CIN/NIC

Care Provider Implementation Guide

Documentation for Care Providers to access MyCareNet Directly

Atos

12/06/2018

Contains all what a relying party should know of MyCareNet that isn’t business oriented? Relying parties are all applications that by itself provide services to care providers but require the services of MyCareNet to do so.

Contents

1 Revision table

Release No.	Date	Revision Description
1.0	31-05-2012	Draft
2.0	11-01-2013	Rework of 3.4.1MyCareNet authentication Adding 4.4 Update MyCareNet signing certificate
3.0	11-06-2018	Add port 9443 to URL in §6
3.1	12-06-2018	Change eHealth URL

2 Introduction

2.1 Audience

This document is intended for the developers and architects of the care providers that connect directly to MyCareNet/NIP-PIN. The care providers do not need to pass via the eHealth ESB for this type of service.

2.2 Goal of the document

This document describes how a care provider can connect to MyCareNet as a client. It is purely limited to establishing a connection; it does not include any information about the payload. For this there is another document: Service Catalogue.

2.3 Document License

[[TODO]]

3 Protocol

This section describes the technical specs of the services. It describes the transport used and the WS-* standards that are used. The last section represents the same info in WS-Policy format.

3.1 Transport

All new services use SOAP 1.1 over HTTPS as transport.

3.2 WS Addressing

Only anonymous WS-Addressing is supported. The only required header it the message id which is used for end-to-end tracking. Some services also require the “to” field, see service catalogue for information on which services.

3.3 MTOM/XOP

MTOM must be used where applicable, the policy in the WSDL indicates if MTOM is required or not. When not indicates, MTOM isn’t required or even allowed.

3.4 WS Security

WS-Security version **1.0** is used, with the following requirements.

3.4.1 MyCareNet authentication

The MyCareNet Services are all authenticated by its SSL certificate. There is no WS-Security signature in the response messages or any other additional means of authentication.

The MyCareNet responses do contain a timestamp that is protected by the SSL-tunnel and should be verified by the relaying party.

The SSL certificate is revocable via CRL. Relaying parties are advised to verify the SSL certificate based on this CRL, but it isn’t a requirement.

Some flows also use the CIN signing certificate issued by eHealth. This certificate is used to sign (part) of the message and provide some kind of practice force. These signatures are always part of the business message. See the service catalogues for which flows and the exact location of this signature and certificate.

3.4.2 Care Provider authentication

The care provider must authenticate following the eHealth SSO principal defined in the Secure Token Service HolderofKey - Cookbook available here : https://www.ehealth.fgov.be/ehealthplatform/fr/service-iam-identity-access-management

The care provider is the WSC, while MyCareNet is the WSP.

The SAMLv1.1 token that was returned by eHealth must be used with MyCareNet according to “Web Service Security: SAML Token Profile 1.0”. Because the received SAML assertion is “Holder-Of-Key” the request must also be signed with the private key corresponding to the certificate embedded in the SAML assertion.

The signature must only sign the WS-Security Timestamp (which is required), but it is allowed to sign additional parts like the body.

See authentication catalogue for the attributes that are required in the SAML assertion, it depends on the sector the care provider is part of.

3.4.3 Package authentication

Each care provider must have a package (can be itself). A package is authenticated via a username password that must be provided in the common input of each request. This username password is issued by the CIN/NIC and is often referred to as “license” since it grans the package the right to use NIP-PIN.

3.5 Resulting WS-Policy

Services have the following security policy:

```
<wsp:Policy wsu:Id="PolicyID">
    <wsp:ExactlyOne>
        <wsp:All>
            <wsaw:UsingAddressing />
            <wsoma:OptimizedMimeSerialization />
            <sp:TransportBinding>
                <wsp:Policy>
                    <sp:TransportToken>
                        <wsp:Policy>
                            <sp:HttpsToken RequireClientCertificate="false" />
                        </wsp:Policy>
                    </sp:TransportToken>
                    <sp:AlgorithmSuite>
                        <wsp:Policy>
                            <sp:Basic128 />
                        </wsp:Policy>
                    </sp:AlgorithmSuite>
                    <sp:Layout>
                        <wsp:Policy>
                            <sp:Lax />
                        </wsp:Policy>
                    </sp:Layout>
                    <sp:IncludeTimestamp />
                </wsp:Policy>
            </sp:TransportBinding>
             <sp:EndorsingSupportingTokens>
                <wsp:Policy>
                    <sp:SamlToken sp:IncludeToken="...AlwaysToRecipient">
                        <wsp:Policy>
                            <sp:WssSamlV11Token10 />
                        </wsp:Policy>
                    </sp:SamlToken>
                </wsp:Policy>
            </sp:EndorsingSupportingTokens>
            <sp:Wss10>
                <wsp:Policy>
                </wsp:Policy>
            </sp:Wss10>
        <wsp:All>
    <wsp:ExactlyOne>
</wsp:Policy>
```

4 Procedures

4.1 Apply as Package

See CIN/NIC

4.2 Apply as Care Provider

See CIN/NIC.

