DATOVÉ SCHRÁNKY - SOUČÁST ICT ŘEŠENÍ TELEFÓNICA O2

Pavel Smolík
Top Account Manager

Obsah prezentace

Obsah

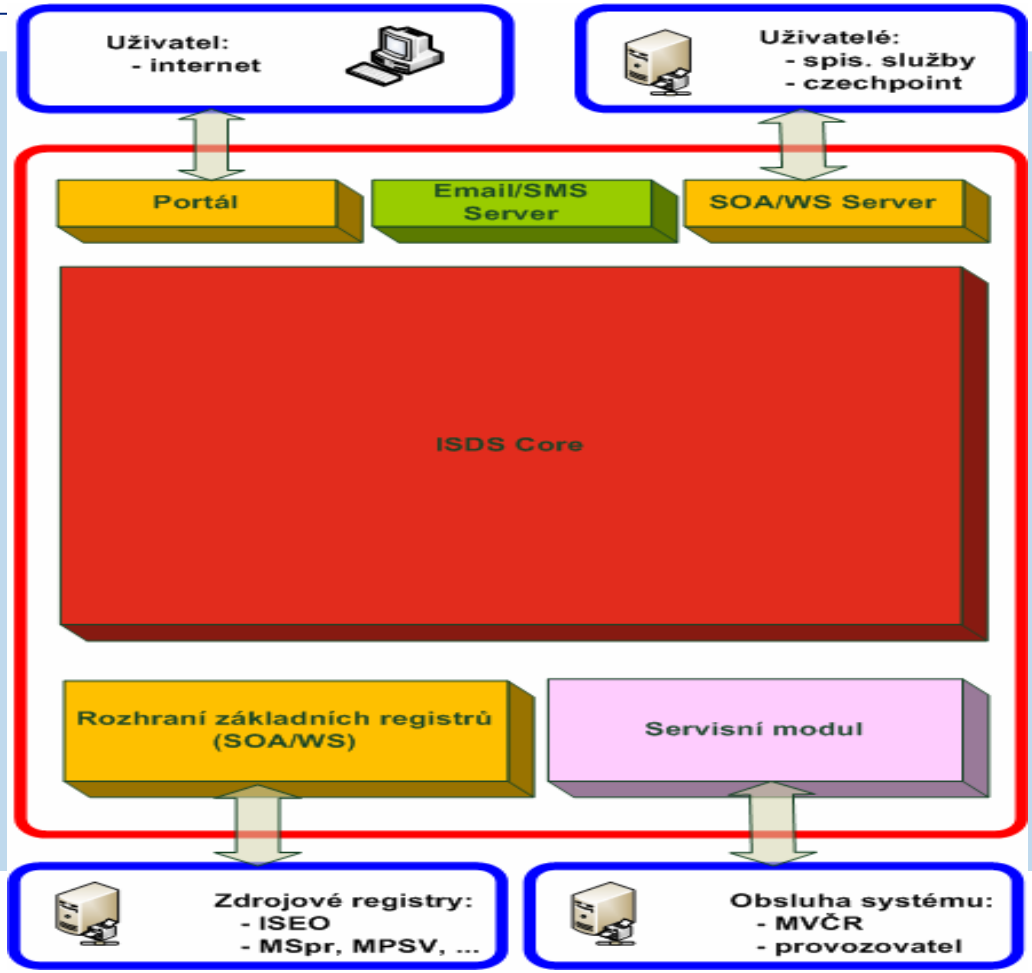
ISDS

- Informační systém datových schránek – ne e-mail, ale komunikační systém s garantovanými vlastnostmi.
- Vznikl na základě soutěže o návrh.
- Návrh byl inspirován následujícími požadavky:
  - Hlavní kritérium – **splnění zákona.**
  - Jedná se o systém, jímž budou procházet citlivé informace, proto důraz na **bezpečnost.**
  - Systém musí být vysoce **dostupný.**
  - Systém musí být uživatelsky přívětivý – **základní komfort**, plánuje se spuštění **doplňkových služeb.**

Návrh řešení splňuje zákonné požadavky

- řešení vychází z dikce zákona č. 300/2008 Sb.,
- zřízení datové schránky zdarma,
- autorizovaný přístup k datové schránce,
- bezpečnost uložených informací,
- komunikace (integrita, důvěrnost),
- uložení datové zprávy (dostupnost, řízení přístupu),
- zajištění životního cyklu datových zpráv včetně evidence a vyrozumění,
- auditovatelnost činností v systému ISDS,
- reporting.

