

Národní distribuce oficiálních dokumentů EU

„IS EU Extranet ČR“

Jiří Truxa, S.ICZ a.s.
06.04.2009, Hradec Králové

Osnova prezentace

- ▶ **Cíl projektu a výchozí stav**
- ▶ **Koncepce řešení**
- ▶ **Základní architektura**
- ▶ **Klíčové vlastnosti**
- ▶ **Bezpečnostní přínosy**
- ▶ **IS EU Extranet 2009 – statistiky**
- ▶ **Problémy při realizaci projektu**

Počáteční cíl projektu

- ▶ **IS který zabezpečí včasnou distribuci oficiálních dokumentů EU :**
 - v elektronickém formátu
 - rozdílným stupněm utajení (PUBLIC, LIMITE, RESTREINT)
 - podle národních pravidel

Požadavky resortů

- ▶ **Zpracování neklasifikovaných dokumentů EU v resortních necertifikovaných IS**
- ▶ **Zpracování klasifikovaných dokumentů EU v resortních certifikovaných IS**
- ▶ **Zpracování utajovaných dokumentů EU v pouze rámci nově vybudovaných akreditovaných uzlů jednotlivých resortů a organizace státní správy**
- ▶ **Možnost napojení na jednotlivé resortní aplikace (rozhrazení pro nadstavbové aplikace)**

Požadavky uživatelů

- ▶ **Po analýze požadavků uživatelů :**
 - národní obousměrná redistribuce připojených dokumentů (podklady, připomínky, odpovědi, stanoviska, ...)
 - zpracování utajovaných dokumentů v rámci stávajících certifikovaných IS resortů a organizace státní správy
 - generování neutajovaných notifikačních zpráv o provedené distribuci utajovaných dokumentů na jednotlivé uživatele

Výchozí stav (leden 2004)

- ▶ **Neexistuje certifikovaný národní IS pro el. distribuci utajovaných dokumentů EU (pouze papír)**
- ▶ **Neexistuje meziresortní komunikační infrastruktura umožňující distribuci utajovaných informací EU**
- ▶ **Různá úroveň schopnosti zpracování utajovaných informací v IS Resortů a organizací státní správy**

