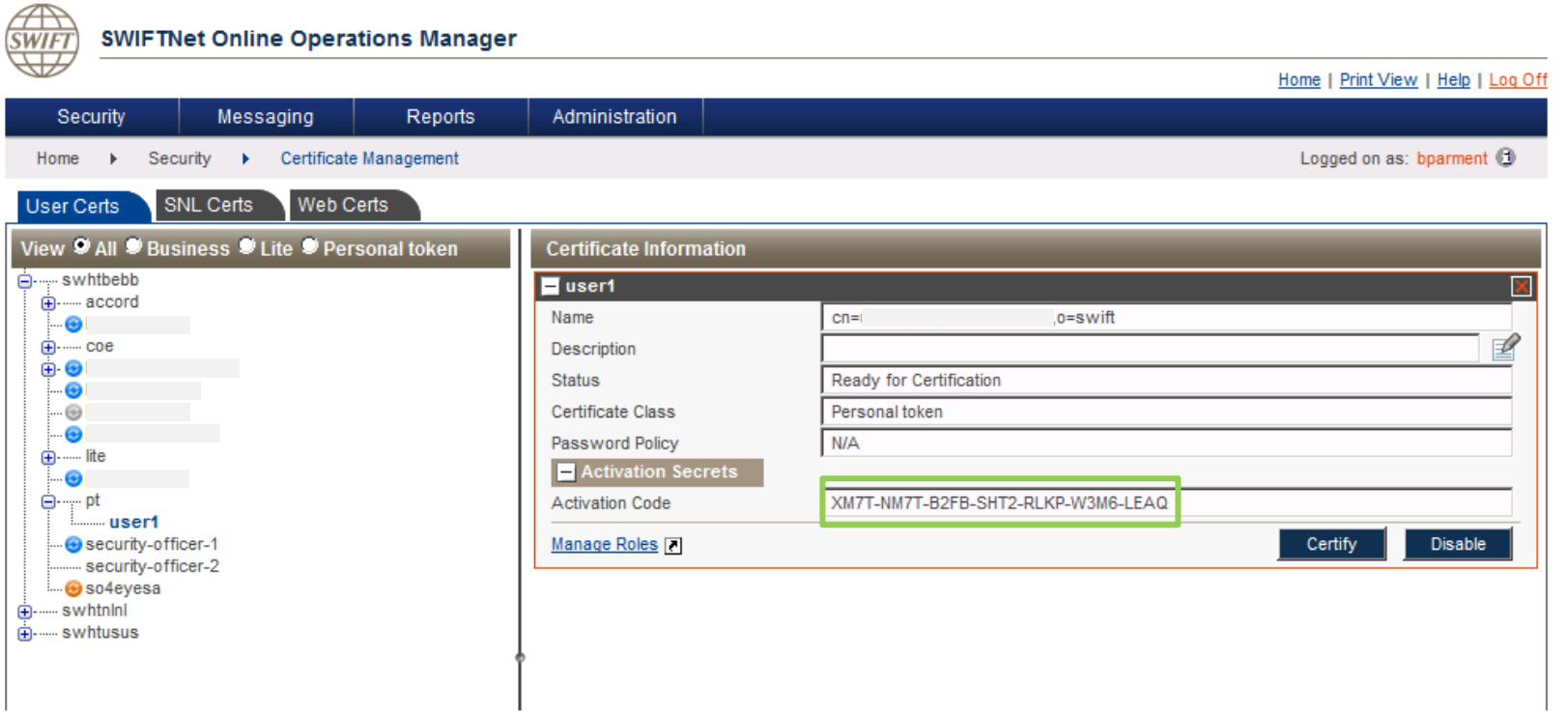


3. Create User DN – If 4-eyes is applicable

O2M - 2nd security officer



3. Create User DN



Ready for certification => pass on the activation secrets:

- For personal token: pass on the activation code, an empty SWIFT-issued personal token, and the default token password sent with the personal token order to the end user.
- For personal HSM certificate: pass on the reference number to the Alliance Gateway administrator and the authorisation code to the end user.

4. Order Personal Tokens

Subscriptions and Configurations	Systems and Network Configurations	Create Certificate	Access ESMIG U2A
1. Subscribe to SWIFT's Solution for ESMIG	5. Network configuration	9. Activate token	11. Access ESMIG U2A
2. Define user DN in ESMIG static data	6. Install Personal Token Software	10. Create personal HSM certificate	
3. Create user DN and setup for certification	7. Install ESMIG U2A SWIFT Login Application		
4. Order personal tokens	8. Prepare end user's workstation		

Only for personal token certificate

Only for personal HSM certificate

4. Order Personal Tokens

Customers have to order personal tokens or can re-use existing tokens. An operator using a personal token today for other SWIFTNet services can re-use its token to access the ESMIG U2A portal.

Re-use of existing tokens

- The personal tokens used today for accessing other services on SWIFTNet (like gpi Tracker, Sanction Screening Portal) can be used to access the ESMIG U2A portal.
- The personal tokens used today for accessing the T2S/TIPS U2A services can be used to access the ESMIG U2A service.

In order to support non-repudiation of origin for some U2A flows, and until July 2022, the personal tokens used for T2S need to have two certificates, one used for authentication purposes and one used for non-repudiation of origin purposes.

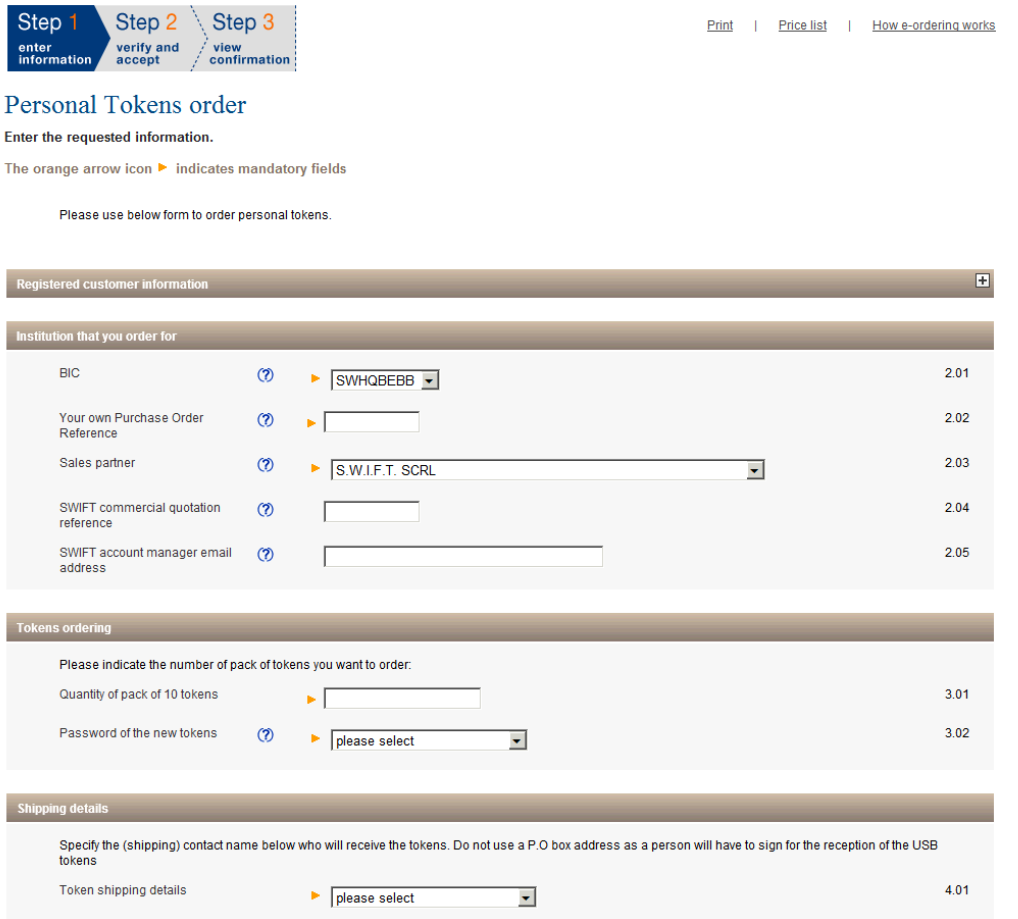
Customers only accessing T2 U2A or TIPS U2A do not need tokens with two certificates.

3SKey tokens **cannot** be used. They do not contain a named user.

4. Order Personal Tokens

Using swift.com ordering page:

After ~2 weeks you receive a box of 10 tokens (with initial password)



5. Network Configuration

Subscriptions and Configurations	Systems and Network Configurations	Create Certificate	Access ESMIG U2A
1. Subscribe to SWIFT's Solution for ESMIG	5. Network configuration	9. Activate token	11. Access ESMIG U2A
2. Define user DN in ESMIG static data	6. Install Personal Token Software	10. Create personal HSM certificate	
3. Create user DN and setup for certification	7. Install ESMIG U2A SWIFT Login Application		
4. Order personal tokens	8. Prepare end user's workstation		

Only for personal token certificate

Only for personal HSM certificate

5. Network Configuration

Users who already have the infrastructure to connect to other browser-based SWIFTNet services, such as O2M, can leverage and take advantage of that infrastructure.

- The network configuration must be set up so that the browser used by the end user has access to the ESMIG U2A web server over HTTPS. The HTTPS flow can be routed over SWIFTNet using HTTP proxies, Network Address Translation (NAT) devices (router, firewall, or another appropriate device), or a combination of both.

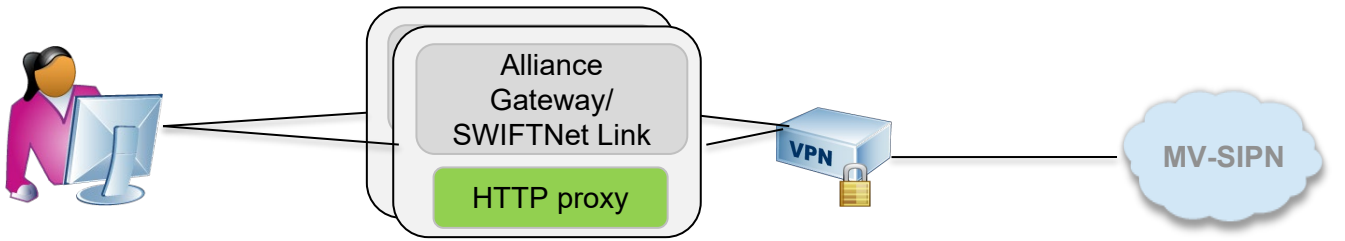
- An HTTP proxy can be installed on the Alliance Gateway/SWIFTNet Link host to concentrate the HTTPS flow. Make sure that the HTTP proxy does not interrupt the end-to-end https connection. In case the HTTP proxy installed on a different host than the Alliance Gateway host, the HTTP proxy must use the SWIFTNet DNS to resolve host names ending with *.swiftnet.sipn.swift.com*

- Customers who use a DNS zone forwarder must ensure that the DNS zone named *common.sipn.swift.com* is allowed.

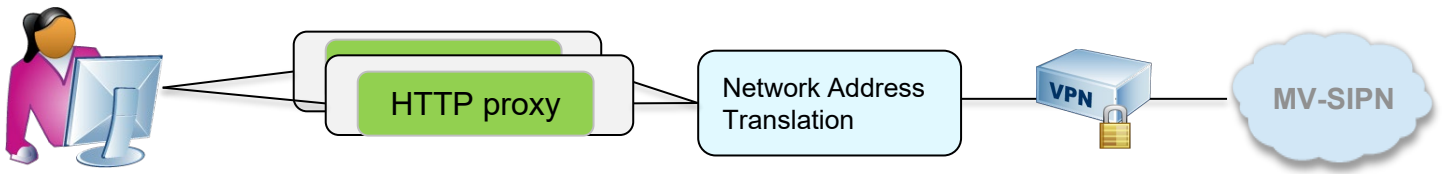
- For customers using Citrix or similar virtualisation environments, additional information is available in Appendix 1.

5. Network Configuration

More details and other possible configurations are available in the Network Configuration section of the SWIFT WebAccess Configuration and Troubleshooting Guide. Note that ESMIG U2A does not use a SWIFT WebAccess GUI package.

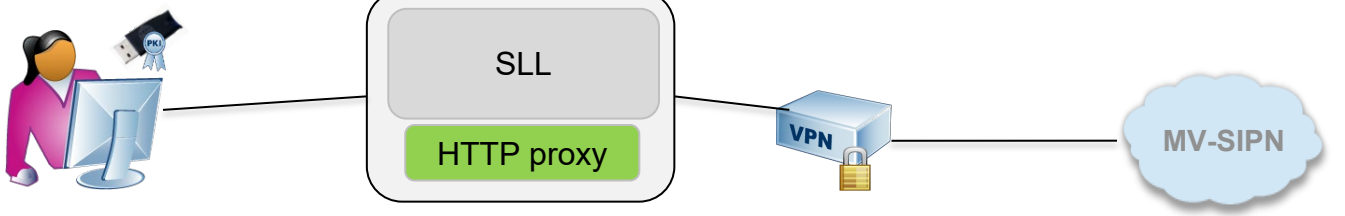


Example of a configuration with HTTP Proxy installed on an Alliance Gateway server



Example of a configuration using Network Address Translation. The IP address of the HTTP proxy must be translated to an IP address provisioned on the VPN box.
The HTTP proxy can be provisioned as a SWIFT Local Link (SLL) Host. In this case Network Address Translation is not needed.

5. Network Configuration – For Alliance Cloud Customer only



Example of a configuration with HTTP Proxy installed on a SWIFT provisioned server

Example Alliance Cloud customer using the Internet to connect to ESMIG U2A

5. Network Configuration - DNS Zone Forwarder

- The “SWIFTProxy” used for the HTTPS flow of the ESMIG U2A solution requires access to the DNS zone named "common.sipn.swift.com“ and “swiftnet.sipn.swift.com”.

- The "common.sipn.swift.com" DNS zone is specific to TIPS and ESMIG U2A. This zone is used to perform the CRL check (validate that the certificate used is not part of the “Certificate Revocation List”).

- In case of re-use of an existing SNL infrastructure, this new domain needs to be configured next to the pre-existing "swiftnet.sipn.swift.com" domain.

- In case of a new infrastructure both zones must be configured, please refer to the Network Configuration Tables Guide – DNS forwarding.

Example :

- If the local SAG/SNL host is used as DNS server, the file "named.conf" should already cover the zones "swiftnet.sipn.swift.com" and “149.134.in-addr.arpa". Additionally, the following lines should be added:

```
zone "common.sipn.swift.com" in {
   type forward;
   forwarders {
     149.134.252.7;
     149.134.244.133;
     };
   forward only;
};
```

5. Network Configuration - Firewall Configuration

Allow the same IPs and ports as for SWIFT WebAccess (as per the Network Configuration Tables Guide).

This includes:

- Outgoing TCP sessions from browse clients to the SWIFT WebAccess Revocation Service on ports 443 and 80/tcp.
- Outgoing TCP sessions from browse clients to the IP address range 149.134.0.0/16 on port 443/tcp. This is a range of IP addresses in CIDR notation.

Note: this setup might not be necessary if it was already done for SWIFT WebAccess services.

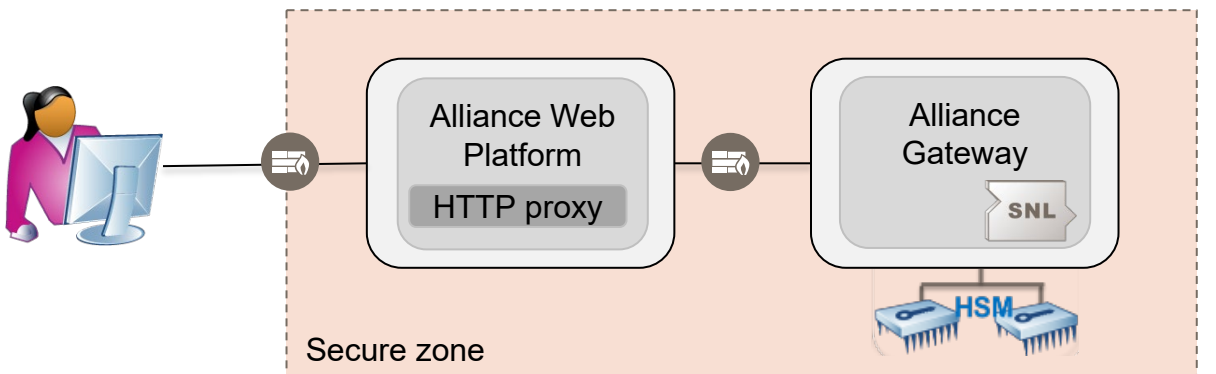
This global SWIFT WebAccess range may be limited to the specific IP addresses used for ESMIG. The list of these specific IP addresses is available in Knowledge Base article 5018711.

5. Network Configuration

The platform hosting the browser session of end users authenticated by **personal HSM certificates** must be able to connect to Alliance Gateway.

To avoid a straight channel between the host running the ESMIG U2A SWIFT Login Application and Alliance Gateway, a similar solution to the one implemented for the WebAccess browse flow can be considered.
The example below uses the embedded HTTP proxy of Alliance Web Platform. This would allow a communication to Alliance Gateway only through the HTTP proxy. The role of this proxy is to forward a TCP request of the incoming call (from the host running the user's browser) and to allow only secure connections to Alliance Gateway.

