CASE STUDY

# IDENTITY MANAGEMENT PRO ČEZ ICT SERVICES

Společnost ČEZ ICT Services je součástí Skupiny ČEZ a patří mezi poskytovatele ICT služeb pro Skupinu ČEZ i jiné subjekty. V souvislosti s expanzivní politikou společnosti ČEZ se podílí na konzultačních a integračních řešeních v tuzemsku i v zahraničních destinacích, a to od návrhu jejich designu až po jejich praktickou implementaci.

ČEZ ICT Services spravuje řádově stovky aplikací a systémů pro zákazníky ze Skupiny ČEZ. Každá aplikace obsahuje velké množství uživatelů, jejich atributů a velké množství aplikačních rolí. Některé systémy využívají i autentizační předměty jako jsou přístupová karta či RSA token. Každý systém obsahuje jinou skupinu i strukturu uživatelů, používá různé atributy u uživatelů a různé aplikační role pro řízení oprávnění. Vzhledem k tomu, že zaměstnanec dostává oprávnění napříč několika systémy, správa všech systémů byla finančně náročná, neefektivní, pomalá a bezpečnostně nevyhovovala stanoveným požadavkům. Situace vyžadovala integraci správy systémů, uživatelských účtů a rolí a standardizaci procesů a pravidel s tím spojených.

## VÝCHOZÍ STAV

- Náročné a neefektivní udržování uživatelských účtů ve více než 100 informačních systémech
- Hrozba existence „spících účtů“
- Různá hesla pro jednotlivé systémy
- Více než 100 000 rolí a oprávnění, 20 000 uživatelských účtů a z toho vyplývající vysoká náročnost dalšího rozšiřování IT

## CÍLE PROJEKTU

Hlavním cílem integračního projektu Identity Management bylo zajistit jednotnou a centralizovanou správu uživatelských účtů a rolí na jednotlivých systémech používaných ve Skupině ČEZ a spravovaných společností ČEZ ICT Services. Tento záměr byl splněn implementací aplikace Sun Java System Identity Manager, který řídí připojené koncové systémy (SAP, MS Active Directory, Oracle Portal a další) a udržuje tak všechny uživatelské účty konzistentní a v souladu s autoritativními zdroji dat (SAP HR, Databáze externích uživatelů).
Dalším cílem projektu bylo zajistit řízení rolí, proces žádosti o role pomocí aplikace Service Desk s výběrem rolí z registru, schvalování přidělení rolí maticí schvalovatelů a auditovatelnost všech změn.
Posledním cílem projektu bylo zjednodušení práce koncových uživatelů a implementace jednotného přihlášení

## POŽADAVKY NA ŘEŠENÍ

- Jednotná a centralizovaná správa uživatelských účtů a rolí
- Větší bezpečnost procesů správy identit a rolí
- Zjednodušení správy požadavků pro nadřízené, zaměstnance a operátory Service Desku

do vybraných aplikací. Po přihlášení do Microsoft Active Directory je tedy uživatel automaticky přihlášen i do ostatních systémů, ve kterých má účet.

## ŘEŠENÍ

Po důkladné analýze bylo navržené centralizované řešení a implementace Sun Java System Identity Manager, který získává data z autoritativního systému SAP HR (přes rozhraní SAP XI) a dále je propaguje (případně zpracovává a propaguje) na ostatní připojené systémy. Pro připojení systémů byly použity standardní adaptéry (SAP, Oracle Portal, RSA SecurID, NDS Novell a další), na kterých byly některé funkcionality doimplementovány v J2EE, a Scripted JDBC adaptéry (AIX, RedHat, Passport), kde byly všechny funkcionality kompletně naprogramovány. Některé systémy (MS AD, NDS Novell, RSA) vyžadují Sun Gateway, která se instaluje k připojovanému systému a zprostředkovává komunikaci mezi Identity Managerem a koncovým systémem. Identity Manager vytváří jednotnou databázi virtuálních účtů všech zaměstnanců s jednotným souborem atributů k nim přiřazených. Na tyto účty jsou pak napárovány účty na jednotlivých koncových systémech a pomocí nich jsou spravovány. Vznik, update i zánik uživatelských účtů na jednotlivých koncových systémech je tak zabezpečen z jedné aplikace (Identity Manager) a jednotným procesem správy. Tento proces je charakterizován různými schvalovacími workflow, které jsou definovány v Identity Manageru. Veškeré procesy jsou pak auditované a je možné je reportovat.
Na požadavek zákazníka byla do Identity Manageru doimplementována funkčnost žádostí, přidělení a správy rolí a oprávnění. Role se spravují v aplikaci BCRR (aplikace interně vyvinutá zákazníkem), odkud

## POPIS ŘEŠENÍ

- Centrální administrace uživatelů založená na produktu Sun Java System Identity Manager
- Implementace automatizovaných workflow
- Vývoj nových adaptéru pro komunikaci s koncovými systémy
- Implementace centrální Password Policy a historie hesel

ami

**KONTAKTUJTE NÁS**

AMI Praha a.s., Pláničkova 11, 162 00 Praha 6
Telefon: +420 274 783 239 | E-mail: obchod@ami.cz | Web: www.ami.cz

## SUN IDENTITY MANAGER

- Produkt vyvíjen od roku 2003
- Rozvoj produktu na základě požadavků trhu
- Postavený na otevřené platformě J2EE
- Nejpoužívanější produkt pro správu identit v České republice