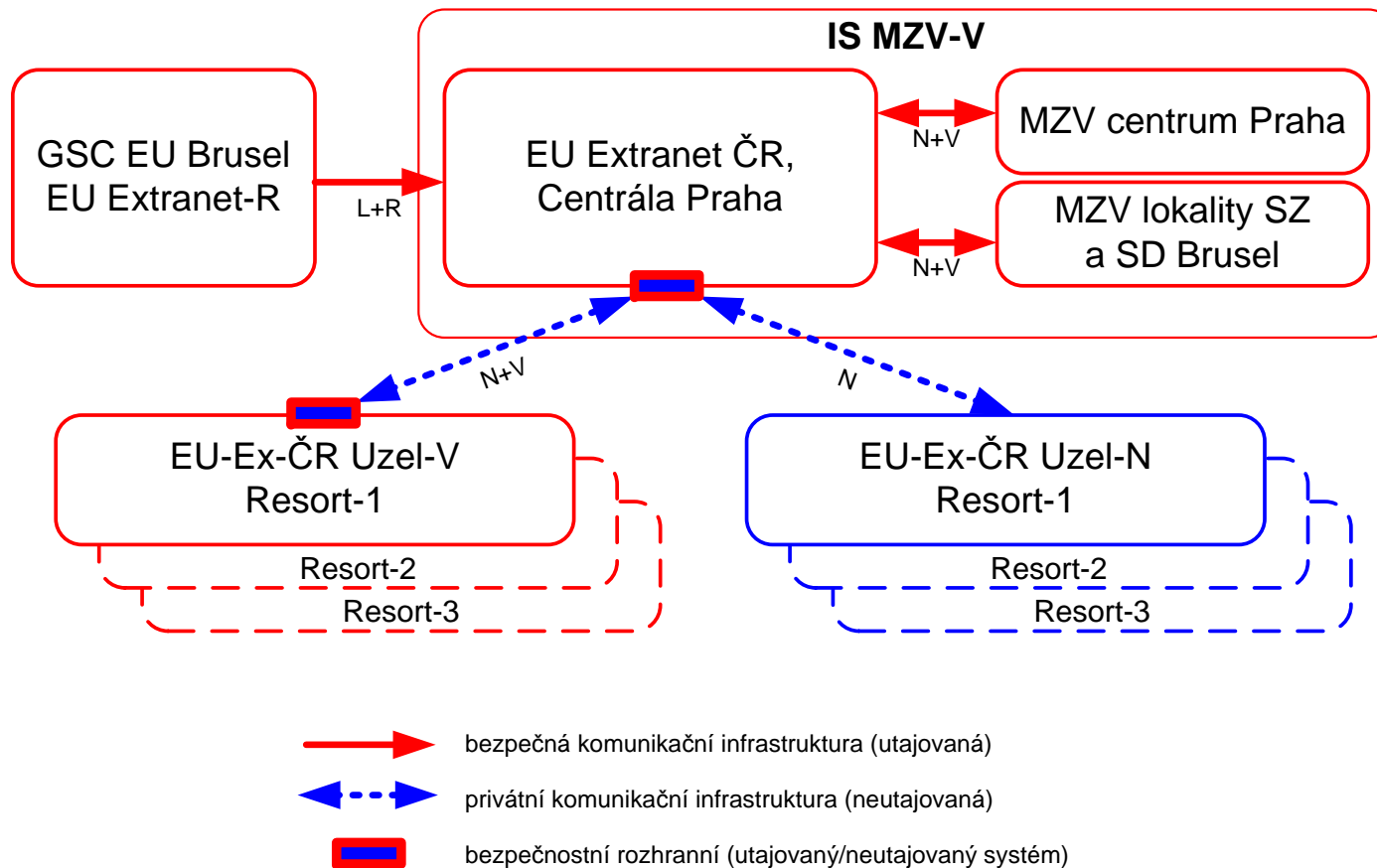
Role v projektu

- ▶ **Zadavatel: MZV ČR**
 - sponzor projektu
 - provozovatel centra
- ▶ **Dodavatel: S.ICZ a.s.**
- ▶ **Komunikační infrastruktura: MV ČR**
- ▶ **Certifikace (hodnotitel): NBÚ ČR**
- ▶ **Jednotlivé resorty a organizace státní správy**
 - sponzor implementace uzlů
 - provozovatel uzlu

