# Pravidlá publikovania služieb do multikanálového prostredia eGovernmentu

# Úvod

Dva kľúčové strategické dokumenty informatizácie (*Strategická priorita: Integrácia a orchestrácia* a *Referenčná architektúra integrovaného informačného systému verejnej správy)*, zadefinovali pre všetky agendové systémy (poskytujúce elektronické služby verejnej správy) **povinnosť publikovať** (formou web služieb) **služby pre spracovanie elektronických podaní, a zároveň všetky pomocné služby** (doťahovanie údajov, validácia vstupov) pre prípravu samotného podania **do multikanálového prostredia**. Typicky ide o služby navrhnuté pre *synchrónnu* komunikáciu. Hlavnou výhodou povinnej publikácie služieb z AIS-ov je samozrejme ich širšia dostupnosť a využiteľnosť v prostredí eGovernmentu (dostupnosť pre všetky prístupové, resp. „kontaktné“ body - aj novovznikajúce) a vzniká tak základný predpoklad pre otváranie týchto služieb (a ich rozhraní) pre využitie systémami tretích strán (mimo eGov) – tzv. koncept „OpenAPI“.

So samotnou publikáciou prichádzajú dve dôležité otázky. Prvá z nich sa sústreďuje na oblasť štandardizácie „formy“ publikovania služieb. Je namieste predpokladať, že pokiaľ budú služby publikované s využitím najnovších štandardov a metodík, a zároveň budú tieto štandardy a metodiky aplikované jednotne – zvyšuje sa dramaticky využiteľnosť daných služieb a zjednodušuje sa situácia pisateľom systémov, ktoré tieto služby konzumujú. Toto uvažovanie potvrdzujú aj štandardizačné aktivity z iných krajín EÚ (napríklad v UK publikovaná špecifikácia pre štandardizáciu API služieb <https://www.gov.uk/guidance/gds-api-technical-and-data-standards>). Druhou zaujímavou témou je centralizácia publikovania *fasády* uvedených služieb (ich rozhraní) do jedného logického bodu a možné výhody z toho vyplývajúce. Pod pojmom *fasáda* služby rozumieme rozhranie, ktoré je publikované v samostatnom (zväčša centralizovanom) bode a ktoré ďalej „smeruje“ komunikáciu na cieľovú službu. Cez *fasádu* tak komunikácia len prechádza - od konzumenta smerom na službu a späť. Predsunutie fasády a jej centralizácia prináša niekoľko výhod – napríklad je možné centrálne merať a vyhodnocovať využívanie a výkonové parametre služieb. Zároveň je možné jednotne implementovať bezpečnostné politiky a protokoly – od autentifikácie, cez autorizáciu a prideľovanie oprávnení na vyvolávanie služieb v mene občana a podnikateľa – až po dynamickú ochranu pred kyber-útokmi (napr. DDoS), atď. Centrálny bod, do ktorého sú fasády rozhraní publikované, sa z pohľadu architektúry stáva dôležitou **vstupnou bránou** (preto ďalej technický pojem „API Gateway“, resp. skrátene „API GW“) pre využívanie služieb eGovernmentu a do značnej miery sa podieľa na vnímaní celkovej kvality poskytovaných elektronických služieb verejnej správy občanmi, podnikateľmi, resp. súkromným, či neziskovým sektorom.

Načrtnuté základné oblasti (štandardizácia formy rozhraní poskytovania služieb a špecifikácia úloh a zodpovednosť centrálnej brány publikujúcej fasády rozhraní služieb) sú premietnuté aj do hlavnej štruktúry dokumentu (dve základné kapitoly). Záverečná kapitola sa venuje vysvetleniu postupu implementácie z pohľadu OVM, keďže príprava služieb do jednotného formátu môže v čase výrazne predbiehať publikáciu fasády tohto rozhrania do centrálneho prvku (API GW).

# Štandardizácia publikovania rozhraní pre elektronické služby VS

V súčasnosti dominantným spôsobom implementácie platformovo nezávislých elektronických služieb sú tzv. **web služby**, fungujúce na báze protokolu HTTP. Úlohou štandardizácie publikovania rozhraní pre elektronické služby verejnej správy sú tak rozhodnutia o technológiách, protokoloch, či štandardoch nad vrstvou základného protokolu HTTP. Pred tým, ako budú predstavené dva, v súčasnosti dominujúce prístupy v implementácii web služieb, sa prvé štandardizačné rozhodnutie dotýka priamo vrstvy základného protokolu (HTTP).:

## HTTPS ako základný protokol pre publikáciu elektronických služieb

Elektronické služby verejnej správy zvyčajne pre svoje fungovanie zbierajú od svojich používateľov citlivé údaje (či už osobné, alebo napríklad o podnikaní), preto je dôležité, aby si tieto údaje neprečítal niekto nepovolaný počas ich prenosu z internetového prehliadača používateľa smerom na server, ktorý el. službu publikuje.

