DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

Export z Národní architektury eGovernmentu ČR

Obsah

Architektonický vzor pro komunikaci informačních systémů v krizovém stavu

Veškeré popsané procesy a pravidla v tomto architektonickém vzoru (dále také jako „Vzor“) jsou v souladu se zákonem č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (dále také jako „Krizový zákon“) ve znění od 1.1.2024. Ostatní zákony, pravidla a procesy jsou podřízeny či upraveny pro potřebu zvládnutí krizového stavu.

Dle definice je **krizovou situací škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy, a také havárie, které ohrožují život, zdraví, majetek nebo životní prostředí a vyžadují provedení záchranných a likvidačních prací, narušení kritické infrastruktury nebo jiné nebezpečí, při nichž je vyhlášen stav nebezpečí, nouzový stav nebo stav ohrožení státu** (dále také jako jen „krizový stav“).

Na krizový stav se tedy nesmí čekat, ale je potřeba se na něj aktivně připravovat, a to i v oblasti propojení informačních systémů a rozhodováním nad daty, která spravují. Povinnosti jednotlivých subjektů v oblasti příprav stanovuje Krizový zákon.

Český eGovernment, jeho systémy a služby, je stavěn na **bezproblémový provoz v nekrizovém stavu**. Dokáže ustát i menší krizové stavy jako například zvýšené poptávky po digitálních službách při zavřených pobočkách veřejné správy, ale nemůže být dimenzován pro velké krizové stavy. Jednalo by se o nepřiměřené výdaje na výstavbu i provoz takového řešení, protože je z logiky věci celoplošné.

Pro zajištění propojení informačních systémů v krizovém stavu je tedy nutné fungovat ve spolupráci se systémy a službami eGovernmentu specificky a k popisu této specifičnosti slouží tento Vzor.

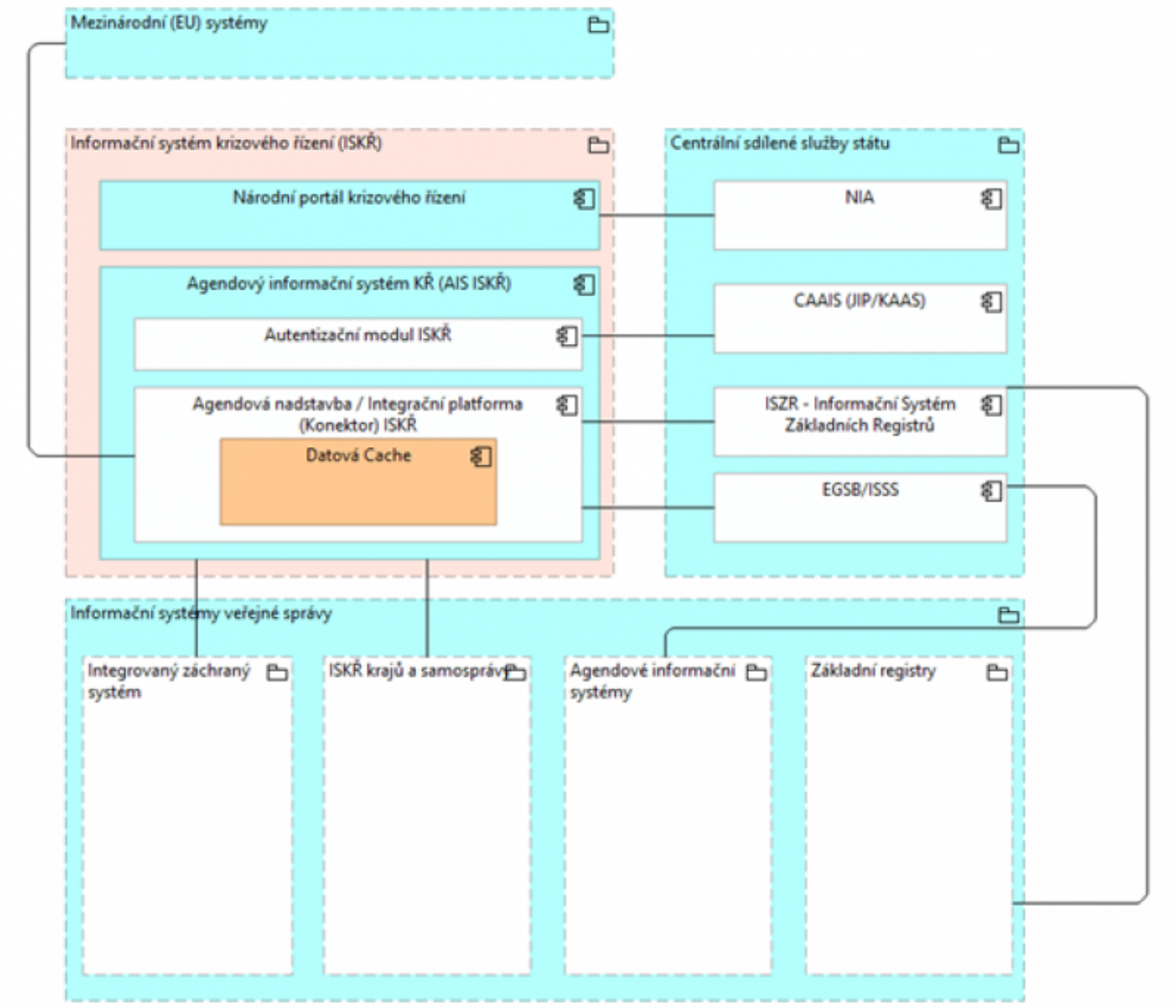
Příprava na krizový stav z pohledu propojení informačních systémů

