edustandaard

RFC Edukoppeling REST/SaaS-profiel aansluiten op Digikoppeling REST-profiel

Edustandaard Edukoppeling REST/SaaS-profiel	
Versie	REST/SaaS-profiel versie 1.0
Datum	December 2021
Prioriteit	Gemiddeld
Complex	Gemiddeld
Impact	Gemiddeld
Categorie	3
Gerelateerde issues	

Achtergrond

Tijdens de bijeenkomst van september 2021 zijn een aantal verschillen tussen het Digikoppeling en het Edukoppeling REST-profiel besproken. Beide maken in de basis gebruik van de API Design Rules. Het Digikoppeling REST-API profiel conformeert zich alleen aan het normatieve deel van de REST-API Design Rules[1]. Het Edukoppeling REST/SaaS-profiel is eerder opgesteld en hierin zijn ook informatieve (beveiligings)extensies[2] opgenomen. Hiermee houden we in het Edukoppeling REST/Saas-profiel een compleet overzicht van de design rules. Deze extensies waren echter in ontwikkeling en sinds het opstellen van het REST/SaaS-profiel hebben er dus ook wijzigingen plaatsgevonden. Zoals in het overzicht aangegeven (zie bijlage A) zijn API-12 en API-14 niet meer opgenomen en zijn er nieuwe principes bijgekomen (zie bijlage B). De beveiligings-extensie is nu wel binnen het Kennisplatform vastgesteld, maar zowel bij het Kennisplatform API's als Logius is men nog niet zeker of dit normatieve voorschriften moeten worden, best practices, of….

Verder gaat ook de ontwikkeling van het Digikoppeling REST profiel gewoon door. Op de roadmap van het Digikoppeling REST profiel staat nu ook het toevoegen van Signing & Encryptie (Q2-4 2022). Men laat zich hierbij o.a. inspireren door IETF[3] en Open Banking Europe[4]. We verwachten dus dat hier een mogelijke interoperable variant beschikbaar gaat komen die we ook binnen Edukoppeling zouden kunnen opnemen.

Gezien het feit dat de Kennisplatform (beveiligings)extensies gewijzigd zijn sinds we ons REST/SaaS-profiel hebben opgesteld en er een Digikoppeling REST-profiel is dat wordt doorontwikkeld vinden we het van belang dat er een nieuwe versie van het Edukoppeling REST/SaaS-profiel komt.

[1] Het is verplicht te voldoen aan alle (normatieve) eisen van de REST-API Design Rules
[2] Gepubliceerde versie API Designrules Extensions (Nederlandse API Strategie IIb) (geostandaarden.nl), Werkversie API Designrules Extensions (Nederlandse API Strategie IIb) (geonovum.github.io)
[3] HTTP Message Signatures (ietf.org)
[4] obe-json-web-signature-profile-for-open-banking.pdf (openbankingeurope.eu)

De vraag is hoe we met deze nieuwe ontwikkelingen het Edukoppeling REST/SaaS-profiel willen inrichten. We onderkennen de volgende alternatieven:

1. Het REST/SaaS-profiel laten overerven van het Digikoppeling REST profiel en de API Design Rules extensies niet meer opnemen. We schrijven dus net als Digikoppeling alleen de normatieve API Design Rules voor door naar Digikoppeling te verwijzen. Als Digikoppeling op termijn extensies gaat opnemen (bijv. Signing en Encryptie) kunnen we daar eventueel ook op aansluiten. Ons REST profiel zal (net als bij WUS) op een aantal punten afwijken, bijvoorbeeld aanvullingen voor de SaaS context, of UBV beveiligingsvoorschriften.
2. Net als bij Digikoppeling alleen normatieve voorschriften opnemen. We sluiten dan indirect aan op het Digikoppeling REST profiel, maar nemen (voor de leesbaarheid) alles op in het profiel. We verwijzen dus niet expliciet naar Digikoppeling, maar doen vrijwel hetzelfde. De documenten staan op zichzelf (maar wel met gebruik van de Kennisplatform API Design rules).
3. REST/SaaS-profiel actualiseren en de wijzigingen die in de (beveiligings)extensies hebben plaatsgevonden verwerken in het profiel. We zijn net als nu ontkoppeld van het Digikoppeling REST profiel.

