

poslední aktualizace:

**22. 4. 2026**

# Digitalizace veřejné správy — příklady dobré praxe

“Digitální transformace dnes není pro moderní vlády volbou, ale nezbytností. Umožňuje zlepšovat veřejné služby, přijímat informovanější rozhodnutí a efektivně spolupracovat napříč úřady i státy. Zároveň je klíčová pro naplnění rostoucích očekávání občanů v době rychlých změn. Aby v tomto úsilí jednotlivé vlády uspěly, potřebují odvážný, ale zároveň vyvážený přístup, opřený o provázané, důvěryhodné systémy a kvalitní řízení,” uvádí OECD ve své publikaci s názvem Digital Government Index (2025).

Globální vývoj v oblasti digitalizace veřejné správy v posledních letech potvrzuje, že digitální transformace již není pouze otázkou technologické modernizace, ale stává se **klíčovým předpokladem efektivního fungování státu**. Data z mezinárodních srovnání ukazují, že většina vyspělých zemí v této oblasti postupuje kupředu, avšak tempo i kvalita této transformace se výrazně liší. Podle OECD **Digital Government Index dosáhly státy OECD v roce 2025 průměrného skóre 0,70 (z 1,0)**, což představuje 14% nárůst oproti roku 2023, zároveň však signalizuje, že **stále není zdaleka dosaženo plného potenciálu**.

**Z globální perspektivy zároveň přetrvává výrazná nerovnováha.** GovTech Maturity Index zveřejňovaný Světovou bankou, který sleduje digitalizaci ve 198 světových ekonomikách, ukazuje, že pokrok je „pozitivní, ale nerovnoměrný“ a že se prohlubuje rozdíl mezi technologicky vyspělými státy a zeměmi s nižšími příjmy. **Zatímco přibližně 41 % zemí (včetně České republiky) spadá do skupiny s nejvyšší úrovní GovTech vyspělosti, významná část světa nadále zaostává**, zejména v oblastech základní digitální infrastruktury, interoperability systémů či digitální identity. Tento trend naznačuje, že digitalizace veřejné správy není lineární proces, ale strukturální transformace, která závisí na širších faktorech, jako jsou institucionální kapacity, legislativní rámec či investice.

Evropský kontext ukazuje relativně vysokou úroveň adopce digitálních služeb, avšak i zde existují výrazné rozdíly mezi jednotlivými státy. Podle **dat Eurostatu z roku 2025 interagovalo s veřejnou správou online 72 % občanů EU**, přičemž v nejvyspělejších zemích, jako je Dánsko, Nizozemsko, Finsko nebo Švédsko, dosahuje tento podíl až 96–98 %. Podobně i **míra**

**využívání elektronické identity vykazuje značnou variabilitu** – od více než 90 % ve státech severní Evropy až po méně než 15 % v některých zemích střední a východní Evropy. Tyto rozdíly naznačují, že faktorem úspěšné digitalizace není pouze dostupnost technologií, ale jejich skutečné využívání občany a důvěra v digitální služby.

Mezinárodní indexy zároveň umožňují **identifikovat skupinu zemí, které dlouhodobě patří mezi lídry v implementaci digitální veřejné správy**. Podle OECD **Digital Government Index** (2025) dosahují nejvyšších hodnot zejména Korejská republika, Austrálie, Portugalsko, Spojené království, Norsko, Estonsko či Dánsko, které vykazují vyvážený výkon napříč klíčovými dimenzemi, jako jsou práce s daty, uživatelská orientace nebo schopnost poskytovat proaktivní služby.

Podobný obraz nabízí i **E-Government Development Index OSN** (2024), kde se na předních příčkách umísťují Dánsko, Estonsko, Singapur, Korejská republika, Spojené království či Austrálie. **Česká republika se v evropském i globálním srovnání pohybuje spíše ve střední části**, zejména z hlediska využívání digitálních služeb. V žebříčku tak Česká republika nepatří mezi technologicky zaostávající země, ale spíše mezi ty, kde digitalizace naráží na limity v adopci, propojení systémů a uživatelské přívětivosti služeb.

Z mezinárodních srovnání vyplývá, že úspěšná digitalizace veřejné správy není výsledkem izolovaných projektů, ale komplexního přístupu, který propojuje digitální infrastrukturu, institucionální řízení, legislativní rámec a uživatelskou zkušenost. Následující kapitoly proto představí konkrétní příklady dobré praxe z vybraných zemí, které ilustrují různé modely a přístupy.

## Estonsko – X-Road

**X-Road** (estonsky X-tee) je **klíčová infrastruktura pro výměnu dat** v digitální vládě Estonska. Jedná se o zabezpečenou digitální platformu, která umožňuje informačním systémům veřejného i soukromého sektoru vyměňovat si data prostřednictvím internetu při zachování důvěrnosti, integrity a interoperability.

Systém X-Road byl **vyvinut estonskou vládou a spuštěn v roce 2001**. Funguje jako distribuovaná vrstva pro výměnu dat, která **propojuje řadu vládních databází a služeb**. Namísto ukládání všech informací v jedné centrální databázi si jednotlivé instituce spravují vlastní informační systémy. X-Road představuje **bezpečnou komunikační vrstvu**, která těmto systémům umožňuje v případě potřeby o data žádat a sdílet je.

Systém funguje prostřednictvím sítě zúčastněných organizací, které publikují konkrétní datové služby. Ostatní autorizovaní členové sítě mohou k těmto službám přistupovat na základě předem definovaných dohod. **Každý datový požadavek prochází přes zabezpečené servery**, kde je komunikace šifrována, digitálně podepsána, autentizována a zaznamenávána v logech. Tím je zajištěno, že data nemohou být během přenosu změněna a že veškerý přístup k informacím lze zpětně dohledat.

Protože **architektura je decentralizovaná, původní data vždy zůstávají v databázi instituce, která za ně odpovídá**. X-Road pouze umožňuje bezpečný přenos informací mezi systémy v okamžiku, kdy je to potřeba. Tento přístup omezuje duplicitní ukládání dat, zvyšuje efektivitu a podporuje interoperabilitu mezi různými technologickými platformami.