Koncepce řešení

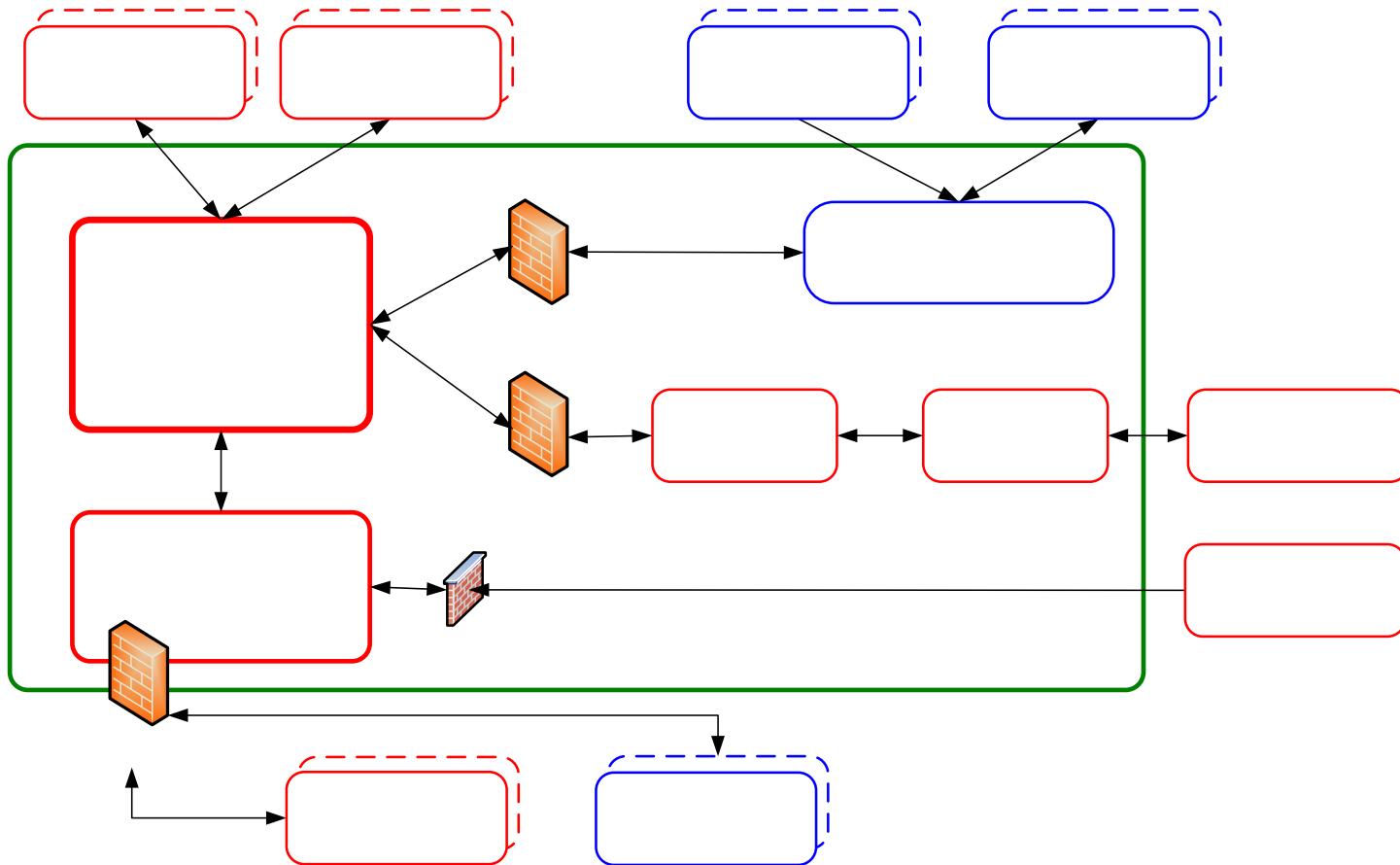
- ▶ **Centrum součástí certifikovaného IS MZV**
- ▶ **Jedno společné centrum pro utajované („V“) i neutajované („N“) resortní uzly**
- ▶ **Privátní komunikační infrastruktura pro komunikaci (pouze neutajované informace)**
- ▶ **Jednotná distribuovaná aplikace a jednotné integrační rozhraní**
- ▶ **Generická řešení vzdálených uzlů (neutajovaný i utajovaný uzel)**