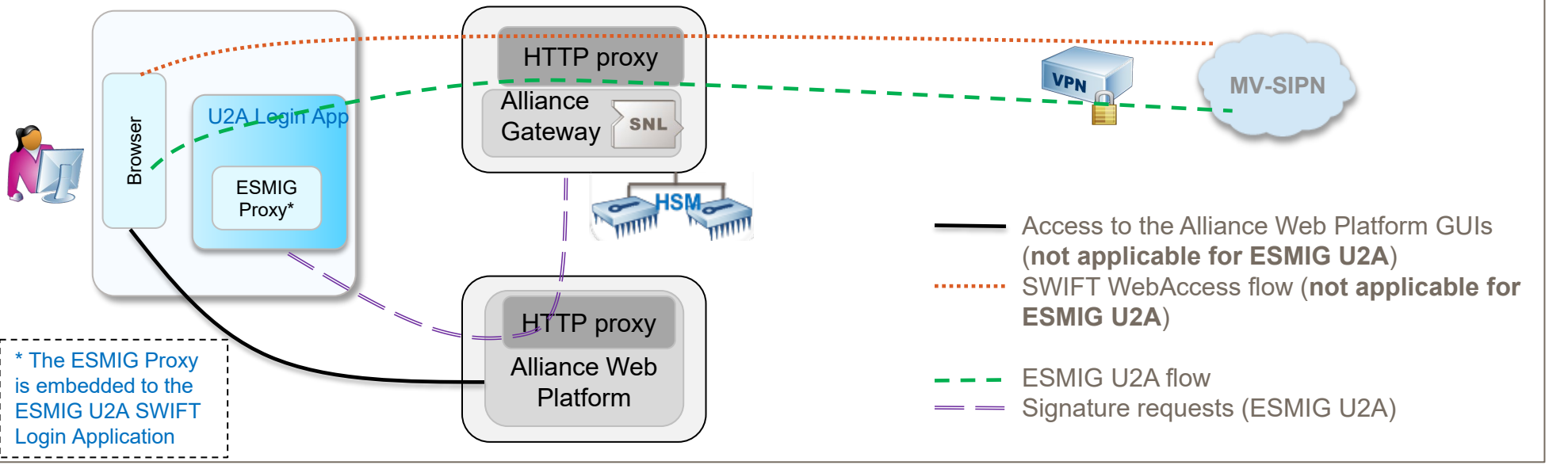
Firewalls between the HTTP Proxy and Alliance Gateway must allow TCP connections to Alliance Gateway on port number 48002 (default Remote API Port Number).



5. Network Configuration

The example below shows different flows related to browse services. This example uses two HTTP proxies. The embedded HTTP proxy of Alliance Web Platform is used to concentrate the signature requests from the end user's systems (only needed if personal HSM certificates are used). The HTTP proxy running on the Alliance Gateway host concentrates the browse flows to SWIFTNet. This is one example of how to concentrate the flows. Other setups can be used to achieve the same result.

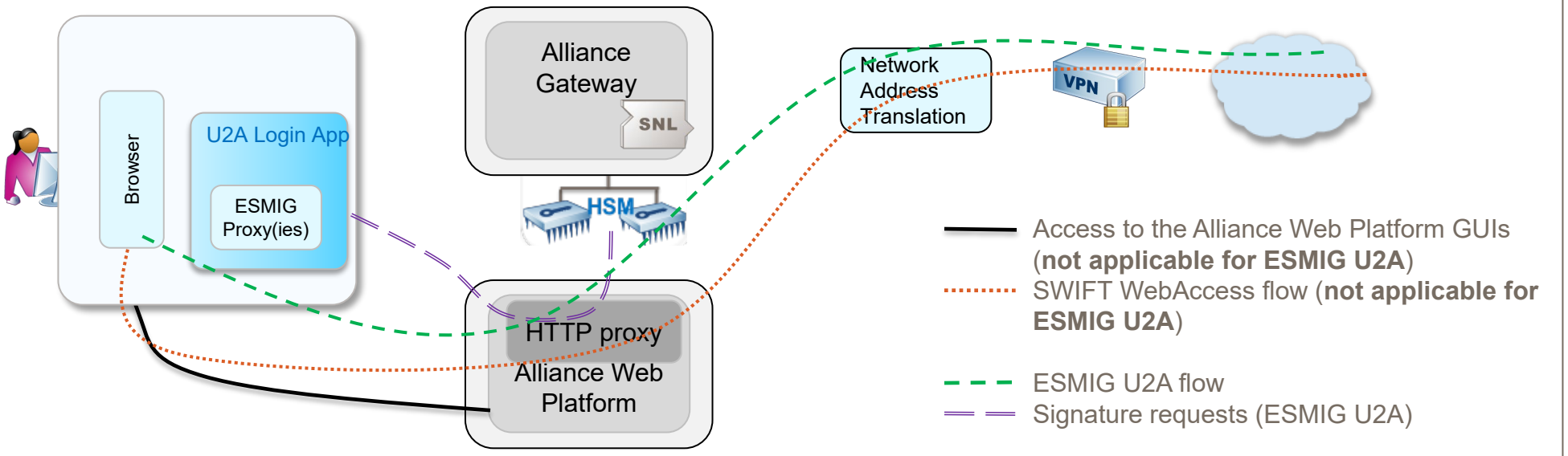
Example of a setup using 2 HTTP proxies



5. Network Configuration

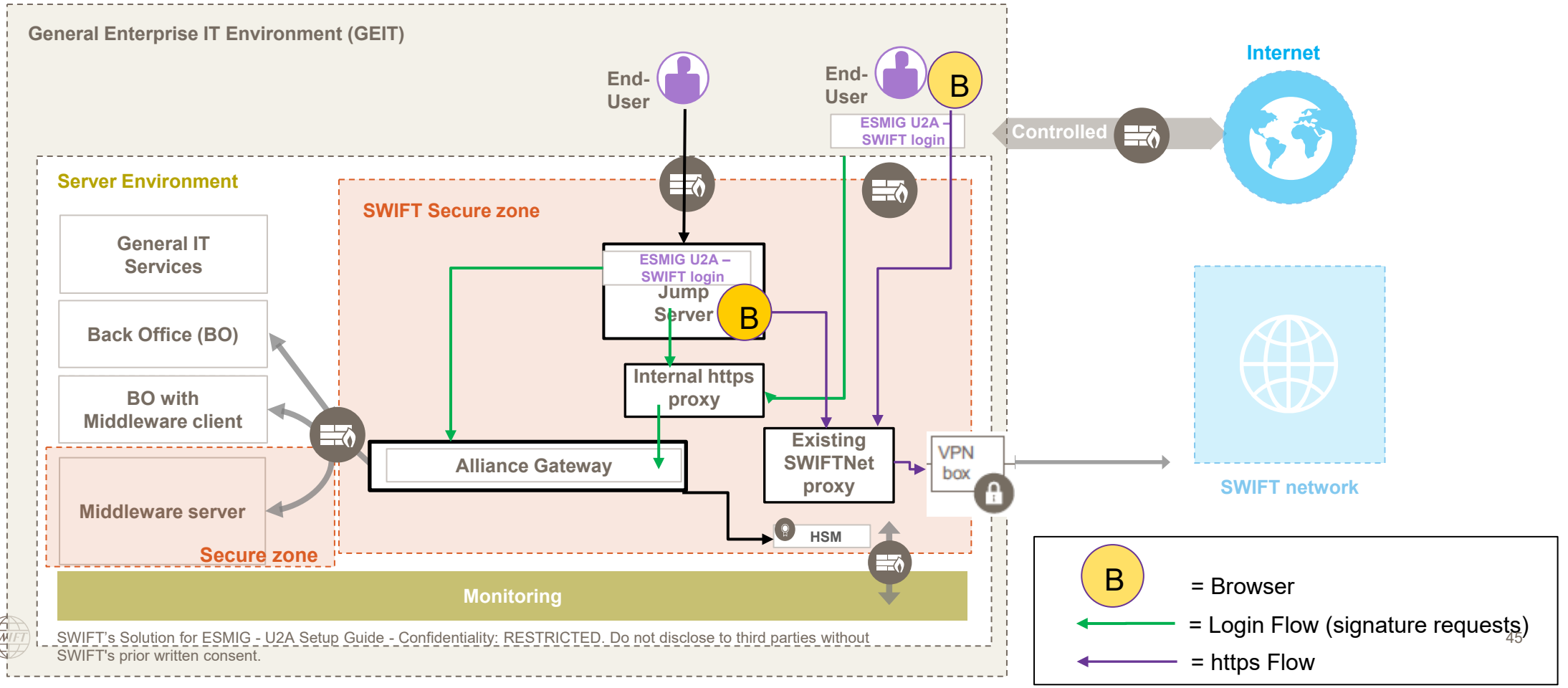
In this example (also showing the different flows related to browse services), the embedded HTTP proxy of Alliance Web Platform is used to concentrate the browse flows to SWIFTNet and the connections to Alliance Gateway.

Example of a setup using the HTTP proxy of the Alliance Web Platform



5. Network Configuration - CSP A1 Architecture type

The example below shows the ESMIG U2A SWIFT Login Application in the context of CSP (Customer Security Programme). The application can be installed on the end user's workstation outside of the SWIFT secure zone or on a jump server (e.g. Citrix host, see Appendix 1) in the SWIFT secure zone. Additional examples of infrastructure are available in the Appendix 2).



6. Install Token Software

Subscriptions and Configurations	Systems and Network Configurations	Create Certificate	Access ESMIG U2A
1. Subscribe to SWIFT's Solution for ESMIG	5. Network configuration	9. Activate token	11. Access ESMIG U2A
2. Define user DN in ESMIG static data	6. Install Personal Token Software	10. Create personal HSM certificate	
3. Create user DN and setup for certification	7. Install ESMIG U2A SWIFT Login Application		
4. Order personal tokens	8. Prepare end user's workstation		

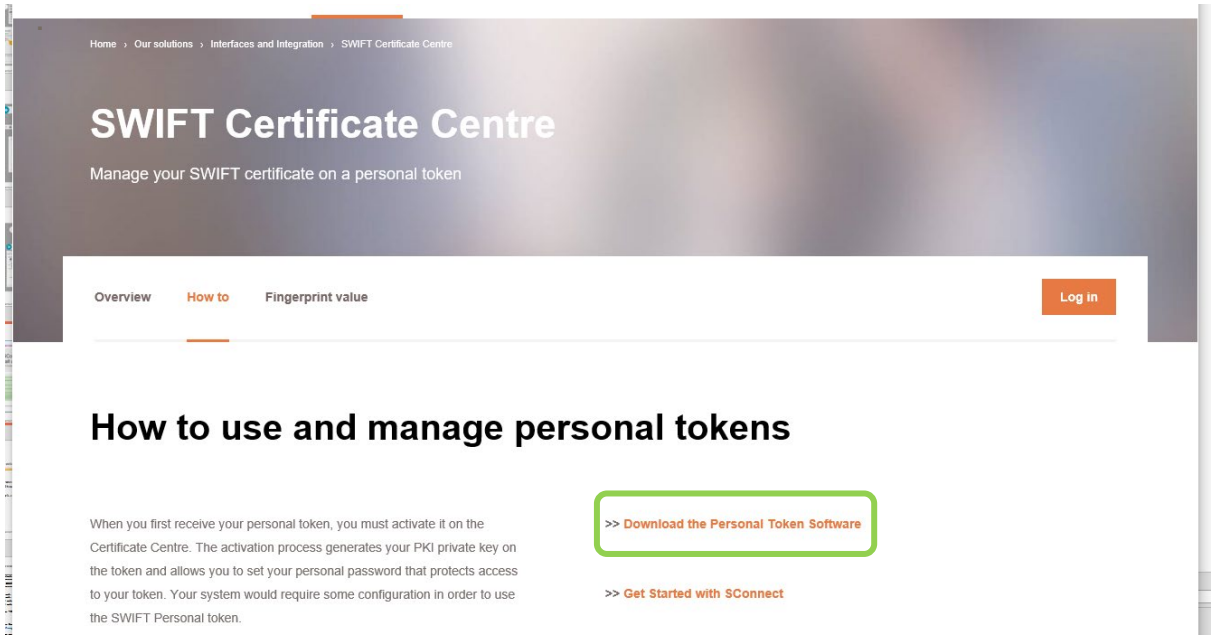
Only for personal token certificate

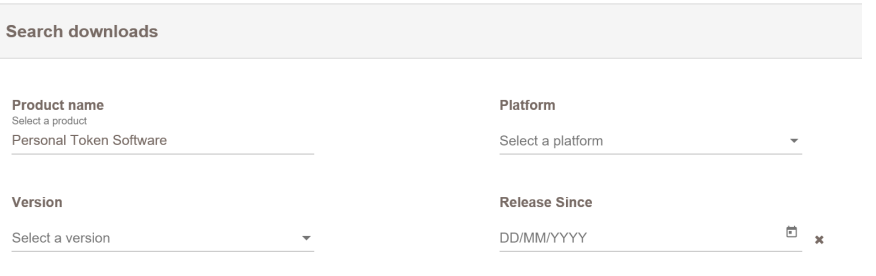
Only for personal HSM certificate

6. Install Personal Token Software

Each computer on which you will use your personal token requires the installation of the Personal Token Software. Personal Token Software requires your user to have administrator rights on the system.

Download the Personal Token installation program from the SWIFT Certificate Centre.



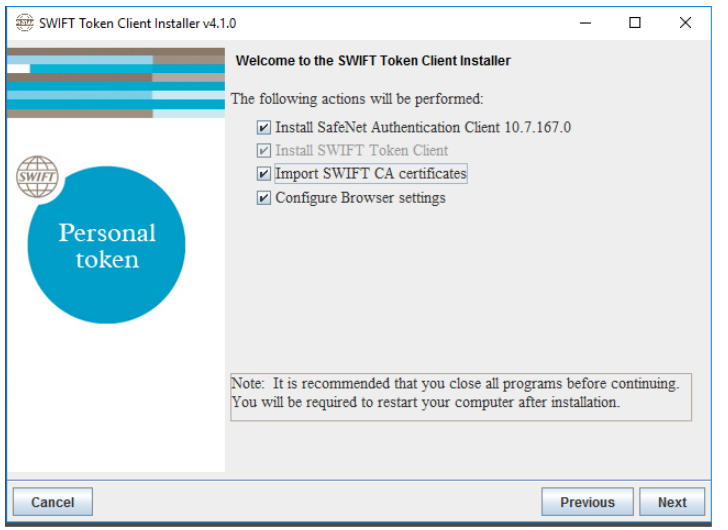


Note. SConnect is not needed for ESMIG U2A. SConnect is needed if the token is also used for SWIFT WebAccess services.

6. Install Personal Token Software

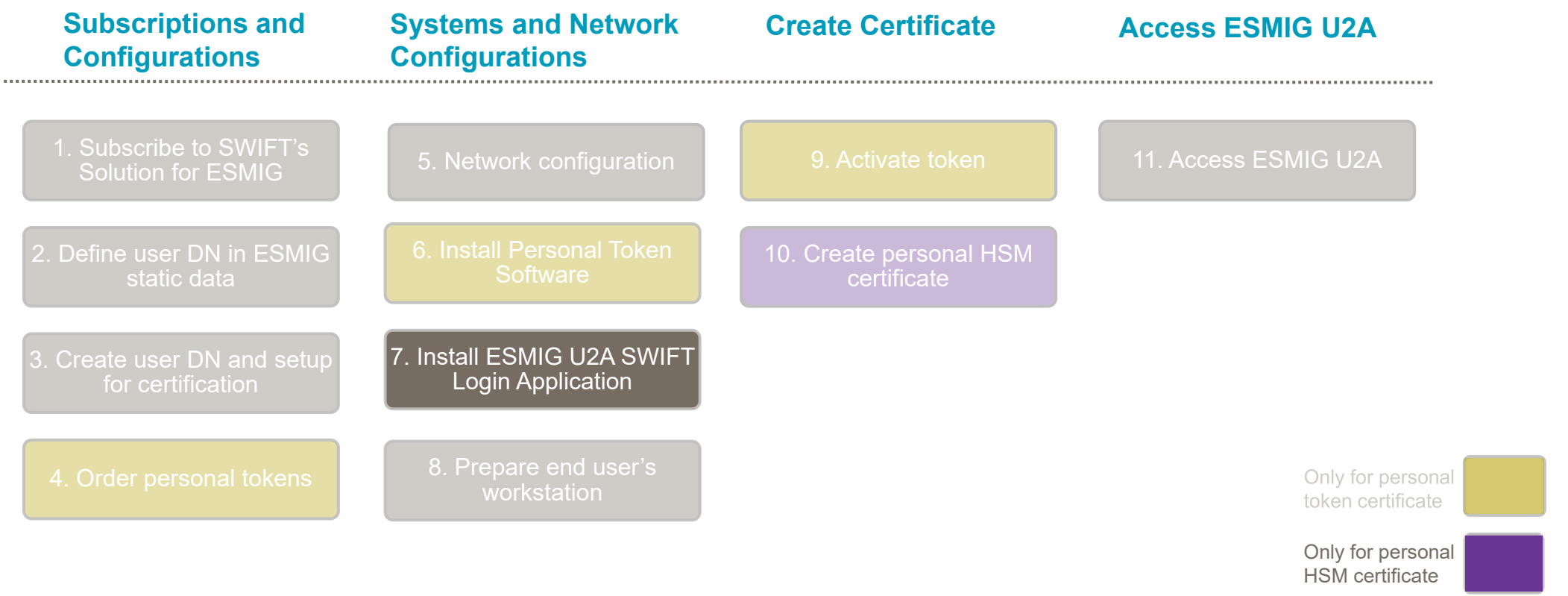
Follow the steps described in the section “Unzip and run the software installation file” in the Personal Token Software Installation Guide.

Select Import SWIFT CA certificates in the “Welcome to the SWIFT Token Client Installer” window. If your security policy does not allow to download the CA certificate, you can download it later.



The token software can also be installed in Silent Mode. In this mode you can remotely install the token software without interactive user input. See section “Install the Token Software in Silent Mode” in the Personal Token Software Installation Guide.

7. Install ESMIG U2A SWIFT Login Application



7. ESMIG U2A SWIFT Login Application

The ESMIG U2A SWIFT Login Application is a software provided by SWIFT. It authenticates the end user before accessing the ESMIG U2A services. The application runs in the background and has an associated icon in the Windows notification area.

The ESMIG U2A SWIFT Login Application can be downloaded from the Download Centre on swift.com

It must be installed on the system running the end user’s browser. The installation requires administrator rights. A silent installation is possible.

The ESMIG U2A SWIFT Login Application uses a configuration file.

7. Install and Update the ESMIG U2A SWIFT Login Application

Installation and configuration steps

- Download the latest software version from the Download Centre on swift.com
- Unzip the file, for example, in *C:\Temp*
- Run the *install.bat* file as administrator.
    - During the installation the following information will be asked:
        Please enter the installation folder. It cannot be in "C:\Users\".
        Press enter for default: "C:\Program Files\SWIFT\U2AApp\"
        Do you want to run the ESMIG U2A SWIFT Login Application when you log in to windows? (default: yes)
        Do you want to create a link to the ESMIG U2A SWIFT Login on the desktop? (default: yes)
    - If you already have the application installed, then you will be asked:
        Do you want to keep your existing configuration? (default: no)
- If you are installing the application for the 1st time or if you have selected not to keep your current configuration, then to configure the application after installation, edit the *C:\Program Files\Swift\U2AApp\config\configuration.ini* file.