V praxi tato platforma umožňuje fungování mnoha digitálních veřejných služeb v Estonsku. Vládní úřady, obce i organizace soukromého sektoru mohou **automaticky získávat ověřené informace z databází ostatních institucí a poskytovat tak služby, jako jsou daňová přiznání, zdravotní služby nebo registrace podniků**. Díky tomu je X-Road považován za páteř estonského digitálního státu, která umožňuje stovkám institucí a tisícům služeb fungovat v rámci jednoho interoperabilního ekosystému.



## X-Road

- Klíčová infrastruktura pro výměnu dat – zabezpečená digitální platforma propojující informační systémy veřejného i soukromého sektoru
- Decentralizovaný model – data zůstávají u jednotlivých institucí, X-Road funguje jako komunikační vrstva
- Páteř digitálního státu – umožňuje automatizované získávání ověřených informací mezi institucemi a fungování širokého spektra služeb

## Finsko – Suomi.fi e-Authorizations

Finská služba **Suomi.fi e-Authorizations** je národní digitální služba, která umožňuje fyzické osobě, firmě nebo organizaci udělit jiné osobě či společnosti právní oprávnění jednat jejím jménem v online službách. **V praxi funguje jako elektronická plná moc.** Místo papírových dokumentů je tudíž oprávnění zaznamenáno digitálně v národním registru a může být **automaticky ověřeno při využívání elektronické služby.** Díky tomu je systém zároveň **bezpečný i efektivní.**

**Hlavním účelem** služby Suomi.fi e-Authorizations je umožnit důvěryhodné zastupování v záležitostech, které často vyžadují formální oprávnění. Například občan může zmocnit jinou osobu, aby vyřizovala jeho osobní záležitosti, zatímco společnost může oprávnit zaměstnance, účetního nebo jiného zástupce k řízení úkolů souvisejících s podnikáním v digitálních veřejných či soukromých službách. Služba tak **podporuje každodenní administrativu a snižuje potřebu manuálního ověřování oprávnění.**

To, co činí tento systém obzvláště významným, je skutečnost, že je **součástí širší infrastruktury digitální veřejné správy ve Finsku.** Pomáhá veřejným i soukromým organizacím spolehlivě ověřit, zda má uživatel skutečně právo jednat za jinou osobu nebo organizaci, bez ohledu na čas či místo. V tomto smyslu není Suomi.fi e-Authorizations pouze nástrojem pro usnadnění práce, ale představuje klíčový mechanismus pro budování důvěry, zajištění legality a plynulé digitální interakce ve finské společnosti.

## Suomi.fi e-Authorizations

- Národní **digitální služba fungující jako elektronická plná moc**, která je automaticky ověřitelná
- Mechanismus umožňující bezpečné zastupování bez manuálního ověřování, který zjednodušuje každodenní administrativu
- Součást širší infrastruktury digitální veřejné správy – propojuje veřejný i soukromý sektor a zajišťuje plynulou digitální interakci

## Itálie – aplikace IO + platební platforma pagoPA

Italský přístup kombinuje **národní platební infrastrukturu** (platformu pagoPA) s **aplikační vrstvou pro občany** (IO). Platforma pagoPA je popisována jako **elektronický platební systém** vytvořený za účelem **zjednodušení, zvýšení bezpečnosti a transparentnosti plateb vůči veřejné správě.** Umožňuje standardizované platby prostřednictvím zapojených poskytovatelů platebních služeb. Aplikace IO je koncipována jako **jednotný přístupový bod pro občany**, kde mohou přijímat zprávy od veřejných institucí, spravovat připomenutí a **přímo z těchto zpráv provádět platby**, čímž fakticky sjednocuje komunikaci i transakce v jednom mobilním kanálu. Platformu provozuje společnost PagoPA S.p.A., která byla vytvořena **s cílem** škálovat digitální interakce napříč rozptýlenými orgány veřejné správy a zároveň zachovat jednotné platební procesy.

To, co z tohoto řešení činí silný „příklad dobré praxe“, je skutečnost, že řeší obecně velmi palčivý problém. **Platby směřované veřejné správě jsou všudypřítomné (poplatky, pokuty, školní služby, obecní poplatky)** a mohou se stát významnou překážkou plně digitálního poskytování služeb, pokud každá instituce používá odlišné platební systémy. **Jednotná platební a komunikační vrstva snižuje fragmentaci** a umožňuje státu navrhovat služby spíše podle životních situací občanů než podle institucionálních hranic jednotlivých úřadů.

Iniciativa je navíc **aktuální** i v politických a správních debatách. V prosinci 2025 se objevily zprávy o dohodě na prodeji státní digitální platební platformy subjektům kontrolovaným státem, přičemž bylo zdůrazněno, že pagoPA zpracovala platby v hodnotě desítek miliard eur a nadále zůstává klíčovým prvkem širší digitalizační strategie Itálie prostřednictvím aplikace IO. Přenositelné poučení spočívá v tom, že platby a bezpečné zaslání zpráv lze chápat jako sdílenou národní infrastrukturu, což **urychluje digitalizaci stovek či tisíců veřejných institucí, aniž by každá z nich musela budovat vlastní technologické řešení.**

## IO + pagoPA

- Kombinace **národní platební infrastruktury a jednotného občanského rozhraní** – pagoPA standardizuje platby vůči veřejné správě, aplikace IO sjednocuje komunikaci i transakce
- Řešení fragmentace – jednotná platební a komunikační vrstva
- Sdílená infrastruktura pro tisíce institucí

## Dánsko – Digital Post + MitID

Dánský systém **Digital Post** je národní řešení, které **umožňuje orgánům veřejné správy zasílat digitální zprávy a dokumenty s právní účinností.** Oficiální popisy zdůrazňují, že existuje zákonná povinnost, aby občané i podniky byli schopni přijímat Digital Post od veřejných institucí, což odráží **národní přístup „digital-first“ v oblasti úřední komunikace.** Legislativní a politický vývoj je přitom **jasně vymezen.** Dánsko přijalo v roce 2012 zákon o veřejné digitální poště, který učinil používání systému povinným pro podniky od roku 2013 a pro občany starší 15 let od roku 2014, přičemž současně umožňuje **udělení výjimek osobám, které nejsou schopny digitální kanály využívat.** Přístup k systému je **propojen s národním systémem digitální identity,** která je na rozdíl od českého modelu **jednotná pro celou zemi.** **Digital Post** lze číst a na zprávy odpovídat prostřednictvím rozhraní, která využívají autentizaci pomocí **MitID,** jenž nahradil dřívější autentizační řešení NemID.

