POINTSHARP

RA role descriptions

Pointsharp Secure Cloud Net iD SweID

Classification:	Public
Publication No.:	PSC-Rd22-05
Document version:	1.1
Document status:	Final
Date:	03 Jun 2022

Table of Contents

1 General

1.1 About this document

This document contains the role descriptions for the necessary RA roles needed for using the service Pointsharp Secure Cloud Net iD SweID (The Service) and to comply with the regulatory requirements related to The Service. It covers the activities and accountability of the persons who fill the roles.

1.2 Who should use these role descriptions

The persons who fill the different roles, the person in the client organization who are responsible for appointing the roles, or persons making other relevant decisions related to the service.

2 SweID - RA Security Officer role description

2.1 General

Description of the tasks that the RA Security Officer performs and what his responsibilities are in the administration of the e-identities in the RA organization.

2.2 Qualifications

Before a person is assigned the role of RA Security Officer, an identity check must be made by a representative within the RA organization with the applicable mandate. At the identity check, the person who shall be assigned to the role must present a valid and nationally approved identity document.

A background check must be done on the person that is assigned the role.

The person assigned the role must not have another assignment within or outside the RA organization that can be considered to conflict with the work as RA Security Officer. For example, other RA roles like RA Auditor or any other RA Officer role.

The RA Security Officer must have sufficient training, time, and resources set aside to carry out his assignment.

2.3 Responsibilities and Duties

The following tasks are performed by the RA Security Officer:

- Has the overall responsibility for establishing an RA domain with sufficient human resources to fulfill the organization's commitments.
- Is responsible for ensuring that the RA domain complies with the rules and procedures of Pointsharp Secure Cloud Net iD regarding the application, ordering, handing out, and revocation of e-identities to persons related to the RA organization.

- Is responsible for ensuring that all individuals who have an RA role have adequate knowledge and are suitable to maintain the organization's commitment, over time.
- Is responsible for the management of permissions for other RA roles within the RA domain for access to the Pointsharp Secure Cloud Net iD Portal, if not handled by Pointsharp (RA organizations strictly handling LoA2).
- Is responsible for reporting security incidents and defects to Pointsharp.
- Is responsible for submitting the Declaration of Compliance to PsPT.
- Is responsible for evaluating the RA domain's compliance with processes for the management of subscribers and e-identities.
- Carries out risk analyzes within the RA domain.
- Contribute to the establishment and management of continuity plans within the RA domain with tested and documented procedures.
- Is responsible to do identity checks and background controls of the persons that will be assigned the following roles within the RA:
  - RA Central Officer
  - RA Local Officer
  - RA Report Officer
  - RA Helpdesk Officer
  - RA Auditor
- Is responsible for the education of the RA officers.
- Is responsible to control and evaluate compliance to the RA's obligations according to the Customer Agreement, the RA Trust Framework, and the CP/CPS for Pointsharp Secure Cloud Net iD SweID.

2.4 Other

If the RA Security Officer leaves the role, the RA organization must appoint a new RA Security Officer. During the absence of an RA Security Officer, the main Security Officer or another person responsible for security management at the RA organization temporarily takes over the obligations normally incumbent on the RA Security Officer. The name of the new person appointed to the RA Security Officer role or any temporary appointment of the role must be reported to PsPT at the time of the appointment.

In the absence of an RA Auditor, the RA Security Officer temporarily takes over the obligations normally incumbent on the RA Auditor. However, the RA Security Officer must not obtain corresponding authorizations in The Service.

3 SweID · RA Auditor role description

3.1 General

Description of the tasks that the RA Auditor performs and what his responsibilities are in the administration of the e-identities in the RA organization.

3.2 Qualifications

The RA Auditor must have adequate knowledge and be suitable to maintain the organization's commitment, over time.

The RA Auditor must have sufficient training, time, and resources set aside to carry out his assignment.

A background check must be done on the person that is assigned the role.

3.3 Responsibilities and Duties

To be able to is review other officers in the system, the RA Auditor has access (read and search) to audit logs regarding actions concerning subscribers, key bearers and e-identities managed in The Service Portal.

The following tasks are performed by the RA Auditor:

- Responsible for evaluating the RA domain's compliance with processes for the management of subscribers and e-identities.
- Responsible for internal audits regarding the management of e-identities.
- Supervision of the RA Officers.

The RA Auditor has access to search and read the audit logs of The Service.

