POINTSHARP

Service description

Pointsharp Secure Cloud Net iD

Classification:	Public
Publication No.:	PSC-Rd22-03
Document version:	1.0
Document status:	Final
Date:	11 Apr 2022

Table of Contents

1 About this document

This document gives possible and existing customers of Pointsharp Secure Cloud Net iD (PoSC Net iD) a description of how the cloud service is designed and works from a technology and security perspective. The document also describes the underlying infrastructure that is required for the service to work.

Pointsharp AB and its product catalogue is under constant development. We therefore reserve the right to make changes and improvements of the service as well as associated documentation without prior notice. Pointsharp AB undertakes to inform its customers in good time before major changes occur that affect the infrastructure and its functionality. See the customer agreement for more information.

1.1 Term dictionary

Term	Synonym	Definition
PKI	public key infrastructure	set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption

2 What is Pointsharp Secure Cloud Net iD?

PoSC Net iD provides a cloud-based service that includes Pointsharp's product catalogue. This means quick installation and start-up. Investments in expensive hardware and time-consuming operation are avoided and a security platform on a par with those used by Sweden's largest companies and organizations is obtained.

Using PoSC Net iD can be compared to a customer not building their own mobile phone network to be able to talk to customers and employees, or their own bank giro center to be able to pay suppliers. Pointsharp's new service PoSC Net iD means access to an easy-to-use cloud service that makes it possible to quickly start using digital identities with the strength that today's cyber threats require.

The previously dominant form of delivery, to build everything yourself on-premise, is outdated. For over 20 years, Pointsharp has developed and delivered important IT security to large companies, banks, authorities, health regions, and municipalities. By using PoSC Net iD, the customer gets a significantly better and stronger platform than what the customer can reasonably afford and be able to develop themselves.

PoSC Net iD is based on the globally standardized information security method public key infrastructure (PKI). PKI is a necessity to protect against identity theft and online fraud. Pointsharp is a leader in applied login security with PKI. PKI is also the information security method on which the internet's security pillars rest.

This is always included in PoSC Net iD:

- High guaranteed availability.
- Cost-effective solution. The customer only pays for actual use per user and month.
- Operation and monitoring any time of day, every day, including holidays,
- Redundant data centers in Sweden with a highest level of security.
- Scalability at the moment it is requested.
- Level of trust according to the organization's needs.

3 Service and products

The PoSC Net iD service includes all the necessary software for the service.

3.1 Service portal

User administration can be perceived as cumbersome and time-consuming. Net iD Portal is therefore used as the service portal PoSC Net iD Portal, which is the market's most flexible tool for administration and life cycle management of certificates, smart cards or other key bearers, and users. The Service portal brings together the organization's life cycle management of the users' digital identities in one and the same easy-to-use interface. Using a single reliable solution provides significantly more for the money than using several parallel solutions and it also simplifies and streamlines the work.

3.2 Clients

The Net iD Client client software is the market's most widely used PKI middleware for establishing strong multifactor authentication (MFA), based on certificates and PKI.

Net iD Client integrates smart cards and other key bearers with all types of applications and IT environments.

The customer chooses which work environment to protect and Pointsharp quickly delivers an optimal solution for the desired operating system, such as Windows, macOS, Linux, and Chrome OS. The highest possible protection is obtained when logging on to computer, domain, applications, iDP, online services, and servers. PoSC Net iD protects login to Office 365 and other cloud services. With a Citrix platform, a very fast and secure single sign-on with session resume is achieved.

- Builds on standard components and works in all common system environments.
- Platform independent; Windows, macOS, Linux, or Chrome OS.
- Support for all common smart cards and hardware tokens.
- Flexibility in choosing integration interfaces for applications.
- Configuration of customized user flows through GPO.
- Unique feature extensions give Citrix users fast single sign-on and session resume.
- Available in thin clients from Dell, Igel, Fujitsu, 10ZIG, and others.