Dánsko ukazuje, jak může digitální vláda překročit rámec pouhé nabídky „online možností“ a přejít k **modelu „digitálního doručování jako výchozího standardu“,** aniž by rezignovala na principy spravedlnosti a inkluze. **Existence** formálního procesu udělování výjimek (spravovaného obcemi) a jasných pokynů, kdy a jak lze výjimku získat, vytváří model řízení zaměřený na začlenění. Uznává totiž, že ne každý obyvatel může v každé situaci prakticky využívat digitální samoobslužné služby. **Materiály** Dánské agentury pro digitální vládu zároveň zveřejňují uživatelská data pro účely veřejné kontroly, například počet registrovaných uživatelů či velikost skupiny osob s udělenou výjimkou v oficiálních statistických přehledech. Silné stránky dánského modelu jsou tak v jasném vymezení právního statusu digitálních zpráv, zajištění podpory uživatelům, **transparentní systematizaci výjimek a ukotvení přístupu k systému v silném autentizačním mechanismu,** aby princip „digital-by-default“ neznamenal „insecure-by-default“.

## Digital Post + MitID

- **Digitální doručování** jako výchozí standard s právní účinností („digital-first“)
- Silný **autentizační mechanismus** (MitID) propojený s komunikací se státem
- Výjimky pro osoby, které nemohou digitální služby využívat

## Rakousko – ID Austria

Rakouský systém **ID Austria,** který funguje od roku 2023, je prezentován jako moderní a **bezpečný způsob, jak se mohou lidé digitálně identifikovat při přístupu k online službám a při vyřizování úředních záležitostí** prostřednictvím internetu. Důležitým prvkem **návrhu** je kontinuita a digitální migrace. ID Austria **navazuje na předchozí rakouské nástroje elektronické identity** (Handy-Signatur a Bürgerkarte) a umožňuje **řízený přechod na nové řešení,** namísto zavedení zcela nového systému bez návaznosti na stávající infrastrukturu. Poskytování služeb občanům je zároveň propojeno se stabilním

katalogem služeb. Portál [oesterreich.gv.at](https://oesterreich.gv.at) popisuje ID Austria jako mechanismus umožňující bezpečné prokázání totožnosti online, díky němuž **mohou uživatelé přistupovat k digitálním službám a elektronicky uzavírat úřední úkony a transakce**. Digitální identita tak není pouze abstraktní infrastruktura, ale nástroj přímo využitelný v praxi.

Tento přístup **ukazuje, jak propojit digitální identitu s reálným poskytováním služeb**, což je oblast, se kterou se mnoho zemí potýká. Namísto toho, aby byla digitální identita řešena jako samostatný projekt, Rakousko ji chápe jako základní nástroj, který je opakovaně využíván napříč různými službami veřejné správy. Právě tato opakovaná využitelnost ospravedlňuje investice do bezpečnosti (např. vícefaktorová autentizace), uživatelské přívětivosti (např. mobilní potvrzování) i administrativních procesů pro registraci obyvatel.

Dalším přenositelným poučením je jasnost v oblasti správy a řízení (governance). Iniciativa je **prezentována prostřednictvím státních kanálů spojených s rakouským Spolkovým kancléřstvím**, což snižuje nejasnosti ohledně odpovědnosti a **pomáhá koordinovat standardy** mezi jednotlivými úřady. Přejít od starších systémů digitální identity k novému standardu navíc ilustruje realistický životní cyklus digitální vlády. Starší systémy musí být postupně ukončeny, nikoli pouze doplněny, a občané musí být procesem migrace prováděni tak, aby nedocházelo k fragmentaci poskytovaných služeb.

## ID Austria

- Bezpečný **způsob digitální identifikace** pro přístup ke službám a úředním úkonům online
- Kontinuita a řízená migrace – navazuje na předchozí systémy
- Digitální identita jako opakovaně využitelný základ

## Španělsko – Mi Carpeta Ciudadana

Španělská **Mi Carpeta Ciudadana** je dobrým příkladem toho, jak může stát **agregovat vztah občana k veřejné správě do jednoho přehledného rozhraní**. Oficiální popis zdůrazňuje, že občan zde může komunikovat s veřejnou správou, sledovat osobní údaje, předchodí úřední úkony, termíny či notifikace, a to v jednom místě. Aplikace i web jsou součástí širšího „**Punto de Acceso General**“, tedy jednotného bodu přístupu k veřejným službám.

To, co ze španělského řešení dělá **příklad dobré praxe**, je **důraz na občanskou perspektivu**. Stát zde **neorganizuje digitální kontakt podle struktury úřadů, ale podle toho, co občan potřebuje** vidět a vyřídit. Uživatel dostává souhrn svého vztahu ke státu: informace, notifikace i návazné kroky. Příklad španělského systému ilustruje, **jak užitečné je vytvořit vedle digitalizace jednotlivých agend i „osobní dashboard občana“**, kde jsou soustředěny klíčové údaje, zprávy a stav řízení napříč veřejnou správou. To posiluje přehlednost i důvěru v systém.

Dalším **důležitým aspektem** španělského řešení je jeho role v posilování transparentnosti a kontroly občana nad vlastními daty. Mi Carpeta Ciudadana **umožňuje uživatelům nahlížet na informace, které o nich veřejná správa eviduje**, a sledovat historii interakcí s jednotlivými institucemi. Tento prvek je zásadní nejen z hlediska uživatelského komfortu, ale i z pohledu důvěry ve veřejnou správu.

Systém zároveň podporuje proaktivní komunikaci ze strany státu. **Notifikace upozorňují na blížící se termíny, povinnosti nebo změny** ve správních řízeních, čímž snižují riziko opomenutí a zvyšují efektivitu interakcí mezi občanem a státem. Tím se Mi Carpeta Ciudadana stává aktivním nástrojem řízení vztahu mezi občanem a veřejnou správou.

## Mi Carpeta Ciudadana

- Jednotné rozhraní („osobní prostor občana“) pro komunikaci se státem a přehled vztahu k veřejné správě
- Důraz na občanskou perspektivu – organizace služeb podle potřeb uživatele, ne podle struktury institucí
- Soustředění informací a notifikací na jednom místě zvyšuje přehlednost a občanskou důvěru

## Portugalsko – gov.pt + princip „once only“

Portugalsko je zajímavé především jako **příklad digitalizace založené na interoperabilitě**, datovém řízení a principu „once only“. Vládní materiály výslovně uvádějí, že cílem je, **aby občané a firmy nemuseli opakovaně dodávat stejné informace různým orgánům veřejné správy**, a že portál **gov.pt** má fungovat jako integrovaná vstupní brána ke službám státu.