Voorstel

Vanuit het beheer binnen Edustandaard heeft de 1e optie de voorkeur. De impact hiervan is beperkt omdat er minder regels zullen gelden. Net als in het huidige REST/SaaS-profiel moeten we wel bij een aantal voorschriften afwijken (bijvoorbeeld API-11: Encrypt connections using TLS following the latest NCSC guidelines, wij zullen naar UBV verwijzen). Als optie 1 niet werkbaar is (bijvoorbeeld omdat we op te veel punten willen afwijken van het Digikoppeling REST profiel) wordt optie 2 voorgesteld. Het risico hier is wel dat mogelijk op termijn ontwikkelingen meer binnen Logius/Digikoppeling zullen plaatsvinden en minder bij het Kennisplatform API's. In dat geval zouden we toch moeten terugvallen op de 1e optie. Zowel optie 1 als 2 hebben echter een beperkte impact omdat er juist een versoepeling optreedt t.o.v. van het huidige REST/SaaS-profiel. Optie 3 heeft niet de voorkeur. Deze heeft ook een grotere impact (op beheerproces en gebruik) omdat de extensies een aantal nieuwe principes bevat. Deze zullen ook eerst stuk-voor-stuk moeten worden vastgesteld door de werkgroep. Het is nu onduidelijk of en wanneer Digikoppeling deze eventueel aan het REST profiel toevoegt.

Bijlage A: Analyse verschil Edukoppeling en Digikoppeling REST-profiel

In het Edukoppeling REST/SaaS-profiel is ook bij deze informatieve principes aangegeven in hoeverre we aansluiten bij dat principe. Een aantal zijn als 'Irrelevant' gekenmerkt omdat dit bijvoorbeeld API's in een andere context betreft (bijv. open data). Bij anderen classificeren we een principe als Fully Conformant of Consistant[5]. Bij de eerdere discussie over deze principes zijn we hierop uitgekomen omdat bepaalde extensies ook toepasbaar kunnen zijn binnen het REST-profiel (Fully Conformant). Of als er wel een bepaalde mate van overlap is en de aspecten die het principe introduceert niet willen uitsluiten, maar wel een (deels) andere invulling aan geven (Consistant).

Hiervan wordt hieronder een overzicht gegeven met de onderbouwing vanuit Edustandaard (EK WG) en/of Logius.

Niveau van conformance*	Principe*	Toelichting uit EK REST Profiel	Onderbouwing keuze EK / DK
Fully Conformant	**API-16**: Documentation conforms to OAS v3.0 or newer		EK: Normatief principe is overgenomen. DK: Dit principe valt binnen de basisregel om normatieve principes te volgen. Is echter niet opgenomen in tabel (fout reeds gecorrigeerd?)
Consistent	**API-11**: Encrypt connections using TLS following the latest NCSC guidelines	LET OP: Het REST/SaaS-profiel heeft eigen voorschriften voor Transportbeveiliging (zie generieke voorschriften UBV). Deze overschrijven dit principe van de API Extensie.	EK: is onderdeel van de informatieve beveiligingsextensie. We zien overlap, maar geven er een eigen invulling aan met UBV DK: Neemt de informatieve extensie principes niet over. Heeft ook eigen DK (generieke) beveiligingsvoorschriften.
Consistent	**API-12**: Allow access to an API only if an API key is provided	LET OP: Het REST/SaaS-profiel maakt geen gebruik van API-key's en heeft hier geen voorschriften voor. Identificatie is op basis van het OIN in het certificaat dat voor de TLS-verbinding gebruikt wordt.	EK: is onderdeel van de informatieve beveiligingsextensie. We sluiten het gebruik van een API-key niet uit omdat partijen aangaven dit binnen het EK REST profiel te willen gebruiken. NB Principe is ondertussen verwijderd uit ADR Extensie lijst, er is navraag gedaan. Mogelijk dubbel ivm API-49

