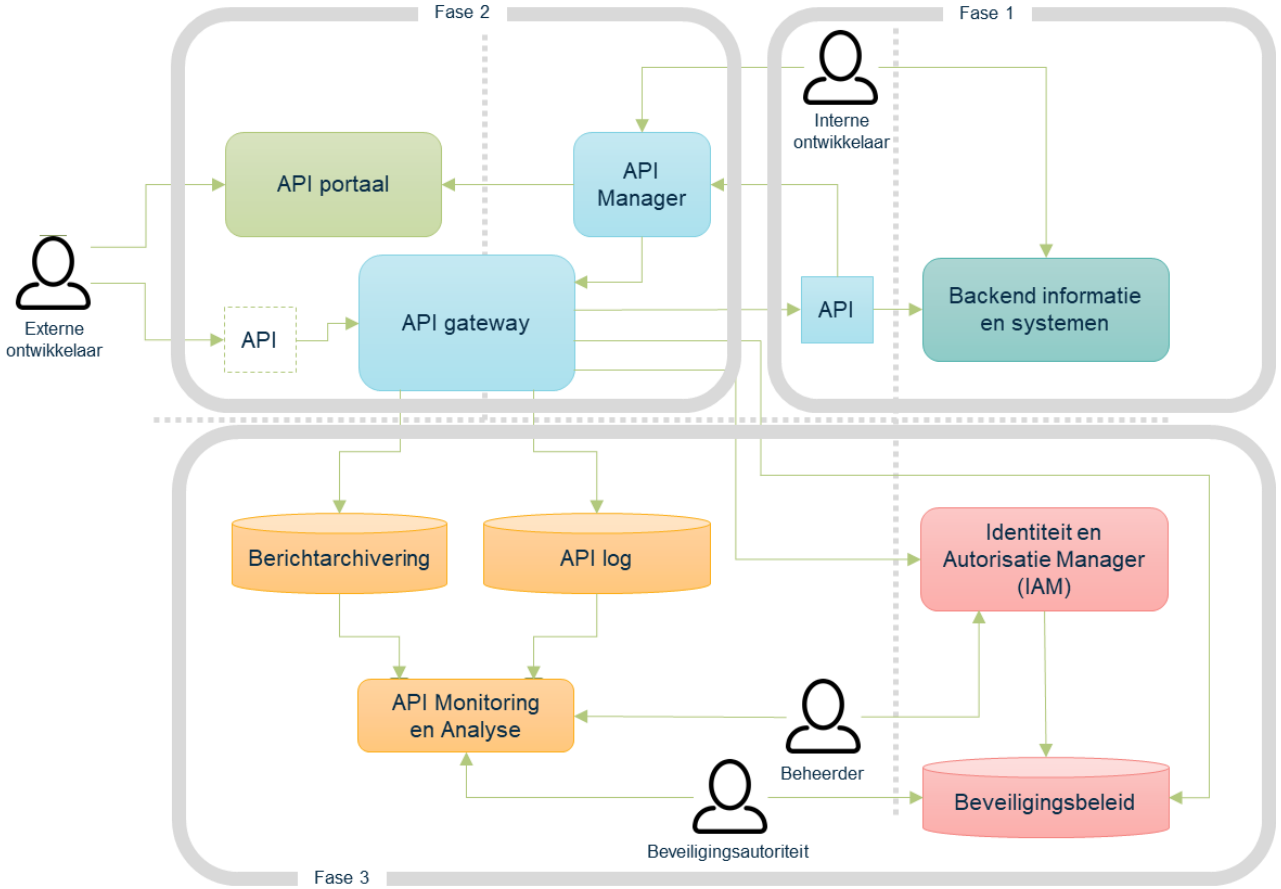
archixl

REST-API onderzoek



ing. A.J. Sloos (tony@architecit.nl)
ir. J.W. van Veen (jwvveen@archixl.nl)

Eindresultaat

edustandaard

Globale Architectuur Schets (GAS)