The details of the installation are logged in the *installation_<timestamp>.log* file.

Additional steps in case of usage of HSM based certificate

- Add a Message Partner in Alliance Gateway.
- Copy the Alliance Gateway TLS certificate (see 7. TLS Certificate (only required if using HSM-based certificate))

Note that users connected to Alliance Gateway through the ESMIG U2A SWIFT Login Application are not counted as part of the maximum concurrent users licence option.

7. Install and Update the ESMIG U2A SWIFT Login Application in Silent Mode

Here are all possible options for installation and uninstallation:

- Install.bat [-help] [-silent] [-noautorun] [-nodesktoplink] [-keepconfig] [installation_folder]
- Uninstall.bat [-help] [-silent] [-nobackup]

-help	Shows the help for install/uninstall.
-silent	Do not prompt for info («installation_folder» / «nodesktoplink» / «noautorun»). If these options are not present, it uses the default behaviour.
-nobackup	Do not back up the configuration files while uninstalling.
-noautorun	If present, the application will not be run at Windows login. Default behaviour is to run the application at Windows login.
-nodesktoplink	If present, no desktop link will be created. Default behaviour is to add a link to the desktop to manually run the application.
-keepconfig	If present, the configuration of the previously installed application will be kept. Default behaviour is to delete the existing application.
installation_folder	Folder full path where to install the application. Default value is «C:\Program Files\SWIFT\U2AApp».

7. Configure the ESMIG U2A SWIFT Login Application – Configuration File

Default configuration file *C:\Program Files\Swift\U2AApp\config\configuration.ini*

```
############################################################
#### This group represents an Alliance Gateway instance #####
#### It can be repeated as many times as needed         #####
############################################################

[Gateway1]
Address=127.0.0.1
Port=48002
Certificate=myCertificate.crt
DN="cn=myDN"
MessagePartner=myMessagePartner
#Proxy=my.proxy.first.com:8080;my.proxy.second.com:8080


# [Gateway2]                        # Name that will be displayed in the user interface
# Address=1.2.3.4                   # The hostname or IP of the Alliance Gateway instance
# Port=48002                        # The RA Port to use (as configured on the Alliance Gateway instance)
# Certificate=myCertificate.crt     # Filename of the SAG certificate or CA. It must be stored in the same folder as this .INI file
# DN="cn=myDN"                      # The DN of the TLS certificate of the Alliance Gateway
# MessagePartner=myMessagePartner   # The name of the Message Partner configured on the Gateway (could be sabmp)
#Proxy=my.proxy.first.com:9090;my.proxy.second.com:9090        # The address of the HTTP proxy between the application and the Alliance Gateway. Optional
                                                               # Can have several proxies separated by ';' for resiliency


# The SSL certificate is required to authenticate the Alliance Gateway connection. In case you are not using a self-signed certificate, you need to provide the root CA.
# If intermediate CAs were used, the full chain must be known by the client. The easiest way to achieve this is to configure the Alliance Gateway to expose the full certificate chain."


############################################################
#### This group represents the global configuration     #####
#### It can only appear once in the configuration file  #####
############################################################
[Configuration]
##AllianceGatewayProxy parameter is obsolete and replaced by the 'Proxy' on the gateways configuration
## Uncomment the following line when the application runs on a Citrix environment
#Citrix=1

## The following parameters enable the use of Personal Tokens and HSM Boxes to login
#ShowPersonalToken=1
#ShowHSMBox=1

SwiftLoginAppConnectionPort=38081
BrowserConnectionPort=38080

## Uncomment the following line to add an HTTP proxy between the Connection Manager and SWIFT
##   Can have several proxies separated by ';' for resiliency
#SWIFTProxy=my.swiftproxy.first.com:8080;my.swiftproxy.second.com:8080
```

Information related to Signature flow. This section is not needed for customers using personal tokens.

Information related to the ESMIG U2A flow. The parameters are explained in the next few pages.

7. Configure the ESMIG U2A SWIFT Login Application – Configuration File

Alliance Gateway section – Only needed for HSM-based certificate

Example of a configuration with two Alliance Gateway instances.

```
[Gateway 1]
Address=saghost1
Port=48002
Certificate=sag1.crt
DN="cn=myDN"
MessagePartner=myMessagePartner
#Proxy=my.proxy.first.com:8080;my.proxy.second.com:8080

[Gateway 2]
Address=saghost2
Port=48002
Certificate=sag2.crt
DN="cn=myDN"
MessagePartner=myMessagePartner
#Proxy=my.proxy2.first.com:8080;my.proxy2.second.com:8080
```

Optional field.
Not needed if there is no proxy between the ESMIG U2A SWIFT Login Application and the Alliance Gateway.

"Gateway 1" and "Gateway 2" will be shown in the Alliance Gateway instance drop-down list of the ESMIG U2A SWIFT Login Application window. These are free text fields, special characters should be avoided.

- **Address** - Mandatory: HostName or IP address of the Alliance Gateway
- **Port** – Mandatory – Port on which the Alliance Gateway is listening.
- **Certificate** - Mandatory – File name of the CA of the SAG certificate (in case of default self-signed certificate, the CA is the certificate itself). It must be stored in the same folder as this .INI file. (see 7. TLS Certificate (only required if using HSM-based certificate))
- **DN** – Mandatory – Complete DN of the SAG TLS certificate. In case of self-signed, it is the same certificate as above. (see 7. TLS Certificate (only required if using HSM-based certificate))
- **MessagePartner** – Mandatory – Name of the Message Partner defined in the Gateway (see Alliance Gateway Configuration (only required if using HSM-based certificate)
- **Proxy –** Optional **–** one or more proxies, if any, to connect to SAG separated by a ";". If the connection fails over the first proxy, the second proxy will be used from the list and so on. The cycle is restored upon restarting the application.

7. Configure the ESMIG U2A SWIFT Login Application – Configuration File

Configuration section

```
[Configuration]
## AllianceGatewayProxy is obsolete and replaced by the 'Proxy' on the gateways configuration.

## Uncomment the following line when the application runs on a Citrix environment
#Citrix=1

## The following parameters enable the use of Personal Tokens and HSM Boxes to login
#ShowHSMBox=1
#ShowPersonalToken=1

SwiftLoginAppConnectionPort=38081
BrowserConnectionPort=38080

## Uncomment the following line to add an HTTP Proxy between the Connection Manager and SWIFT.
## Can have several proxies separated by ';' for resiliency.
#SWIFTProxy=my.swiftproxy.first.com:8080;my.swiftproxy.second.com:8080
```

Field remains for backward compatibility with previous versions. If no proxy defined per Alliance Gateway instance, this global value will be used as proxy if defined. Not needed when using personal tokens.

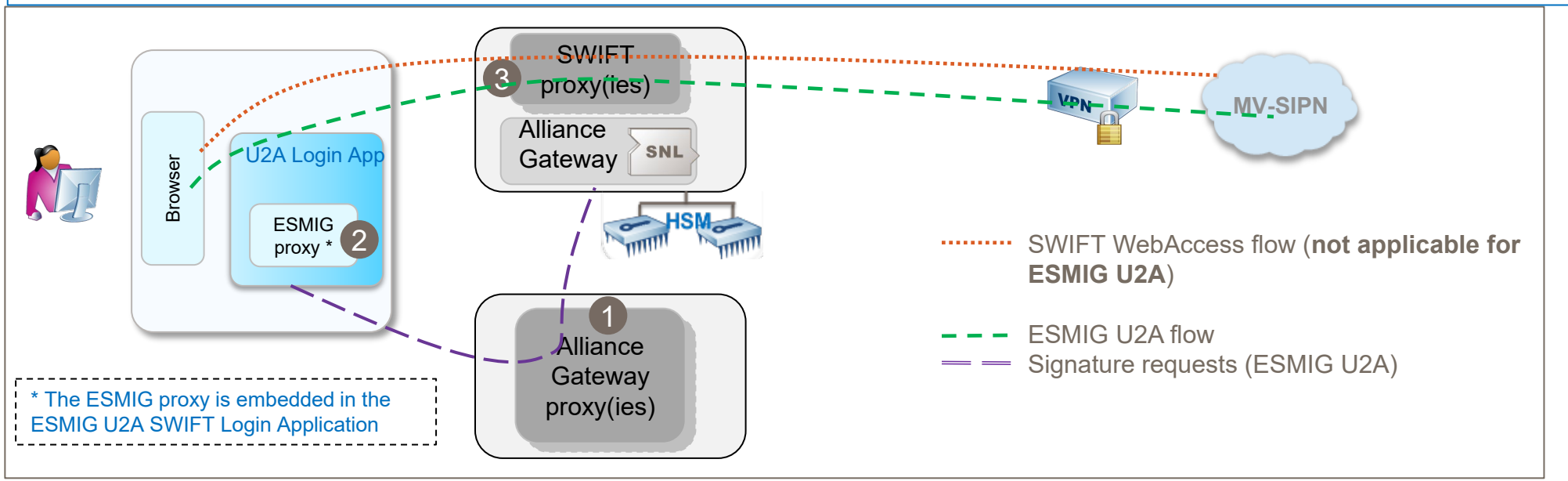
- **Citrix** - Optional field – If the application runs on a Citrix environment, then the value must be set to 1.
- **ShowHSMBox** – Optional field - Define the visible option on the ESMIG U2A SWIFT Login Application
- **ShowPersonalToken** – Optional field - Define the visible option on the ESMIG U2A SWIFT Login Application
- **BrowserConnectionPort**– Mandatory field - Setup the port for the communication between the browser and the SWIFT Login Application (as defined in the PAC file – see 8. Prepare End User's Workstation – Browser)
- **SwiftLoginAppConnectionPort** – Mandatory field – Setup the port for the internal communication between the ESMIG U2A Proxy and the SWIFT Login Application – Assign an unused port.
- **SWIFTProxy – Optional field -** Configure one or more proxies to connect to SWIFT separated by a ";". If the connection fails over the first proxy, the second proxy will be used from the list and so on. The cycle is restored upon restarting the application. If this parameter is not used, the server on which the application is installed must have access to SWIFT.

7. Configure the ESMIG U2A SWIFT Login Application – Configuration File

```
[Gateway 1]
…
# Proxy=5.6.7.8:8080;9.10.11.12:9090  # The address of the HTTP proxy between the application and the Alliance Gateway. Optional
                                      #   Can have several proxies separated by ';' for resiliency

SwiftLoginAppConnectionPort=38081
BrowserConnectionPort=38080

## Uncomment the following line to add an HTTP proxy between the Connection Manager and SWIFT
##   Can have several proxies separeted by ';' for resiliency
#SWIFTProxy=5.6.7.8:4243;9.10.11.12:9090
```



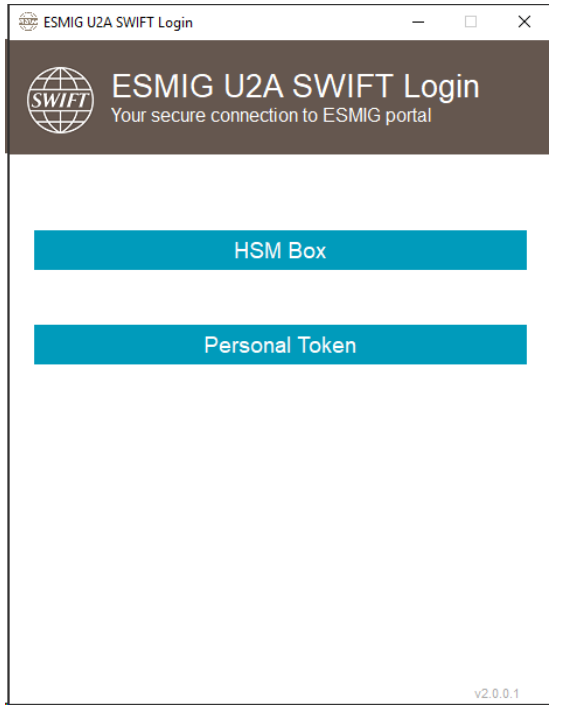
7. Configure the ESMIG U2A SWIFT Login Application – Configuration File

Parameters to choose which option (token and/or HSM) are shown in the ESMIG U2A SWIFT Login Application

```
## The following parameters enable the use of Personal Tokens and HSM Boxes to login
#ShowHSMBox=1
#ShowPersonalToken=1
```

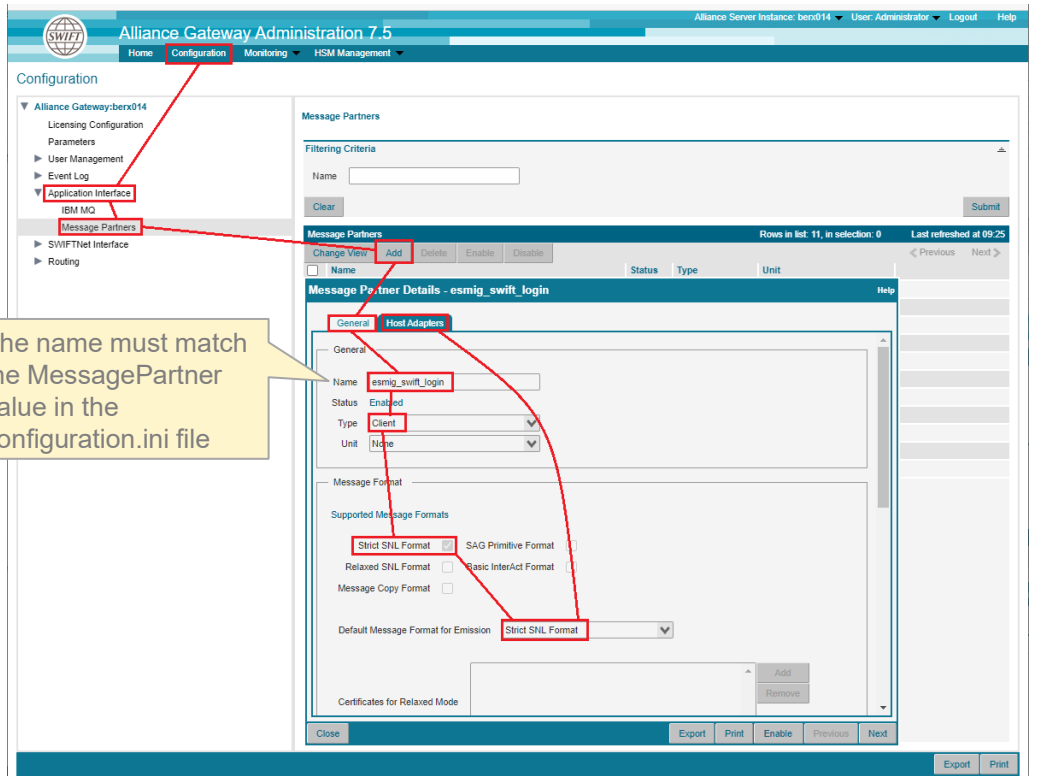
- Each parameter can have 3 values:
  - **Value of 1,** then the option is **active**
  - **Value of 0,**then the option is **inactive**
  - **Not present** (can happen when migrating from phase 1), then it is considered as **active**
- After the installation, both parameters are commented. In that case, their default value (“1”) is used and both options are visible.

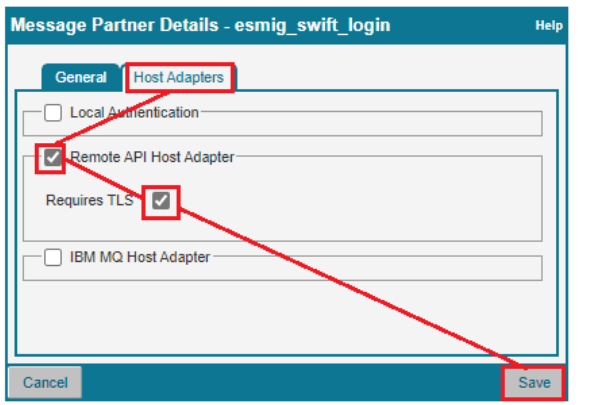
The configuration file is loaded at the start of the application only! Please restart the application or the host after each modification of the configuration.ini file.

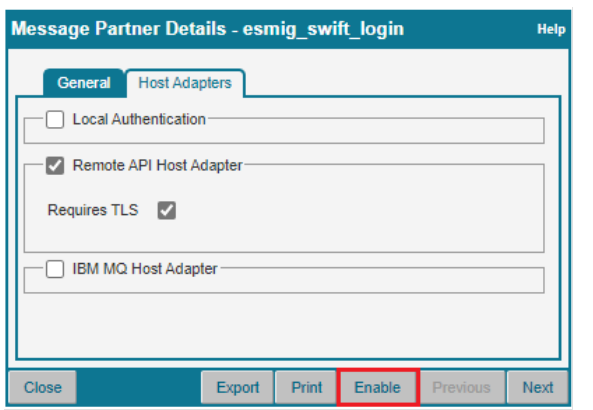


7. Alliance Gateway Configuration (only required if using HSM-based certificate)

A Message Partner must be added in the Alliance Gateway.
Message Partner configuration details: Client, Strict SNL format, Remote API Host Adapter, with TLS but without LAU.







7. TLS Certificate (only required if using HSM-based certificate)

Similar to the communication between Alliance Web Platform and Alliance Gateway, a client certificate is used to secure the communication between the ESMIG U2A SWIFT Login Application and Alliance Gateway.

The certificate can be a self-signed TLS certificate. However, it is recommended to use a certificate from a Certification Authority (CA). This avoids having to copy the certificate on all end users' systems if the certificate changes.

The self-signed certificate or the CA certificate must be copied to the <installation path>*config* folder (.crt file).

The DN (distinguished name) of the certificate and the certificate file name are configured in the configuration file.

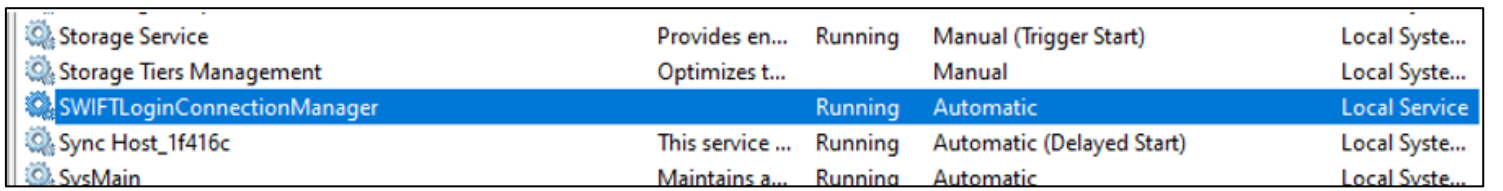
The TLS certificate presented on this slide should not be mixed up with the "cacert.pem" file in the *C:\Program Files\Swift\U2AApp\config* folder. That one is created during the installation and must not be modified or moved.