[5] Zie bijlage C voor toelichting van de niveaus van conformance

			DK: Neemt de informatieve extensie principes niet over.
Consistent	**API-14:** OAuth 2.0 can be used for authorisation	LET OP: Het REST/SaaS-profiel maakt geen gebruik van OAuth en heeft hiervoor geen voorschriften.	EK: is onderdeel van de informatieve beveiligingsextensie. We sluiten het gebruik van een OAuth niet uit omdat partijen aangaven dit binnen het EK REST profiel te willen gebruiken. NB Principe is ondertussen verwijderd uit ADR Extensie lijst, er is navraag gedaan, mogelijk dubbel ivm API-52 DK: Neemt de informatieve extensie principes niet over.
Fully Conformant	**API-21:** Inform users of a deprecated API actively		EK: is onderdeel van de extensie versioning. We vinden het belangrijk dat afnemers geïnformeerd worden. DK: Neemt de informatieve extensie principes niet over.
Fully Conformant	**API-22:** JSON first - APIs receive and send JSON	API's ontvangen en versturen JSON. (Bovendien worden alleen JSON-objecten toegepast, dus geen (naamloze) arrays of primitieve datatypes als "top-level" element. Het gebruik van alleen JSON-objecten als "top-level" element vergroot de uitbreidbaarheid.)	EK: is onderdeel van de extensie JSON. We vinden het belangrijk dat bij het REST profiel JSON gebruikt wordt. DK: Neemt de informatieve extensie principes niet over.
Fully Conformant	**API-23:** APIs may provide a JSON Schema		EK: is onderdeel van de extensie JSON. We vinden het belangrijk dat bij het REST profiel gevalideerd kan worden op basis van een schema.

			DK: Neemt de informatieve extensie principes niet over.
Fully Conformant	**API-24:** Support content negotiation	LET OP: Als er XML gebruikt moet worden dan is het wenselijk het WUS/SaaS-profiel te gebruiken.	EK: is onderdeel van de extensie JSON. In principe wordt voor XML WUS gebruikt, maar we sluiten de combinatie REST/XML niet uit. DK: Neemt de informatieve extensie principes niet over.
Fully Conformant	**API-25:** Check the Content-Type header settings		EK: is onderdeel van de extensie JSON. Dit is een passende aanvulling op HTTP niveau in de berichten zelf. DK: Neemt de informatieve extensie principes niet over.
Fully Conformant	**API-26:** Define field names in camelCase		EK: is onderdeel van de extensie JSON. Deze naamgevingsconventie verhoogt de interoperabiliteit en leesbaarheid. DK: Neemt de informatieve extensie principes niet over.
Fully Conformant	**API-27:** Disable pretty print		EK: is onderdeel van de extensie JSON. Hiermee is er een meer efficiënte gegevensoverdracht. DK: Neemt de informatieve extensie principes niet over.
Fully Conformant	**API-28:** Send a JSON-response without enclosing envelope		EK: is onderdeel van de extensie JSON. Een response zonder enclosing envelope wordt meer toekomst vast geacht.

			DK: Neemt de informatieve extensie principes niet over.
Fully Conformant	**API-29:** Support JSON-encoded POST, PUT, and PATCH payloads (Support JSON request body for POST and PUT operations**)		EK: is onderdeel van de extensie JSON. Dit ondersteunt extra het gebruik van JSON (media type). DK: Neemt de informatieve extensie principes niet over.
Fully Conformant	**API-30:** Use query parameters corresponding to the queryable fields	Gebruik unieke query-parameters die gelijk zijn aan de velden waarop gefilterd kan worden.	EK: is onderdeel van de extensie Filtering. DK: Neemt de informatieve extensie principes niet over.
Fully Conformant	**API-31:** Use the query parameter sorteer to sort (Use the query parameter sort to apply sorting**)		EK: is onderdeel van de extensie Sorting. DK: Neemt de informatieve extensie principes niet over.
Fully Conformant	**API-32:** Use the query parameter zoek for full-text search (Use the query parameter search for full-text search**)		EK: is onderdeel van de extensie Search. DK: Neemt de informatieve extensie principes niet over.
Fully Conformant	**API-33:** Support both * and ? wildcard characters for full-text search APIs	API's die vrije-tekst zoeken ondersteunen kunnen overweg met twee soorten wildcard karakters: * Komt overeen met nul of meer (niet-spatie) karakters ? Komt precies overeen met één (niet-spatie) karakter	EK: is onderdeel van de extensie Wildcards. DK: Neemt de informatieve extensie principes niet over.
Fully Conformant	**API-42:** Use JSON+HAL with media type application/hal+json for pagination	Voor het opnemen van hyperlinks in JSON biedt de Hypertext Application Language (HAL) een set conventies. ….	EK: is onderdeel van de extensie Pagination. DK: Neemt de informatieve extensie principes niet over.