1. Overzicht resultaten
2. Relevante standaarden
3. Vervolgwerk

Resultaten 1/3

- Compleet overzicht van standaarden (p. 4-5)

Naam standaard	Versie	Beschrijving	Toepassing	Bron		
HTTPS	RFC2818, RFC6797	HTTP beveiligd met SSL/TLS	Beveiligde berichtuitwisseling	IETF	⊕	=
Open API Specification	3.0	Specificatiekstandaard voor API's	Specificatie/documentatie	OpenAPI Initiative	⊕	≥
TLS	1.3 (1.2 of hoger)	Translaag encryptie	Beveiliging	IETF	⊕	≥
Ades Baseline Profiles	2.x of hoger	Geavanceerde en gekwalificeerde digitale handtekeningen	Beveiliging	ETSI	⊕	=
DNSSEC	RFC 4033, RFC4034, RFC4035	Domeinnaambeveiliging	Beveiliging	IETF	⊕	=
IP V4/V6	RFC 4033, RFC4034, RFC4035	Internetprotocol versie 4 en 6	Netwerk	IETF	⊕	=
SAML	2.0	Standaard voor het uitwisselen van beveiligingsinformatie	Beveiliging	OASIS	⊕	≥
NEN-ISO/IEC 27001	NEN-ISO/IEC 27001:2013	Informatiebeveiligingsrichtlijn	Beveiliging	NEN	⊕	=
NEN-ISO/IEC 27002	NEN-ISO/IEC 27002:2013	Informatiebeveiligingsrichtlijn	Beveiliging	NEN	⊕	=
E-Portfolio NL	NEN 2035:2014 nl	Onderwijs en ontwikkeling	Gegevensdomein	NEN	⊕	=
NL LOM	1.0	Vindbaarheid van leermaterialen	Gegevensdomein	EduStandaard	⊕	=
SKOS	SKOS W3C Recommendation 18 August 2009	Linked data en begrippenlijsten	Linked-data	W3C	⊕	=
HTTP	V1.1 / RFC 7230	Hypertext transportprotocol	Berichtuitwisseling	IETF	●	=
JSON	RFC 7159	JavaScript Object Notatie standaard	Berichtuitwisseling	IETF	●	≥
JSON schema	json-schema.org (draft-07 of hoger)	Schemastandaard voor JSON structuurvalidatie	Berichtvalidatie	IETF	●	≥
JWT	RFC 7519	JSON Web Token standaard	Beveiliging	IETF	●	≥
OAuth	2.0 / RFC6749	Autorisatiestandaard	Beveiliging	IETF	●	≥
Problem Details for HTTP APIs	RFC 7807	Standaard voor retourneren foutmeldingen	Berichtuitwisseling	IETF	●	≥
URI	RFC 3986	Resource locator standaard: URI, URN, URL	Bronidentificatie	IETF	●	≥
JWS	RFC 7515	Standaard voor digitale handtekening in JSON-structuur	Beveiliging	IETF	●	~
Cross-Origin Resource Sharing	16 januari 2014	Standaard voor realiseren CORS-policy	Beveiliging	W3C	●	≥
Bearer token	RFC 6750	Standaard voor token-gebaseerde toegang	Beveiliging	IETF	●	≥