7. Connection Manager service

The Connection Manager Service is automatically installed (or uninstalled) by the Installer (or Uninstaller) of the ESMIG U2A SWIFT Login Application. It ensures a secure connection between the Windows system and SWIFT.

The Connection Manager Service starts and stops automatically with Windows and must remain up and running all the time (from Windows startup till shutdown).

The service must be started for the ESMIG U2A SWIFT Login Application to work.



The following operations can be run via the command line :

- ConnectionManager.exe install (Administrator rights required)
- ConnectionManager.exe uninstall (Administrator rights required)
- ConnectionManager.exe start
- ConnectionManager.exe stop

After the installation or a change of the configuration of the ESMIG U2A SWIFT Login Application, it might be needed to restart the host of the application to have the Connection Manager Service properly started.

8. Prepare End User's Workstation

Subscriptions and Configurations	Systems and Network Configurations	Create Certificate	Access ESMIG U2A
1. Subscribe to SWIFT's Solution for ESMIG	5. Network configuration	9. Activate token	11. Access ESMIG U2A
2. Define user DN in ESMIG static data	6. Install Personal Token Software	10. Create personal HSM certificate	
3. Create user DN and setup for certification	7. Install ESMIG U2A SWIFT Login Application		
4. Order personal tokens	8. Prepare end user's workstation		

Only for personal token certificate

Only for personal HSM certificate

8. Prepare End User's Workstation - Browser

- Import the SWIFT CA certificate to the browser trust store. See section *SWIFT CA Certificate* in the SWIFT WebAccess Configuration and Troubleshooting Guide.
  This step is not needed if the certificate was imported as part of the Personal Token Software installation.

- For Mozilla Firefox, please refer to the Knowledge Base article 5020826.

These instructions might change depending on the version of the Browser used.

8. Prepare End User’s Workstation - Browser

PAC file - The basics

The end-to-end HTTP-S session between the end user’s browser and the ESMIG U2A portal is set up by the ESMIG proxy (embedded to the ESMIG U2A SWIFT Login Application).

The end user's browser must be configured to route the ESMIG browse flow to the ESMIG proxy embedded in the ESMIG U2A SWIFT Login Application. This can be done by using a proxy automatic configuration script (.pac file).

The proxy automatic configuration script contains a JavaScript function to determine which HTTP proxy server to forward browser traffic to based upon the destination URL address. The proxy automatic configuration script must be published on a web server that is accessible from the end user's PC.

The ESMIG proxy used for the ESMIG U2A browse flow can also be used for the existing TIPS browse flows. A dedicated java proxy is used for the T2S U2A browse flow listening on a different port. See example of a .pac file on the next pages.

8. Prepare End User's Workstation - Browser

PAC file example

```
function FindProxyForURL(url, host)
{
      if( shExpMatch( url, "*t2s-*.ssp.swiftnet.sipn.swift.com*" ) &&
          !shExpMatch( url, "*t2s-*-proxy.ssp.swiftnet.sipn.swift.com*"))
      {
                  return "PROXY 127.0.0.1:18080";
      }

      if( ( shExpMatch( url, "*.tips.swiftnet.sipn.swift.com*" ) ||
            shExpMatch( url, "*.t2.swiftnet.sipn.swift.com*" ) ||
            shExpMatch( url, "*.t2s.swiftnet.sipn.swift.com*" ) ||
            shExpMatch( url, "*.emip.swiftnet.sipn.swift.com*" ) ||
            shExpMatch( url, "*.ecms.swiftnet.sipn.swift.com*" ) ) )
      {
                  return "PROXY 127.0.0.1:38080";
      }

// Forwarding proxy. Example below uses a proxy on Alliance Gateway.
      if (shExpMatch(url,"*.scc.swiftnet.sipn.swift.com*") ||
          shExpMatch(url,"*.common.sipn.swift.com*"))
      {
          return "PROXY sag01.swift.corp:48600";
      }
return "DIRECT";
}
```

Only needed if you also require access to the «Old , Pre-ESMIG» T2S U2A. A dedicated proxy listens on port 18080.

Port on which the ESMIG U2A Login Application is listening ("BrowserConnectionPort" in the config file of the application). This port is defined in the configuration file of the Application – see 7. Install ESMIG U2A SWIFT Login Application – Configuration File

For customers who already have a TIPS U2A connectivity configured, it is important to combine T2 and TIPS so the URLs are resolved using the port of the ESMIG U2A SWIFT Login Application – as shown here.

Only needed if you want to use the Test Web Portal – see Test web portal.

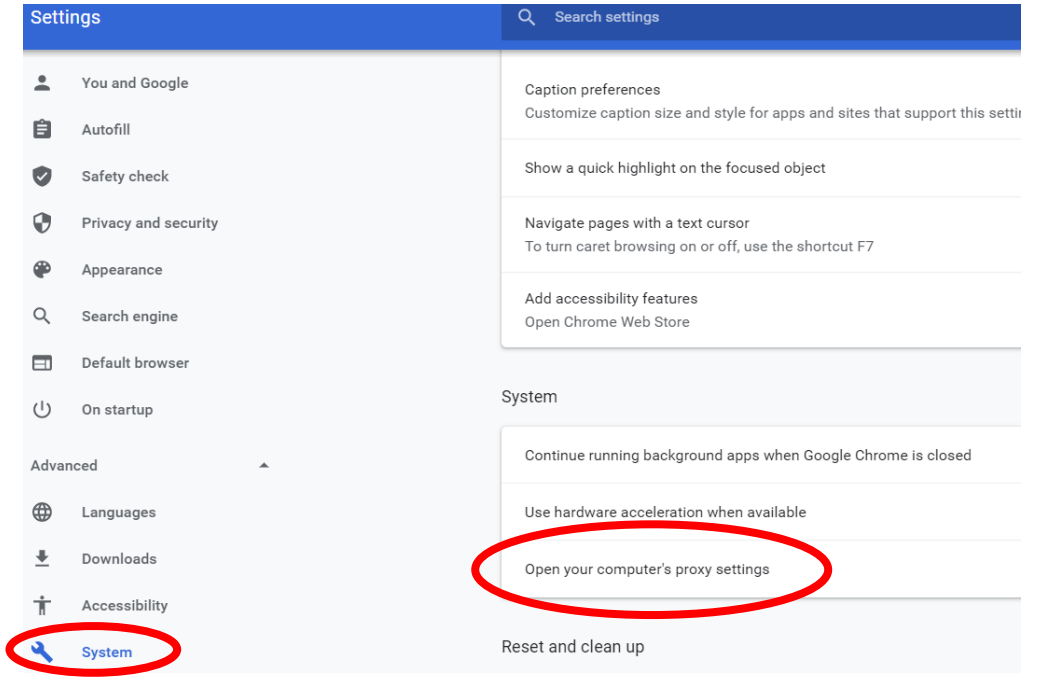
Only needed if you also require access to the SWIFT Certificate Centre from the end-user workstation. (only for Personal Token certificate).

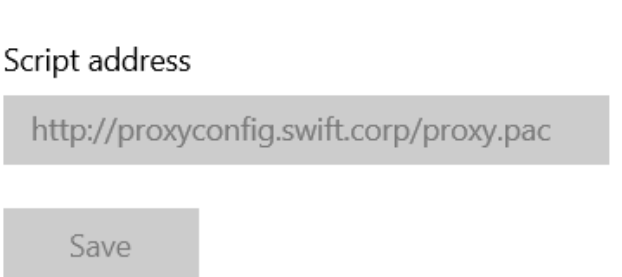
8. Prepare End User's Workstation - Browser

PAC file in Chrome browser settings

The instructions to configure the browser to use a PAC file depends on the browser used. The instructions below are for Chrome.

1. Open the Chrome menu, then click ***Settings***. The Settings window appears.
2. Click ***Advanced*** *in the column menu on the left* then **System**.
3. Click on **Open your computer's proxy settings**
4. The address of the PAC file can be entered in the field Script address. Click **Save** before leaving.





These instructions might change depending on the version of the Browser used.

8. Prepare End User's Workstation - Browser

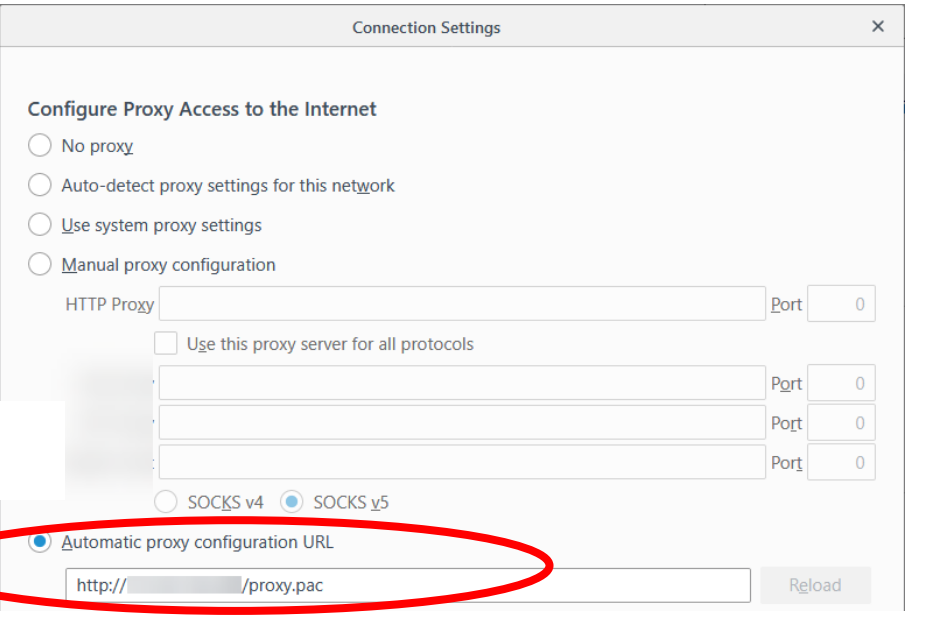
PAC file in Firefox browser settings

The instructions to configure the browser to use a PAC file depends on the browser used. The instructions below are for Firefox.

1. Open the Firefox browser, then click ***Options.***
2. Click ***General***.
3. In the ***Network Settings*** section, click ***Settings.***
4. In the ***Connection Settings*** window, select ***Automatic proxy configuration URL*** and enter the address of the PAC file

   http://proxyconfig.swift.corp/proxy.pac

5. Click ***OK***.



These instructions might change depending on the version of the Browser used.

9. Activate Token

Subscriptions and Configurations	Systems and Network Configurations	Create Certificate	Access ESMIG U2A
1. Subscribe to SWIFT's Solution for ESMIG	5. Network configuration	9. Activate token	11. Access ESMIG U2A
2. Define user DN in ESMIG static data	6. Install Personal Token Software	10. Create personal HSM certificate	
3. Create user DN and setup for certification	7. Install ESMIG U2A SWIFT Login Application		
4. Order personal tokens	8. Prepare end user's workstation		

Only for personal token certificate

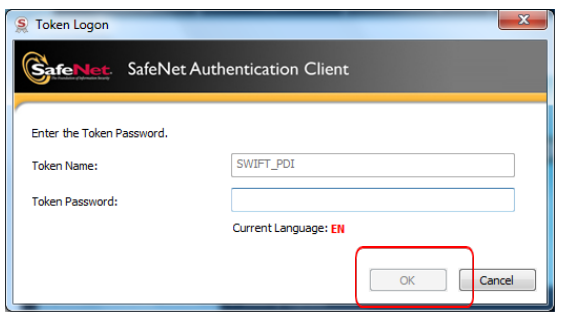
Only for personal HSM certificate

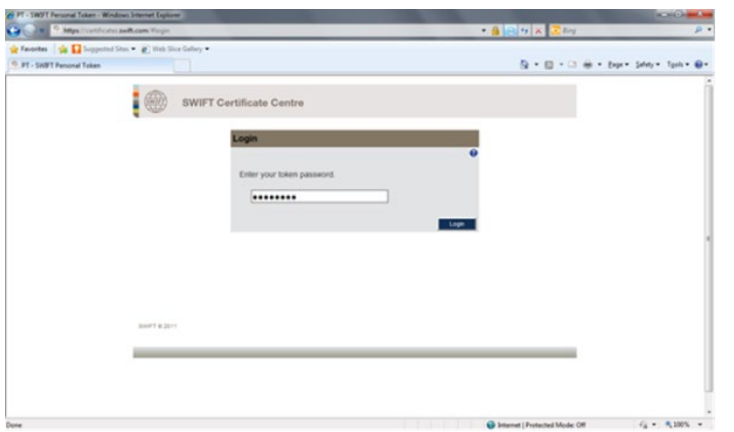
9. Activate Token

www.swift.com/certificates
accessible over Internet
and MV-SIPN

To activate your token, insert it into a PC on which you have installed the token software and log in to the SWIFT Certificate Centre. The activation process starts automatically.

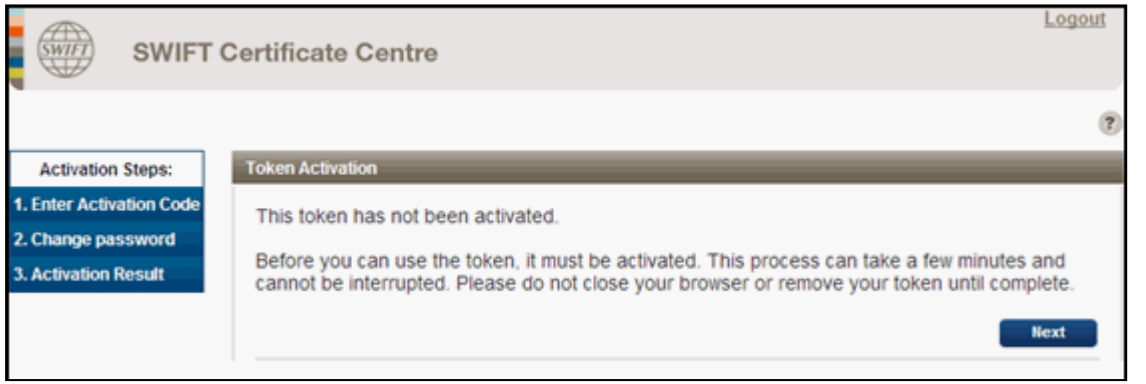
- Insert your token into a free USB port of your computer.
- Click Login. The **Confirm Certificate** window appears.
- Select the certificate and click OK. The **Token Logon** window appears.
- Type the initial password that was supplied with the token in the **Token Password** field and click **OK**. You may have to provide the password a second time.

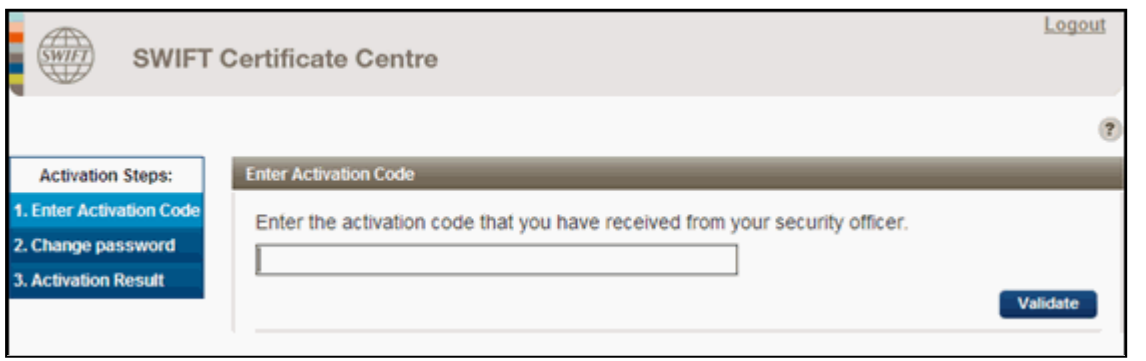




9. Activate Token

- In the **Enter Activation Code** window, type the activation code that you received from your security officer.



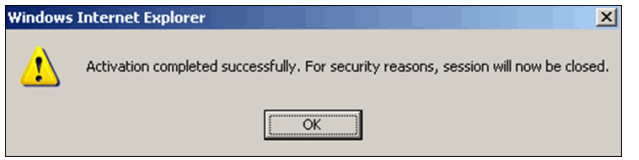


9. Activate Token

You must now set your own password for the token. Read the password policy rules on the **Change password** window, then complete the following fields:

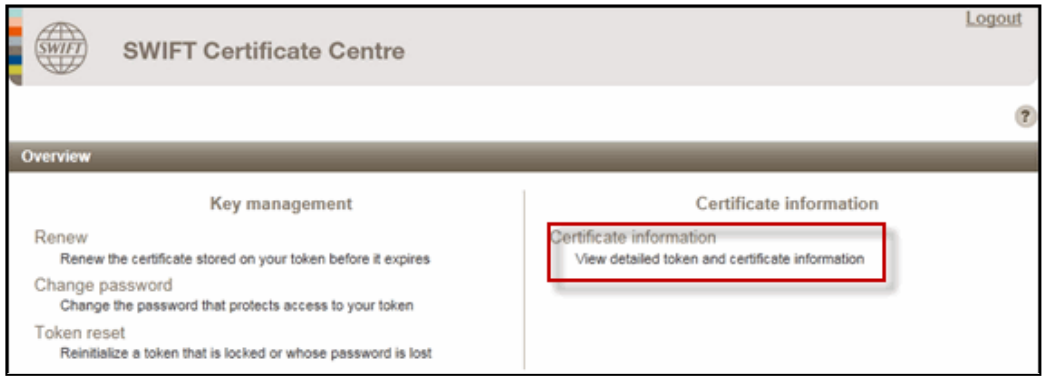
- Current Password: enter the initial password that was supplied with the token.
- New password: provide a strong new password.
- Confirm new password: re-enter the new password.