Fully Conformant	**API-43:** Apply caching to improve performance		EK: is onderdeel van de extensie Caching. DK: Neemt de informatieve extensie principes niet over.
Fully Conformant	**API-44:** Apply rate limiting		EK: is onderdeel van de extensie Rate limiting. DK: Neemt de informatieve extensie principes niet over.
Fully Conformant	**API-45:** Provide rate limiting information		EK: is onderdeel van de extensie Rate limiting. DK: Neemt de informatieve extensie principes niet over.
Consistent	**API-49:** Use public API-keys	LET OP: Het REST/SaaS-profiel maakt geen gebruik van API-key's en heeft hier geen voorschriften voor, zie ook API-12	EK: is onderdeel van de extensie Rate limiting. DK: Neemt de informatieve extensie principes niet over.
Consistent	**API-52:** Use OAuth 2.0 for authorisation with rights delegation	LET OP: Het REST/SaaS-profiel maakt geen gebruik van OAuth en heeft hier geen voorschriften voor, zie ook API-14	EK: is onderdeel van de extensie Authorization. DK: Neemt de informatieve extensie principes niet over.

* Normatief principe in API Design rules[6]

** Principe is gewijzigd

[6] https://publicatie.centrumvoorstandaarden.nl/api/adr/

- API-58: Do not put any sensitive information in URIs when communicating over shared networks
- API-59: Use spinal-case for path segments
- API-60: Normalize characters with diacritics to their base characters for path segments
- API-61: Do not explicitly indicate that a resource is an API
- API-62: Do not use file extensions in path segments
- API-63: Do not use nonstandard abbreviations as resource names
- API-64: Do not use compound words for nested objects
- API-65: Use enumerations only for fixed sets of values that will not change
- API-66: Use UPPER_SNAKE_CASE for enumeration values
- API-67: Omit symbols and punctuation marks other than hyphens from path segments
- API-68: Use meaningful enumeration values
- API-69: Use lowerCamelCase for query parameter keys
- API-70: Provide absolute URIs for hyperlinks
- API-71: Support the HAL media type for every GET response
- API-72: Provide at least an `href` attribute for every link object
- API-73: Provide self-referencing links for all resources
- API-74: Provide navigational links pointing to GET operations only
- API-75: Only provide navigational links when there is a clear functional goal
- API-76: Treat external links as regular resource attributes

Bijlage C: Niveaus van conformance

Irrelevant	Er is geen relatie tussen het REST/SaaS-profiel en het principe van de API Design rules of Extensies. Deze mate van conformance wordt bijvoorbeeld gebruikt als we stellen dat het principe niet binnen de context van het REST/SaaS-profiel wordt gebruikt.
Consistent	Er is overlap tussen het REST/SaaS-profiel en het principe van de API Design rules of Extensies. Binnen die overlap is het REST/SaaS-profiel conform het principe, de overlap is echter niet volledig, de scope van het principe wordt niet volledig overgenomen, en het REST/SaaS-profiel heeft onderdelen die een relatie hebben met het principe maar er niet door worden gedekt. Deze mate van conformance wordt bijvoorbeeld gebruikt als we in het REST/SaaS-profiel functioneel een andere invulling geven aan het principe, maar de aanvullende aspecten die het principe introduceert niet willen uitsluiten.
Compliant	Het REST/SaaS-profiel valt volledig binnen het principe van de API Design rules of Extensies. De scope van het principe gaat wel verder dan de scope van het betreffende functionele deel van het REST/SaaS-profiel.
Conformant	Het principe van de API Design rules of Extensies geeft slechts een beperkte dekking voor wat we op dat deel met het REST/SaaS-profiel willen bereiken.
Fully conformant	Het principe van de API Design rules of Extensies dekt het geheel van wat we op dat deel met het REST/SaaS-profiel willen bereiken. De scope van het principe valt samen met de scope van het betreffende functionele deel van het REST/SaaS-profiel.
Non-conformant	Er is (functionele) overlap tussen het principe van de API Design rules of Extensies en het REST/SaaS-profiel, en binnen die overlap is het REST/SaaS-profiel niet conform het principe van de API Design rules of Extensies.