OpenID Connect	1.0	Autorisatiestandaard gebaseerd op Oauth	Beveiliging	OpenID	●	≥
PKIoverheid	zie TSP's	Digitale certificaten Nederlandse overheid	Beveiliging	Logius	●	=
OAuth 2.0 Dynamics client registration protocol	RFC 7591	Standaard voor het registeren van clients	Beveiliging	IETF	●	≥
OAuth 2.0 Token introspection	RFC 7662	Standaard voor het controleren van tokens	Beveiliging	IETF	●	≥
SAML as OAuth client grant	RFC 7522	Standaard voor SAML bearer assertion	Beveiliging	IETF	●	≥
XML schema	Second Edition	Schemastandaard voor XML structuurvalidatie	Berichtvalidatie	W3C	○	≥
JOSE	draft-ietf-jose-cookbook-08	Standaard voor tekenen en versleutelen van berichten	Beveiliging	IETF	○	~
JWA	RFC 7518	Standaard voor registeren van algoritmes voor JWS en JWE	Beveiliging	IETF	○	≥
JWE	RFC 7516	Standaard voor versleuteling in JSON-structuur	Beveiliging	IETF	○	~
Forwarded HTTP Extension	RFC 7239	Standaard voor exentsie-headers zoals X-Api-key	Berichtuitwisseling	IETF	○	=
JWK	RFC 7517	Standaard voor sleuteldata in JSON-structuur	Berichtuitwisseling	IETF	○	≥
JSON HAL	draft-kelly-json-hal-08	Standard conventie via Hypermedia in REST/JSON API's	Berichtuitwisseling	IETF	○	~
JSON-LD	1.0, 16-01-2014	Standaard voor linked-data in JSON-structuur	Linked-data	IETF	○	≥
SHA-2	ISO/IEC 10118- 3:2016	Authenticatie en integriteitscontrole	Beveiliging	ISO	○	=
SCIM	RFC 7642, 7643 en 7644	Uitwisseling identiteitsinformatie	Beveiliging	IETF	◊	=
XS09	RFC5280 en update RFC6818	Authenticatie (PKI Certificaten)	Beveiliging	IETF	◊	=
ETSI TS 119 312	v1.1.1 (2014-11)	Digitale handtekening	Beveiliging	ETSI	◊	=
GeoJSON	RFC 7946	Geografische gegevensstructuren	Geo-data	IETF	◊	≥
DCAT	Recommendation 16-01-2014	Beschrijven van datasets	Linked-data	W3C	◊	≥
OWL	OWL 2	Beschrijvingstaal semantisch web	Linked-data	W3C	◊	≥
RDF	1.1	Resource Description Framework	Linked-data	W3C	◊	=
LDP	1.0 of hoger	Linked Data Platform	Linked-data	W3C	◊	≥
CKAN (JSON API)	2.8 of hoger	Hulpmiddel voor open data websites	Open data	W3C	◊	≥
OData	4.0	Bevraging van REST APIs	Open data	OASIS	◊	=