3.3 Net iD Access

Net iD Access gives the customer full PKI-based multifactor authentication for accessing mission-critical information and applications on all types of client devices. Thanks to iOS and Android support, security is maintained also with mobile devices such as mobile phones and tablets. Users are secured with file certificates or smart cards via external card readers. Net iD Access works just as well with web applications as mobile apps.

- Access to business-critical information everywhere.
- Integrates with existing PKI infrastructure.
- Manages client applications' need for integration with card readers, cards, keys, and certificates.
- Free for download to iOS and Android.
- Also available for Windows, macOS, Linux, and Chrome OS.
- Allows derived identities.

4 Environments

4.1 Production

Each customer has access to a production environment of PoSC Net iD. This gives users access to all the features (subsystems, options, integrations, etc.) included in the agreement. In the production environment, the customer's data is processed and stored in encrypted form in the cloud service.

The production environment contains a version of PoSC Net iD that has undergone the required testing and quality assurance.

4.1.1 Temporary and customer-unique environments

In addition to the production environment, customers can need their own environments of PoSC Net iD for test of new functionality, demos, educational purposes, or for other reasons. Contact your Pointsharp sales contact for more information.

5 Service architecture

Everything is located in redundant data centers with full high availability (HA). If necessary, the number of servers is increased dynamically.

6 Service requirements

To use the service, the customer and the customer's technical environment must meet the technical requirements described in the following paragraphs.

6.1 Client, computer, and software

By client is meant the computer or mobile device which the end user connects to the service.

Name	Description
Communication	Internet connection
Operating system	At least Windows 8.1
Web browser	• Internet Explorer 11 • Edge Chromium
Software	Net iD Enterprise

6.2 Client for mobile application (Net iD Access Client)

Name	Description
Communication	Internet connection
Operating system	• iOS • Android
App	Net iD Access Client

6.3 Authentication

The service uses TLS and its own encryption channel. Client certificate is required to log in to the service.

7 Functions within the service

7.1 Issuing procedures

The service has solutions for issuing certificates according to the trust levels LoA2 and LoA3. In order to say that you issue certificates according to these levels of trust, it is required that the requirements for these trust levels are met. Customers (or RAs) can only claim LoA2 or LoA3 compliance through self assessment.

A valid registration certificate must be received, and a domain validation must be carried out. When this is done, the smart cards of the first RA officers are issued on site at the customer by staff from the service owner, according to LoA3. In order to achieve that level of trust, it is required that two people from the service owner are involved and identify the person on site before the order is sent to an external card supplier, and that another administrator from the service owner hands out the card on site to the recipient.

To issue a certificate in accordance with LoA3, the recipients must identify themselves with an approved ID document.

8 Technical and organizational security measures

PoSC Net iD is designed to meet the high security requirements set by our customers.

8.1 Physical security

PoSC Net iD is operated in modern data centers (in physically separated halls). The data centers are self-sufficient and completely independent of, for example, external power and cooling supply. This means that the facility also functions during extensive power outages or other crisis situations. Only authorized personnel who in their work need physical presence are given access to the data centers. See *PoSC Net iD Certificate Policy and Certification Practice Statement* for detailed information.

8.2 Network and communication

The physical architecture is divided in logical layers and only specific ports and IP addresses are open to ensure that data is not accessible directly via the internet. See *PoSC Net iD Certificate Policy and Certification Practice Statement* for detailed information.

8.2.1 Communication to and from PoSC Net iD

Connection to services in PoSC Net iD takes place via the internet. The connection is redundant and the capacity ("bandwidth") is gradually scaled up as demand increases. See Operation and maintenance.

8.2.2 Firewall

All services and their underlying servers are behind a physical and redundant firewall. See Operation and maintenance.

8.2.3 Encryption of traffic

All traffic to and from the service is encrypted via the HTTPS protocol and its built-in support for the encryption technology TLS (v1.2 or later, SHA256), as well as a supplementary proprietary encryption layer.

8.3 Data storage and backup

The information created and handled by the service is stored in encrypted form on database servers that are not exposed to the internet.

