Název projektu:
Redesign Statistického informačního systému v návaznosti na zavádění eGovernmentu v ČR
Příjemce: Česká republika – Český statistický úřad
Registrační číslo projektu: CZ.1.06/1.1.00/07.06396

Příloha k zadávací dokumentaci veřejné zakázky „Integrační nástroje, vstupní a výstupní subsystém“

Příloha č. 12

Systém společného přihlašování, tzv. Single Sign On, ochrana dat

Název souboru: RSIS_ZD001P12_SSO.pdf
Počet stran přílohy (bez tohoto krycího listu): 4
Administrace přílohy: Ing. Vladimír Holý

Verze ke zveřejnění

Systém společného přihlašování, tzv. Single Sign On, ochrana dat

Úvod

1 | V rámci VŘ projektu IOP – Redesign SIS (subsystémy: SMS, CENTRAL a systém integrace všech věcných zakázek) se požaduje:

A. Technická specifikace pro ZŘ Redesign SIS- požadavky na jednotné přihlašování uživatelů (SSO)

2 | U ČSÚ je v současné době provozován systém správy identit (dále pouze IdM), který je vybudován pomocí technologie Novell® Identity Manager® (dále NIM) na adresářové službě eDirectory a vyhovuje požadavkům LDAP X500. Základem tohoto systému je tzv. trezor identit (dále TI), který je z důvodů průběžného získávání dat o zaměstnancích a jejich pracovních vztazích propojen s personálním informačním systémem ODYSEA – při nástupu nového zaměstnance ČSÚ je účet v eDirectory vytvořen automaticky a při odchodu zaměstnance ČSÚ je účet automaticky zneplatněn/zrušen.

3 | Pro potřeby intranetového portálu ČSÚ je v současné době provozována adresářová služba Oracle Internet Directory (dále OID), která slouží jako repository uživatelských účtů pro Single Sign On (Oracle SSO 10 g, Oracle portál). Tuto službu OID využívají též některé Oracle Forms aplikace – uživatelské účty v OID jsou spravovány manuálně a bez jakékoliv vazby na TI (např. při odchodu zaměstnance ČSÚ je účet deaktivován správcem OID na základě informace z personálního oddělení).

4 | V rámci rozvoje IdM je vyvíjeno úsilí k integraci NIM se službou OID s cílem vybudovat v ČSÚ komplexní systém, který umožní propojit TI s vybranými aplikacemi a umožnit uživateli zavedenému v personálním informačním systému (ODYSEA) se přihlašovat při spuštění PC do příslušných aplikací pouze jednou (pomocí jednoho hesla) a zajistit tak spolehlivé a bezpečné ukládání informací o identitách ve všech systémech/aplikacích ČSÚ. Tzn cílem rozvoje IdM je zajistit kontrolované, rychlé, pružné a spolehlivé propůjčování dat o identitách určeným navázaným databázím, adresářům nebo aplikacím (systémům) tak, aby se uživatelské účty v provozních systémech vytvářely, upravovaly a rušily automaticky, případně na základě schválení příslušných odpovědných pracovníků ČSÚ.

5 | V rámci poptávaného díla se požaduje vytvořit systém společného přihlašování, tzv. Single Sign On (dále jen SSO), který **bude integrován s již provozovaným systémem NIM (Novell Identity Manager version 3. 5. 1**.) a OID (Oracle SSO, Oracle portál), který je v ČSÚ používán ke správě identit interních uživatelů. Systém bude pracovat na základě vstupů z interního personálního systému ČSÚ (dále jen „PIS“).

6 | Vzhledem k tomu, že se v rámci dodávaného díla počítá se vznikem nové množiny externích uživatelů, kteří budou přistupovat k externě přístupným rozhraním statistického informačního systému, je nutno v rámci dodávaného díla zajistit rozdělení správy uživatelů, tzn. **rozšíření o SW aplikaci** určenou jak ke správě interních tak nově ke správě externích uživatelů.

Pro splnění tohoto cíle je nutné:

- Provést analýzu prostředí ICT ČSÚ (zaměření na realizaci konektoru mezi provozovaným systémem NIM, OID a aplikačním programovým vybavením Redesing SIS;
- Zpracovat návrh a odsouhlasit finální podobu datového modelu (ve spolupráci s pracovníky správy ICT a bezpečnostními pracovníky ČSÚ);
- Definovat požadavky na funkčnost vzhledem k datovému modelu;
- Zpracovat prvotní návrh integrace NIM a OID a aplikací určených ke správě interních a externích uživatelů;
- Vytvořit první funkční verzi aplikace určené ke správě externích uživatel;
- Provést pilotní ověření funkčnosti aplikace ke správě externích uživatelů (ve spolupráci s pracovníky správy ICT a bezpečnostními pracovníky ČSÚ);
- Zpracovat požadavky na změny, customizace;

- Integrovat stávající systém NIM a OID s aplikačním programovým vybavením Redesing SIS, konsolidovat hesla mezi adresářovými službami buď synchronizací nebo pomocí autentizačního OID paginu.