Deze standaarden zijn relevant voor REST-API's en kunnen worden beschouwd als kandidaat voor een onderwijsstandaard.

Belang

- ⊕ Pas toe of leg uit
- ● Vereist REST-API
- ○ Gewenst REST-API
- ◊ Optioneel

Status

- ~ In ontwikkeling
- ≥ Stabiele doorontwikkeling
- = Stabiel

Resultaten 2/3

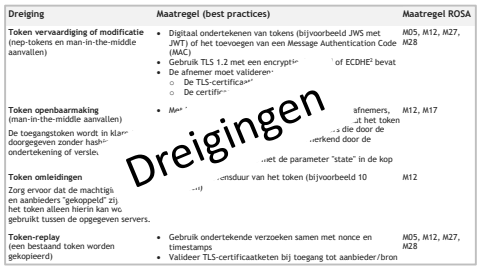
- Compleet overzicht maatregelen / dreigingen (p. 5-6, 15, 21)

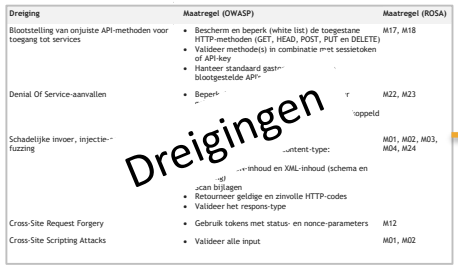
			Niveau 1			Niveau 2			Niveau 3			
#	Maatregel	Standaard/techniek	B	I	V	B	I	V	B	I	V	Categorie
M01	Berichtvalidatie	JSON schema/XML schema		●			●			●		Berichthygiëne
M02	Aangeleverde JSON altijd correct enoderen	JSON serialisatie		●			●			●		Berichthygiëne
M03	Aangeleverde XML altijd correct enoderen	XML serialisatie		●			●			●		Berichthygiëne
M04	Content- en response-type afdwingen	Validatie van content-type en accept headers		●			●			●		Berichthygiëne
M05	Bericht met digitale handtekening	JOSE/JWS/JWT		○			○			●		Encryptie en ondertekening
M06	Berichtversleuteling	JOSE/JWE/JWT			○			○			●	Encryptie en ondertekening
M07	Transportversleuteling (o.b.v. TLS tunnel)	HTTPS (HTTP niet toestaan)			●			●			●	Encryptie en ondertekening
M08	Gebruikersnaam en wachtwoord	HTTP basic-profiel			●			X			X	Gebruikerauthenticatie
M09	Multi-factor authenticatie	MFA hardtoken (RSA, Vasco)			○			●			●	Gebruikerauthenticatie
M10	Multi-factor authenticatie	MFA softtoken			○			●			X	Gebruikerauthenticatie
M11	Multi-factor authenticatie	MFA SMS			○			●			X	Gebruikerauthenticatie
M12	Token-gebaseerde authenticatie	HTTP Bearer-profiel, HTTP MAC-profiel			○			●			●	Gebruikerauthenticatie
M13	Rolgebaseerd autorisatie	OAuth2, SAML 2.0 (RBAC), JWT (rol in payload)			●			●			●	Gebruikerautorisatie
M14	Attribuut gebaseerde autorisatie	OAuth2, SAML 2.0 (ABAC), JWT (pseudo-id)			○			○			●	Gebruikerautorisatie
M15	Gedelegeerde autorisatie	OAuth2, OpenID connect, JWT			○			○			○	Gebruikerautorisatie
M16	Single sign-on (SSO)	SAML 2.0, OAuth2, OpenID connect, JWT			○			○			○	Gebruikerautorisatie
M17	Beperk toepassingsbereik van API-keys	API-key verbonden met aanroeper, domein, …			○			●			●	Gebruikerautorisatie
M18	Bescherm geprivilegieerde acties en informatie	Whitelist toegestane HTTP methoden		●			●			●		Gebruikerautorisatie
M19	Gecontroleerde cross-domain toegang	CORS-headers		○			●			●		Gebruikerautorisatie
M20	Archivering berichten	Berichtarchief		○			○			○		Governance
M21	Horizontaal schalen (clusteren)	API gateway: balancer + autoscaler	○			●			●			Governance
M22	Afknijpen # verzoeken per dag (volume)	API gateway: throttling	○			○			●			Governance
M23	Afknijpen # verzoeken per seconde (frequentie)	API gateway: rate limiting	○			●			●			Governance
M24	Gestandaardiseerde foutinformatie	RFC 7807 / Problem Details for HTTP APIs		●			●			●		Governance
M25	Voorkomen van datalekken in GET	Gevoelige data alleen in request-headers			●			●			●	Governance
M26	Voorkomen van datalekken in POST/PUT	Gevoelige data alleen in request-headers/body			●			●			●	Governance
M27	Enkelzijdige authenticatie (digitaal certificaat)	TLS 1.2 of hoger			○			○			X	Systeemauthenticatie
M28	Tweezijdige authenticatie (digitaal certificaat)	TLS 1.2 of hoger			○			●			●	Systeemauthenticatie

