eIDAS – eLECTRONIC IDENTITY PORTAL SOLUTION

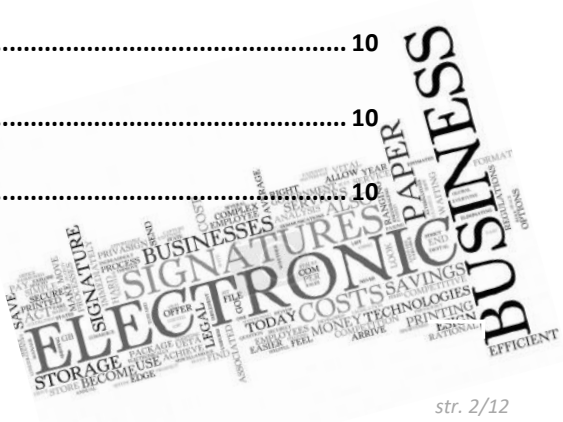
DEFINICE PRODUKTU

TS-MyeID PORTAL

Označení dokumentu		**STÁDIUM:**	**Schváleno**
Release TS-MyeID	2.0 a vyšší	**DŮVĚRNOST:**	Veřejné
ZE DNE:	1. 7. 2018	**DATUM AKTUALIZACE:**	1. 7. 2018
ZPRACOVAL / AUTOR:	JAN HAMERNIK	**VERZE DOKUMENTU:**	1.0

1 OBSAH

Obsah



2 ÚVOD

TS-MyeID PORTAL je portálové řešení, které umožňuje externím uživatelům organizace, jako jsou např. občané, pacienti, zákazníci apod. objednávat, konzumovat, platit či rušit některé vybrané služby dané organizace, a to výhradně elektronicky a za využití moderních nástrojů důvěryhodnosti v souladu s nařízením Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu, obecně označovaným jako eIDAS.

Obrázek 1 - Logo TS-MyeID PORTAL

TS-MyeID PORTAL v části určené pro veřejnost obsahuje různé druhy informací včetně možnosti řešení různých životních situací a také poskytuje integrační vazby zajišťující komunikaci s interním Informačním Systémem dané organizace v prostředí Internetu. Toto se děje zejména prostřednictvím on-line formulářů, s integrací na vnitřní systémy organizace umožňující následnou automatizovanou distribuci podání a souvisejících metadat v rámci úřadu elektronickou cestou.

Cílem je mimo jiné vytvořit takové softwarové řešení, které poskytne prostředí pro využití nové vznikající **důvěryhodné elektronické identity občanů (eID).** Toto portálové řešení využívá pro identifikaci a autorizaci uživatele (občana) systémů elektronických identit v souladu s nařízením eIDAS. Kromě podpory elektronických identit z celé EU a dalších subjektů poskytující elektronické identity, obsahuje TS-MyeID podporu dalších procesů i potřebné funkcionality, integrační nástroje a další moduly vedoucí k možnosti elektronické komunikace. Samozřejmostí je podpora elektronického podpisu a časového razítka, vč. ukládání takto vytvořených dokumentů v souladu s evropskými normami eIDAS, resp. ETSI.

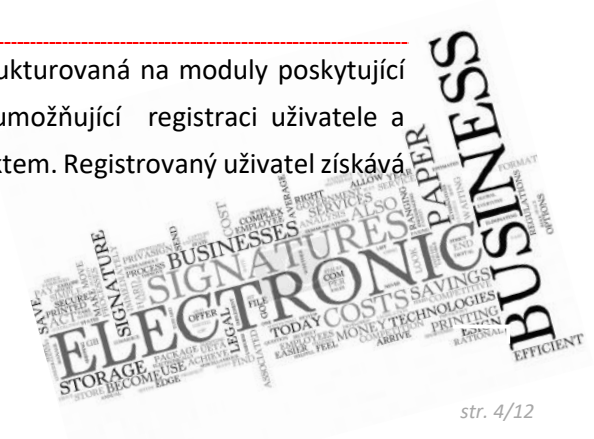
Vnitřní část řešení TS-MyeID slouží k práci interních zaměstnanců organizace, a to jak ke sdílení dat, komunikaci s externími uživateli, tak i administraci a customizaci řešení jako celku.

Kompletní popis produktu a další o informace o řešení TS-MyeID PORTAL je možné dohledat na https://www.techniserv-it.cz/produkty/ts-myeid/.