**Portugalský příklad** ukazuje strategický rámec, který **propojuje zjednodušování procesů, práci s daty a koordinaci napříč veřejnou správou**. Portugalská vláda navíc výslovně **formuluje** princip „**simplify first, digitalise second**“, což je pro veřejnou správu velmi cenné pravidlo. Důležitým prvkem je redesign procesů. Portugalsko explicitně zdůrazňuje, že digitalizace nemá být pouhým „převodem papírových procesů do online prostředí“, ale má vést k jejich zjednodušení a racionalizaci. Tento přístup **pomáhá předcházet situacím, kdy digitalizace pouze reprodukuje existující neefektivitu**.

Model vzniklý v Portugalsku je dále charakteristický silným důrazem na koordinaci a řízení digitalizace na centrální úrovni. Portál gov.pt není pouze technickým rozhraním, ale **součástí širší strategie digitální transformace, která propojuje služby napříč ministerstvy a úřady**. Tato koordinace umožňuje sjednocovat standardy, sdílet data a postupně eliminovat duplicitu v administrativních procesech.

## gov.pt

- **Integrovaná vstupní brána ke službám státu** propojující data, procesy a instituce
- Digitalizace založená na principu „once only“ – občané a firmy nemusí opakovaně poskytovat stejné informace
- Nejprve zjednodušení procesů, až poté jejich digitalizace

## Nizozemsko – MijnOverheid + DigiD

Nizozemský model kombinuje národní digitální identitu **DigiD** s občanským portálem **MijnOverheid**. Podle oficiálních informací funguje MijnOverheid jako **osobní digitální prostor, kde občan přijímá digitální poštu od státu** a na jednom místě vidí své **údaje a vybrané informace od veřejných institucí**. Přihlášení probíhá přes DigiD. Významným prvkem nizozemského řešení je postupné zavádění digitální komunikace jako standardu, včetně právě rozšiřování digitální pošty a elektronických notifikací.

Z pohledu možné inspirace je cenné hlavně to, že Nizozemsko nesází jen na „online formuláře“, ale na **stálý občanský účet vůči státu**: digitální stránku, přehled údajů a bezpečný identifikační nástroj. Takový model je uživatelsky srozumitelný a dobře škáluje mezi různými institucemi. Pro stát je toto cesta, jak dlouhodobě budovat jednotný vztah s občanem, ne jen digitalizovat jednotné izolované procesy.

Nizozemský přístup je dále charakterizován **důrazem na dlouhodobou konzistenci a postupný rozvoj digitální infrastruktury**. DigiD funguje jako stabilní národní identifikační nástroj, který je využíván širokým spektrem veřejných služeb, a jeho rozšíření do praxe umožnilo budovat nad ním další vrstvy služeb, jako je MijnOverheid.

## MijnOverheid + DigiD

- Kombinace **národní digitální identity** a **osobního digitálního prostoru** občana pro komunikaci se státem
- Občan má na jednom místě digitální poštu i všechny informace od institucí
- Model „stálého účtu občana vůči státu“ místo izolovaných online formulářů

## Francie – FranceConnect

Francouzský systém **FranceConnect** je státní řešení pro **přístup k online službám pomocí již existujícího důvěryhodného účtu**. Stát uvádí, že přes FranceConnect lze přistupovat k více než 1400 online službám a že uživatel může využít přihlašovací údaje od již zavedených veřejných či důvěryhodných poskytovatelů identity.

Síla tohoto modelu spočívá v tom, že **zmenšuje bariéru pro vstup do digitálních služeb**. Namísto zakládání nových účtů pro každý úřad stát vytváří federovaný přihlašovací rámec, který zjednodušuje uživatelskou zkušenost a podporuje širší adopci online služeb.

Přenositelnou inspirací je, že **digitalizace nemusí vždy začínat budováním úplně nového identitního řešení**. V některých zemích může být efektivnější model, který propojí již existující důvěryhodné identity do jednoho státního vstupního bodu.

## FranceConnect

- **Federovaný přihlašovací rámec**, který umožňuje přístup k online službám pomocí existujících důvěryhodných účtů
- Snižování bariér vstupu – není nutné vytvářet nové účty pro každý úřad
- Podpora širší adopce digitálních služeb díky jednoduché uživatelské zkušenosti

# Země mimo EU

## Ukrajina – Diia

Ukrajinský systém **Diia** představuje **jeden z nejpropracovanějších současných příkladů digitální veřejné správy** postavené kolem jednoho občanského rozhraní. Diia propojuje mobilní aplikaci a webový portál pro občany i podnikatele; **v jednom ekosystému sdružuje digitální doklady, přístup ke službám státu i elektronické podávání žádostí**. Ukrajinská vláda tento projekt prezentuje jako klíčový nástroj budování digitálního státu a uvádí, že aplikace slouží desítkám milionů uživatelů. Portál nabízí **více než stovku různých služeb**.

Důležité je zmínit, že Diia není jen jednotlivá aplikace, ale ucelený servisní model, v němž stát občanovi nabízí **digitální kontakt přes jeden hlavní kanál**. Zároveň jde o příklad odolnosti: digitální stát zde nebyl budován pouze v době stability, ale i v podmínkách války a krizového řízení. Právě tím je Ukrajina politicky i komunikačně **silný příklad** – ukazuje, že digitalizace není zbytečný luxus, ale součást funkčního státu.

Ukrajinský příklad ilustruje, že stát může občanům nabídnout **jednotné mobilní rozhraní pro dokumenty, služby i notifikace**, místo aby byli nuceni přecházet mezi několika různými portály. Zajímavý je i další vývoj směrem ke **konverznímu rozhraní** Diia.AI, které má uživatele navést podle potřeby.