Obr.1 - Jednoduché schéma koncepce řešení



IS MZV-V

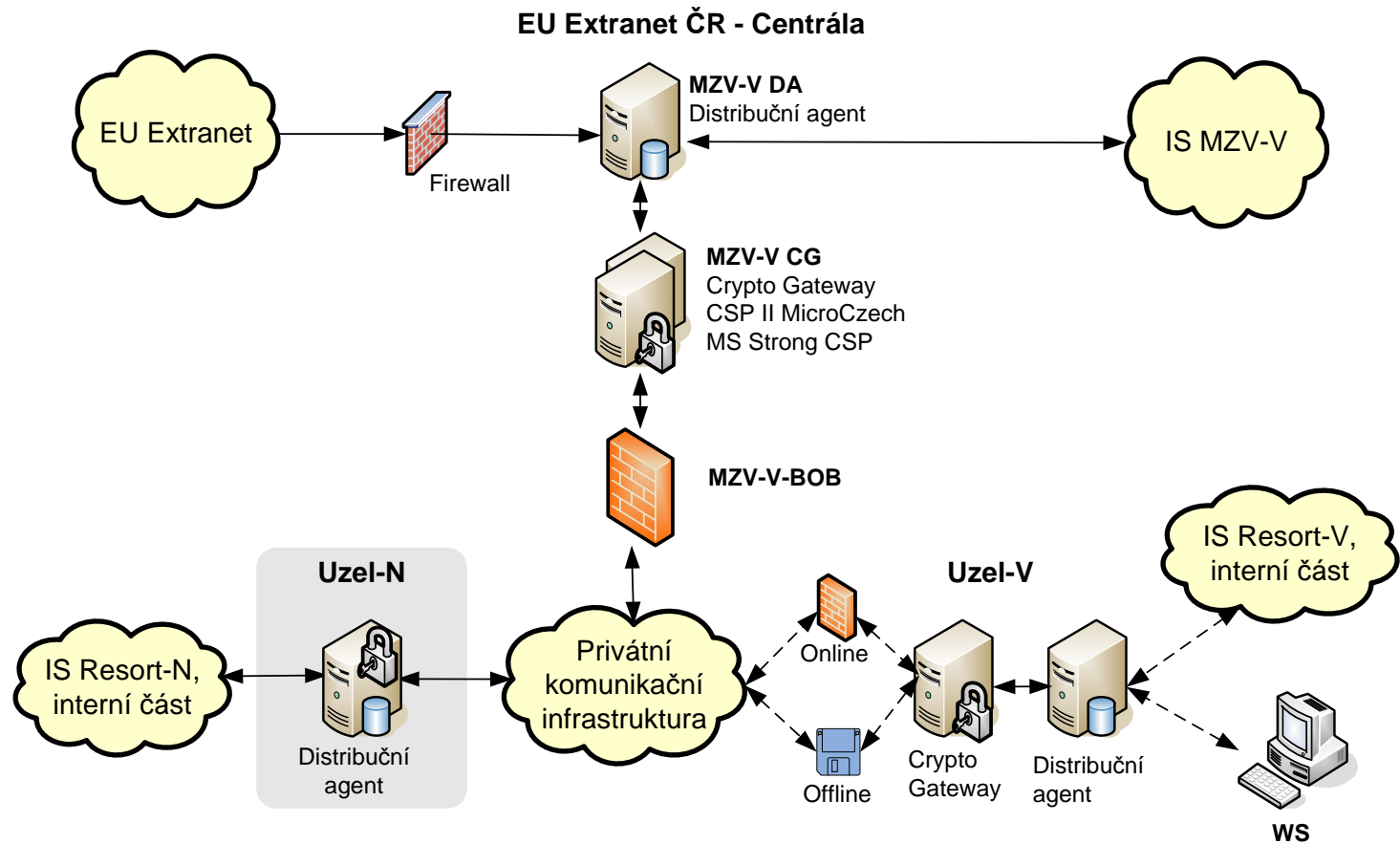
- ▶ **Certifikovaný utajovaný systém pro („V“)**
- ▶ **Primární (hlavní) IS pro pracovníky MZV**
- ▶ **Rozlišuje klasifikaci informací („N“ a „V“)**
- ▶ **Rozlišuje informační kategorie (ČR, EU, NATO)**
- ▶ **Lokality Praha a Brusel**
- ▶ **Celkem cca 1000 uživatelů**
- ▶ **Bezpečné napojení na jiné IS (certifikované i necertifikované)**



Základní architektura (vysoká míra bezpečnosti)

- ▶ **Jednotná distribuovaná aplikace „Distribuční Agent“**
- ▶ **Jednotná aplikace pro zajištění komunikační bezpečnosti „Crypto Gateway“**
- ▶ **Jednotné bezpečnostní rozhraní oddělující centrálu („V“) od resortních uzlů („N“ nebo „V“) „Bezpečnostní Oddělovací Blok“**