Informační systémy sloužící pro zvládnutí krizového stavu **fungují v rámci přípravy stejně, jako jakékoliv jiné informační systémy veřejné správy.** Neplatí pro ně žádné výjimky, ani specifická komunikace. Výjimky popsané např. v § 3 zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů se vztahují na správce daného informačního systému, ale už ne na samotný informační systém a jeho vazby.

Je tedy potřeba stavět informační systémy pro zvládnutí krizového stavu tak, aby:

- Orgány veřejné moci, soukromoprávní uživatelé údajů, činnosti, oprávnění, údaje a další informace byly ohlášeny v příslušných agendách v základním registru práv a povinností
- Vazby na jiné informační systémy byly činěny prostřednictvím referenčního rozhraní veřejné správy
- Komunikace probíhala v prostředí Centrálního místa služeb
- Klienti a úřední osoby byly identifikování pomocí kvalifikovaného systému elektronické identifikace, tedy zprostředkovaně pomocí Národního bodu pro identifikaci a autentizaci pro klienty a Jednotného identitního prostoru pro úřední osoby Jednotného identitního prostoru pro úřední osoby

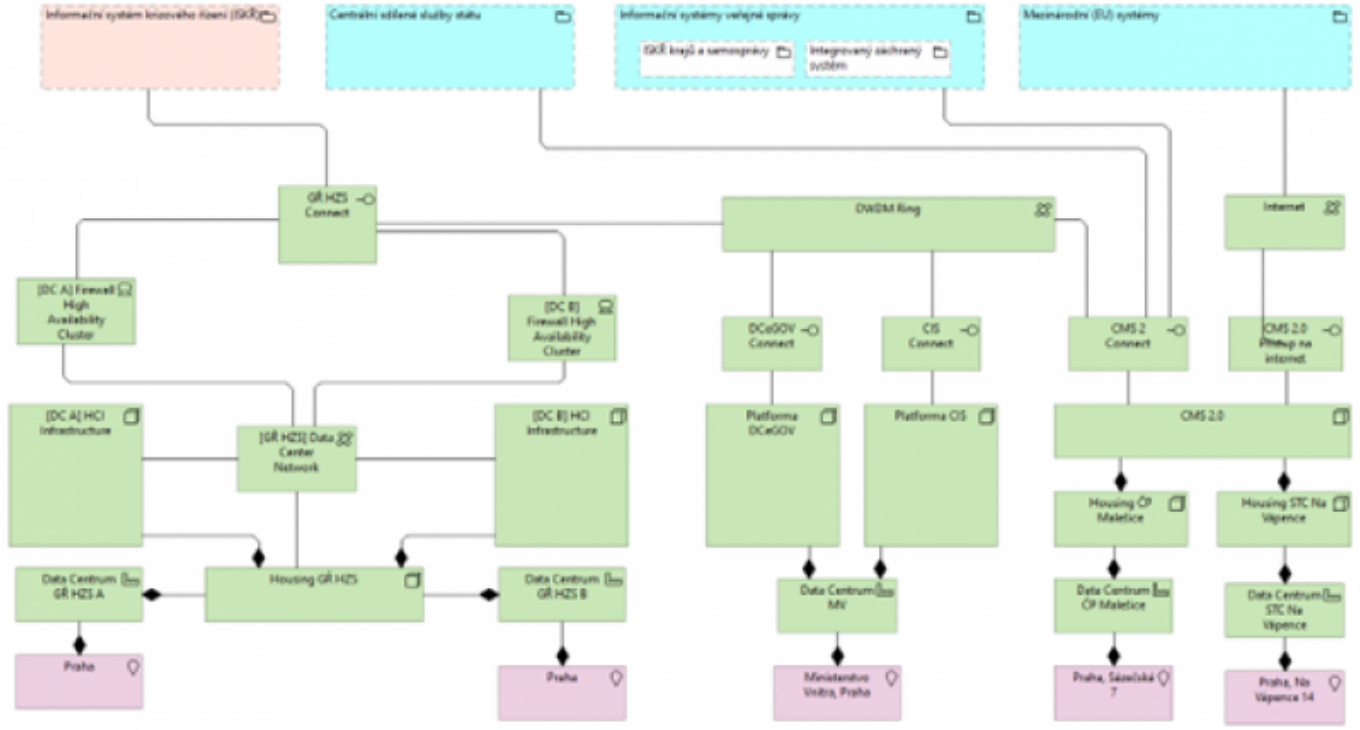
Logická komunikace a propojení informačních systémů



Zásadní funkčností pro přípravu na krizový stav je vytváření si tzv. Datové cache (datové úložiště), které se bude plnit dle agendového zmocnění z propojeného a veřejného datového fondu. Tato Datová cache zůstává nevyužívána do doby, než nastane krizový stav.

Správce ISKŘ udržuje Datovou cache tak, aby bylo možné v krizovém stavu správně propojovat a párovat údaje o subjektech práva. Aby toto bylo možné, je nutné správně s celou evidencí pracovat a udržovat si pravidla pro tvorbu a správu subjektů v datovém kmeni.

Fyzická komunikace a propojení informačních systémů



Fyzické propojení, tedy infrastruktura, pomocí které jsou dopravovány jednotlivá data a informace je v přípravě na krizový stav realizováno pomocí Komunikační infrastruktury veřejné správy a Centrálního místa služeb. Veškeré informační systémy jsou na tuto infrastrukturu napojeny a neexistuje mezi nimi žádný přímý propoj.