2.1 Moduly řešení TS-MyeID PORTAL

2.1.1 TS-MyeID SERVER

Komponenta tvořící základní, serverovou, část řešení, dále strukturovaná na moduly poskytující konkrétní služby. Jedná se o centrální část portálového řešení umožňující registraci uživatele a následné ověření elektronické identity poskytované externím subjektem. Registrovaný uživatel získává přístup do svého účtu.



2.2 Popis modulů částí TS-MyeID SERVER

2.2.1 Základní modul řešení (TS-MyeID/BASE)

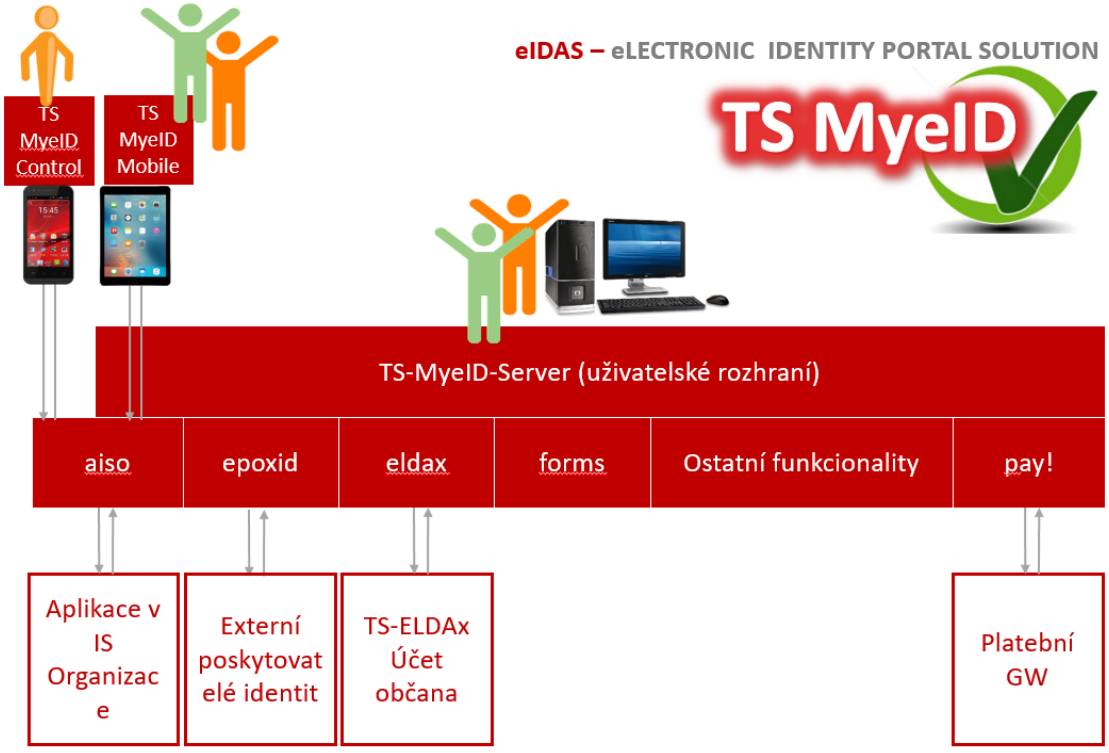
Jedná se o základní modul celého řešení, bez kterého řešení není možné implementovat, který se následně doplňuje dalšími moduly a komponentami.

TS-MyeID/BASE kromě samotného rozhraní a funckionalit portálu určených pro externího uživatele, možnosti registrace, obsahuje i management nástroje pro správu celého řešení prostřednictvím administrátora nebo pověřeného interního uživatele.

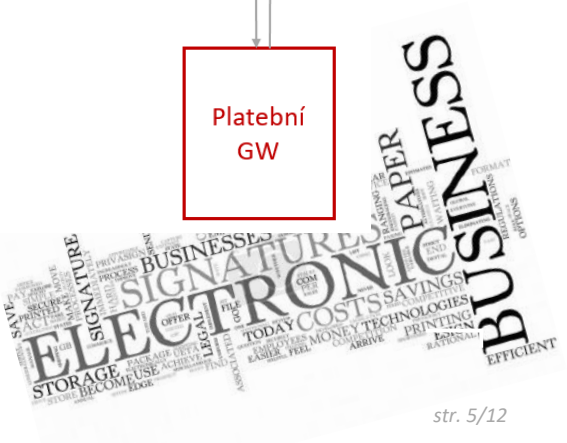
TS-MyeID/BASE obsahuje možnost konfigurace celého portálu, zveřejňování informací, součástí jsou i nástroje CMS pro správu obsahu.