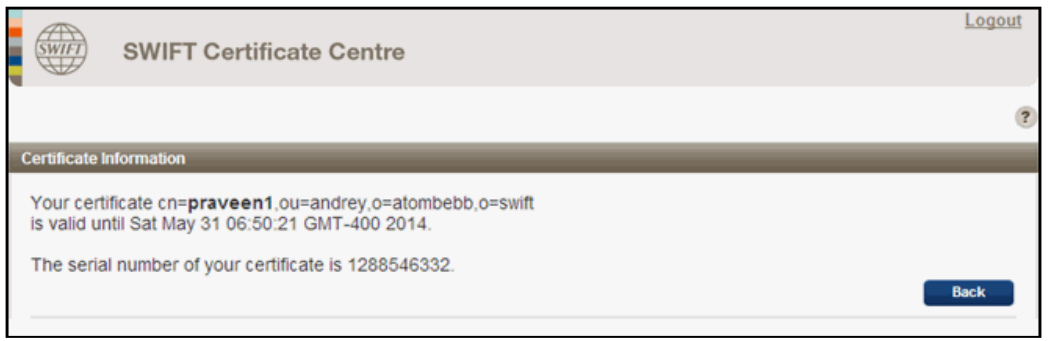
9. Activate Token



9. Activate Token

Welcome Page & Certificate information





10. Create Personal HSM Certificate

Subscriptions and Configurations	Systems and Network Configurations	Create Certificate	Access ESMIG U2A
1. Subscribe to SWIFT's Solution for ESMIG	5. Network configuration	9. Activate token	11. Access ESMIG U2A
2. Define user DN in ESMIG static data	6. Install Personal Token Software	10. Create personal HSM certificate	
3. Create user DN and setup for certification	7. Install ESMIG U2A SWIFT Login Application		
4. Order personal tokens	8. Prepare end user's workstation		

Only for personal token certificate

Only for personal HSM certificate

10. Create Personal HSM Certificate - Real and Virtual SWIFTNet Users

Real and virtual SWIFTNet users

You can access the ESMIG U2A service through Alliance Gateway using a SWIFTNet user, which can be either a real SWIFTNet user or a virtual SWIFTNet user.

When a certificate is created in Alliance Gateway, Alliance Gateway automatically creates a real SWIFTNet user associated with that certificate. The real SWIFTNet user and the certificate share the same name.

You can prevent direct usage of SWIFTNet PKI profiles by creating a virtual profile for every SWIFTNet PKI profile. Preventing direct use enables you to take full advantage of the stronger Alliance Gateway password management policies and the possibility to use a multi-factor authentication method, in case Lightweight Directory Access Protocol (LDAP) or Remote Authentication Dial-In User Service (RADIUS) are configured with multi-factor authentication on the server side.

10. Create Personal HSM Certificate - Real and Virtual SWIFTNet Users

Real and virtual SWIFTNet users

Several virtual SWIFTNet users, each with a unique password, can share the same SWIFTNet certificate. This can be useful in a test environment but is not recommended in a production environment. For the ESMIG platform, virtual SWIFTNet users sharing the same SWIFTNet certificate are seen as one operator, identified by the DN of the certificate.

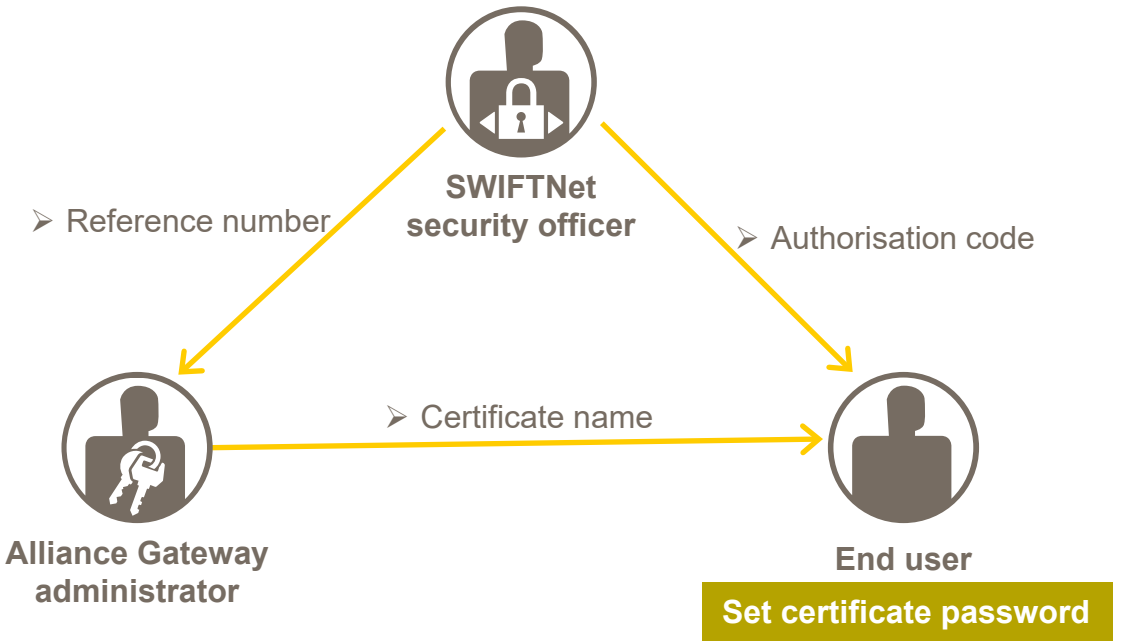
Virtual SWIFTNet users can be set up with a multi-factor authentication method, in case Lightweight Directory Access Protocol (LDAP) or Remote Authentication Dial-In User Service (RADIUS) are configured with multi-factor authentication on the server side. For further information about how to set up these authentication methods, see the Alliance Gateway - Administration and Operations Guide.

Note:

The Security Assertion Markup Language (SAML) protocol is not available for the ESMIG U2A SWIFT Login Application. Also, Lightweight Directory Access Protocol (LDAP) or Remote Authentication Dial-In User Service (RADIUS) can support multi-factor authentication if configured on the server side, which is supported and does not require any additional configuration on Alliance Gateway other than to set it up.

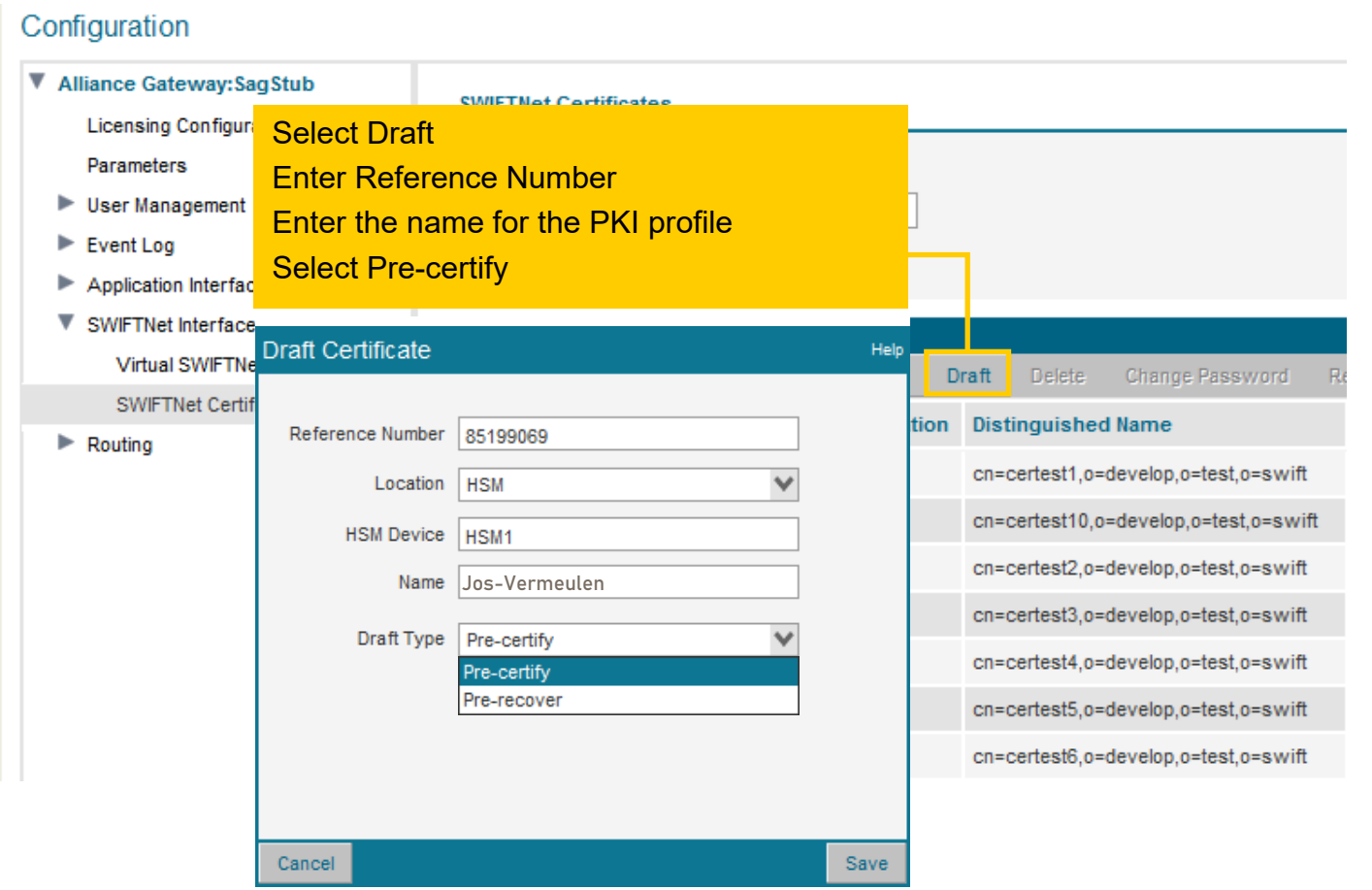
10. Create Personal HSM Certificate - Real SWIFTNet User - Draft Mode

In case the ESMIG U2A service will be accessed through real SWIFTNet users, SWIFT recommends that security officers distribute the initial secrets in such a way that the certificate is set up and managed in Alliance Gateway using the draft mode. Within this draft mode, the certificate is pre-certified by an Alliance Gateway administrator but only the end user can complete the certification process and set the certificate password.



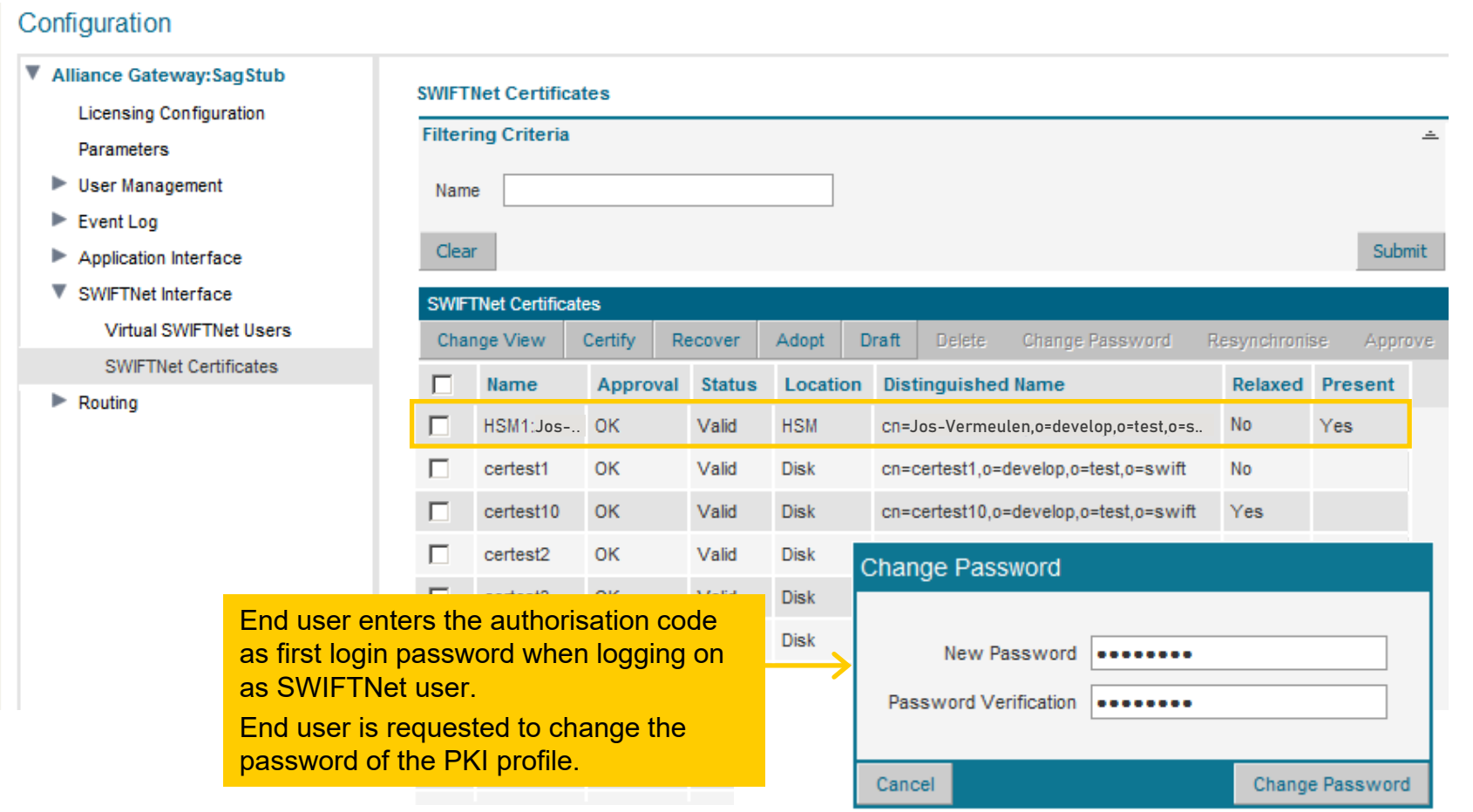
10. Create Personal HSM Certificate - Real SWIFTNet User - Draft Mode

The Alliance Gateway administrator places the SWIFTNet certificate in *Draft* status.



10. Create Personal HSM certificate - Real SWIFTNet User - Draft Mode

The security officer provides the authorisation code to the end user who uses it as a password when logging on as SWIFTNet user.



10. Create Personal HSM Certificate - Virtual SWIFTNet User

In case the ESMIG U2A service will be accessed through virtual SWIFTNet users, the certification process is executed by an Alliance Gateway operator who will manage the password of the certificate.

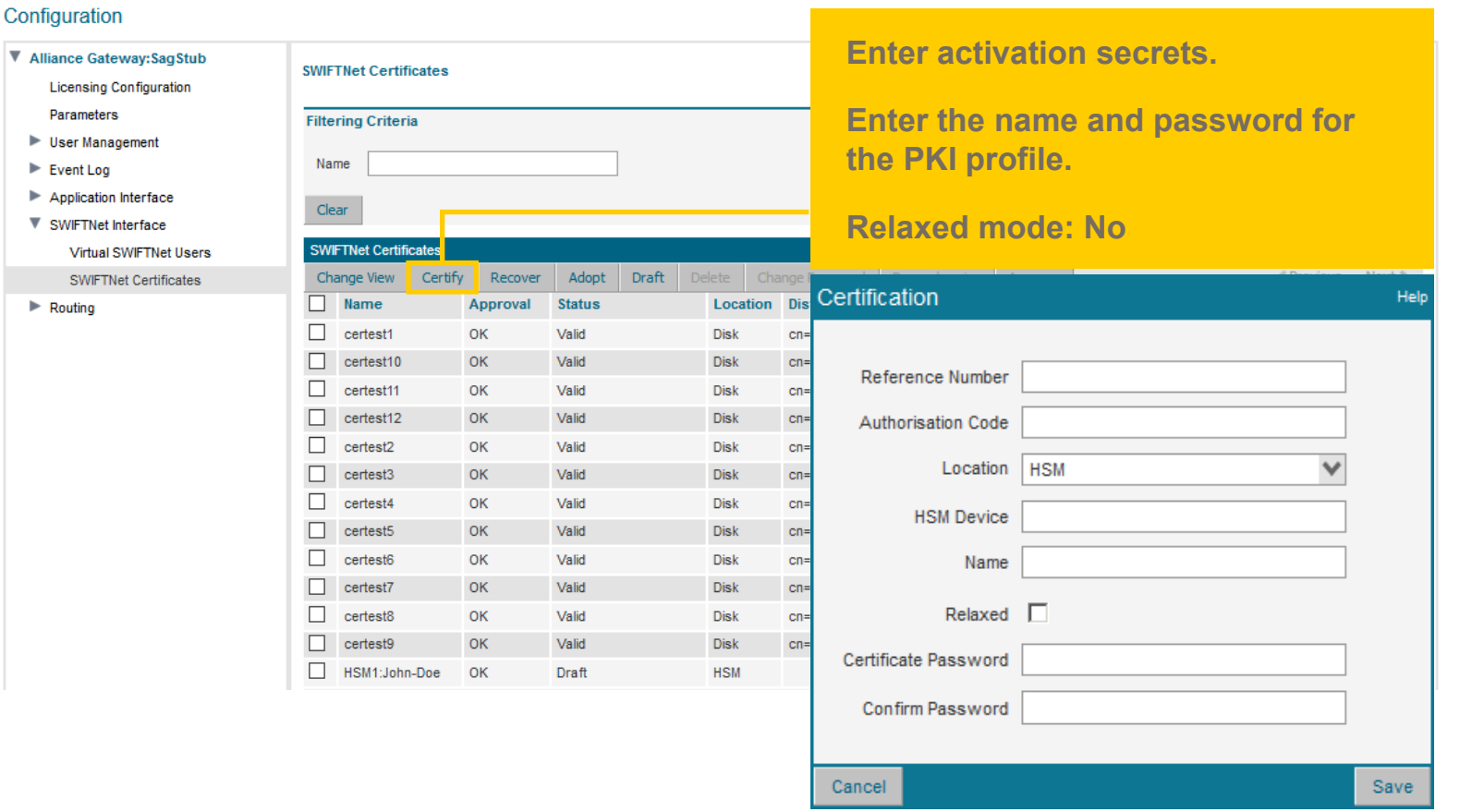
In case of virtual SWIFTNet users, the SWIFTNet Link option “Human Password Expiry Enforcement” should be set to FALSE. This option is used to not block certificates with an expired human password.
The option can be modified by running the following SWIFTNet Link command:

swiftnet parametermodify -p PROFILE_PASSWORD_EXPIRY -v FALSE

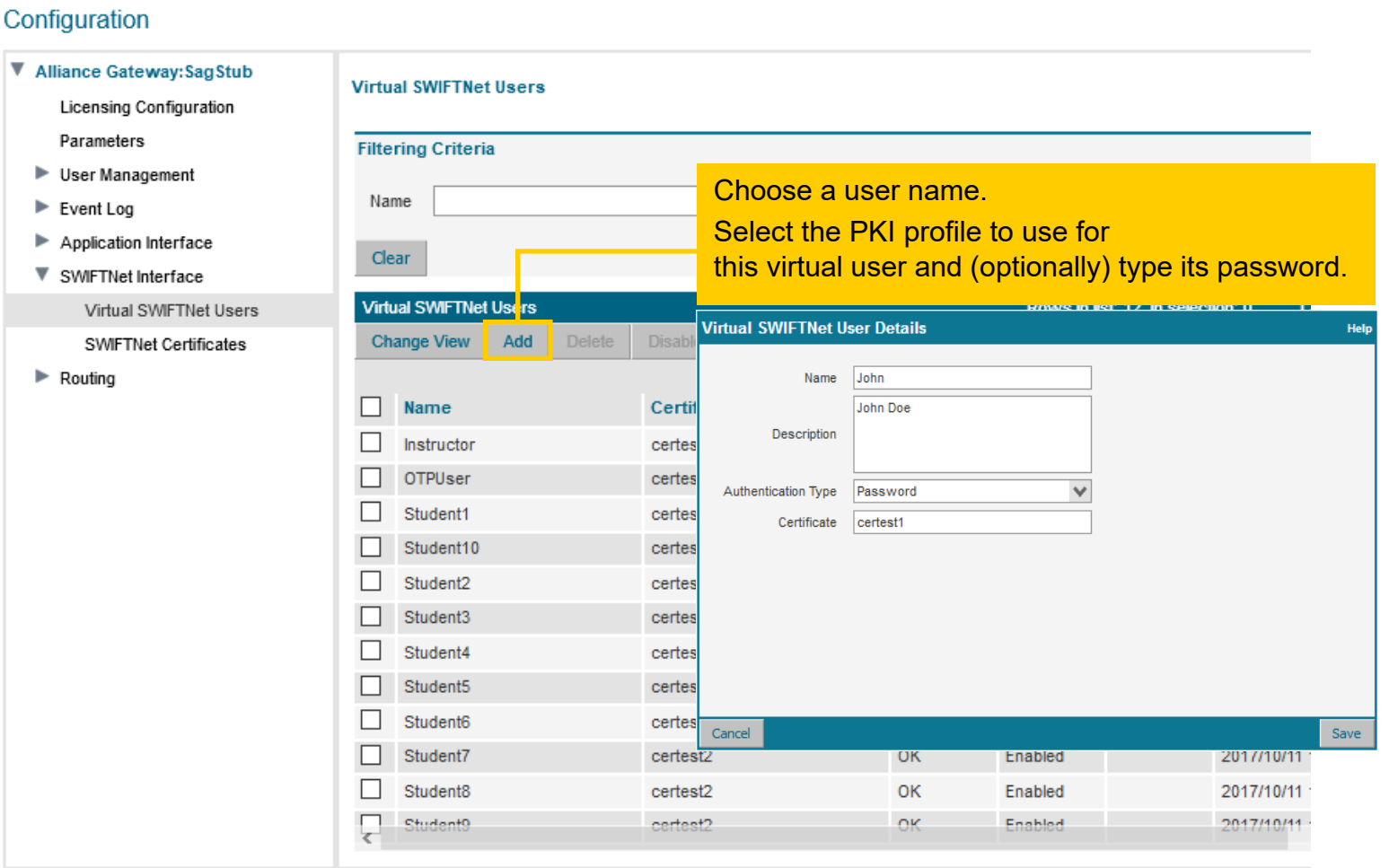
More details are provided in the SWIFTNet Link 7.5 Operations Guide.

10. Create Personal HSM Certificate - Virtual SWIFTNet User - Certify Certificate

The security officer obtains activation secrets and provides them to an Alliance Gateway operator.

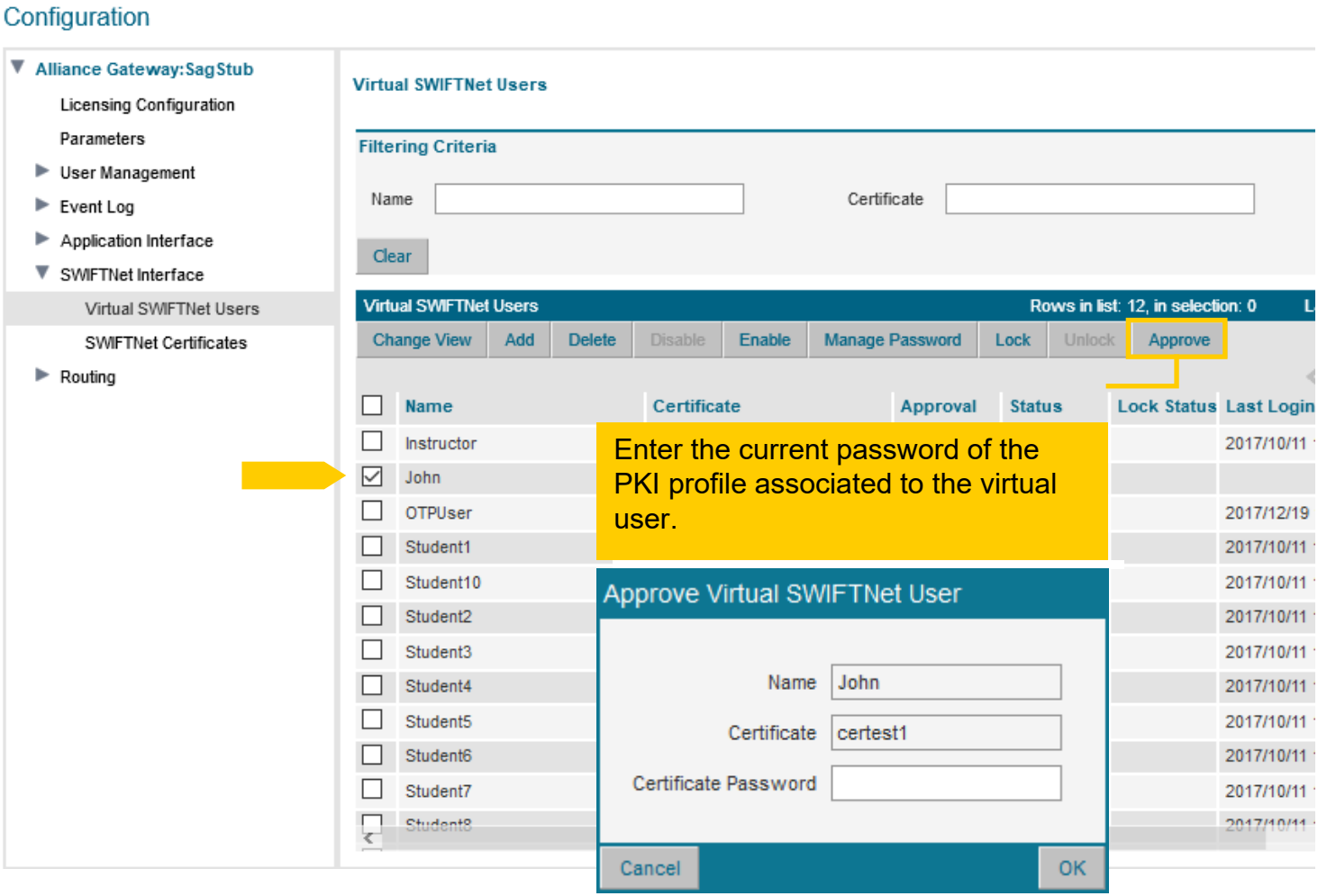


10. Create Personal HSM Certificate - Add New SWIFTNet Virtual User



10. Create Personal HSM Certificate - Approve SWIFTNet Virtual User

...



11. Access ESMIG U2A

Subscriptions and Configurations	Systems and Network Configurations	Create Certificate	Access ESMIG U2A
1. Subscribe to SWIFT's Solution for ESMIG	5. Network configuration	9. Activate token	11. Access ESMIG U2A
2. Define user DN in ESMIG static data	6. Install Personal Token Software	10. Create personal HSM certificate	
3. Create user DN and setup for certification	7. Install ESMIG U2A SWIFT Login Application		
4. Order personal tokens	8. Prepare end user's workstation		

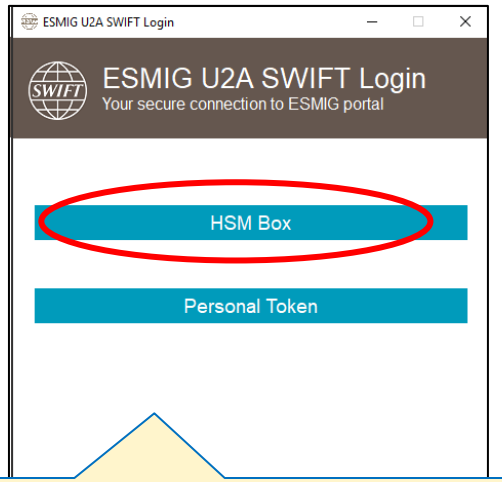
Only for personal token certificate

Only for personal HSM certificate

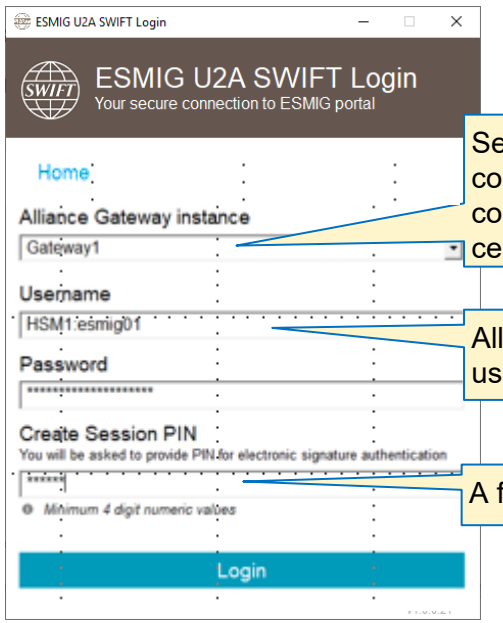
11. Access ESMIG U2A – Using an HSM-based certificate

You must log in to the ESMIG U2A SWIFT Login Application before entering the ESMIG URL in the browser.

- Double-click the ESMIG U2A SWIFT Login icon in the Windows notification area. In a virtualised environment like Citrix, there is no icon in the Windows notification area. The ESMIG U2A SWIFT Login window will be shown automatically when you start the session with the virtualisation server.



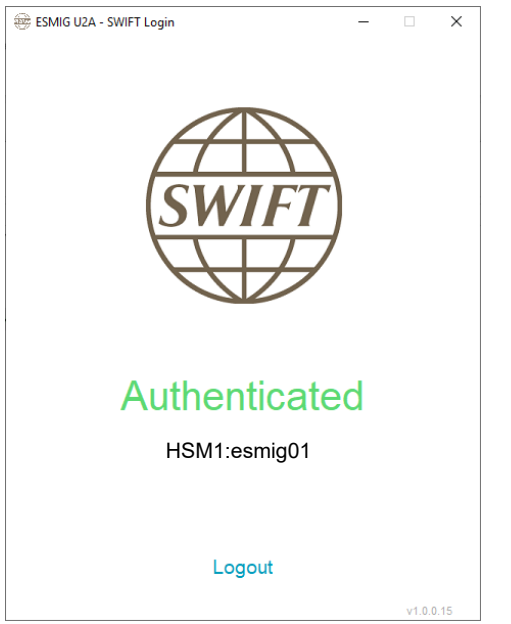
* This screen will only be shown if both HSMBox and PersonalToken are set to 1 (Active) in the configuration file. If the PersonalToken option is set to 0 and HSMBox set to 1, then you immediately get to the second screen: the HSM Box login.



Select the Alliance Gateway connected to the HSM cluster containing the personal HSM certificate.

Alliance Gateway SWIFTNet user name (virtual or real)

A freely chosen session PIN

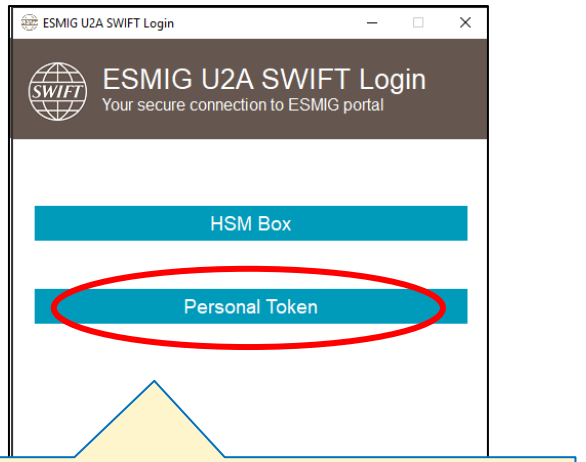


1 → 2 → 3

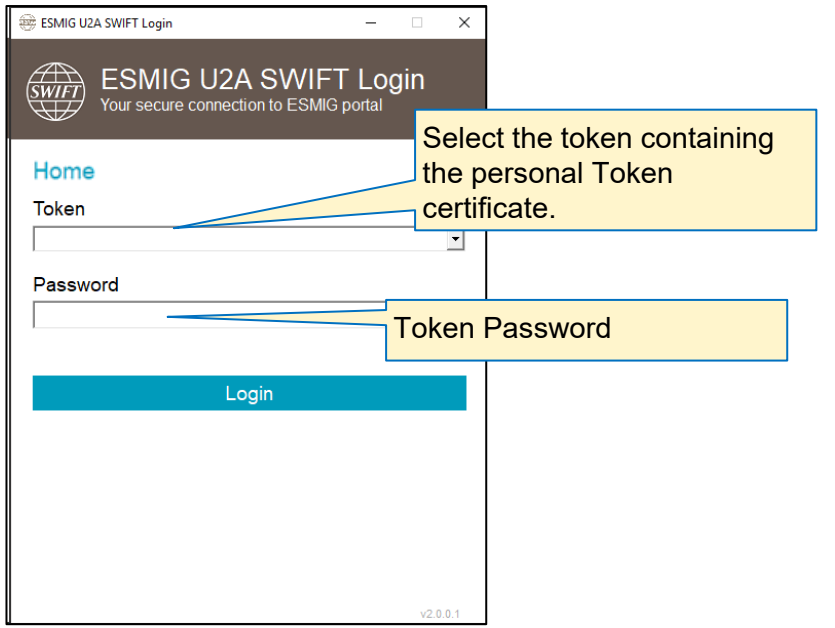
11. Access ESMIG U2A – Using an Token-based certificate

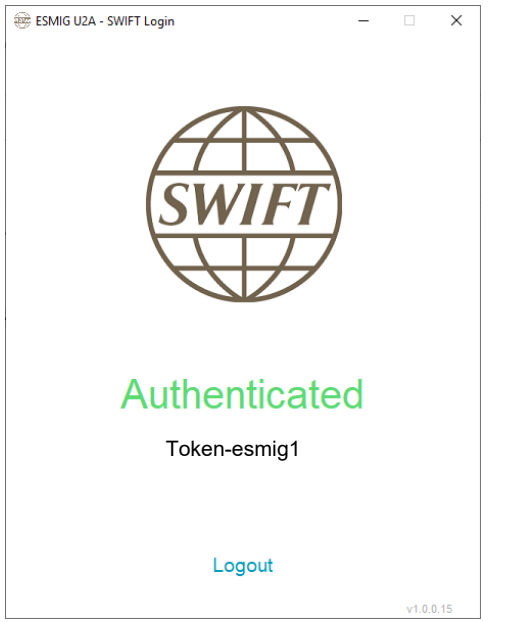
You must log in to the ESMIG U2A SWIFT Login Application before entering the ESMIG URL in the browser.

- Double-click the ESMIG U2A SWIFT Login icon in the Windows notification area. In a virtualised environment like Citrix, there is no icon in the Windows notification area. The ESMIG U2A SWIFT Login window will be shown automatically when you start the session with the virtualisation server.



* This screen will only be shown if both HSMBox and PersonalToken are set to 1 (Active) in the configuration file. If the HSMBox option is set to 0 and PersonalToken set to 1, then you immediately get to the second screen: the Personal Token login.





1 → 2 → 3

11. Access ESMIG U2A - URLs

The final step is to access the ESMIG U2A page.

Type	Application	Environment	URL
Live usage	ESMIG portal	PROD	https://esmig-portal.emip.swiftnet.sipn.swift.com
User testing	ESMIG portal	CERT	https://esmig-cert-portal.emip.swiftnet.sipn.swift.com
Acceptance testing	ESMIG portal	EAC*	https://esmig-eac-portal.emip.swiftnet.sipn.swift.com

Notes :

- **These URLs must be used to access TIPS using the ESMIG U2A SWIFT Login App v2.x.**
- If you want to test your configuration beforehand independently of the ESMIG U2A services, you can use the SWIFT test web portal. See Test web portal.

* The EAC environment is restricted to NCBs and CSDs.

Contents

Contents

Troubleshooting

- **DNS error**
- Test web portal
- ESMIG U2A SWIFT Login Application
- Connection Manager cannot be reached

Troubleshooting - DNS error

The ESMIG U2A solution requires access to the DNS zone named “swiftnet.sipn.swift.com” and “common.sipn.swift.com”: See section 5. Network Configuration – DNS zone forwarder.

The following check can be used to validate if the DNS setting is correct to resolve addresses from the domain “swiftnet.sipn.swift.com”. This check must be run from the system with an access to SWIFT.

