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.

Revision #5
Created 4 July 2025 09:47:04 by Jorrit Spee
Updated 18 December 2025 10:44:04 by Jorrit Spee