## Diia

- Jednotné digitální rozhraní (aplikace + portál) pro dokumenty, služby i komunikaci se státem
- Ucelený servisní model – stát nabízí digitální kontakt přes jeden hlavní kanál
- Příklad odolnosti – systém funguje i v podmínkách krizového řízení během války

## Velká Británie – GOV.UK

Ekosystém **GOV.UK** ve Spojeném království představuje příklad přístupu označovaného jako „digitální vláda jako produktový management“, který je založen na publikovaném Service Standardu a sdíleném design systému. Service Standard **stanovuje, jak mají týmy navrhovat a provozovat veřejné služby**, včetně porozumění potřebám uživatelů, řešení celých problémů (nikoli pouze jejich částí) a poskytování propojených zkušeností napříč různými komunikačními kanály. Na operační úrovni **poskytuje sdílený „design systém“** znovupoužitelné komponenty a **vzory, díky nimž mohou vládní služby zůstat konzistentní napříč ministerstvy a agenturami**, což podporuje přístupnost, jednotné modely interakce a rychlejší implementaci. Tento přístup je institucionálně veden organizací Government Digital Service, která chápe GOV.UK nikoli pouze jako webovou stránku, ale jako systém standardů, platform a postupů pro poskytování veřejných služeb.

Jako současný příklad dobré praxe **má tento model klíčovou hodnotu v replikovatelnosti**. Jiné státy mohou převzít schéma service standard + design systém + centrální meziresortní kapacitní centrum, i když nemohou reprodukovat přesnou historickou trajektorii vzniku GOV.UK. Spojené království zároveň udržuje tuto agendu aktuální. **Dokument** „State of digital government review“ (publikovaný v lednu 2025) explicitně hodnotí, jak efektivně veřejný sektor využívá digitální technologie k poskytování služeb, a identifikuje systémové příčiny, které brání pokroku, čímž ukazuje, že **digitální transformace je chápána jako průběžná reforma, nikoli jako již dokončený projekt**. Nedávno **publikovaný** „roadmap“ z roku 2026 dále popisuje akční plán moderní digitální vlády do roku 2030, což odráží živý politický a strategický proces, nikoli statický narativ typu „digitalizace je hotová“. Přenositelné poučení spočívá v institucionalizaci poskytování služeb orientovaných na uživatele a sdílených stavebních prvků a následném průběžném aktualizování strategie na základě pravidelného vyhodnocování toho, co funguje a kde systém stále selhává.

## GOV.UK

- Service Standard stanovující, **jak mají být navrhovány a provozovány veřejné služby** – sdílený design systém
- Konzistentní a znovupoužitelné komponenty napříč institucemi
- Digitalizace jako průběžná reforma založená na evaluaci a aktualizaci

## Singapur – Singpass + MyInfo

Singapur dlouhodobě staví digitalizaci veřejné správy na robustní digitální identitě **Singpass**. Ta slouží jako **jednotný a bezpečný způsob přihlášení ke službám veřejného i soukromého sektoru**; podle vládních zdrojů umožňuje přístup k tisícům služeb napříč stovkami institucí a firem. Singpass **zároveň podporuje** vícefaktorové přihlašování, digitální podpis i mobilní potvrzování transakcí.

Silnou stránkou singapurského modelu je, že **samotná identita není izolovaný nástroj, ale součást širšího ekosystému**, zejména služby **MyInfo**, která umožňuje bezpečné předvyplňování údajů z důvěryhodných státních zdrojů se souhlasem uživatele. To **v praxi snižuje opakované vyplňování formulářů a zrychluje vyřizování služeb**.

Tento příklad je přenositelný hlavně v tom, že ukazuje propojení tří faktorů: digitální identity, sdílení dat se souhlasem občana a uživatelsky jednoduchého přístupu ke službám. Nejde tedy jen o bezpečné přihlášení, ale o **model, v němž se jednou ověřená identita stává základem pro pohodlnější a rychlejší veřejné služby**.

## Singpass + MyInfo

- **Jednotná digitální identita propojená s ekosystémem služeb** napříč veřejným i soukromým sektorem
- MyInfo umožňuje bezpečné předvyplňování údajů z důvěryhodných zdrojů se souhlasem uživatele
- Důraz na uživatelskou přívětivost

## Kanada – GCKey + Interac sign-in service

Charakteristickým znakem kanadské digitální veřejné správy je její federální model přihlašování.

**Občané mohou přistupovat k mnoha federálním online službám prostřednictvím:**

1. GCKey (přihlašovací údaje ve formě uživatelského jména a hesla vydané vládou, použitelné napříč více podporovanými službami).
2. Přístupu Sign-In Partner (využívajícího existující přihlašovací údaje k online službám zúčastněných finančních institucí, které jsou federálními službami označovány jako partneři fungující prostřednictvím Interac).

Hodnota tohoto **modelu** nespočívá v „jednom portálu pro všechno“, ale spíše v opakovaně použitelné autentizační vrstvě, kterou mohou **jednotlivé úřady využívat, aniž by si každá instituce musela budovat vlastní přihlašovací infrastrukturu**, což podporuje postupnou digitalizaci v oblastech, jako je imigrace, sociální dávky, daně a další vysoce zatížené agendy.

Druhým prvkem dobré praxe je explicitní **směrování k posílení bezpečnosti účtů** ve velkém měřítku, včetně **povinné vícefaktorové autentizace u hlavních federálních účtů** (na základě oficiálních pokynů pro My Service Canada účet). Důležité je, že kanadský systém dohledu považuje správu digitální identity za aktuální politické téma, nikoli za „uzavřenou“ oblast. Sdělení generálního auditora z prosince 2024 **upozornilo** na absenci interoperabilního národního přístupu a zároveň poukázalo na **federální záměr sjednotit přihlašovací prostředí** (nahrazením mnoha oddělených portálů) **a zlepšit jeho konzistenci**. Ministerská reakce **popsala** práci na „GC Sign in“ (produkt určený k jednorázovému ověření údajů uživatele pro více služeb) a na schopnostech „vydávat a ověřovat“ digitální pověření, což naznačuje, že se systém vyvíjí směrem k moderním přístupům (jednotné přihlášení + ověřitelné digitální údaje), namísto setrvání u zastaralých modelů správy identity.

## GCKey + Interac sign-in

- **Federální model přihlašování – sdílená autentizační vrstva** využívající státní i bankovní identity
- Opakovaně použitelná struktura pro různé služby bez nutnosti budování vlastních systémů
- Důraz na bezpečnost (vícefaktorové ověřování) a postupný rozvoj systému

## USA – Login.gov

Široce citovaným příkladem „dobré praxe“ v USA je **budování digitální veřejné správy na sdílených platformových službách** namísto duplikace funkcionalit napříč jednotlivými úřady.

