## Popis cílového stavu SAU

V cílovém stavu bude SAU představovat **univerzální řešení zprostředkující přístup systémů a aplikací provozovaných v rezortu MZe k externím a interním autentizačním službám**. Cílem je minimalizovat dopady využití externích identitních služeb na existující systémy a aplikace a tím i náklady vynaložené na implementaci autentizačního řešení.

Poptávané řešení na jedné straně umožní naplnit požadavky platných právních předpisů EU i ČR a na straně druhé přinese náhradu stávajících již nevyhovujících autentizačních technologií a procesů. Popis cílového stavu SAU je realizován s ohledem na následující skutečnosti:

* SAU je v souladu s ustanovením § 2 písm. d) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále též „ZoKB“) **významným informačním systémem**;
* SAU je **informačním systémem veřejné správy** dle zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů (dále též „ISVS“);
* Řešení SAU zohlední bezpečnostní politiku MZe .

Nové komplexní řešení SAU je budováno s následující vizí cílového stavu:

* Funguje nové komplexní řešení pro autentizaci uživatelů přistupujících k on-line službám rezortu MZe, které je **postaveno na základě moderní solution architektury a na perspektivních technologiích, jež je možno do budoucna efektivně rozvíjet a škálovat** bez nutnosti nahrazovat dílčí či všechny komponenty SAU (minimalizace rizik zmaření investic MZe);
* **MZe je vlastníkem zdrojových kódů všech částí SAU**, které nejsou v souladu se Smlouvou klasifikovány jako standardní software a byly tedy vyvíjeny pro prostředí MZe jako součást implementace a parametrizace řešení SAU, aby nenastala situace „vendor lock-in“;
* **MZe disponuje efektivními nástroji pro naplňování požadavků** vyplývajících z platných právních předpisů a rovněž architektonických principů jako nástroje pro naplňování cílů Informační koncepce ČR;
* **Jsou na vysoké úrovni naplněny bezpečnostní standardy**;
* **Uživatelé aplikací/on-line služeb v resortu MZe mohou žádat o zřízení účtu plně elektronicky** (tj. bez nutnosti osobní návštěvy na SZIF nebo MZe – již ověřeno v rámci PoC (viz výše));
* **Uživatelé vlastnící více účtů nemusí složitě spravovat velké množství hesel;**
* **SAU je možno snadno integrovat** na okolní informační systémy (nové SeP a IdP);
* **Vyvíjené funkční komponenty řešení (EFS, IFS, konfigurace F5 BIG-IP) je možné pružně upravovat s ohledem na změny v právních předpisech**;
* **Struktura a formát přijímaných dat do SAU odpovídají obvyklým bezpečnostním a datovým standardům v oblasti autentizace** (zejména SAML 2 a WS-Federation);
* **Konfigurace navrženého řešení nesmí negativně ovlivnit stávající provozní parametry, dostupnost a výkon on-line služeb MZe**;
* Je zpracován návrh a **dokumentace metodiky SAU pro integraci nových SeP a IdP**, jsou poskytovány konzultace a součinnost dodavatelům aplikací/on-line služeb rezortu MZe v oblasti napojení na řešení SAU;
* Dodavatelem jsou zpracovány **testovací scénáře a provedeny testy nového řešení SAU** a jednotlivých implementovaných integrací;
* Je zajištěn **provoz a rozvoj řešení** od okamžiku předání Díla.

Vznik SAU je v souladu a naplňuje následující strategické dokumenty eGovernmentu ČR a strategické dokumenty MZe:

* Informační koncepce ČR, vč. Národního architektonického plánu (MAP);
* Informační koncepce MZe;
* Strategie koordinované a komplexní digitalizace České republiky 2018+ (Digitální Česko);[[1]](#footnote-1)
* Strategický rámec rozvoje veřejné správy České republiky pro období 2014-2020;[[2]](#footnote-2)
* Další strategické dokumenty ČR v oblasti eGovernmentu.

Funkční řešení SAU spolu s jasně definovanými procesy a standardy umožní v budoucnu maximálně hospodárně implementovat autentizaci a jednotné přihlašování v nově budovaných či upravovaných systémech a aplikacích. Bezpečné předávání identity sníží rizika zranitelnosti a napadnutelnosti systémů a aplikací.

SAU bude poskytovat služby jednotné identifikace (autentizace) a jednotného přístupu (single-sing-on/SSO) k on-line službám (aplikacím) v prostředí rezortu MZe.

Řešení SAU bude poskytovat sadu aplikačních služeb a konzumovat služby poskytované aplikacemi či využitou technologickou infrastrukturou. Zároveň služby SAU mohou využívat služeb externích poskytovatelů identitních služeb (IdP). Mimo to mohu být služby SAU využívány externími poskytovateli služeb (SeP) pro autentizaci klientů přistupujících ke službám SeP. Vzájemné využití služeb je znázorněno na následujícím obrázku .