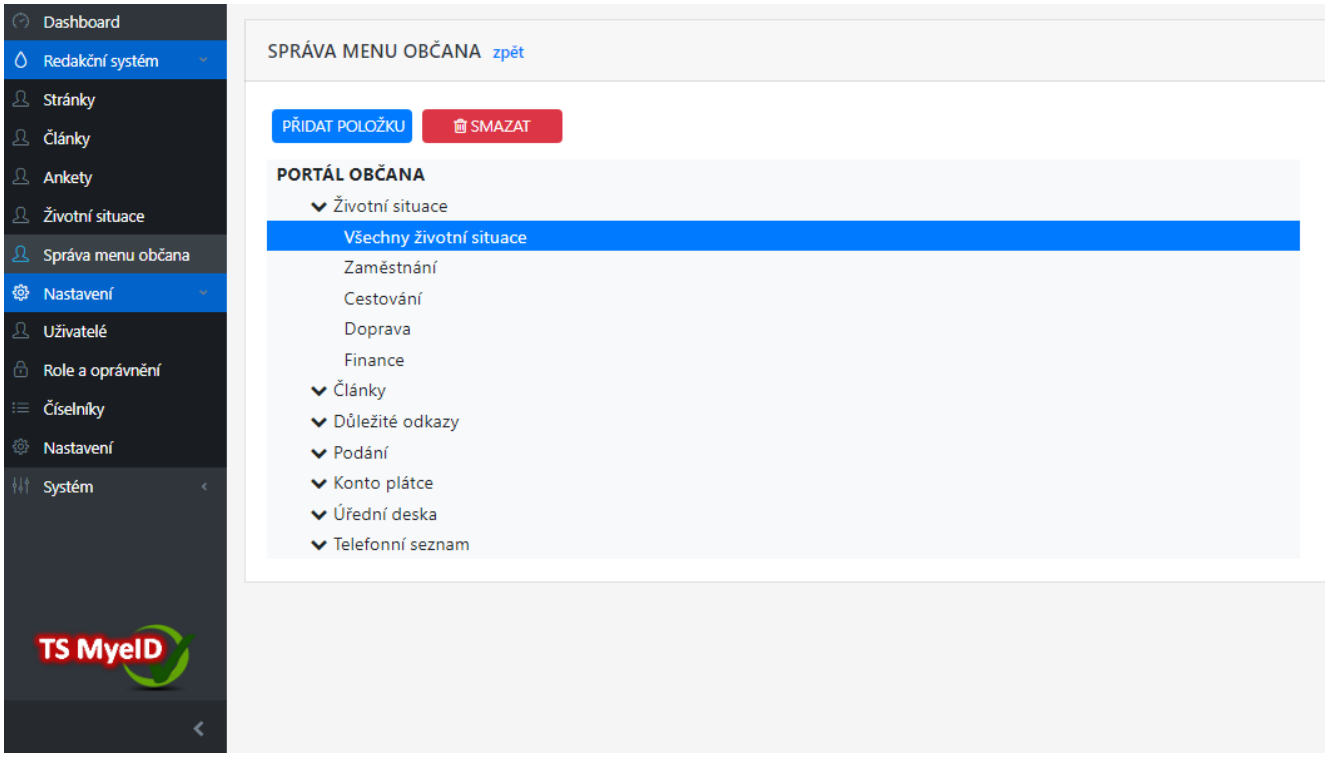
Dostupné jsou funkce jako notifikace, Osobní účet Uživatele s profilem uživatele, a plno komponent pro zobrazení důležitých informací jako je např. telefonní seznam, kalendář, možnost objednávání přes vyvolávací systém apod. (podmíněno rozhraním TS-MyeID/aiso), rozcestník životních situací, plánovač pravidelných úloh, správa menu apod.