3.4 Other

The RA Auditor role must not be combined with another role within the RA domain, except during circumstances mentioned below.

In the absence of an RA Auditor, the RA Security Officer temporarily takes over the obligations normally incumbent on the RA Auditor.

4 SweID · RA Central Officer role description

4.1 General

Description of the tasks that the RA Central Officer performs and his responsibilities in the administration of subscribers and e-identities in the RA organization.

4.2 Qualifications

The RA Central Officer must have adequate knowledge and be suitable to maintain the organization's commitment, over time.

The RA Central Officer must have sufficient training, time, and resources set aside to carry out his assignment.

A background check must be done on the person that is assigned the role.

4.3 Responsibilities and Duties

The RA Central Officer has a large part in the administration of subscribers, e-identities, and key bearers within the organization, such as adding subscribers in The Service Portal, assigning privileges for RA Officers, or ordering personalized cards.

An important task for the RA Central Officer is to create RA subscribers and assign privileges to the RA Officer roles. When adding a subscriber, the RA Central Officer is responsible for verifying that an order to add the subscriber has been made and that the subscriber exists in the organization's trusted directory.

The RA Central Officer is mainly involved in the following subscriber and privilege processes:

- Manage subscribers
- Assign privileges to RA officers
- Revoke e-identities and key bearers
- Upload photo of subscribers
- Error-handling in portal processes

For details, please refer to *Pointsharp Secure Cloud Net iD Officer's guide.*

5 SweID · RA Local Officer role description

5.1 General

Description of the tasks that the RA Local Officer performs and his responsibilities in the administration of the e-identities in the RA organization.

5.2 Qualifications

The RA Local Officer must have adequate knowledge and be suitable to maintain the organization's commitment, over time.

The RA Local Officer must have sufficient training, time, and resources set aside to carry out his assignment.

A background check must be done on the person that is assigned the role.

5.3 Responsibilities and Duties

The RA Local Officer has a large part in the administration of subscribers, e-identities, and key bearers within the organization both on site and remote.

The RA Local officer is responsible to check the identity of the persons when issuing primary or temporary e-identities. This is done by checking a valid and nationally approved identity document and that the user exists in the organization's trusted directory.

The RA Local Officer is mainly involved in the following subscriber and privilege processes:

- Issue primary and temporary e-identities on site (LoA3)

- Enroll mobile e-identities (LoA3)
- Register orders of personalized cards (LoA3)
- Unlock e-identities and key bearers
- Revoke e-identities and key bearers
- Order batches with cards
- Upload photo of subscribers
- Error-handling in portal processes

For details, please refer to *Pointsharp Secure Cloud Net iD Officer's guide.*

6 SweID · RA Helpdesk Officer role description

6.1 General

Description of the tasks that the RA Helpdesk Officer performs and his responsibilities in the administration of the e-identities in the RA organization.

6.2 Qualifications

The RA Helpdesk Officer must have adequate knowledge and be suitable to maintain the organization's commitment, over time.

The RA Helpdesk Officer must have sufficient training, time, and resources set aside to carry out his assignment.

A background check must be done on the person that is assigned the role.

6.3 Responsibilities and Duties

The RA Helpdesk Officer is not involved in the management of the e-identities. But the RA Helpdesk Officer can view existing subscribers, key bearers, and e-identities in The Service Portal in order to give support to the subscribers.

The RA Helpdesk Officer cannot change any information regarding subscribers, key bearers, and e-identities.

For details, please refer to *Pointsharp Secure Cloud Net iD Officer's guide.*

7 SweID · RA Report Officer role description

7.1 General

Description of the tasks that the RA Report Officer performs and what his responsibilities are in the administration of the e-identities in the RA organization.

7.2 Qualifications

The RA Report Officer must have adequate knowledge and be suitable to maintain the organization's commitment, over time.

The RA Report Officer must have sufficient training, time, and resources set aside to carry out his assignment.

A background check must be done on the person that is assigned the role.

7.3 Responsibilities and Duties

The RA Report Officer creates, views, and exports reports regarding subscribers, key bearers, and e-identities managed in The Service Portal.

For details, please refer to *Pointsharp Secure Cloud Net iD Officer's guide.*

POINTSHARP

Website
https://www.pointsharp.com

Classification:	Public
Publ. No.:	PSC-Rd22-05
Document version:	1.1
Document status:	Final
OID:	
Published:	03 Jun 2022