Základní schéma



Parametry

- Robustní architektura.
- Škálovatelnost.
- Otevřenost.
- Bezpečnost.
- Garance vysokých parametrů SLA:
  - redundantní technologie,
  - dedikovaný ServiceDesk,
- Optimální rozhraní pro jednotlivé kategorie uživatelů.

Datová zpráva

- datová zpráva bude mít obecný nebo specifický formát
  - PDF, Doc/Docx, HTML/HTM, XLS, JPG, TIF, PNG, PPT, XML, ODF a další
- obecný formát je určen pro jakýkoliv (povolený) obsah,
- specifické formáty se budou používat pro formuláře (OVM i občané a právnické subjekty),
  - formuláře
- do vlastní zprávy systém ISDS nezasahuje, pouze kontroluje:
  - obálku (vnější datový formát),
  - přítomnost nebezpečného obsahu (antivirová kontrola),
- podpora standardu Moreq 2.

Služby poskytované ISDS

Služby ze zákona a další

- ISDS nabídne všechny služby vyplývající ze zákona,
- úřady budou moci prostřednictvím rozhraní:
  - odesílat zprávy,
  - přijímat zprávy,
  - zjišťovat stavy odeslaných zpráv,
  - přijímat doklady o dodání a doručení,
- úřady mohou měnit některé parametry datové schránky.

Adresáře

- datová schránka je pouze jedna, proto je nezbytné její vnitřní členění (vnitřní adresář),
- úřady samy stanoví členění datové schránky (podřízené úřady, agendy, oddělení apod.),
- formát datové struktury pro adresář bude včas zveřejněn,
- úřady si naplní tento adresář, dále jej pak budou spravovat samy,
- spisové služby budou muset umět pracovat s identifikátory položek adresáře – musí umět rozpoznat cílového adresáta (např. oddělení) a dále s ním pracovat,
- pokud nebude úřadem poskytnut adresář, budou všechny zprávy muset být rozdělovány manuálně.

Služby poskytované ISDS

PostServis

- Co v případě, že adresát nemá datovou schránku nebo tato je nedostupná?
- ISDS bude v budoucnu umět „přeposlat“ zprávu jiným kanálem – listinnou poštou.
- Použity budou služby PostServis.
- Systém převede datovou zprávu do listinné podoby, vloží do obálky a odešle standardní poštou.
- Nelze použít pro všechny typy datových zpráv, pro jednoduchá oznámení ano.
- Systém vrátí úřadu zpět informaci o způsobu doručení včetně doručenek.
- Výhody:
  - jednotná cesta doručování z pohledu úřadu,
  - jednotný systém doručenek (elektronické).

Používání ISDS

Fyzický uživatel

- uživatel si zřídí (nebo mu bude zřízena) datová schránka,
- obdrží přístupové údaje,
- definuje strukturu uživatelů a požádá o přístupové údaje pro pověřené osoby,
- dále si vše (co se týče oprávněných a pověřených osob) určuje sám,
- může měnit oprávnění,
- může si zvolit vyšší formu přístupových údajů,
- po prvním přihlášení je datová schránka zpřístupněna pro doručování.

Architektura ISDS

Portál

- slouží k využívání služeb ISDS fyzickými osobami, ale rovněž administrátory úřadů,
- uživatel vybere formulář a adresáta, systém předvyplní potřebné údaje,
- uživatel vloží zprávu (vlastní data), případně připojí přílohu,
- zprávu bude možné i elektronicky podepsat,
- bude možné prohlížet seznamy:
  - odeslaných zpráv,
  - přijatých zpráv,
  - historii včetně doručenek.
- mohou využívat i úřady.