Součástí tohoto modulu jsou i interní globální funkcionality prostupující napříč ostatními moduly zajišťující soulad s legislativou a nařízením GDPR, bezpečností nástroje, logování událostí, notifikace, apod. Součástí je také standardní integrační rozhraní celého řešení, sloužící pro integraci ostatních externích aplikací k TS-MyeID.



eIDAS – eLECTRONIC IDENTITY PORTAL SOLUTION





Obrázek 2 - Ukázka interní části portálu

2.2.2 Možnost plateb přímo z portálu TS-MyeID/pay!

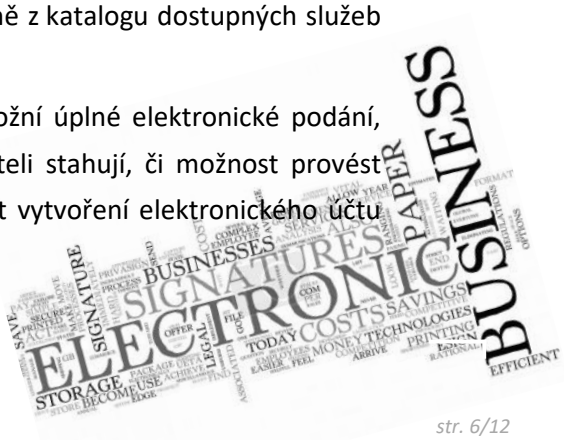
Kromě možností objednávání služeb a řešení životních situací je také díky modulu TSMyeID/pay! Možné provádět za platby přímo z prostředí portálu. TSMyeID/pay! obsahuje integrační vazby na standardní platební brány, jako je například global payments nebo Go pay.

2.2.3 Služby a Formuláře (TS-MyeID/Forms)

Řešení je standardně doplněno komponentou zajišťující potřebné formulářové služby. Implicitně TS-MyeID obsahuje řešen InQ Forms, případně je možné integrovat na formulářový server, např. společnosti SW 602. Potřebné rozhraní a služby pro komunikaci se SW 602 již TS-MyeID obsahuje.

Uživatel může prostřednictvím portálu komunikovat s organizací pomocí formulářů životních situací, přistupovat ke kontaktním údajům v dynamickém telefonním seznamu, či využívat služeb notifikací, ve které si bude moci nastavit možnost upozornění např. na exspiraci svých dokladů, nutnou prohlídku, nebo kontrolovat seznam konzumovaných služeb, případně z katalogu dostupných služeb objednat a zaplatit novou službu.

Při vhodné integraci na interní IS organizace TS-MyeID umožní úplné elektronické podání, objednání, získání přehledu o poplatcích, které se k danému uživateli stahují, či možnost provést úhradu poplatku přímo prostřednictvím portálu, případně i možnost vytvoření elektronického účtu



uživatele vč. možnosti vlastní elektronické důvěryhodné složky, kde lze důvěryhodně uchovávat jeho elektronické dokumenty.

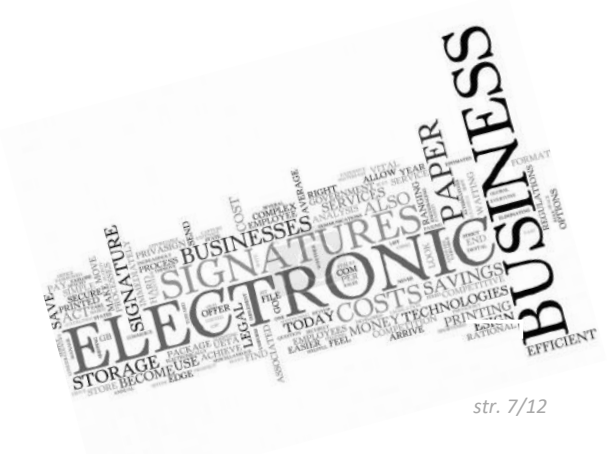
TS-MyeID umožňuje odeslat vyplněné formuláře ve formátu PDF/A se všemi metadaty, a to buď přes systém datových schránek (ISDS), popřípadě pomocí podepsaného e-mailu. Součástí podání, tedy odeslané datové zprávy či podepsaného e-mailu, jsou kromě formuláře ve formátu PDF/A i data z formuláře ve struktuře XML dokumentu, která je možno vytěžit a využít pro další zpracování v organizaci.