1) nslookup on “esmig-cert-portal-proxy.emip.swiftnet.sipn.swift.com”:

- *nslookup esmig-cert-portal-proxy.emip.swiftnet.sipn.swift.com*
  Non-authoritative answer:
  Name: esmig-cert-portal-proxy.emip.swiftnet.sipn.swift.com
  Address: 149.134.64.13

2) checkip “esmig-cert-portal-proxy.emip.swiftnet.sipn.swift.com“ 443 returns:

```
[esmig-cert-portal-proxy.emip.swiftnet.sipn.swift.com 443 TCP]                    : FULL_SUCCESS
================================================================================
  Host IP                :149.134.64.13
  Result                 : FULL_SUCCESS
  Total Time             : 61 ms
================================================================================
```

Troubleshooting - DNS error (continued)

3) nslookup on “esmigu2a.common.sipn.swift.com”:

```
$ nslookup esmigu2a.common.sipn.swift.com

Non-authoritative answer:
Name:   esmigu2a.common.sipn.swift.com
Address: 149.134.64.25
```

4) checkip “esmigu2a.common.sipn.swift.com”:

```
$ checkip esmigu2a.common.sipn.swift.com 443

 [esmigu2a.common.sipn.swift.com 443 TCP]                    : FULL_SUCCESS
================================================================================
  Host IP              :149.134.64.25
  Result               : FULL_SUCCESS
  Total Time           : 62 ms
================================================================================
```

If the URLs are resolved over Public Internet, the IP addresses returned by the above commands will be in the range 149.134.170.X. Unless you are an Alliance Cloud Customer connecting via the Public Internet to the ESMIG Portal, this is incorrect as you are not allowed to connect via Public Internet. This will result in an error while trying to reach the portal.

Contents

Troubleshooting

- DNS error
- **Test web portal**
- ESMIG U2A SWIFT Login Application
- Connection Manager cannot be reached

Troubleshooting - Test Web Portal

SWIFT is providing a test web portal that facilitates troubleshooting in case you do not succeed to access the ESMIG U2A portal.

There are 2 test URLs.

Step 1 – Test basic connectivity to SWIFT

- URL: https://basicconnectivitycheck.common.sipn.swift.com/status

Step 2 – Test subscription to ESMIG U2A services

- URL: https://esmigsubscriptioncheck.common.sipn.swift.com/status

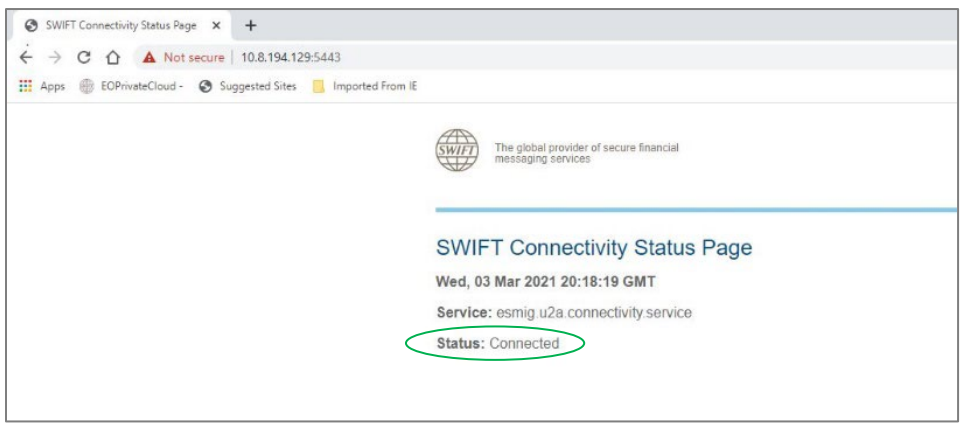
Troubleshooting - Test Web Portal

Step 1 – Test basic connectivity to SWIFT

This step tests the basic connectivity to the SWIFT U2A solution.

- URL: https://basicconnectivitycheck.common.sipn.swift.com/status

If you receive the following response, then the connection is successful and you can proceed to Step 2.



Troubleshooting - Test Web Portal

Step 1 – Test basic connectivity to SWIFT – Troubleshooting

If a positive connection response is not received, then check the following:

- Your institution's firewalls and DNS are configured for the U2A domain "common.sipn.swift.com". See Network Configuration – DNS zone forwarder
- Your browser is configured to trust the SWIFT CA. See Install Personal Token Software and Prepare End User's Workstation.

Troubleshooting - Test Web Portal

Step 2 – Test subscription to ESMIG U2A services

This step checks that 1) your personal certificate (on token or HSM) is reachable from your browser; 2) you have a valid SWIFT certificate; 3) you (identified by the DN of the certificate) are subscribed to one of the ESMIG U2A services.

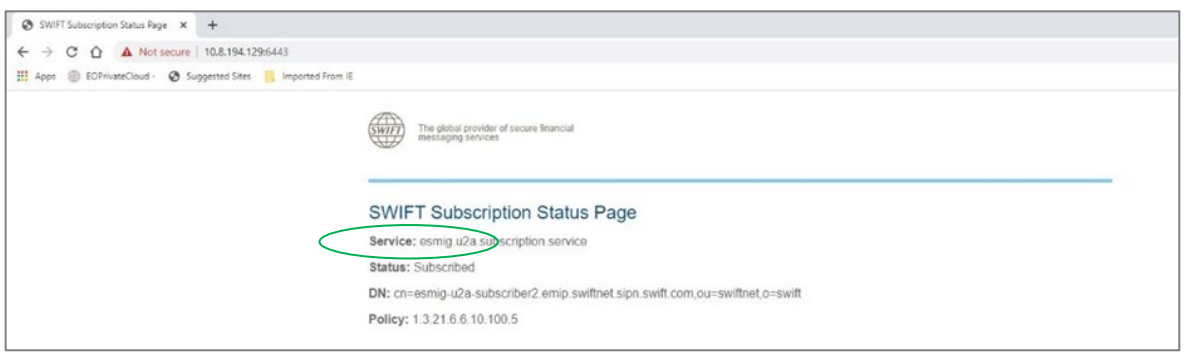
The step will authenticate your certificate, check whether you are a member of one of the ESMIG U2A Closed User Groups, and establish a 2-way TLS connection.

- URL: https://esmigsubscriptioncheck.common.sipn.swift.com/status

You should receive a prompt to enter your certificate password.

If you receive the following response after entering your password, then the subscription check is successful.

Passing Step 2 is no guarantee that you will be able to access each of the ESMIG services. This step only verifies whether you are registered in at least one of them.



Troubleshooting - Test Web Portal

Step 2 – Test subscription to ESMIG U2A services – Troubleshooting

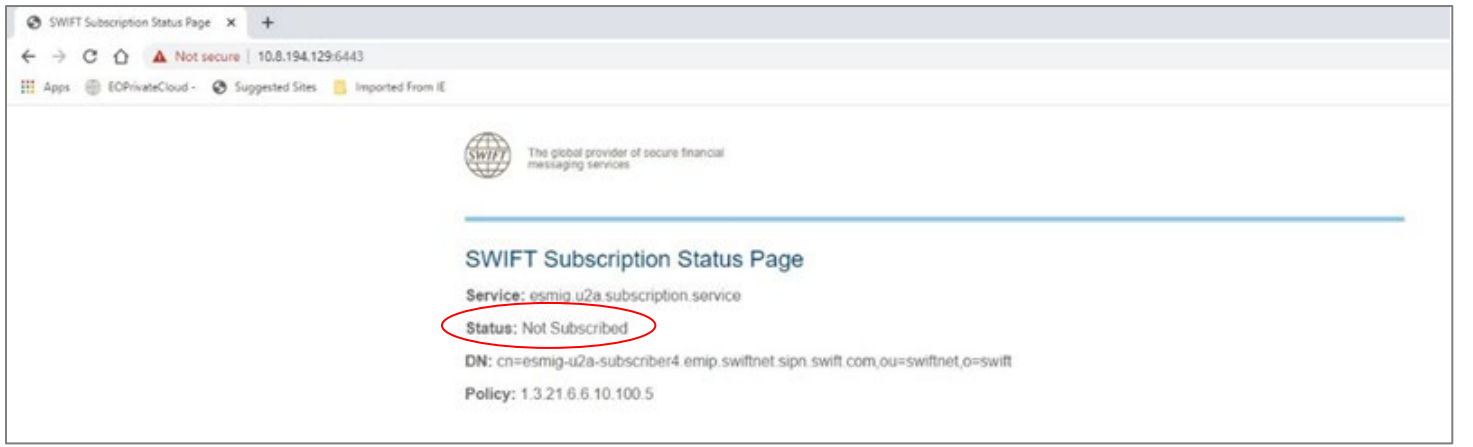
If you are not prompted for a certificate password:

- Check that your browser is configured to trust the SWIFT CA. See Prepare End User's Workstation.
- Check that the ESMIG U2A SWIFT Login Application is installed, running, and that you are logged in – see 7. Install ESMIG U2A SWIFT Login Application.
- If using a personal token:
  - Check that the token software is installed. See Install Personal Token Software.
  - Check that the token is inserted in the USB drive.

Troubleshooting - Test Web Portal

Step 2 – Test subscription to ESMIG U2A services – Troubleshooting (continued)

If you entered a password and received the following error response, then check with your administrator that the DN of your certificate has been provisioned for at least one of the ESMIG U2A services. To add your DN in one of the ESMIG U2A CUGs, you need to submit the corresponding Configuration form on swift.com, for example the T2 Configuration form for UTEST (available as from 1 July 2021).



Even when correctly subscribed to the ESMIG U2A service, it is possible to get the status: Not Subscribed.
This can happen if you are meant to connect over the MV-SIPN connection but the common.sipn.swift.com URL is being resolved over the Internet. See note in Troubleshooting - DNS error.

Troubleshooting - Test Web Portal

Step 2 – Test subscription to ESMIG U2A services – Troubleshooting (continued)

If you entered a password and received an SSL error message, then check with your administrator that your certificate has not expired.

Additional potential error conditions:

- Invalid username or password error: retry or contact your administrator.
- Connection to Alliance Gateway failed. Restart the application, or contact your administrator: close the login window and restart the application by double-clicking the ESMIG U2A SWIFT Login icon in the Windows notification area, and try again.

Contents

Troubleshooting

- DNS error
- Test web portal
- **ESMIG U2A SWIFT Login Application**
- Connection Manager cannot be reached

ESMIG U2A SWIFT Login Application – Logs and trace

- Log:
  - Location: “C:\users\<USER>\AppData\Local\SWIFT\SwiftU2AApp\log\SwiftU2AApp.log”
  - Contains logs made by the application itself
  - Logging is always active
  - Logs are truncated at the start of the application

- Trace:
  - Location: “C:\users\<USER>\AppData\Local\SWIFT\SwiftU2AApp\log\SwiftTray.out”
  - Traces must be activated using « SwiftTrace.exe on » located in the installation folder

- Connection Manager log:
  - Location: “C:\Windows\ServiceProfiles\LocalService\AppData\Local\SWIFT\SwiftU2AService\log”
  - Contains logs made by the service
  - Logging is always active

ESMIG U2A SWIFT Login Application – Installation tree

- After the installation of the ESMIG U2A SWIFT Login Application, the following files should be present on the system.

<INSTALL_FOLDER>
 |- config
 | |- configuration.ini
 | |- cacert.pem
 |- data
 | |- ExcStatus.xml
 |- libsagapp_70.dll
 |- libsagextractor.dll
 |- libswcomm.dll
 |- libswexception.dll
 |- libswposl.dll
 |- libswposl2.dll
 |- libswstring_20.dll
 |- libswtrace.dll
 |- libswtransport.dll
 |- xerces-c_3_2.dll
 |- SwiftTrace.exe
 |- SwiftU2ATray.exe
 |- uinstall.bat
 |- ConnectionManager.exe
 |- installation_notice.txt

C:\windows\system32
 |- SWIFTKSP.dll
 |- swiftp11.dll

C:\windows\SysWOW64
 |- SWIFTKSP.dll
 |- swiftp11.dll

C:\users\Default\Desktop
 |- ESMIG U2A SWIFT Login.lnk

Registry
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\SwiftU2AApp
- HKLM\Software\SWIFT\SwiftU2AApp\InstallPath
- HKEYLM\SYSTEM\CurrentControlSet\Control\Cryptography\Providers\SWIFT KSP

Contents

Troubleshooting

- DNS error
- Test web portal
- ESMIG U2A SWIFT Login Application
- **Connection Manager cannot be reached**

Troubleshooting – Connection Manager cannot be reached

When you receive the error ‘Connection Manager cannot be reached’ upon login, it is very likely that the Windows Connection Manager service is down.

See 7. Connection Manager service to verify whether the service is started. If not, restart the service.

Appendix 1

Access ESMIG U2A services using a Citrix environment

Access ESMIG U2A Services using a Citrix Environment

This appendix is only for users who want to access the ESMIG U2A services through Citrix or similar virtualisation environments.

The solution can also be used to access the current TIPS U2A services through Citrix. This is explained further in this appendix.

As of release 2.0, the ESMIG U2A SWIFT Login Application includes a service (“Connection Manager”) that replaces both the Java proxy and the Java-based Connection Manager software. There is no need anymore to install a separate Connection Manager on top of the ESMIG U2A SWIFT Login Application.

Citrix Support

SWIFT has carried out a confidence test in a Citrix environment at SWIFT, using the APPS and the DESKTOPS mode.

- Due to the many versions/technologies possible, SWIFT does not qualify specific virtualisation versions or setups.

- SWIFT provides reasonable support, and may ask customers to work with the virtualisation vendor directly, if the problem is suspected to be caused by the vendor software (Knowledge Base article 2237576).

Note that the communication between the remote clients and the virtualisation server, as well as the whole setup and sizing of the virtualisation solution, is under customer control and responsibility.

Thin clients

- SWIFT supports users using thin clients on best-effort basis.
- SWIFT has no capabilities to test such a setup, and will not qualify specific thin clients.

Personal Token Software and ESMIG U2A SWIFT Login Application

The ESMIG U2A SWIFT Login Application must be installed on the Citrix host.

The ESMIG U2A SWIFT Login window will be shown automatically when the user starts its session with the virtualisation server.

The configuration file (*configuration.ini)* must include “Citrix=1”.

```
[Configuration]
## Uncomment the following line to add an HTTP proxy between this application and the Alliance Gateway
#AllianceGatewayProxy=5.6.7.8:8080

## Uncomment the following line when the application runs on a Citrix environment
#Citrix=1
```

Inside a Citrix environment (“Citrix=1”),

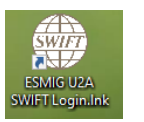
- The application icon will not appear on the workstation Windows notification area (Tray) but directly on the desktop of the end user.
- When a Citrix timeout occurs, the application may stay alive and the user stays logged in. The next time the user tries to open the application, Citrix will show the one already running.
- If **personal token** are used, the Personal Token software must be installed on both the client as well as the Citrix host. It is possible to install a Minidriver on the client side in case of disk space limits. See Knowledge Base article 5018973. The token must be inserted before starting the Citrix session.

Disabling the automatic launch of the ESMIG U2A SWIFT Login Application

This section is dedicated to customers who use CITRIX servers that run multiple applications, not all related to ESMIG.

- During the installation of the ESMIG U2A SWIFT Login Application, the administrator chose that the application has to be launched every time a user opens a session on the server (default configuration).

- Administrators may want to disable the automatic launch of the ESMIG U2A SWIFT Login Application
- **Administrators must :**
  - **either** ensure that the ESMIG U2A SWIFT Login Application is launched prior to invoking the ESMIG U2A url, in the same CITRIX session
  - **or** offer a CITRIX desktop with
    - the shortcut to the ESMIG U2A SWIFT Login Application that has been automatically created by the installation procedure that points to "**%InstallationFolder%\SwiftU2ATray.exe**"
    - A shortcut to invoke the ESMIG url



- How to disable the automatic launch of the ESMIG U2A SWIFT Login Application ?

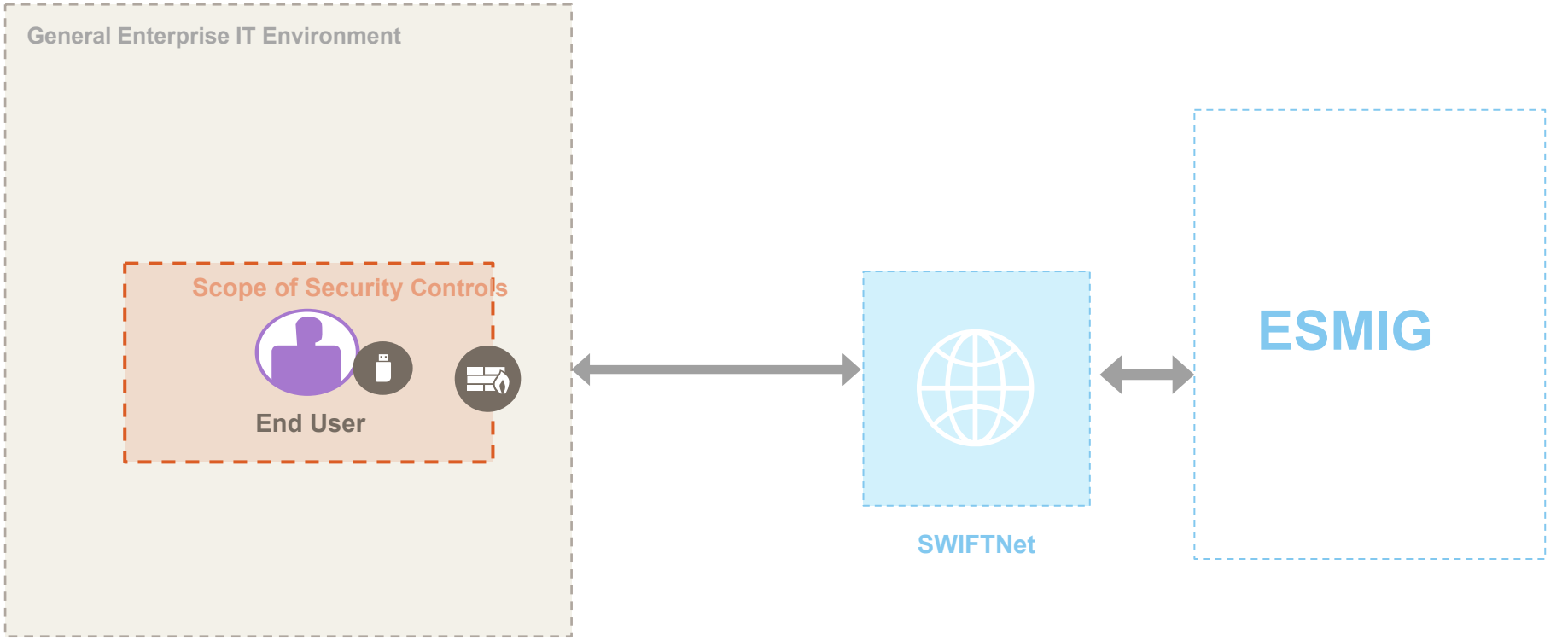
  After having installed the ESMIG U2A SWIFT Login Application, the administrators can remove the CITRIX server registry entry :

