Generic Technical Agreements (generieke bouwblokken)

This chapter describes the generic technical agreements (in Dutch: "generieke bouwblokken") that can be used in many different specific use cases. Use cases that use these generic technical agreements refer to these elements in Volume 2a of the use case specification.

Identifying health organizations

Version	2025-07-04
Status	draft

Introduction

This techincal agreements descibes how health organizations should be identified in the context of data exchanges.

Agreements

Decision

Health organizations are identfied using URA-number (UZI-Register Abonneenummer)

Rationale

1. Conform to nation information model for health orgnizations (Zorginformatiebouwsteen Zorgaanbieder: https://zibs.nl/wiki/Zorgaanbieder-v3.6(2024NL))
2. The URA-number is issued by a public organization (CIBG)
3. The URA-number is cryptographically verifiable because it is contained in a PKI-certificate (UZI-servercertificaat, CPS: https://www.uziregister.nl/over-het-register/certificeringsbeleid/archief-certification-practice-statement)

Identifying vendor organizations

Version	2025-07-04
Status	draft

Introduction

This techincal agreements descibes how vendor organizations should be identified in the context of data exchanges.

Agreements

Decision

Vendor organizations are identfied using KvK-number (Kamer van Koophandel nummer, in English: Chamber of Commerce number)

Rationale

1. The KvK-number is issued by a public organization (KvK
2. The KvK-number is cryptographically verifiable because it is contained in a PKI-certificate (PKIoverheid-certificate, CPS: https://cps.pkioverheid.nl)

Identifying professionals

Version	2025-07-04
Status	draft

Introduction

This techincal agreements descibes how professionals should be identified in the context of data exchanges.

Agreements

Decision 1

Professionals are identfied using local employee number

Rationale

1. All professionals have a local employee number
2. A national healthcare professional number ("zorgverlener-id") is not yet available for all professionals

Decision 2

When a Dezi-number is available, that number is used for identification.

Rationale

1. A national number makes it easeier to cross-organizationally identify professionals.

Authenticating health organizations

Version	2025-07-04
Status	draft

Introduction

This technical agreement descibes how health organizations should be authenticated in the context of data exchanges.

Agreements

Decision

Health organizations are authenticated using a X509credential based on a UZI-servercertificate.

Rationale

1. UZI-servercertificate is issued by a public organization (CIBG)
2. URA-number is contained as attribute in the UZI-servercertificaat, CPS: https://www.uziregister.nl/over-het-register/certificeringsbeleid/archief-certification-practice-statement
3. The URA-number can securely be contained in a X509credential using the open source software did:x509 and X509Credential Toolkit

Authenticating vendor organisations

Version	2025-09-10
Status	draft

Jorrit Spee: This needs rework: Using PKIo is not really authenticating but merely a means of security. Action: talk to Steven about this.

Introduction

This technical agreement descibes how vendor organizations should be authenticated in the context of data exchanges.

Agreements

Decision 1

Production environments: Vendor organizations are authenticated on the network level using server- and client-authentication (mutual TLS) based on PKIoverheid-certificates.

Rationale

1. PKIoverheid-certificate is a national standard
2. All vendor organizations can obtain a PKIoverheid certificate, as long as they are subscribed in the Dutch Chamber of Commerce (KvK).
3. Vendor organizations can choose from several service suppliers to obtain a PKIoverheid-certificate
4. The PKIoverheid-certificate makes the KvK-number (see Identifying vendor organisations) cryptographically verifiable because it is contained in the PKIoverheid-certificates as attribute `RelativeDistinguishedName.organizationIdentifier` (see section 3.1.4 of CPS: https://cps.pkioverheid.nl).

Decision 2

Acceptance environments: Vendor organizations are authenticated on the network level using server- and client-authentication (mutual TLS) based on PKIoverheid-certificates or .

Rationale

1. Use a PKIoverheid-certificate if you want to be as close to a production situation as possible.

Decision 3

Test environments: Vendor organizations are authenticated on the network level using server- and client-authentication (mutual TLS) based on PKIoverheid-certificates or any public trust certificates.

Rationale

1. Use a PKIoverheid-certificate if you want to be as close to a production situation as possible.
2. In a test environment it is allowed to use any public trust certificate to save time and/or costs.

Authenticating professionals

Version	2025-07-04
Status	draft

Introduction

This technical agreement descibes how professionals should be authenticated in the context of data exchanges.

Agreements

Decision 1

Professionals are "authenticated" (it is probably better ot refer to this solution as "federating the identity of the professional") using a NutsEmployeeCredential when cross-organizational authentication by Dezi is not in place.

Rationale

1. NutsEmployeeCredential can be used now and is not dependent of other (national) initiatives

Decision 1

When cross-organizational authentication by Dezi is in place, professionals are authenticated using Dezi.

Rationale

1. t.b.d.

Localisation

to do

Addressing

to do

Authorizing incoming requests

Version	2025-07-04
Status	draft

Introduction

This technical agreement descibes how incoming requests must be authorized in the context of data exchanges.

Agreements

Decision 1

Authorization rules are technically defined using access policies written in Rego.

Rationale

1. Rego makes access policies readable for both humans and machines.

Decision 2

Parties are free to choose their own way to implement a Policy Decision Point (PDP).

Rationale

1. Open source software for implementing a PDP is available (PDP) but parties are free to implement access policies in another way.

Local explicit consent

Version	2025-07-04
Status	draft

Introduction

This technical agreements descibes the needed technical agreements for the use of local explicit consent by data holders.

Agreements

Decision 1

Data holders are free to implement local explicit consent in a way that fits them, as long as the contents of the local explicit consent can be used when authorizing incoming requests.

Rationale

1. to do

Decision 2

Local explicit consent can be specific or categoral.

Rationale

1. to do