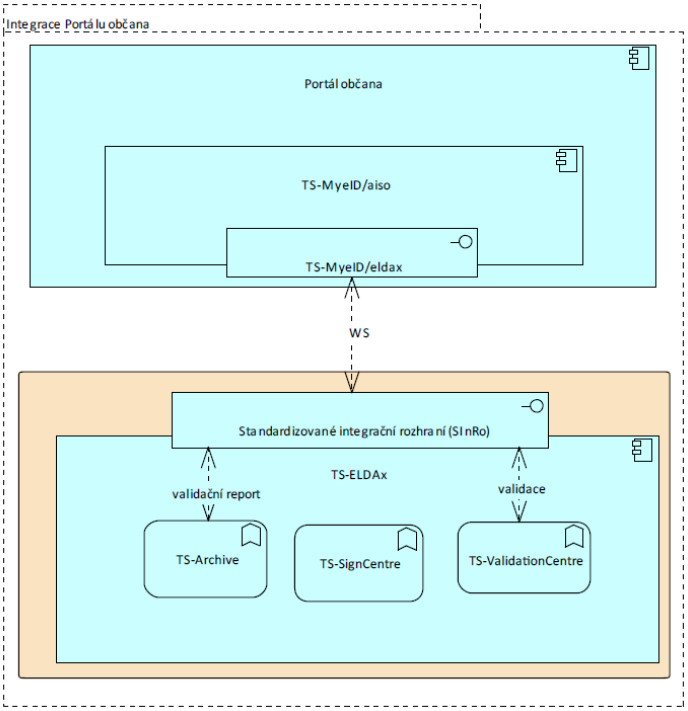
V rámci řešení je podporován PDF/A archivní formát dle standardu ISO a ETSI norem EU, tento formát je využíván jako výstupní formát formulářů. Součástí řešení je možno využívat pro validaci formuláře elektronické podpisy, případně i vícenásobné elektronické podepisování více osobami. Pokud je ověření uživatele na dostatečné úrovni nebo pokud podání obsahuje kvalifikovaný platný elektronický podpis, může podání proběhnout zcela automatizovaně až po založení v příslušném interním systému organizace. Dostatečnou úrovní je myšleno ověření přes ISDS nebo prostřednictvím validovaného účtu MojeID, případně pomocí eObčanky, případně jiného zvoleného kvalifikovaného poskytovatele eIdentit.

Samozřejmostí je možnost podpory elektronického podpisu a časového razítka, vč. ukládání takto vytvořených dokumentů v souladu s evropskými normami eIDAS, resp. ETSI.

2.2.4 Integrace na interní systémy organizace (TS-MyeID/aiso).

Rozhraní na ostatní systémy jsou zapouzdřeny v komponentě TS-MyeID/aiso, která obsahuje konektory na velké množství interních systémy organizace, jako jsou NIS, agendové informační systémy či spisové služby, včetně podpory NSeSSS. Předání interní částí IS a další zpracování dat např. z formuláře a jeho příloh systémem je standardně provedena antivirová kontrola. V systému je vyčleněna pro tyto účely karanténní zóna, do které jsou umísťovány nově příchozí formuláře i s přílohami. Tyto formuláře jsou postupně kontrolovány pomocí antiviru a v případě úspěchu postoupeny k dalšímu zpracování. V případě detekce viru nebo jiného škodlivého kódu je vytvořen incident pro správce systému, kteří je postoupen k řešení.





Obrázek 3 - Ukázka integrace na TS-ELDAx

Kromě standardní komunikace prostřednictvím webových služeb TS-MyeID/aiso podporuje komunikaci prostřednictvím některých specializovaných protokolů, jako je DASTA, HL7 apod.

Mimo klasické softwarové integrace modul TS-MyeID/aiso podporuje rozhraní na vyvolávací systémy, kde je možné se objednat přímo z portálu na konkrétní termín.

2.2.5 TS-MyeID/eldax

Pomocí tohoto samostatného modulu TS-MyeID/eldax je možné zajistit uživateli jeho osobní důvěryhodnou složku, kde je možné uchovávat elektronické dokumenty tak, aby byla zaručena jejich důvěryhodnost. Základem důvěryhodné složky je řešení TS-ELDAx (www.ELDAX.cz), které lze pořídit v rámci TS-MyeID POARTAL.

2.2.6 TS-MyeID/epoxid

TS-MyeID podporuje prostřednictvím modulu TS-MyeID/epoxid celou řadu možností přihlášení do portálu. Obsahuje možnost využití jak *interních* identit, spravovaných prostřednictvím portálu, tak zejména *externích* elektronických identit spravovaných pomocí externích poskytovatelů identit.