8.4 System accounts

System accounts and services are always created with the lowest possible permissions. If necessary, authorization is given for specific purposes, for example, access to a specific file area, access to a specific certificate, etc. Accounts are of the type group managed service account (gMSA).

8.5 Management of personal data

Pointsharp AB complies with EU legislation and Swedish law for the handling of personal data.

Access to PoSC Net iD is only only given to personnel who are checked and approved by Pointsharp. Access to the system is provided through authentication, see Authentication.

All access to information and changes to the system are logged for traceability. See *PoSC Net iD Certificate Policy and Certification Practice Statement* and Privacy Policy for detailed information.

8.6 Backup and reload of data

All parts of PoSC Net iD are backed up (OS, applications, configuration, and data).

- Backup of transaction logs and sensitive data is done every hour.
- Re-reading test is done:
  - Continuously at least once a quarter or in case of major changes.
  - With the latest backup from the production environment.
  - Always to a, for this purpose, dedicated test environment. It has no effect on availability to the customer's production environment.

8.7 Antivirus

All servers are equipped with continuously updated software for antivirus and other security protection.

8.8 Authentication

To access the service, personal client certificates are required whose private key is protected by a key bearer such as a smart card or hardware token, that is, through two-factor authentication. These are obtained when signing the service agreement.

8.9 Cookies

The service stores the user's image for login dialog as well as the ten most recently logged in users to select default users for multiple certificates and cards in cookies. The language resource is stored in the client for the service, that is, cache in Net iD Enterprise.

The cookies we use are so-called temporary session cookies which are mainly used to know if the user is authorized. They disappear when the user logs out, closes the browser, or shuts down the computer.

8.10 Traceability and logging

Logging takes place in all stages and parts of PoSC Net iD to provide the best possible traceability. The logging provides invaluable help in troubleshooting and following up on security audits.

9 Operation and maintenance

9.1 Continuous use

PoSC Net iD is operated almost exclusively on virtual servers. The few physical servers used are all redundant.

PoSC Net iD, and the services and applications operated there, are managed by a dedicated team that works exclusively with operation, monitoring, and maintenance. In addition, there are a number of experts who are members of the team for various needs such as network, Windows, SQL, etc.

The team automatically receives alarms via predefined events about, for example, status of service applications and infrastructure. For example, performance and resource utilization are monitored so that capacity can be expanded as needed.

All servers are located in at least two separate data centers to obtain so-called high availability.

9.2 Change management

Change management of environments such as servers, networks, firewalls, etc. is handled via change requests (CR) in the data center supplier's service management system. If CR templates are not used, the Service Desk can be contacted via email or by telephone. The data center supplier has a designated Change Manager for each customer. The Change Manager is responsible for ensuring that all changes are made and documented for traceability in a correct manner. The Change Manager also prioritizes between change requests.

Changes and updates of the service applications are first tested and verified in test environments before they are put into the production environment after any errors and deficiencies have been rectified.

Changes concerning the application are handled at Pointsharp through tickets.

9.3 Incident management and escalation

Errors and problems discovered by customers are usually reported as incidents which are entered into Pointsharp's incident management system Support Suite. Either they are written by the customer directly in Support Suite or by Pointsharp Support Desk after contact with the customer and a description of the problem.

Analysis is done by Pointsharp's support. The customer is kept updated on the status of the incident and sometimes via direct contact if additional information is needed.

Errors and other events that occur in PoSC Net iD's service delivery (hardware, network, applications, urgent updates, etc.), and that risk affecting customers, are usually escalated through the various business' service desks and support organizations.

9.4 Service levels

Refer to *PoSC Net iD Customer agreement*.

Website
https://www.pointsharp.com

Copyright

Disclaimer
Specifications subject to change without further notice, unless stated otherwise in agreement.

Classification:	Public
Publ. No.:	PSC-Rd22-03
Document version:	1.0
Document status:	Final
OID:	
Published:	11 Apr 2022