Používání ISDS

Úřady (+ větší PO)

- oprávněná osoba obdrží přístupové údaje,
- definuje strukturu uživatelů a požádá o přístupové údaje pro definované osoby,
- je vhodné určit administrátora, ten dále definuje vybrané parametry datové schránky,
- administrátor dále spravuje schránku včetně oprávnění uživatelů,
- kromě toho je potřebné nastavit spisovou službu jako uživatele,
- spisová služba bude pro přístup kromě standardních přístupových údajů využívat další speciální přístupové údaje (z důvodů zajištění bezpečnosti),
- po prvním přihlášení je datová schránka zpřístupněna pro doručování.

Architektura ISDS

Rozhraní spisových služeb

- slouží k využívání služeb ISDS spisovými službami,
- je definováno rozhraní pro připojení spisových služeb,
- bude umožněno automatizovaně přijímat a odesílat zprávy včetně elektronicky podepsaných,
- kromě odesílání a přijímání datových zpráv bude možné stahovat seznamy:
  - odeslaných zpráv,
  - přijatých zpráv,
  - historii včetně doručenek,
- odpadnou listinné evidence, vše bude ve spisové službě, resp. podatelně,
- spisová služba musí být ovšem na uvedené připravena …

Bezpečnost ISDS

Požadavky na bezpečnost

- dostupnost systému,
- integrita systému,
- integrita zpráv,
- důvěrnost,
- evidence důkazů (prokazatelnost),
- audit,
- dohled.

Bezpečnost ISDS

Dostupnost systému

- garance vysoké dostupnosti,
- v rámci standardního provozu dostupnost 99,9% (povolený výpadek cca 8 hodin ročně!!!),
- robustní architektura postavená na zdvojení systému,
- automatické rozdělování zátěže,
- dílčí výpadky jsou řešeny bezprostředně za chodu systému,
- geografické rozložení jako prevence proti „zásahům vyšší moci“.

Bezpečnost ISDS

Integrita systému a dat

- integrita systému zajištěna vhodnou architekturou a použitím osvědčených komponent,
- integrita zpráv zajištěna použitím kryptografických komponent,
- použití časového razítka a systémové elektronické značky,
- výhody:
  - žádná zpráva nemůže být změněna bez následků,
  - lze zpětně detekovat, kdy ke změně došlo a kdo ji způsobil,
  - systém kontroluje integritu zprávy vždy před jakoukoliv operací.

Bezpečnost ISDS

Důvěrnost

- komunikační kanály jsou vždy šifrované,
- zprávy jsou v datových schránkách uloženy rovněž v šifrované podobě,
- klíč je pro administrátory nedostupný (princip oddělených rolí),
- použity kvalitní šifrové algoritmy,
- praktické naplnění požadavku zákona – „provozovatel nemá přístup k datům“.

Bezpečnost ISDS

Evidence důkazů

- jsou logovány a podepisovány veškeré události spojené s provozem ISDS,
- logy jsou v pravidelných intervalech označovány časovým razítkem,
- veškeré podstatné informace jsou ukládány v tzv. důvěryhodném úložišti,
- toto úložiště za pomoci kryptografických metod zajišťuje validitu uložených údajů neomezeně dlouho.

Bezpečnost ISDS

Audity, dohled

- dohled pomocí nástrojů i obsluhou (24 x 7 x 365),
- zápisy z dohledu ukládány důvěryhodným způsobem,
- systém bude pravidelně auditován,
- certifikace ISVS.

Doplňkové služby ISDS

Doplňkové služby

- budou implementovány postupně,
- slouží ke zvýšení komfortu a pro řešení specifických situací, např.:
  - prodloužení doby uložení (nemá vliv na doručení!),
  - přesměrování doručení,
  - zasílání extrémně objemných zpráv,
  - nadstandardní způsob doručení do vlastních rukou,


O2
Presentation title
Author's name
12 October 2006
Confidential
A Telefónica company