TSMyeid/epoxid podporuje například autorizaci pomocí systému ISDS, disponuje konektorem na Národní Identitní Autoritu (NIA) nebo podporuje poskytovatele MojeID.

MojeID je specifické a velmi často používané v prostředí českého internetu a nabízí poskytovatelům služeb další výhody oproti standardnímu OpenID, například rozšířenou sadu osobních údajů v identitách a jejich předávání, více přihlašovacích metod s možností požadovat určitou úroveň autentizace apod.

Příklad procesu přihlášení pomocí MojeID

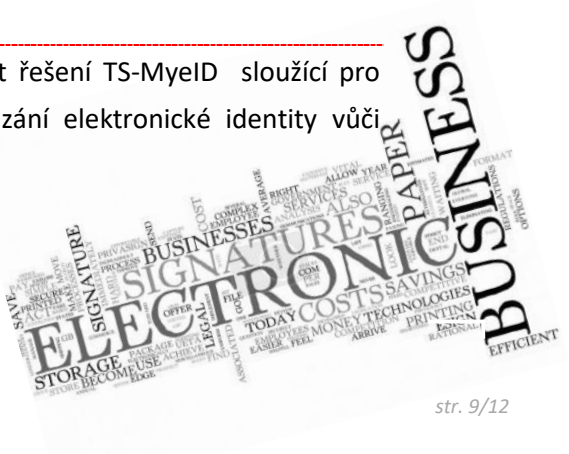
a. Ustanovení asociace – dohodnutí sdíleného tajemství, pomocí kterého se budou ověřovat zprávy od poskytovatele OpenID.
b. Žádost o přihlášení přes MojeID – uživatel klikne na tlačítko *Přihlásit přes MojeID*.
c. Iniciace – v rámci iniciace se získají metadata o poskytovateli OpenID.
d. Žádost o ověření identity – systém sestaví žádost o ověření identity a tu nepřímo skrze přesměrování uživatelova prohlížeče odešle na koncový bod poskytovatele OpenID, kde se uživatel autentizuje.
e. Provedení autentizace – uživatel se na přihlašovací stránce MojeID přihlásí pomocí některé z přihlašovacích metod a tím je jeho identita ověřena. V současnosti je podporováno heslo, digitální certifikát a jednorázové heslo.
f. Odpověď s výsledkem ověření identity – uživatel portálu je přesměrován zpět na stránky portálu a přes uživatelův prohlížeč je mu předána odpověď s výsledkem ověření identity.
g. Ověření odpovědi – každá zpráva, kterou systém obdrží od poskytovatele OpenID nepřímo přes uživatelův prohlížeč musí být ověřena, zda opravdu pochází od poskytovatele OpenID a nebyla změněna. To se udělá pomocí asociace, viz bod a.
h. Zpracování odpovědi – na základě toho, zda se jedná o úspěšné či neúspěšné přihlášení, portál reaguje přesměrováním na úvodní stranu v režimu přihlášeného uživatele nebo zobrazením zprávy o neúspěšném přihlášení a výzvy na opakování procesu.

Modul TS-MyeID/epoxid je koncipován a z pohledu architektury a způsobů využití jako zcela samostatná komponenta řešení a kromě implementace v rámci řešení TS-MyeID umožňuje samostatnou implementaci v rámci jakéhokoliv jiného portálového řešení, kde poskytuje výše popsané funkcionality.

2.3 Mobilní část (Externí části) TS-MyeID PORTAL

2.3.1 TS-MyeID/mobile

Komponenta mobilní aplikace s nativní vazbou na centrální část řešení TS-MyeID sloužící pro využití eID v prostředí mobilních zařízení. Primárně slouží k prokázání elektronické identity vůči



kontrolním orgánům a to včetně možnosti ověření konzumovaných služeb daným občanem vůči kontrolnímu orgánu.

Z této aplikace je také možné přistupovat důvěryhodné elektronické složce účtu občana.

2.3.2 TS-MyeID/control

Komponenta mobilní aplikace umožňuje kontrolu stavu konzumovaných služeb občanem navázaných na elektronickou identitu občana kontrolním orgánům za využití mobilních zařízení přímo v terénu.

2.4 Technologie

Technologicky je řešením webová aplikace postavená na konceptu MVC (Model-view-controller). Tato architektura odděluje datový model, aplikační (řídící) logiku a uživatelské rozhraní. Z infrastrukturního hlediska je možné aplikaci provozovat na různých typech serverových farem.