**Login.gov** je prezentován jako „jeden účet veřejnosti pro státní správu“, který nabízí **společnou autentizaci** a (tam, kde je to vyžadováno) **i ověření identity jako znovupoužitelnou komponentu pro zapojené instituce**. Jeho návrh ověřování identity je pozoruhodný tím, že **nabízí více cest dokončení procesu**, včetně vzdálených ověřovacích postupů (ověření pomocí dokladu totožnosti + selfie v rámci variant s vyšší úrovní záruky) a **osobního ověření** identity na pobočkách United States Postal Service, což je **přínosné z hlediska dostupnosti i prevence podvodů** v případech, kdy vzdálené ověření selže.

Vývoj v letech 2024–2025 poukazuje na **aktivní trajektorii modernizace**. V říjnu 2024 U.S. General Services Administration **oznámila** nezávislou certifikaci služby splňující úroveň IAL2 (vyšší úroveň záruky identity) a popsala zavedení individuálního párování obličeje (selfie porovnávaná s fotografií na dokladu totožnosti) spolu s rozšířením možností osobního ověřování. V srpnu 2025 GSA rovněž **oznámila** ověřování identity na základě pasu, tedy porovnání snímku pasu uživatele se záznamy prostřednictvím meziřesortního API přístupu. Provozní rozsah je doložen v **materiálech** k roadmapě programu (např. více než 100 milionů účtů a stovky napojených služeb).

Klíčovou v oblasti správy je také skutečnost, že **platforma byla podrobena dohledu a byly veřejně prezentovány její výsledky**. **Zprávy a audit** amerických kontrolních institucí identifikovaly nedostatky a vydaly doporučení (např. sladění se standardy digitální identity a posílení provozních kontrol), což potvrzuje, že **digitální identita je vnímána jako kritická infrastruktura vyžadující odpovědnost**.

## Login.gov

- **Jednotný účet pro přístup ke službám veřejné správy** jako sdílená platformová služba
- Více metod ověření identity (distančně i osobně), což zajišťuje dostupnost a bezpečnost
- Platforma podléhá veřejnému dohledu a průběžnému zlepšování

## Austrálie – myID

Austrálie představuje silný příklad „dobré praxe“ v tom, jak regulovat národní ekosystém digitální identity, namísto toho, aby byla digitální identita chápána pouze jako jedna aplikace. Zákon **Digital ID Act 2024** (účinný od 30. listopadu 2024) **vymezuje digitální identitu jako bezpečný, pohodlný, dobrovolný a inkluzivní nástroj pro online transakce se státní správou** (a postupně i se soukromým sektorem) a stanoví principy, správu a požadavky na dohled nad subjekty poskytujícími nebo využívajícími služby digitální identity. Nejviditelnějším nástrojem pro občany je aplikace **myID** (dříve myGovID), popisovaná jako aplikace australské vlády pro digitální identitu, která umožňuje prokázat totožnost online a toto ověření znovu využívat napříč službami.

To, **co z tohoto příkladu činí „dobrou praxi“ ve veřejné správě, je institucionální rámec**. Oficiální **popisy** systému identifikují více rolí (funkce správce systému, regulátora, dohled nad ochranou soukromí a standardizační orgány) a vysvětlují, že **poskytovatelé musí splňovat vysoké standardy** (v oblasti ochrany soukromí, bezpečnosti, prevence podvodů

a použitelnosti/přístupnosti), aby mohli získat akreditaci a zapojit se do systému. **Regulační přehlednost** je patrná také v **metodických pokynech**, včetně role Australian Competition and Consumer Commission (ACCC) jako regulátora digitální identity. Pro potřeby veřejné správy systém výslovně **podporuje** i scénáře zastupování prostřednictvím konceptu Relationship Authorisation Manager (jednání jménem firmy v zapojených službách), což je běžný praktický požadavek, který v raných řešeních eGovernment identity často chybí. **Model se zároveň i nadále rozšiřuje**. Oficiální systémové pokyny uvádějí, že do prosince 2026 se očekává rozšíření australského systému digitální identity o další poskytovatele a subjekty ze soukromého sektoru, což naznačuje existenci budoucí roadmapy, nikoli již „uzavřenou“ implementaci.

## myID

- Digitální identita jako součást regulovaného národního systému s jasně definovanými rolmi
- Důraz na bezpečnost, ochranu soukromí a akreditaci poskytovatelů
- Rozšiřování systému i do soukromého sektoru

## Nový Zéland – RealMe + Trust Framework Act

Přístup Nového Zélandu prostřednictvím **RealMe** představuje vyzrálý příklad oddělení

1. bezpečného přihlášení
2. ověřené identity

Tedy **rozdělení, které často zlepšuje použitelnost i řízení rizik v digitálních veřejných službách**. Oficiální vládní materiály definují RealMe jako službu autentizace a ověřování identity, která se používá k přihlašování do mnoha veřejných služeb a k bezpečnému prokazování totožnosti online. Zvláště relevantním rysem z pohledu veřejné správy je pravidlo správy platformy. Podle **katalogu** digitální vlády **musí státní instituce využívat přihlašovací službu RealMe**

namísto vývoje vlastních autentizačních systémů, což eliminuje duplicitu a urychluje zapojování nových služeb.

V oblasti ověřené identity oficiální dokumentace **uvádí**, že **ověřená identita RealMe je znovupoužitelná napříč téměř 200 vládními i komerčními službami**, má platnost 10 let a je navržena tak, aby ji bylo možné používat opakovaně „kdykoli a jakkoli často je potřeba“. To ilustruje klíčový princip. **Ověřování identity je nákladné a pro uživatele zatěžující, proto by mělo být navrženo jako znovupoužitelná infrastruktura**, nikoli jako jednorázový krok v každé jednotlivé službě.

Nový Zéland zároveň **aktualizoval** širší rámec správy prostřednictvím zákona Digital Identity Services Trust Framework Act 2023, který stanovil **právní rámec pro důvěryhodné služby digitální identity** a zřizuje **regulační orgán odpovědný za akreditaci poskytovatelů a služeb digitální identity**. Program je aktuální nejen z hlediska legislativy, ale i provozu. Vládní **sdělení** z března 2025 popisuje zjednodušení schvalovacího procesu pro organizace usilující o přístup k RealMe, s odklonem od zdoluhavých schvalovacích postupů při současném zachování požadavků na ochranu soukromí a další standardy.