4.3 Update MyCarenet authentication

4.3.1 Triggers

- MyCareNet SSL certificate is about the be expired
- MyCareNet SSL private key has been compromised (exceptional)

4.3.2 Provided info

- SSL certificate + entire chain in base64 format
- Impact MyCareNet environments
- Planned due date

4.3.3 Actions

1) Optional: Evaluate risk of compromised private key
    a. If risk high: CIN/NIC revokes old SSL certificate
2) CIN/NIC orders new SSL certificate
3) CIN/NIC communicates provided into to all Care Provider
4) All Care Providers do required updates (if any) before due date
5) Atos updates new SSL certificate on due date

Risk evaluation is only applicable when SSL private key has been compromised.

4.3.4 Remaks

- Revocation will block all relaying parties that actively do verification (not standard)

4.4 Update MyCareNet signing certificate

4.4.1 Triggers

- MyCareNet signing certificate is about to expire
- MyCareNet signing key has been compromised (exceptional)

4.4.2 Provided info

- signing certificate + entire chain in base64 format
- Impact MyCareNet environments
- Planned due date

4.4.3 Actions

6) Optional: Evaluate risk of compromised private key
   a. If risk high: CIN/NIC revokes old signing certificate
7) CIN/NIC orders new signing certificate
8) CIN/NIC communicates provided info to Packages
9) Packages do required updates (if any) before due date
10) Atos updates new signing certificate on due date

Risk evaluation is only applicable when signing key has been compromised.

4.4.4 Remarks

- Revocation will block any organization implementing signature verification (which is recommended!)
- There is one signing certificate for non-production environments and one (distinct) for production environments.

4.5 Update Care Provider authentication

See eHealth (transparent for MyCareNet)

4.6 Trace message

4.6.1 Triggers

- MyCareNet accepted the request but did not return a response (should not occur, but possible)
- …

4.6.2 Requirements

- Relaying party must provide WS-Addressing message ID in every request
- Required information
  - Required: problem description with indication of expected action
  - Required: unique trace ID of request
  - MyCareNet Environment
  - MyCareNet Service
  - Date/Time
  - Care Provider info
  - Request

  - …

4.6.3 Actions

1) Package sends required information to service desk
2) Lookup of trace
3) Investigation problem
4) Response to relaying party

4.6.4 Remarks

- The more information is provided besides the unique trace ID the more efficient we can provide an answer.

5 MyCareNet Environments

5.1 Test

This environment is intended for the MyCareNet Team only. It is publicly available and may be used by relaying parties for very early (alpha) integration but there aren't any guarantees about availability or stability. Experience tells us that this changes often (up to several times a day) and is sometimes very instable (out for several days or longer).

This requires access to the eHealth *Acceptance* STS to request Sender-Voucher SAML-Tickets.

5.2 Acceptance

This environment is intended for CIN and secondly for the MyCareNet Team. This is also publicly available and can be used by relaying parties for early (beta) integration. There aren't any guarantees about availability or stability. Experience tells us that this version is less volatile (only a few release per month), rather stable and available most of the time.

This requires access to the eHealth *Acceptance* STS to request Sender-Voucher SAML-Tickets.

5.3 Pilot

This environment is intended for MyCareNet clients; including the Care Provider to perform their test. It is very stable, only fully tested versions of MyCareNet are installed here. It is available 24/7 with the releases planned after business hours.

This requires access to the eHealth *Acceptance* STS to request Sender-Voucher SAML-Tickets.

5.4 Production

This environment is intended for the MyCareNet users. It is available 24/7 and releases are planned on predefined release windows.

This requires access to the eHealth *Production* STS to request Sender-Voucher SAML-Tickets.

6 URLs

Test Service: https://dev.mycarenet.be:9443/...?wsdl

Acceptance Service: https://acc.mycarenet.be:9443/...?wsdl

Pilot Service: https://pilot.mycarenet.be:9443/...?wsdl

Production Service: https://prod.mycarenet.be:9443/...?wsdl