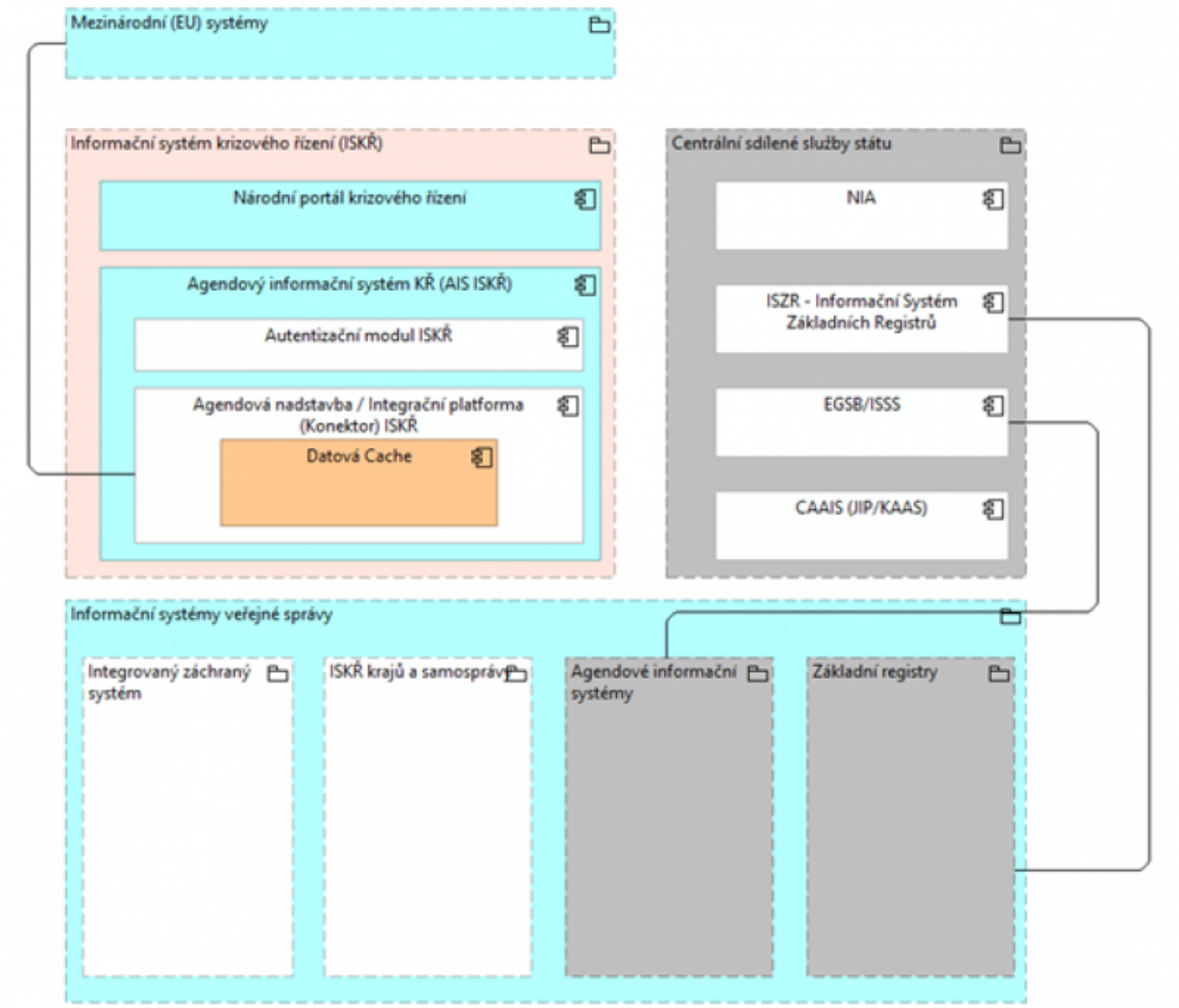
Krizový stav z pohledu propojení informačních systémů

Popis fungování v krizovém stavu předpokládá správné provedení přípravy dle kapitoly výše. Nyní se informační systémy jak v logickém, tak fyzickém propojení musí spolehnout na jiné mechanismy a postupy, pro které nejsou navrženy systémy a služeb eGovernmentu.

Jde především o práci nad lokálními daty a informacemi a zajištění propojení jen s nejpotřebnější skupinou informačních systémů nutných ke zvládnutí krizového stavu.

Důležité je především zvládnutí krizového stavu, ovšem je potřeba nezapomenout, že samotný Krizový zákon stanovuje rovnost mezi písemnými a elektronickými údaji. Jelikož se dá předpokládat rychlejší a efektivnější rozhodování nad elektronickými údaji, není možné propojení a komunikaci informačních systémů neřešit s tím, že se případně bude rozhodovat nad písemnými údaji.