## RealMe

- **Oddělení přihlášení a ověřené identity** jako princip pro lepší použitelnost a řízení rizik
- Povinnost státních institucí využívat centrální autentizační službu místo vlastních řešení
- Ověřená identita jako znovupoužitelný nástroj napříč službami

## Japonsko – Digital Agency využívající My Number Card + Mynaportal

Japonská Digital Agency poskytuje ucelený soubor komponent „digitálního státu“, soustředěný kolem průkazu **My Number Card** a portálu **Mynaportal**. Oficiální popisy charakterizují

Mynaportal jako **online kontaktní místo pro vyřizování správních agend** (např. péče o děti či dlouhodobá péče), které **umožňuje podávat žádosti online, kontrolovat osobní údaje vedené veřejnou správou a přijímat oficiální oznámení**, čímž je portál výslovně chápán jako více než pouhá informační webová stránka. Trvalým prvkem dobré praxe je **integrace právně relevantní identity a elektronického podpisu**. **„Japonská infrastruktura veřejných klíčů“ (JPKI)** využívá elektronické certifikáty uložené na čipu průkazu k **autentizaci uživatelů online a k ověřování integrity dokumentů** (ochrana proti manipulaci), což umožňuje transakce jak ve veřejném, tak soukromém sektoru.

Nejaktuálnějším vývojem a zároveň zásadním posunem z hlediska použitelnosti je **přechod od závislosti na fyzické kartě k identitě založené na chytrých telefonech**. Aktualizace Digital Agency z ledna 2026 popisuje „Smartphone My Number Card“ jako službu, která přenáší funkce průkazu My Number Card do mobilních zařízení (iPhone a Android), umožňuje biometrické ověřování identity (obličej/otisk prstu) namísto zadávání PIN kódu a rozšiřuje oblasti využití, jako je Mynaportal, vydávání certifikátů na přepážkách v samoobslužných kioscích, použití jako průkaz zdravotního pojištění ve zdravotnických zařízeních (s postupně rostoucím pokrytím) či podávání daňových přiznání prostřednictvím e-Tax. Agentura zároveň **zveřejnila** časový harmonogram zavedení pro iPhone (plánovaný start 24. června 2025), což představuje pokus o transparentnost veřejné správy ohledně implementačních milníků.

**Japonsko také propojuje digitální identitu s konkrétními životními situacemi**. Například **dokládán** k „online službě pro změnu bydliště“ vysvětluje, jak lze oznámení o vystěhování podat online u původní obce a předběžně sdílet údaje s cílovou obcí, čímž se za běžných podmínek snižuje potřeba osobních návštěv úřadů. Celkový pokrok je **dokládán** i významnými signály přijetí (např. přibližně 70% míra vlastnictví karty „My Number“ a rozšíření online postupů), avšak zavádění této reformy je spíše průběžným procesem než uzavřeným projektem.

## MyNumber + Mynportal

- Propojení **digitální identity, elektronického podpisu a portálu služeb**
- Mynportal jako kontaktní místo pro agendu a správu osobních údajů
- Posun k mobilní identitě a biometrickému ověřování

## Korejská republika – GOV24

Model **GOV24** v Koreji je často uváděn jako příklad „one-stop“ digitální veřejné správy, který se nadále vyvíjí, nikoli stagnuje. V červenci 2025 Ministry of the Interior and Safety oznámilo, že obnovený portál GOV24+ (GOV.KR) byl oficiálně **znovu spuštěn** 10. července 2025, přičemž byly představeny **inovace jako jednotné přihlášení do dalších hlavních portálů, lepší mobilní podpora pro stahování úředních dokumentů** a nová služba Benefit Notification Service určená k **zasílání personalizovaných upozornění na dostupné dávky**. To je důležité, protože portál má skutečnou hodnotu tehdy, když není pouze katalogem informací, ale také transakční platformou, která snižuje fragmentaci a omezuje „nevyužité nároky“ občanů.

Aktuální **uživatelské popisy** mobilní aplikace Government 24 (dostupné v běžných aplikačních obchodech) ji představují jako **hlavní portál integrující podání žádostí, informace o dávkách a dotacích i přehled veřejných politik**. Zdůrazňují, že uživatelé mohou online podávat žádosti a získávat úřední dokumenty a zároveň dostávat personalizované informace o dávkách prostřednictvím služby „Subsidy 24“. Zaměření na dávky je zásadní. **Proaktivní či personalizované služby snižují nároky na občany**, kteří by jinak museli sami zjišťovat, který úřad spravuje konkrétní program, a zároveň **zvyšují využívání oprávněných podpor**.

Nezávislé hodnocení rovněž považuje korejský přístup za významný referenční bod. **Analýza** OECD publikovaná v roce 2025 (Digital

Government Review of Korea) popisuje pokrok směrem k uživatelsky orientovaným a proaktivním veřejným službám, vyzdvihuje silné stránky, jako je škálovatelnost a transparentnost, a současně identifikuje prostor pro hlubší zapojení uživatelů a integraci služeb. **Kombinace rozsáhlého sjednocení služeb spolu s průběžným zlepšováním dokumentovaným externím hodnocením** představuje silný znak „dobré praxe“ pro vlády, které usilují o omezení duplicit a přechod k integrované zkušenosti občana.

## GOV24

- Inovovaný **portál pro služby, dokumenty a informace** např. o sociálních dávkách
- Proaktivní služby (notifikace upozorňující na nároky občana, zejm. ohledně dávek)
- Průběžné zlepšování a rozšiřování funkcionalit

## Indie – DigiLocker + Unique Identification Authority of India

Indický **DigiLocker** představuje vlajkovou schopnost „bezpapírové správy“. Jde o **bezpečnou cloudovou digitální peněženku dokumentů**, která umožňuje občanům přístup k **autentickým digitálním dokumentům a certifikátům, získávaným přímo od vydávajících institucí** a použitelným pro sdílení i ověřování. Z pohledu veřejné správy spočívá hlavní přínos v tom, že stát a zapojené veřejné instituce mohou upustit od opakovaného požadování nahrávání skenů či předkládání kopií dokumentů. Místo toho mohou služby pracovat s dokumenty, které pocházejí přímo od vydavatele a jsou ověřitelné, což **snižuje prostor pro podvody i administrativní náklady**. Oficiální **materiály** Digital India Corporation shrnují rozsah systému počtem zapojených vydavatelů a objemem výstupů (miliardy vydaných dokumentů, tisíce vydavatelů) a výslovně uvádějí, že vydané digitální dokumenty jsou považovány za rovnocenné fyzickým dokumentům podle příslušného regulačního rámce IT Rules.