**Schéma č. 2** – Globální pohled na architekturu SAU (bez modulu RIZ)

Vytvoření vztahu důvěry (tzv. Circle of Trust) mezi jednotlivými rezortními organizacemi umožní vzájemně akceptovat identity autentizované v jiných důvěryhodných systémech či aplikacích rezortu MZe a přinese řešení pro celorezortní jednotné přihlašování (SSO). Celorezortní jednotné přihlašování sníží náročnost správy identit v jednotlivých systémech či aplikacích a přispěje k zjednodušení práce a zvýšení uživatelského komfortu koncových uživatelů.

S ohledem na velkou škálu provozovaných informačních systémů v resortu MZe uvedených výše vyžaduje MZe nezbytně zajistit úpravu všech veřejně přístupných informačních systémů či portálových řešení tak, aby pro přihlášení akceptovaly externí identity spravované externími poskytovateli identitních služeb (IdP). Externí identity zahrnují identity zprostředkované NIA a JIP/KAAS (a v budoucnu z dalších autoritativních zdrojů identit), včetně zahraničních identit, identity z důvěryhodných systémů provozovaných rezortními organizacemi MZe, případně dalšími externími zdroji identit.

Aby nebylo třeba realizovat úpravy všech aplikací/on-line služeb MZe a tyto dotčené systémy byly odstíněny od detailů integrace na jednotlivé poskytovatele identitních služeb má být v prostředí MZe navrženo centrální řešení SAU, jehož úlohou je zprostředkovat přístup všech aplikací/on-line služeb MZe ke službám identitních providerů (interního i externích IdP). Řešení musí být navrženo tak, aby v průběhu integrace minimalizovalo požadavky na úpravy koncových systémů a funkční dopady do těchto systémů. SAU, by se měl dále stát centrálním autentizačním prvkem rezortu MZe a měl by zajišťovat přístup ke službám nejen externích, ale i interních poskytovatelů identit. Integrované systémy či aplikace tak budou zcela odstíněny od detailů autentizace a využití interní či externí identity pro ně bude zcela transparentní. Z pohledu integrovaného systému či aplikace bude identita poskytnuta vždy řešením SAU bez ohledu na to, zda bylo pro přístup k systému či aplikaci využito interních či externích identitních služeb.

Navržené řešení SAU musí zohledňovat skutečnost, že jednotliví poskytovatelé identitních služeb mohou poskytovat **autentizační služby na různé úrovni záruky** (Level of Assurance, LoA), tedy s odlišnou mírou spolehlivosti prostředků pro elektronickou identifikaci. Každý systém či aplikace v rezortu MZe potom může vyžadovat různou LoA použité autentizační služby. Uživateli, který se bude přihlašovat k jakémukoli systémů či aplikaci v rezortu MZe bude řešením SAU zobrazena úvodní stránka s přehledem identitních služeb, které lze využít pro přihlášení k požadovanému systému či aplikaci. Přehled identitních služeb bude obsahovat pouze ty služby, které mají LoA rovnu anebo vyšší úrovni požadovanou cílovou aplikací či on-line službou. SAU tedy bude přebírat informaci o cílovém systému či aplikaci, ke které uživatel přistupuje, o síťové lokalitě, ze které uživatel přistupuje a nabízet identitní služby platné pouze pro daný kontext (kombinaci požadované LoA a přístupové lokality/sítě). Dle zvolené identitní služby bude následně uživatel přesměrován na přihlašovací stránku příslušné identitní služby.

Klíčovým požadavkem na cílové řešení SAU je, aby bylo možné nový systém autentizace nasadit **bez nutnosti modifikovat cílové aplikace**. Řešení rovněž musí podporovat stávající model funkcionality zastupovaní, tedy model využití více uživatelských účtů (více interních identit) pro jednotlivé zastupované subjekty.

Jednou integrovaný externí poskytovatel identit, resp. externí identitní služba, bude automaticky přístupný všem systémům či aplikacím v rezortu MZe. Jednoduše tak bude moci být přidána podpora pro dalších externích (autoritativních) zdrojů identit (tzv. kvalifikovaných systémů dle ustanovení § 3 zákona č. 250/2017 Sb., o elektronické identifikaci, ve znění pozdějších předpisů) do všech požadovaných on-line služeb a aplikací rezortu MZe.

Uživatel bude mít možnost zvolit si preferovanou, pro něj nejlépe využitelnou identitní službu s požadovanou úrovní LoA. Tím dojde ke zvýšení uživatelského komfortu a zlepšení uživatelské zkušenosti při práci se systémem.

Integrované systémy a aplikace automaticky obdrží všechny potřebné informace o identitě přistupujícího uživatele, vč. úrovně LoA a tyto informace mohou, kromě vlastní identifikace uživatele, v případě potřeby využít pro předvyplnění formulářových či jiných dat v aplikaci. Na další informace mohou aplikace položit dotaz do adresářové služby MZe a v budoucnu i do Registru identit a zmocnění (RIZ) ohledně zastupování (příp. je přímo obdrží v assertions v SAML2 tokenu).