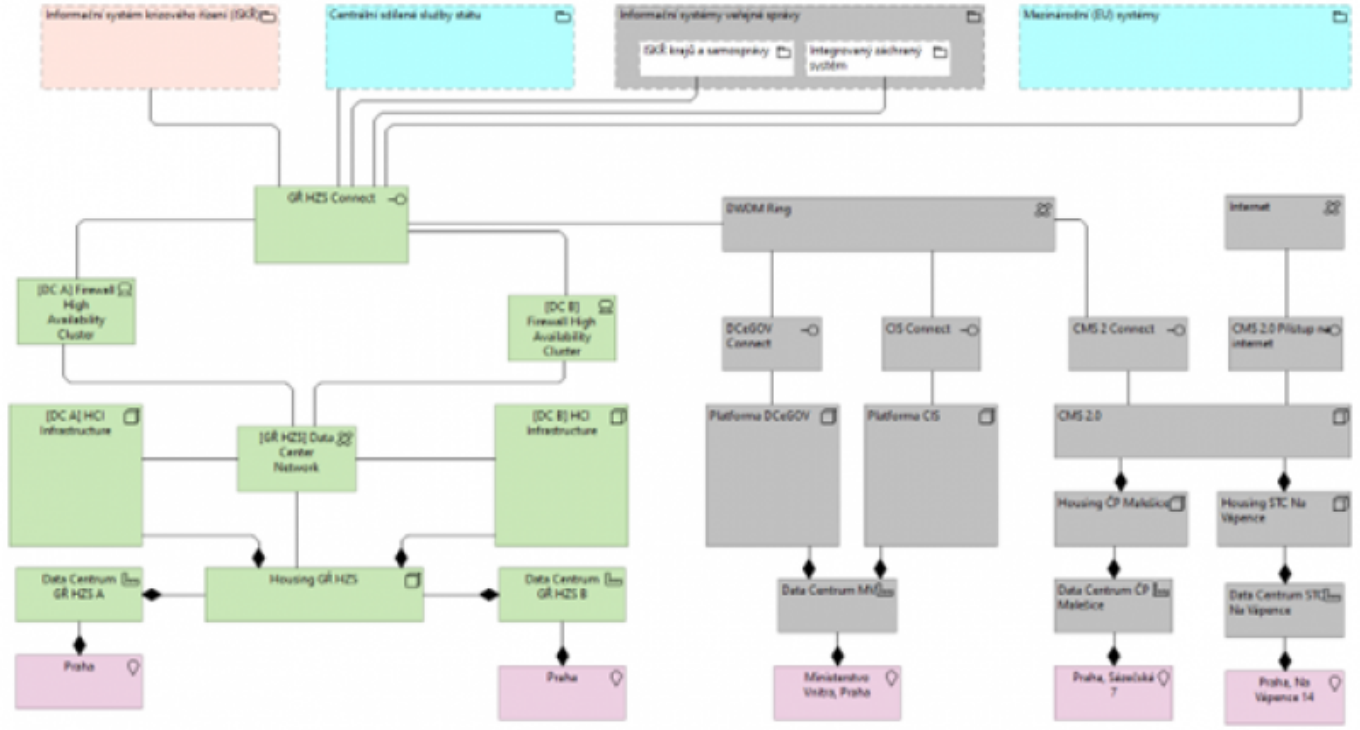
Logická komunikace a propojení informačních systémů



V krizovém stavu se musí počítat s tím, že nebudou fungovat systémy a služby eGovernmentu. V takovém případě je nutné spolehnout se na Datovou cache, která byla dle agendových zmocnění průběžně udržována v době přípravy. Nyní se jedná o hlavní datový zdroj pro rozhodování. Další kritické informační systémy jsou napojeny na ISKŘ napřímo.

Správné udržování evidence subjektů v přípravě na krizový stav má nyní za následek, že je možné párovat jednotlivé záznamy o subjektech i bez nutnosti překladu Agendových identifikátorů fyzických osob.