Efektivita DigiLockeru je **úzce propojena s širší infrastrukturou digitální identity v Indii**, zejména se systémem Aadhaar. UIDAI (statutární orgán spravující Aadhaar) **definuje** autentizaci Aadhaar jako ověření čísla Aadhaar spolu s demografickými nebo biometrickými údaji vůči centrálnímu registru identit (Central Identities Data Repository). UIDAI také **nabízí funkci „historie autentizací“, která umožňuje jednotlivcům zobrazit záznamy o provedených autentizačních transakcích za určité období**, což představuje důležitý prvek důvěry v rozsáhlých systémech digitální identity. Iniciativa je aktuální nejen technologicky, ale i z hlediska veřejné politiky. Vládní sdělení Indie ze 6. března 2026 **popisuje** koncept „JAM trinity“ (účty Jan Dhan + Aadhaar + mobilní konektivita) jako **základní infrastrukturu, která umožnila přímé převody sociálních dávek na bankovní účty**, což ukazuje, že identita a digitální infrastruktura jsou chápány jako klíčové prvky poskytování veřejných služeb.

## DigiLocker + Aadhaar

- **Digitální peněženka dokumentů** vydaných přímo institucemi – právně rovnocenné fyzickým dokumentům
- Propojení s národní digitální identitou (Aadhaar)
- Eliminace potřeby nahrávání kopií a snížení administrativní zátěže

## Spojené arabské emiráty – UAE PASS

**UAE PASS** představuje jasný mimoevropský příklad budování digitální veřejné správy na základě národní digitální identity doplněné o elektronický podpis, **navržený pro fungování v rámci federální struktury emirátů**. Oficiální vládní portál SAE popisuje UAE PASS jako první národní řešení digitální identity, které **umožňuje uživatelům prokazovat svou totožnost vůči poskytovatelům služeb napříč všemi emiráty**. Federal Authority for Identity, Citizenship, Customs & Port Security dále **uvádí** UAE PASS jako jednotnou digitální identitu pro občany, rezidenty i návštěvníky, výslovně propojenou

s přístupem ke službám veřejného, poloveřejného i soukromého sektoru a s možností digitálního podepisování dokumentů.

Rozměr „dobré praxe“ spočívá v tom, že UAE PASS není omezen pouze na přihlášení. Jeho **cílem je umožnit plně digitální transakce, které dříve vyžadovaly fyzickou přítomnost**. Technická dokumentace **uvádí**, že mobilní aplikace UAE PASS poskytuje autentizační i podpisové služby a je součástí iniciativy Smart Government National Plan, spravované Digital Dubai ve spolupráci s Telecommunications and Digital Government Regulatory Authority a Abu Dhabi Digital Authority, což potvrzuje, že **jde o sdílenou národní infrastrukturu, nikoli o produkt jediné instituce**.

Z pohledu **uživatelské zkušenosti** je UAE PASS prezentován jako nástroj, který **eliminuje potřebu spravovat více uživatelských účtů pro různé vládní služby** a zároveň **umožňuje právně relevantní digitální úkony**. **Oficiální popis** aplikace od Digital Dubai ji označuje jako „národní řešení digitální identity a elektronického podpisu“, čímž zdůrazňuje její dvojí funkci (identita + podpis), která je klíčová pro plně digitální správní procesy (např. povolení, ověření dokumentů či převody vlastnictví).

## UAE PASS

- **Národní digitální identita doplněná o elektronický podpis** umožňující plně digitální transakce
- Jednotný přístup ke službám napříč veřejným i soukromým sektorem
- Sdílená infrastruktura napříč federální strukturou

## Saúdská Arábie – Absher

Platforma Absher v Saúdské Arábii představuje silný příklad **digitalizace často využívaných a administrativně náročných služeb ministerstva vnitra** (oblast identity a pobytu, služby související s mobilitou, oprávnění, evidence obyvatelstva) **do jednotného ekosystému eGovernmentu**. Absher je na svém oficiálním rozhraní

**popisován** jako platforma poskytující služby ministerstva vnitra občanům, rezidentům i návštěvníkům, dostupná prostřednictvím webu i mobilní aplikace. Také **oficiální popis** e-slужeb saúdského zastupitelského úřadu charakterizuje Absher jako elektronickou platformu Ministerstva vnitra, jejímž cílem je poskytovat služby digitálně „integrováním způsobem“ s **důrazem na spolehlivost, bezpečnost a uživatelskou** přívětivost prostřednictvím automatizovaných procesů.

Jedním z hlavních znaků „dobré praxe“ je zde kombinace šíře služeb a jejich kontinuálního rozšiřování. Zprávy Saudi Press Agency **dokumentují průběžné zavádění nových funkcí Absheru** (např. aktualizace údajů v rodinném registru či další služby evidence obyvatelstva), což ukazuje, že Absher je chápán jako dynamický nástroj poskytování služeb, nikoli statický portál. Dalším důležitým faktorem je rozsah využití. Přehled digitální infrastruktury Ministry of Communications and Information Technology **uvádí** Absher jako jednotnou elektronickou platformu poskytující služby jednotlivcům i firmám a zmiňuje **milióny uživatelů** (např. přibližně 11,5 milionu registrovaných uživatelů), což potvrzuje, že jde o systém s významným dopadem na celostátní poskytování služeb.

Popisy služeb Absheru **zahrnují** mimo jiné možnost zobrazovat oficiální dokumenty v elektronické podobě, což podporuje **odklon od fyzického předkládání dokumentů při běžných úkonech**. Dále **služby jako elektronické zmocnění** (tj. oprávnění jednat jménem jiné osoby) **reflektují** reálné administrativní situace, kdy je potřeba právně jednat za někoho jiného, což je dimenze, která bývá v raných systémech eGovernmentu často nedostatečně rozvinutá.

## Absher

- **Jednotná platforma pro široké spektrum služeb** (zejména agenda ministerstva vnitra)
- Integrace dokumentů, oprávnění a administrativních procesů do jednoho systému
- Kontinuální rozšiřování služeb a vysoký rozsah využití