Technicky je řešení vyvinuté za pomocí ABP Frameworku (https://aspnetboilerplate.com), což je Framework postavený na .NET Core. Pro objektově relační mapování je využit Entity Framework. Pro vývoj Front-End je využito technologií, vue.js, jquery a webpack.

2.5 Architektura

Produkt TS-MyeID je postaven na SOA architektuře, tedy i vazby na externí systémy jsou realizovány pomocí webových služeb. Rozhraní využívá standardy a doporučení W3C. Způsoby zabezpečení či procesu autentizace se mohou lišit v závislosti na konkrétní integrační vazbě. Preferovaným způsobem zabezpečení je využívání standardu WS-Security a komunikačního protokolu HTTPS.

2.6 Způsoby pořízení

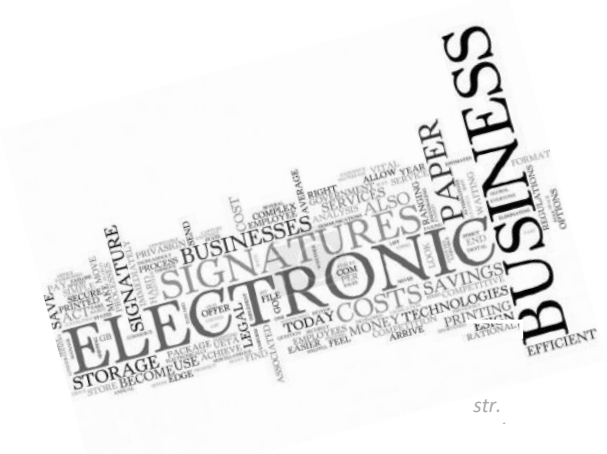
SW řešení jako celek je možné poskytovat jako služba v cloudu, nebo formou pořízení licence do majetku organizace

2.7 Licencování

Základem je pořízení licence TS-MyeID, která obsahuje základní funkcionality řešení a následně lze tuto základní licenci konfigurovat (přidávat/odstraňovat) další moduly. Základní licence je umožňuje instalaci do produkčního, provozního a testovacího prostředí.

Licence TS-MyeID PORTAL obsahuje tyto moduly s poskytující následující služby a funkcionality. (Detailní popis služeb lze je obsažen v katalogu funkcionalit)

	Moduly TS-MyeID	Popis	KOMPONENTA
1	**TS-MyeID/BASE**	Základní Framework. Obsahuje hlavní procesy pro registraci, ověření vč. podpůrných procesů a služeb, workflow na souhlas se zpracováním osobních dat a údajů, Content management systém pro správu webového obsahu a administraci.	SERVER
2	**TS-MyeID/pay!**	Modul pro realizace plateb s integrací platební Gateway.	SERVER
3	**TS-MyeID/form**	Formulářové řešení, vč. automatického předvyplnění údajů o občanovi.	SERVER
4	**TS-MyeID/eldax**	Rozhraní pro komunikaci s důvěryhodným úložištěm pro vytváření vlastních důvěryhodných složek občana sloužící k ukládání elektronických dokumentů.	SERVER
5	**TS-MyeID/epoxid**	Integrační rozhraní na externí poskytovatele elektronických identit vč. NIA.	SERVER
6	**TS-MyeID/aiso**	Rozhraní pro komunikaci s interními aplikacemi IS organizace. Obsahuje sadu konektorů na spisové služby (podpora NSESSS), vybrané ekonomické systémy atd. Konektory jsou postupně doplňovány s ohledem na rozvoj TS-MyeID.	SERVER
7	**TS-MyeID/mobile**	Mobilní zařízení umožňující přístup k centrální části a prokazování oprávnění konzumace služeb vůči kontrole za použití modulu TS-MyeID/control.	Mobilní app
8	**TS-MyeID/control**	Mobilní aplikace zajišťující přístup k centrální části a umožňující kontrolu.	Mobilní app



3 SOUVISEJÍCÍ DOKUMENTY

	Název dokumentu	Popis
1	**Licenční podmínky TS-MyeID PORTAL**	*Konkrétní licenční podmínky a způsob použití*
2	**Konfigurátor, Kalkulátor a katalog funkvionalit TS-MyeID PORTAL**	Soubor na vytváření konfigurací a základních cenových kalkulací