7 | Rámcovou představu o implementaci přístupového portálu pro přihlašování uživatelů prostřednictvím funkcionality SSO představuje Technická specifikace pro Přístupový portál SMS, viz příloha č. 33 („*RSIS_ZD001P33_SMS_TP_PRISTUPOVY_PORTAL*“). Dokument specifikuje základní návrh pro implementaci přístupového portálu pro aplikace SMS (KLAS, UKAZ, ULOHY) s využitím funkcionality SSO v Oracle Protal.

B. Kategorie dat dle citlivosti

8 | Pro účely definice požadavků na úroveň ochrany dat spravovaných a používaných ČSÚ jsou definovány jednotlivé kategorie dat takto:

- Veřejná data – jedná se o ostatní statistické informace a anonymní data;
- Důvěrné statistické informace – důvěrné statistické informace dle Zákona 89/1995 Sb., o státní statistické službě;
- Citlivá data – jedná se o citlivá data dle §4 odst. b) Zákona č. 101/2000 Sb., o ochraně osobních údajů.

C. Požadavky na ochranu dat

Obecná pravidla

9 | Pro všechny ICT systémy zpracovávající statistická data (anonymní, důvěrná, citlivá) musí být dodržena následující pravidla:

- Přístup k systému umožňující změny dat musí být chráněn alespoň uživatelským jménem a heslem;
- Každý uživatelský účet musí být přiřazen konkrétní osobě, aby bylo možné identifikovat autora změn;
- Přístupová práva musí být nastavena tak, aby změny nemohl provádět neoprávněný uživatel;
- Pro změny dat je nutné logovat datum, čas a autora změny;
- Veškerá data mají definovaného vlastníka a správce, který je zodpovědný za jejich správnost a aktuálnost.

Pravidla pro důvěrné statistické informace

10 | Pro tuto kategorii dat platí všechna obecná pravidla:

Navíc je nutné dodržet:

- Přístup k systému musí být chráněn alespoň uživatelským jménem a heslem;
- Změny dat je nutné logovat tak, aby byl k dispozici datum, čas, autor a typ změny;
- Přístupová práva musí být nastavena tak, aby uživatel mohl pracovat pouze s daty, která potřebuje pro svou práci;
- Přidělení oprávnění pro změny dat schvaluje vlastník dat (informačního aktiva);
- Přenosy dat mezi datovým úložištěm a uživatelem musí být zabezpečeny proti neoprávněnému odposlechu nebo zfalšování;
- Doporučuje se metoda šifrování komunikačního kanálu.

Pravidla pro citlivá data

11 | Pro citlivá data je nutné dodržet veškerá pravidla, která platí pro důvěrné statistické informace.

Navíc je nutné dodržovat:

- Přidělení oprávnění pro čtení dat schvaluje vlastník dat;
- Správce systému nemá přístup k citlivým datům;

- Zálohy dat nesmí umožnit neoprávněný přístup k datům, doporučuje se šifrování dat v datovém úložišti, případně šifrování záloh;
- Veškeré přístupy k datům (i čtení) musí být logované, pro změny dat je nutné zaznamenat i původní a novou hodnotu;
- Datová komunikace mezi jednotlivými datovými zdroji musí být zabezpečena proti neoprávněnému odposlechu nebo zfalšování. Doporučuje se metoda šifrování komunikačního kanálu.

Aplikace pravidel ochrany dat

Platnost pravidel:

12 | Pravidla ochrany dat v prostředí ČSÚ musí být respektována všemi nově zaváděnými systémy. Pro existující systémy musí být vytvořen plán, který stanoví postup úprav daného systému tak, aby v budoucnu vyhovoval této koncepci. Plán musí být schválen bezpečnostním manažerem ČSÚ.