  "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v "SwiftU2AApp" /t REG_SZ /f /d "%InstallationFolder%\SwiftU2ATray.exe"

Appendix 2

Examples of Infrastructure diagram in the context of CSP

1. ESMIG – U2A Customer - No Footprint - architecture type B



2. ESMIG U2A Customer using the SAG infrastructure (Architecture Type A1) - High level view - Legend and recommendations

= Browser

= Login Flow (signature requests)

= https Flow

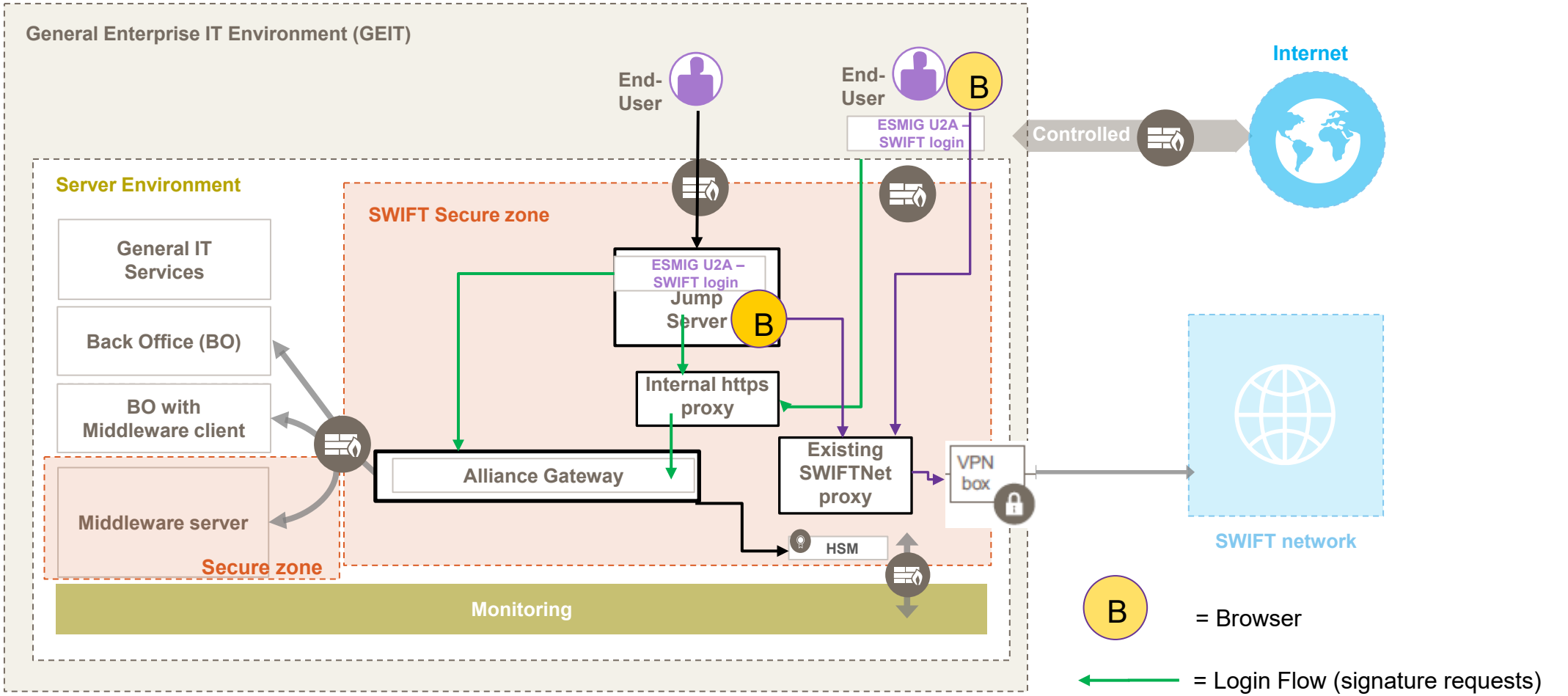
1. SWIFT recommends to separate the existing SWIFTNet proxy (https flow) from the new internal proxy (signature request flow) to prevent from malicious and unexpected usage of the proxies functions, denial of service, identity theft …

2. Conditions for co-hosting the existing SWIFTNet proxy with the SAG Software

- Have different users running the SAG/Proxy applications
- Have non privileged profiles running the applications
- The proxy is subject to relevant cyber hygiene CSP controls

3. The new **internal** proxy can rely on any solution from the market (Squid, Apache, network appliance, or the AWP proxy if not already used for the SWIFTNet proxy) located in the secure zone.

2. ESMIG U2A Customer using the SAG infrastructure (A1) - SWIFT Login signature and https flows High level view



Examples of implementation for ESMIG U2A customers – SAG Users – A1 (Non Exhaustive)

Legend:

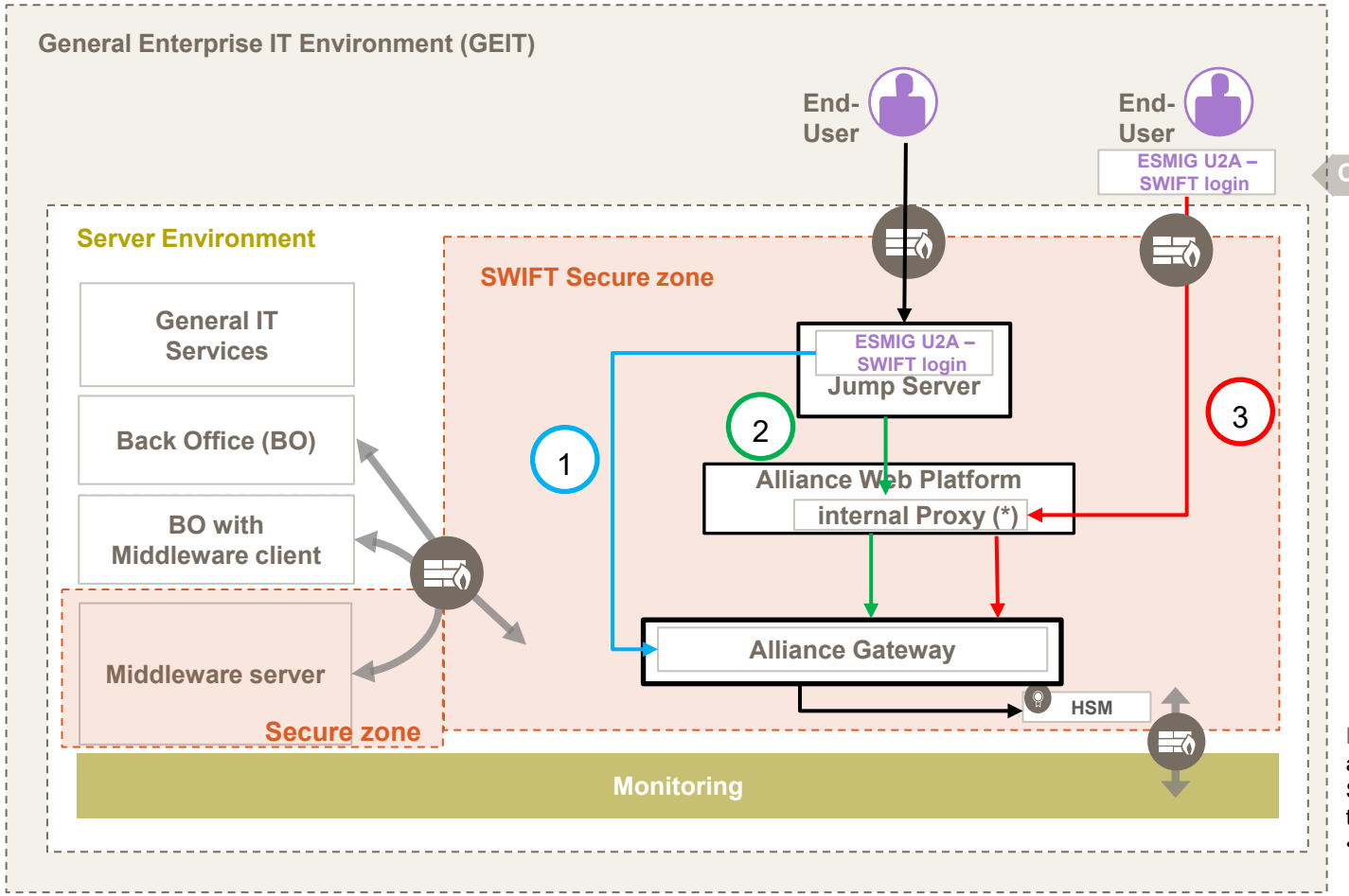
Numbers used on the coloured arrows in the first slide:

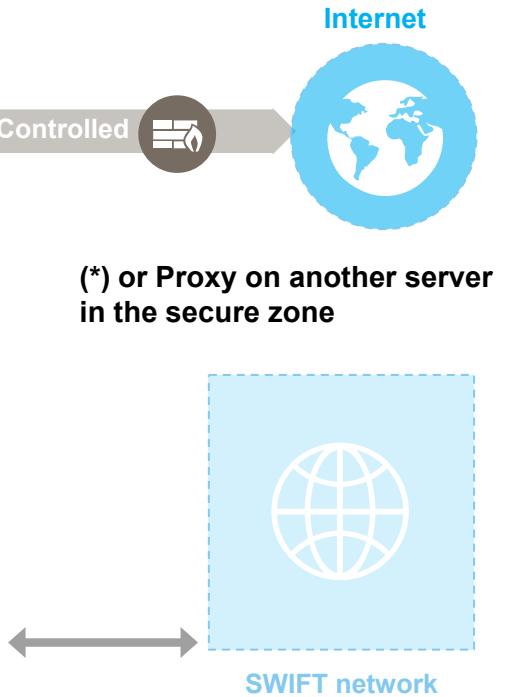
1x. Flows using a browser on a Jump server and using an Alliance **Gateway**

2x. Flows using a browser on a Jump server and using an **AWP**

3x. Flows originating from a user with a local browser app on a local PC
indicates the usage of a potential other secure zone

ESMIG U2A Customer using the SAG infrastructure (A1) - SWIFT Login signature flows

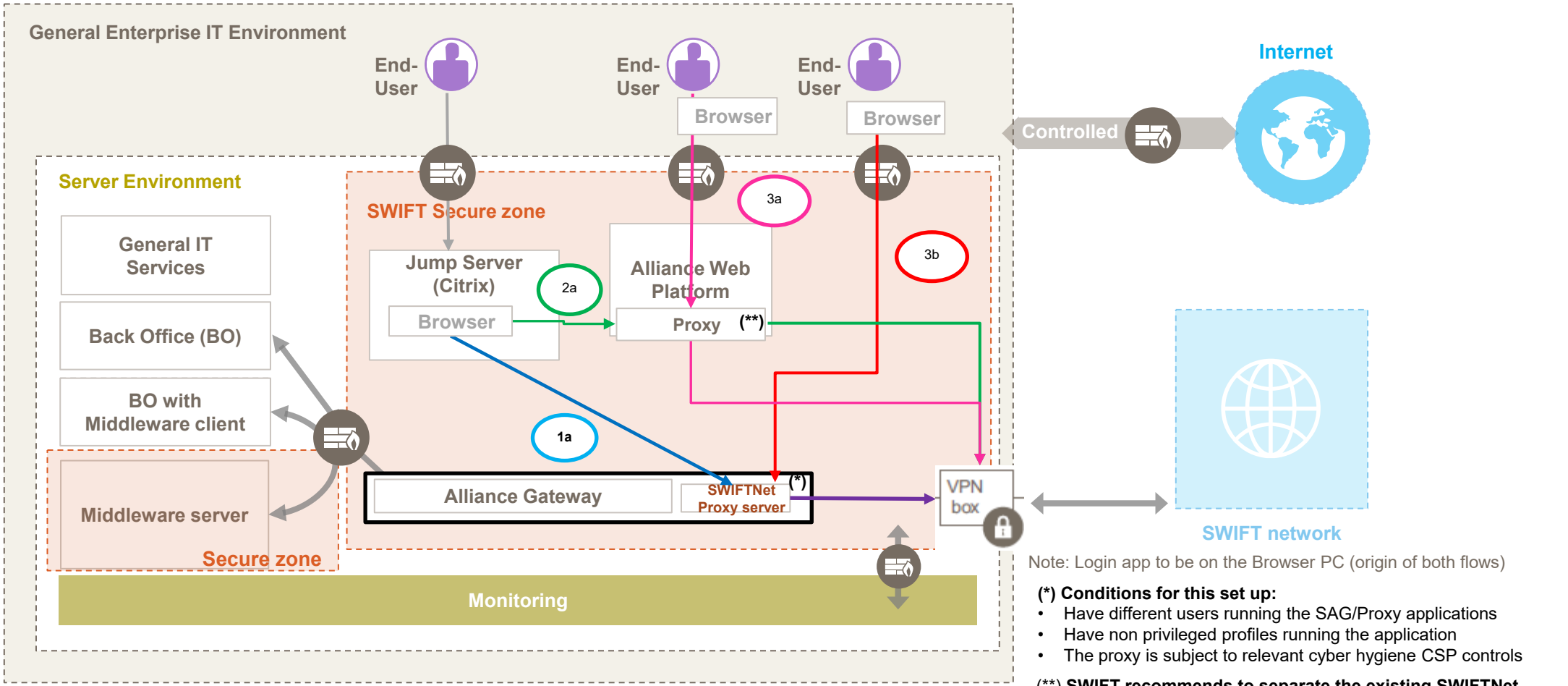




Note: The **Red** #3 flow is a new flow introduced with the ESMIG application and going from the app to the Gateway .
Some condition apply to users accessing directly the AWP from the GEIT:

- AWP is in the secure zone and logically separated from messaging and communication interface.
- Multi-factor authentication is implemented where appropriate
- This setup cannot be used for operating system administration activities

ESMIG U2A Customer using the SAG infrastructure (A1) - https flows – within SWIFT secure zone only



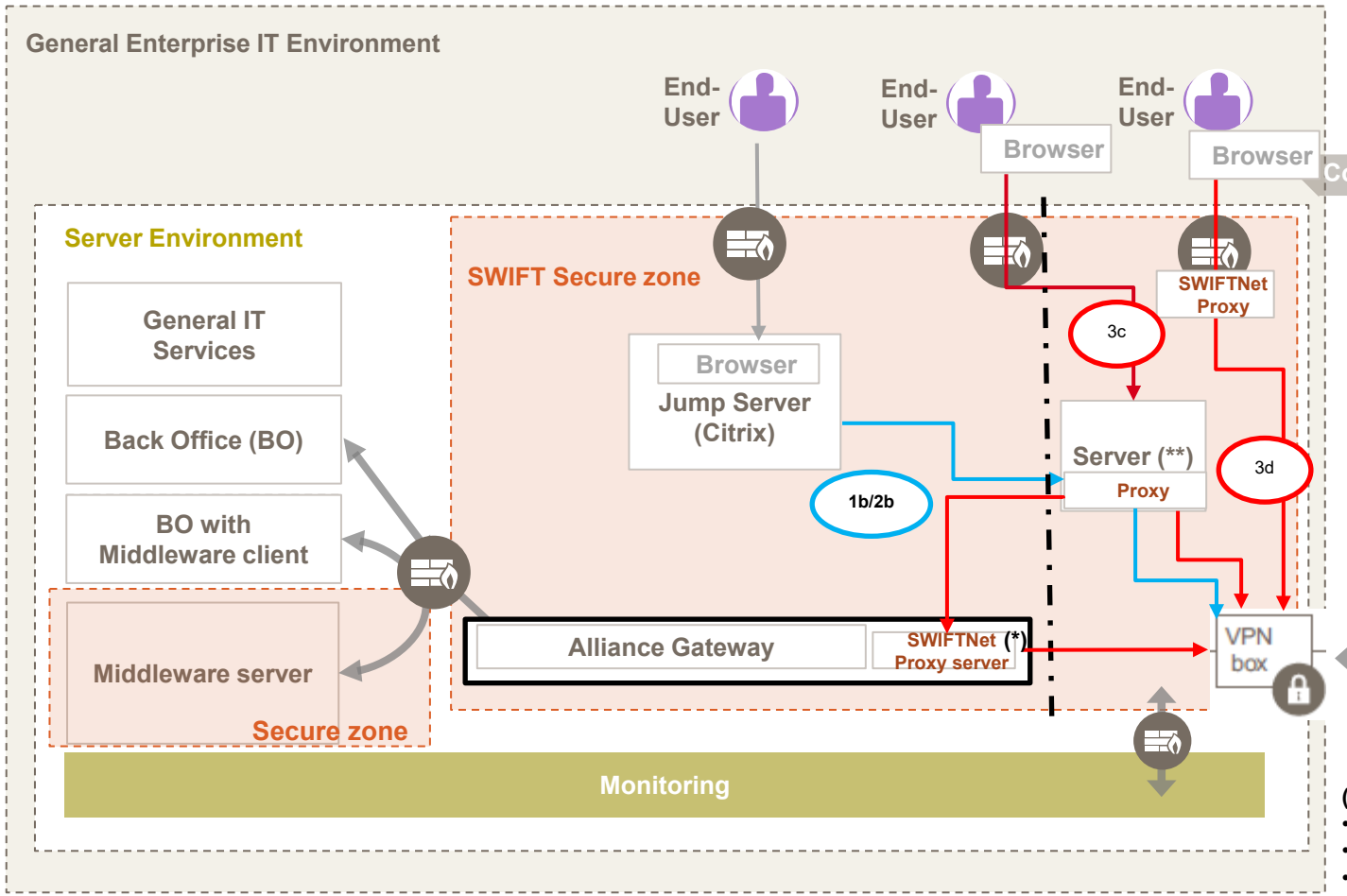
Note: Login app to be on the Browser PC (origin of both flows)

(*) Conditions for this set up:

- Have different users running the SAG/Proxy applications
- Have non privileged profiles running the application
- The proxy is subject to relevant cyber hygiene CSP controls

(**) **SWIFT recommends to separate the existing SWIFTNet proxy (https flow) from the new internal proxy (signature request flow to prevent from malicious and unexpected usage of the proxies functions, denial of service, identity theft …**

ESMIG U2A Customer using the SAG infrastructure (A1) - https flows - using a separate server or through the VPN box



(**) must be in a secure zone

(*) Conditions for this set up:

- Have different users running the SAG/Proxy applications
- Have non privileged profiles running the application
- The proxy is subject to relevant cyber hygiene CSP controls

www.swift.com