Fyzická komunikace a propojení informačních systémů

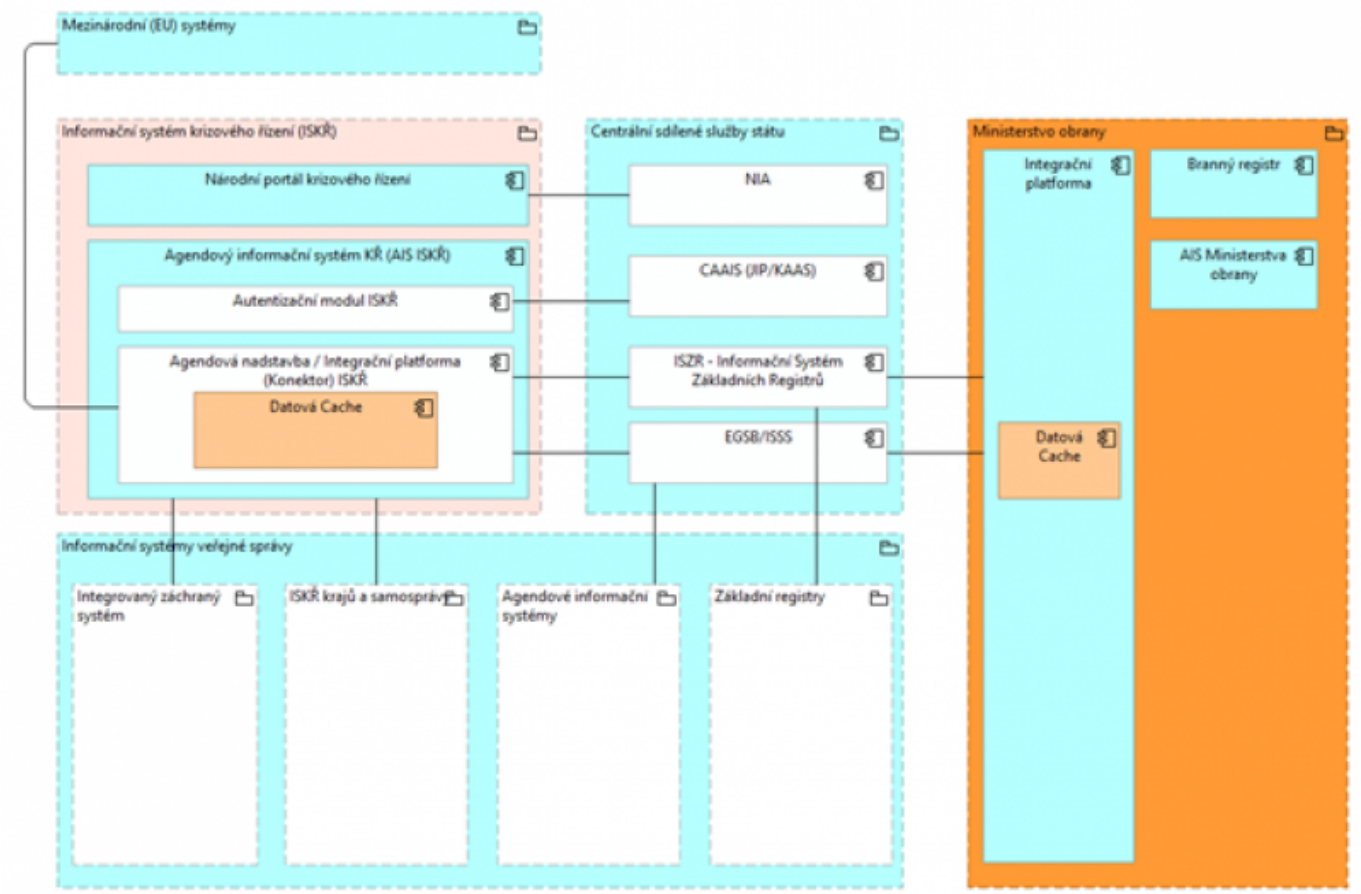


V krizovém stavu se musí počítat s tím, že nebude fungovat Komunikační infrastruktura veřejné správy a Centrální místo služeb. V takovém případě je nutné spolehnout se na záložní síťové propojení mezi kritickými systémy, které musí komunikovat s ISKŘ.

Specifický příklad Ministerstva obrany

Ministerstvo obrany vystupuje v přípravě na krizový stav stejně jako správce ISKŘ. Neplatí pro ně žádné výjimky, ani specifická komunikace. Komunikuje tedy pro své potřeby v rámci agendových zmocnění, pomocí referenčního rozhraní a využívá Centrální místo služeb.

Logická komunikace a propojení informačních systémů v přípravě na krizový stav



V případě krizového stavu je Ministerstvo obrany samostatnou složkou, která si kromě propojení na ISKŘ udržuje i vlastní Datovou cache a funguje pro své potřeby samostatně. Opět zde přestávají fungovat služby a systémy eGovernmentu a je proto nutné zajistit vlastní propojení. Zde se předpokládá využití stejného mechanismu jako u správce ISKŘ.

Logická komunikace a propojení informačních systémů v krizovém stavu