**POŽADAVKY**

Dodavatel vypracuje detailní specifikaci legislativních, funkčních (i ostatních funkčních), technických a bezpečnostních požadavků řešení eSSL na úrovni Solution architektury řešení.
Požadavky budou rozděleny do následujících kategorii:
1. Požadavky legislativy,
2. Funkční požadavky,
3. Ostatní funkční požadavky (nefunkční požadavky),
4. Bezpečnostní požadavky,
5. Požadavky na provoz systémů.

**1. Požadavky legislativy**
Jedná se o vymezení legislativních norem, které – přímo či nepřímo – definují požadavky na cílové řešení eSSL. Jde o právní předpisy, normy a vnitřní řídící dokument FS ČR vztahující se k problematice spisové služby.

**2. Funkční požadavky**
Funkční požadavky představují požadavky na funkcionality systému, které doplňují procesní rozsah oblasti eSSL:
- Požadavky na příjem a označování dokumentů a spisů,
- Požadavky na podatelny/výpravny,
- Požadavky na obecné postupy předcházející zpracování podání,
- Požadavky na evidenci dokumentů,
- Požadavky na rozdělování a oběh dokumentů,
- Požadavky na vyřizování dokumentů,
- Požadavky na vyhotovování dokumentů,
- Požadavky na podepisování dokumentů,
- Požadavky na odesílání dokumentů,
- Požadavky na jmenný rejstřík,
- Požadavky na spisovnu
- Požadavky na spisovou rozluku,
- Požadavky na konverzi dokumentů,
- Požadavky na historii a transakční protokol,
- Požadavky na správu spisu,
- Požadavky na vyhledávání,
- Požadavky na administraci,
- Požadavky na skartaci,

**3. Ostatní funkční požadavky (nefunkční požadavky)**
Jedná se o kvantitativní a technické požadavky na funkcionality, vyplývající přímo z procesů oblasti eSSL:
- Kvantitativní a kvalitativní požadavky,
- Požadavky na správu číselníků,
- Požadavky na reporting a výkaznictví,
- Technické a bezpečnostní požadavky,
- Požadavky na implementaci,
- Požadavky na migrace a převod dat,
- Požadavky na integrace,
- Požadavky na testování,
- Požadavky na dostupnost a odezvy systému,
- Požadavky na školení,
- Požadavky na řízení výstupů, autentizace, autorizace a oprávnění,
- Požadavky na architekturu,
- Požadavky na spolehlivost,
- Požadavky na správu životního cyklu aplikací,
- Požadavky na dokumentaci systému,
- Požadavky na ochranu osobních údajů dle GDPR.

**4. Požadavky na bezpečnost**
Z pohledu bezpečnosti je eSSL kategorizován následovně:
1. eSSL je v souladu s ustanovením § 2 písm. b) ZoKB významným informačním systémem,
2. eSSL je IS veřejné správy dle zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů), ve znění pozdějších předpisů,
3. eSSL spadá do působnosti bezpečnostní dokumentace FS ČR,
4. Prostřednictvím eSSL bude docházet ke zpracování a významné koncentraci osobních údajů pro vysoký počet subjektů údajů. Z pohledu dopadu na práva subjektů údajů se z pohledu obecného nařízení GDPR jedná o kritický stupeň dopadu.

S ohledem na kritický charakter aktiva eSSL přijala FS ČR vhodná technická organizační opatření, a to v souladu s principy „PROTECTION BY DESIGN“[1] již v rámci přípravné (předimplementační) fáze projektu. V souladu s bodem 1.4 přílohy č. 5 VoKB obsahuje bezpečnostní dokumentace FS ČR pravidla řízení Dodavatelů, přičemž FS ČR tímto stanoví dále uvedené požadavky na úroveň služeb Dodavatele a způsob a úroveň realizace bezpečnostních opatření.
Dodavatel v rámci detailní specifikace podrobně analyzuje charakter aktiva eSSL s ohledem na výše uvedenou bezpečnostní kategorizaci eSSL, identifikuje hlavní bezpečnostní rizika, připraví návrh zabezpečení řešení eSSL a realizuje dále popsaná bezpečnostní opatření (technická a organizační).

**5. Požadavky na provoz systému**
Úkolem Dodavatele Přípravy eSSL bude vypracovat minimální požadavky na zajištění provozu, a to především na
- Expertní činnosti monitoringu,
- Řízení a správy systému eSSL,
- Služby uživatelské podpory,
- Služby správy a monitoringu prostředí.

Návrh specifikace musí být sestaven tak, aby byla zachována technologická neutralita, tj. nepředjímal použití konkrétních platforem, prvků a produktů a nevylučoval a nezvýhodňoval nedůvodně žádného z potencionálních zájemců o veřejnou zakázku na realizaci řešení.

[1] Protection by design je princip, jenž počítá se zabezpečením aktiva již od počátku návrhu praktického řešení, tj. preventivně a nikoliv reaktivně (ex-post), až dojde k realizaci bezpečnostního incidentu.