Popis jednotlivých logických komponent v architektuře SAU je popsán v následujícím přehledu.

### Externí federátor (EFS)

EFS je komponenta zprostředkovávající autentizaci klientů využitím externích anebo interních IdP. Úlohou EFS v budoucnu je nabídnout klientovi seznam použitelných IdP, dle kontextu cílové on-line služby, případně filtrovaný seznam IdP s omezením pouze na ty IdP, které jsou podporovány pro přístup k cílové on-line službě, umožnit klientovi výběr preferovaného IdP a přesměrovat klienta na službu zvoleného IdP.

EFS bude poskytovat klíčovou službu v řešení claims-based autentizace - Security Token Service (STS). STS bude odpovědná za vydávání, validaci, obnovování a zneplatňování bezpečnostních tokenů externí identity určené pro preautentizaci k IFS (PARP-IFS) a pro samotný přístup k IFS.

### Interní federátor (IFS)

IFS je komponenta zajišťující mapování externích identit na interní identity a vystavování a podepisování SAML tokenů interní identity. IFS bude podobně jako EFS poskytovat klíčovou službu v řešení claims-based autentizace - Security Token Service (STS). Služba STS bude odpovědná za vydávání, validaci, obnovování a zneplatňování bezpečnostních tokenů interní identity určené pro preautentizaci na PARP před cílovou on-line službou (PARP-app1) či pro autentizaci k samotné cílové on-line službě či aplikaci.

### F5 BIG-IP

F5 BIG-IP je zařízení provozované MZe jako páteřní prvek zprostředkovávající přístup ke všem on-line službám MZe. F5 BIG-IP je modulární zařízení zajišťující funkcionality Zařízení v prostředí MZe zastává roli preautentizační reverzní proxy (PARP), load balanceru (LB), routeru, reverzní aplikačního firewall atd. Pro účely řešení SAU jsou klíčovými moduly APM, LTM a ASM.

### Registr identit a zmocnění (RIZ)

Klient přistupující k on-line službám rezortu MZe vyžadujícím autentizaci se před využitím on-line služby musí autentizovat lokálním účtem MZe. Pokud má klient zájem pro autentizaci využít externí autentizační službu (IdP) anebo je pro přístup k on-line službě využití externí autentizační služby s příslušným LoA přímo požadováno musí být externí identita klienta nejprve zaregistrována v identitním prostoru MZe, vytvořena lokální identita MZe, související uživatelský profil (profil identity), uživatelské účty a provedeno mapování mezi externí a interní identitou. Za tímto účelem poskytuje interní federační služba MZe webovou aplikaci a webové formuláře Registru identit a zmocnění (RIZ) umožňující registraci uživatele a vytvoření uživatelského profilu (profilu identity), a to výhradně pro farmářské účty (ostatní identity jsou vytvářeny a spravovány výhradně přes IDM MZe – aktuálně Orchitech OpenIDM, verze 4.0.1, v budoucnu může být nahrazeno jinou platformou).

RIZ má 2 základní funkční komponenty:

* **Samoobslužnou webovou aplikaci/GUI rozhraní**;
* **RIZ backend** – komponenta zajišťující poskytování informací o identitách evidovaným v RIZ cílovým aplikacím/on-line službám webovými službami implementovanými v RIZ a vazbu na adresářové služby MZe (aktuálně LDAP) za účelem mapování externích a interních identit, zakládání nových účtů atp. (více viz Katalog požadavků).

Cílové řešení autentizace uživatelů v rezortu MZe zajišťující federaci externích a interních identit, mapování externích identit na interní identity a jednotné přihlášení do cílových on-line služeb, tak bude doplněno o funkční celek RIZ zajišťující evidenci a mapování externích a interních identit a v budoucnu i pověření klientů zastupovat jiné subjekty a další informace (problematika evidence zastupování v RIZ není předmětem této veřejné zakázky, SAU však musí být možno o problematiku řešení zastupování rozšířit bez nutnosti významněji předělávat či nahrazovat řešení SAU).

Předmětem této veřejné zakázky je jak návrh, implementace, nasazení a provoz SAU, tak i funkční oblasti/komponenty RIZ v části evidence a mapování externích a interních identit.

Veškeré podrobné požadavky na požadované řešení SAU jsou popsány v dokumentu „Katalog požadavků na SAU“.

1. Viz https://www.digitalnicesko.cz/. [↑](#footnote-ref-1)
2. Strategický rámec rozvoje veřejné správy České republiky pro období 2014 – 2020 je jediným národním koncepčním dokumentem v ČR, který stanovuje rozvoj veřejné správy na vymezené období. Tento dokument má v gesci Ministerstvo vnitra ČR a navazují na něj podrobné implementační plány. [↑](#footnote-ref-2)