Obr.3 - jednoduché schéma architektury



Klíčové vlastnosti řešení

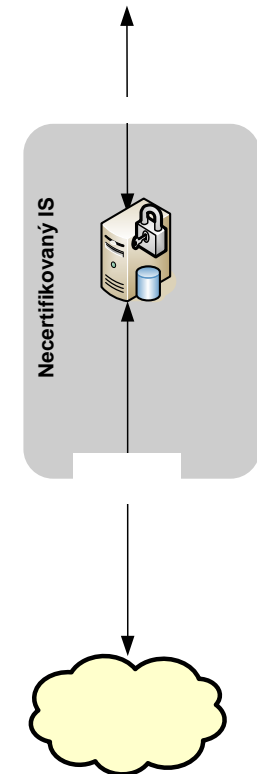
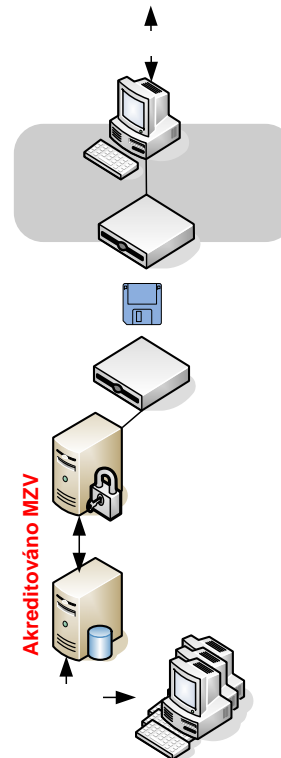
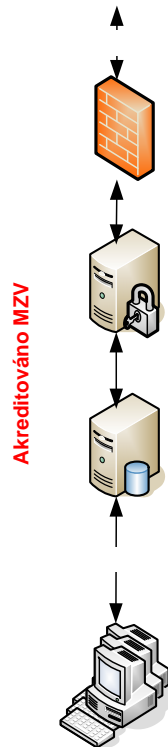
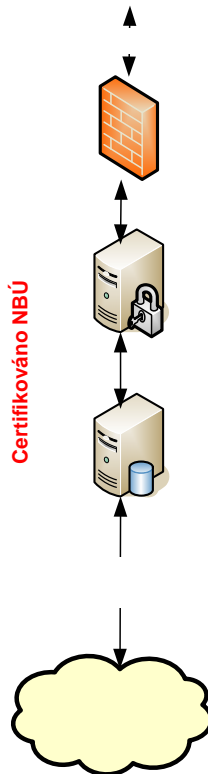
- ▶ **Jeden IS pro všechny stupně utajení (jednotná aplikace, jednotná báze dat)**
- ▶ **Distribuce dokumentů z Centra do dvou bezpečnostních domén „V“ a „N“ (resortních uzlů rozdílné bezpečnosti)**
- ▶ **Nadřazený IS EU Extranet-R je pouze jeden ze vstupů (import dokumentů)**
- ▶ **Národní IS s rozšířenou funkcionalitou (národní distribuční pravidla, obousměrný datový tok, rozšířená funkcionalita jako připojený dokument)**
- ▶ **Vysoká míra odolnosti a imunity mezi jednotlivými částmi systému (centrum, uzly) – vysoká míra bezpečnosti celého IS (reálný rozsáhlý certifikovaný systém)**

Bezpečnostní přínosy

- ▶ **Nezávislá akreditace jednotlivých uzlů**
- ▶ **Nezávislost na bezpečnosti meziresortní komunikační infrastruktury**
- ▶ **Minimalizace bezpečnostně významných administrátorských operací na vzdálených uzlech**
- ▶ **Vyloučení potřeby zavádět pracovníky kryptografické ochrany pro generické uzly**

Vzdálené uzly

- ▶ **Generický uzel „V“ s OffLine rozhraním (vzdálený uzel MZV)**
- ▶ **Generický uzel „V“ s OnLine rozhraním (vzdálený uzel MZV)**
- ▶ **Resortní IS („N“, „V“) s OnLine rozhraním (vlastní resortní IS)**



Resor
Generické rozhraní

IS EU Extranet ČR 2009

- ▶ **Počet uživatelů celkem**
 - počet uživatelů na centru: 682
 - počet uživatelů na uzlech: 763
- ▶ **Počet neutajovaných uzlů**
 - počet uzlů: 34
- ▶ **Počet vyhrazených uzlů**
 - generických offline: 18
 - generických online: 2
 - certifikovaných online: 1
- ▶ **Počet distribučních pravidel**
 - počet pravidel: 1144

IS EU Extranet ČR 2009

- ▶ **Průměrná doba doručení dokumentu do**
 - neutajovaných uzlů (online): 3 – 35 minut
 - generických uzlů offline: cca 60 minut
 - generických nebo certifikovaných uzlů online: 6 – 23 minut

- ▶ **Počet dokumentů v roce 2009**
 - PUBLIC distribuováno: 6794
 - LIMITE distribuováno: 3312
 - RESTREINT distribuováno: 608

Klíčové vlastnosti pro uživatele

- ▶ **Notifikace distribuce utajovaných dokumentů („V“) jednotlivým příjemcům do resortních neutajovaných uzlů („N“)**
- ▶ **Možnost ruční redistribuce dokumentu dle potřeby gestora (na centrále i resortních uzlech)**
- ▶ **Možnost připojení národního dokumentu gestorem (na centrále i resortních uzlech)**

Problémy při realizaci projektu

- ▶ **Vyšší nároky (složitost) pro distribuované aplikace**
- ▶ **Zpoždění při doručování dokumentů do offline uzlů**
- ▶ **Notifikace distribuce utajovaných dokumentů jednotlivým příjemcům**
- ▶ **Požadavky na klíčové komponenty s ohledem na proces bezpečnostního hodnocení**

Děkuji za vaši pozornost



Jiří Truxa
jiri.truxa@i.cz

S.ICZ a.s.
www.i.cz