***Rozhodnutie.:*** *Je nevyhnutné, aby všetky elektronické služby verejnej správy aplikovali šifrovanie už na úrovni transportnej vrstvy, čo v prípade základného protokolu znamená* ***HTTPS*** *optimálne s nadstavbou* ***HSTS*** *(HTTP Strict Transport Security).*

## REST ako jediný podporovaný prístup implementácie web služieb

V súčasnosti sú web služby implementované pomocou dvoch základných prístupov. Starším z nich je SOAP, ktorý je postavený na báze výmeny správ v štandarde XML, novším je REST v prevedení s výmenou správ v štandarde JSON. Výhodou novšieho prístupu, je širšia podpora zariadení (napríklad aplikácie v smartfónoch a tabletoch dokážu volať len REST služby) a aj jednoduchšie špecifikácie autorizačných, či autentifikačných (nadstavbových) protokolov. Nevýhodou bol ešte donedávna pretrvávajúci nedostatočný formalizmus napríklad v popise rozhraní REST služieb, no dnes už existuje otvorený štandard (OpenAPI 3.0), podporený voľne dostupnými nástrojmi (napr. Swagger).

Otázkou teda zostáva, či v rámci usmernenia pre verejnú správu podporovať len jeden (a keď tak ktorý) spôsob publikácie web služieb, prípadne oba. Simultánna podpora oboch spôsobov predražuje implementácie v eGovernmente (najmä u tzv. centrálnych prvkov) a hovorí proti nej aj fakt, že prístup REST je dnes už v podstate plnohodnotnou, ale modernejšou alternatívou k prístupu SOAP.

***Rozhodnutie.:*** *Vzhľadom na jeho vyššiu penetráciu a širšiu podporu zariadení (smartfóny a tablety), bude pre publikovanie služieb do multikanálového prostredia eGov podporovaný výhrade prístup na báze REST služieb.*

## Pre všetky dotazy a odpovede z web služieb využívať štandard Unicode

Unicode je medzinárodný štandard, ktorého cieľom je definovať kódovaciu schému schopnú reprezentovať väčšinu znakov používaných v písaných jazykoch spolu s inými symbolmi. Unicode je dominantná kódovacia schéma používaná pri internacionalizácii softvéru a viacjazyčných prostredí..

***Rozhodnutie.:*** *Povinnosť používať štandard Unicode Transformation Format (UTF-8) pre kódovanie všetkých dotazov a odpovedí v rámci služieb v celom prostredí eGov.*

## JSON ako preferovaný formát pre telá dotazov a odpovedí v rámci REST web služieb

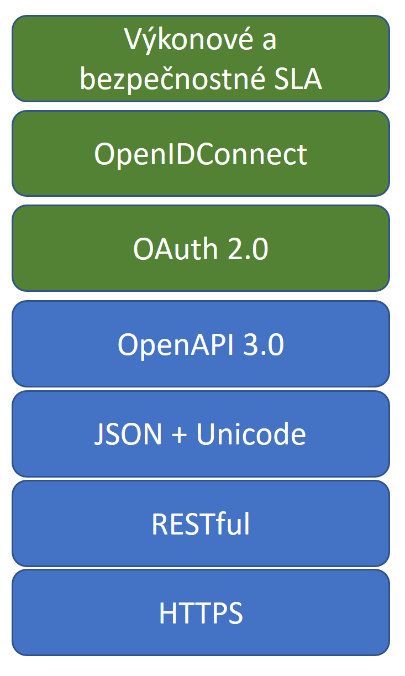
JSON (JavaScript Object Notation) je novší formát pre výmenu údajov v rámci dotazov a odpovedí web služieb, ktorý sa pre svoju jednoduchosť presadil najmä v spojení s REST web službami. Výhodou je najmä jeho jednoduchšia implementácia oproti predchádzajúcemu štandardu - XML (parsovanie údajov vo formáte JSON je jednoduchšie ako parsovanie údajov vo formáte XML). Je preto logické vyžadovať, aby nové služby boli vytvárané aplikovaním novšieho a jednoduchšieho štandardu. Zároveň však vzhľadom na to, že už existuje časť služieb, ktoré je potrebné publikovať do multikanálového prostredia eGovernmentu, a tieto služby boli písané s využitím štandardu XML pre výmenu údajov – je v takomto prípade povolené podporovať aj tento.

***Rozhodnutie.:*** *Všetky nové publikované REST služby (do multikanálového prostredia eGov) budú využívať štandard JSON ako formát pre definovanie obsahu dotazov a odpovedí. Pre publikáciu existujúcich služieb (ktoré sa nebudú v dohľadnej dobe meniť) je možné použiť štandard XML.*

Zároveň odporúčame v súvislosti s aplikáciou JSON formátu aplikovať nasledovné.:

* Vytvárať odpovede (web služieb) vo formáte JSON objektov a nie vo formáte JSON polí – polia môžu limitovať schopnosť rozhraní komunikovať metadáta o výsledkoch (operácie), resp. pridávať do budúcna do najvyššej úrovne API ďalšie atribúty.
* Zadefinovať (v dokumentácii služby) a implementovať konzistentné zoraďovanie záznamov v JSON poliach v snahe predchádzať chybám, ktoré vzniknú vďaka nepresným predpokladom zo strany klientov web služieb.

## OpenAPI 3.0 a dokumentácia rozhraní (+ REST design guidelines)



**Stack:**

WEB API GW: Performance & Security SLA (rate limiting, cachovanie, proti akým útokom je API chránené)

WEB API GW: (SAML2)OpenIDConnect (autentifikácia)

WEB API GW: (SAML2)Oauth2 (autorizácia)

(dokumentácia, lifecycle manažment – verzionovanie, breaking changes, non-breaking changes)

Služba: (WSDL)OpenAPI 3.0

Služba:(XML)JSON

Služba:(SOAP)RESTFull

Služby: HTTPS