Doporučení pro aplikaci pravidel:

- Přístup k systému umožňující změny dat musí být chráněn alespoň uživatelským jménem a heslem;
- Všechny aplikace, které umožňují měnit data, musí realizovat ověření pomocí uživatelského jména a hesla;
- Každý uživatelský účet musí být přiřazen konkrétní osobě, aby bylo možné identifikovat autora změn. Doporučuje se napojení aplikací a databází na adresářovou službu obsahující záznamy všech interních i externích uživatelů. Tím bude jednoduchým způsobem zaručena identifikovatelnost jednotlivých uživatelů;
- Přístupová práva musí být nastavena tak, aby změny nemohl provádět neoprávněný uživatel. Realizace přístupových práv by měla být na všech úrovních, tedy i na úrovni databáze;
- Aplikace musí předávat informace o koncovém uživateli databázi. Tím se zajistí ochrana dat i při přístupu k datům přes jiné nástroje, než je k tomu určená aplikace;
- Pro změny dat je nutné logovat datum, čas a autora změny. Vhodnou metodou realizace je audit na úrovni databáze. Je možné využít standardní databázový audit nebo novější metodu fine grained audit;
- Veškerá data mají definovaného vlastníka a správce, který je zodpovědný za jejich správnost a aktuálnost. Toto pravidlo je nutné aplikovat především procesně organizačním opatřením;
- Na úrovni aplikací a databází má vlastník/správce dat nejvyšší práva pro práci s těmito daty;
- Přístup k systému musí být chráněn alespoň uživatelským jménem a heslem;
- Všechny aplikace musí realizovat ověření pomocí uživatelského jména a hesla;
- Změny dat je nutné logovat tak, aby byl k dispozici datum, čas, autor a typ změny. Vhodnou metodou realizace je audit na úrovni databáze. Je možné využít standardní databázový audit nebo novější metodu fine grained audit;
- Přístupová práva musí být nastavena tak, aby uživatel mohl pracovat pouze s daty, která potřebuje pro svou práci. Doporučuje se realizovat omezení nejen na tabulky a sloupce, ale též omezení na řádky;

  To například znamená, že pracovník zodpovědný za údaje určitého regionu bude v dané tabulce smět pracovat pouze s daty příslušnými k tomuto regionu. Ostatní data mu zůstanou skryta. Vhodnými prostředky jsou například Oracle Virtual Private Database nebo Oracle Label Security;
- Přidělení oprávnění pro změny dat schvaluje vlastník dat. Jedná se především o procesní a organizační opatření;
- Přenosy dat mezi datovým úložištěm a uživatelem musí být zabezpečeny proti neoprávněnému odposlechu nebo zfalšování. Doporučuje se metoda šifrování

komunikačního kanálu. Vhodným způsobem ochrany je aplikace SSL šifrování, případně symetrického šifrování pro Oracle Net protokol, které je součástí Oracle Advanced Security;

- Přidělení oprávnění pro čtení dat schvaluje vlastník dat. Jedná se především o procesní a organizační opatření;
- Správce systému nemá přístup k citlivým datům. Toto opatření zabezpečuje data před zneužitím práv správce systému. Vhodným prostředkem pro realizaci tohoto opatření je Oracle DB Vault;
- Zálohy dat nesmí umožnit neoprávněný přístup k datům, doporučuje se šifrování dat v datovém úložišti, případně šifrování záloh;
- Pro šifrování citlivých dat je vhodné využít prostředků databáze – Transparent Data Encryption. Tento modul databáze zajistí zašifrování určených sloupců nebo celých tablespaců. Tím je zajištěna ochrana dat při neoprávněném přístupu k datovým souborům databáze;
- Veškeré přístupy k datům (i čtení) musí být logované, pro změny dat je nutné zaznamenat i původní a novou hodnotu. Pro záznam a čtení je vhodné použít standardní databázový audit, případně Fine Grained Audit. Pro ukládání dat změny (stará a nová hodnota) je vhodné realizovat logování pomocí trigerů, kdy jsou změny zaznamenávány do logovacích tabulek;
- Datová komunikace mezi jednotlivými datovými zdroji musí být zabezpečena proti neoprávněnému odposlechu nebo zfalšování. Doporučuje se metoda šifrování komunikačního kanálu. Vhodným způsobem ochrany je aplikace SSL šifrování, případně symetrického šifrování pro Oracle Net protokol, které je součástí Oracle Advanced Security;
- Pro přenos dat se nedoporučuje metoda pracovních souborů v čitelném tvaru. Doporučovaná metoda je využití ETL nástrojů pracujících s daty přímo v databázích.

13 | Pravidla ochrany dat v prostředí ČSÚ musí být respektována všemi nově zaváděnými systémy.