

Endpoints and TLS certificates

Which endpoints you expose, to whom, and with which TLS certificate. This repeats the [recommended deployment](#) for spec v2 use cases; see there for details.

Nuts node endpoints

Your reverse proxy terminates TLS for the public endpoints.

Endpoint	Interface	Who uses it	Protection
/iam	Public (:8080)	Other parties resolving your did:web DID documents	HTTPS with a publicly trusted server certificate
/.well-known	Public (:8080)	Other parties: DID documents, OAuth2 metadata	HTTPS with a publicly trusted server certificate
/oauth2	Public (:8080)	Other Nuts nodes requesting access tokens from you	HTTPS with a publicly trusted server certificate
/statuslist	Public (:8080)	Parties checking whether credentials you issued are revoked	HTTPS with a publicly trusted server certificate
/discovery	Public (:8080)	Only if your node runs a Discovery Service server	HTTPS with a publicly trusted server certificate
/internal	Internal (:8081)	Your own applications, Nuts Admin	Never public: restrict access through network separation
/status, /status/diagnostics, /health, /metrics	Internal (:8081)	Monitoring, health checks	Restrict access through network separation
/n2n, /public, gRPC (:5555)	—	Spec v1 (did:nuts) only	Don't expose them

Your data endpoints

Protect your FHIR API (or other data API) with mutual TLS (mTLS) based on PKIoverheid certificates: both your server and the calling vendor's client authenticate with a PKIoverheid certificate. Check the use case's IG for what's allowed in test environments.

Don't mix up the certificates

Certificate	Used for
-------------	----------

UZI server certificate	Creating the care organization's X509Credential (see "Get an X509Credential from a UZI certificate")
Publicly trusted TLS certificate	The Nuts node's public endpoints
PKloverheid certificate	mTLS on your data endpoints

Revision #1
Created 2026-10-27 14:05:52 UTC by Rein Krul
Updated 2026-10-27 14:06:11 UTC by Rein Krul