X niet toegstaan
○ optioneel
● verplicht

Maatregelen

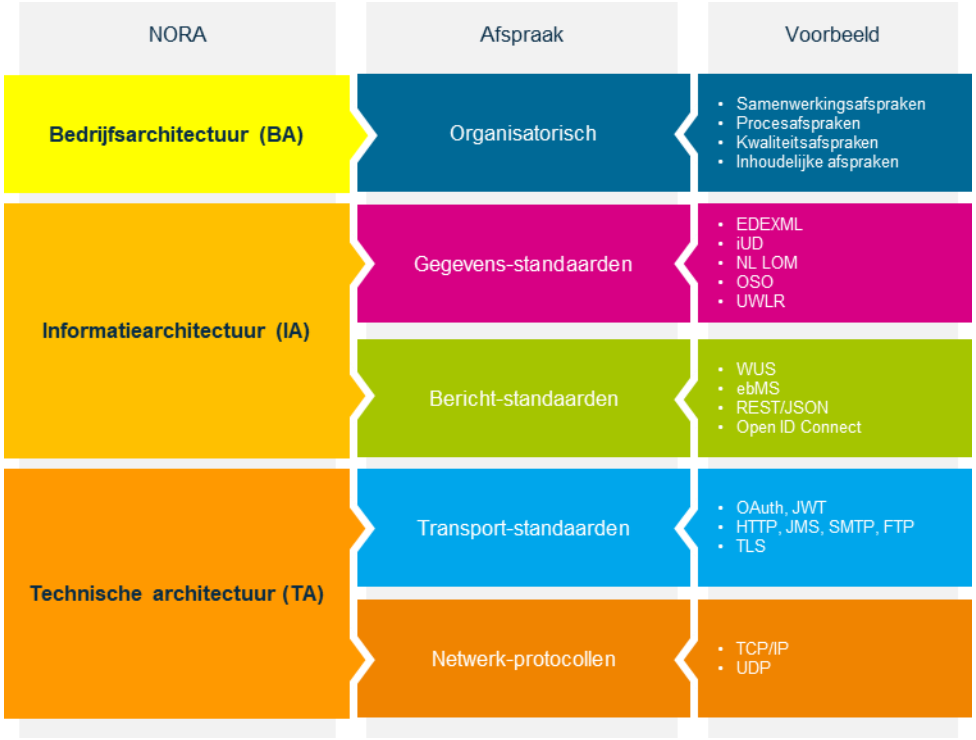
M01, M02, M03, M04, M24

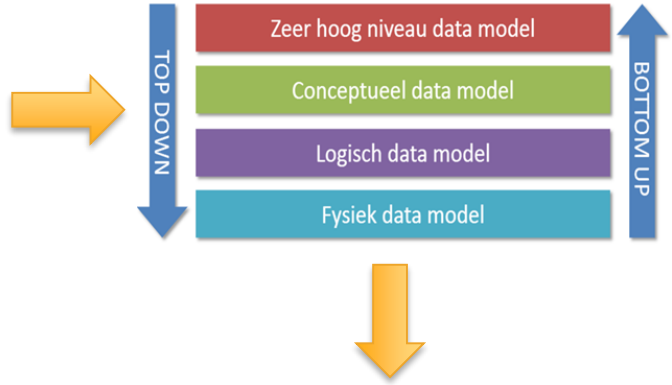




Resultaten 3/3

- Samenhang en verdieping





Een conceptueel datamodel vormt in de praktijk een goede basis voor het vinden van zogenaamde resources (zelfstandige naamwoorden) in de context van een RESTful API-ontwerp.

Samenvatting

- De “standaardiseerbaarheid” van op REST-API gebaseerde koppelvlakken is in beeld gebracht met:

  1. Een concrete lijst van relevante standaarden;
  2. Een koppeling van standaarden en maatregelen op basis van een BIV classificatie en reële dreigingen (o.a. OWASP);
  3. Een koppeling met veelvoorkomende interactiepatronen en gegevensstandaarden.

- Om berichtuitwisseling in het “veiligste spectrum” met REST API’s te kunnen realiseren en handhaven is er naast een koppelvlakstandaard ook modulaire referentiearchitectuur nodig. Modulair in de zin dat zowel “lichtere” als “zwaardere” varianten kunnen worden ondersteund.

Vervolgwerk

- Routeren achter de voordeur
  - Een verdieping waarmee REST-API's in een cloud-setting gebruikt kunnen worden voor betrouwbare en veilige berichtafhandeling, waarbij dienstaanbieders voor en/of namens de "formele partij" acteren.

- Verdieping richting 1e stap Edustandaard
  - Koppelvlakspecificatie op basis van REST-API's
  - Referentiearchitectuur gekoppeld BIV-classificatie

edustandaard

REST-API's

- Uitwerking toepassing: OSR, RIO, …