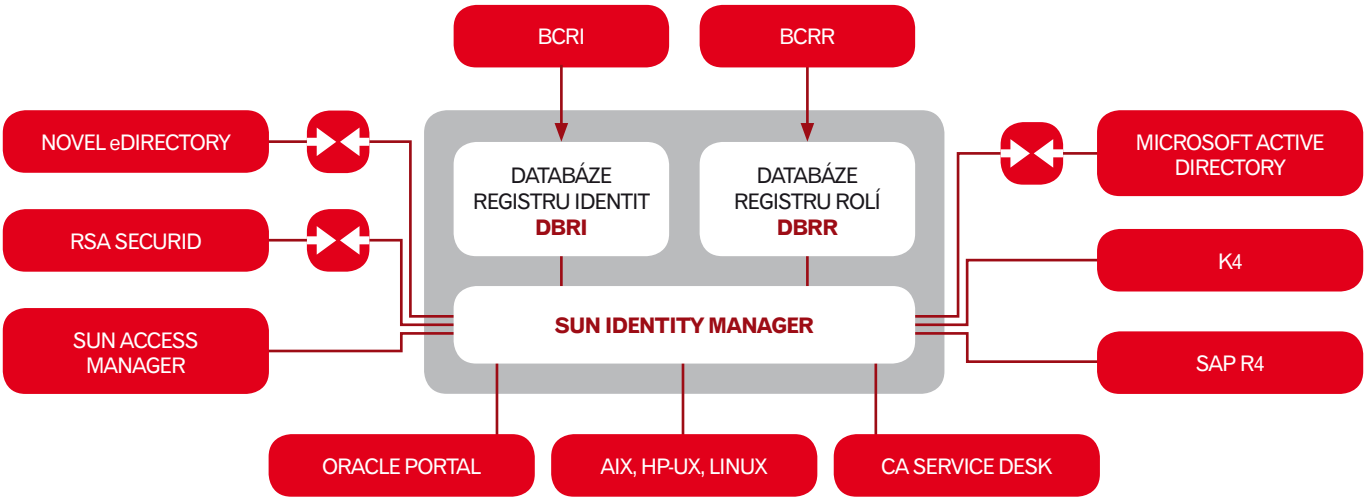
si je načítá Identity Manager a přiřazuje je jednotlivým uživatelům. Jsou využívány role aplikační (přiděluje určité oprávnění), login role (přiděluje přístup k systému) a business role(sdružují několik rolí dle požadavků businessu). O tyto role může žádat jak příslušný zaměstnanec, tak jeho nadřízený napříč všemi připojenými systémy. Vlastností role může být časové omezení a může nést i licenci. Povinnou součástí definice role je matice schvalovatelů. Proces přidělení role je podmíněn jejím schválením, a to dle workflow na několika úrovních (např. licence, metodik, nadřízený, správce systému). Veškeré schvalování probíhá přímo v aplikaci Identity Manager a přidělení i schvalování rolí je auditované a zároveň je přenášeno do aplikace ServiceDesk, kde je žádost iniciována a sledována.
V projektu byla implementována centrální politika a historie hesel, která centrálně hlídá sílu a platnost hesel, vynucuje jejich změnu a posílá informace uživatelům. Zde byl kladen velký důraz na kvalitní šifrování hesel při jejich přesunu i uložení.
Kvůli velkému množství hesel a bezpečnostním standardům byla v rámci projektu řešena i problematika jednotného přihlášení (Single Sign-On). Primárně se jednalo o samotné IdM pomocí aplikace Access Manager od společnosti Sun Microsystems, pro systémy SAP, SAP Portal a Oracle Portal byly použity Kerberos tickety. Pro Identity Manager byly zvoleny 2 politiky přihlašování – do uživatelského rozhraní byla použita jednofaktorová autentizace, která probíhá ověřením jména a hesla v MS Active Directory a využívá jednotné přihlášení (SSO). Do administračního rozhraní byla využita dvoufaktorová autentizace, která probíhá ověřením jména ze systému RSA SecurID a tzv. passcode a následně hesla z Microsoft Active Directory.

## O SPOLEČNOSTI AMI PRAHA A PARTNERECH REALIZACE

Projekt byl realizován a řízen specialisty společnosti AMI Praha a.s. a ČEZ ICT Services, a. s. Partner Sun Microsystems dodal projektové know-how a zaštítil realizaci zkušeným IT architektem. K vývoji některých funkcionalit přispěly společnosti Avnet a Profinit. Významnou část vývoje v oblasti registrů identit a rolí zajistila ČEZ ICT Services, a.s.
AMI Praha a.s. je softwarová společnost poskytující komplexní služby v oblastech podnikových IT řešení a internetu. Je členem Asociace BIZ a partnerem společností Adobe Systems, Asseco Solutions, Oracle a Sun Microsystems. Společnost je držitelem certifikátů pro řízení jakosti dle normy ISO 9001:2001 a pro řízení bezpečnosti informací dle normy ISO 27001:2006.

## PŘÍNOSY PRO ZÁKAZNÍKA

- Automatické akce a kontroly zvyšující bezpečnost
- Jednotný proces správy uživatelských účtů a rolí
- Auditovatelnost změn a žádostí
- Jednotná politika hesel
- Jednotné přihlášení napříč systémy
- Zjednodušení práce pro operátory Service Desku
- Jednotná data uživatelů ve všech systémech




**KONTAKTUJTE NÁS**

AMI Praha a.s., Pláničkova 11, 162 00 Praha 6
Telefon: +420 274 783 239 | E-mail: obchod@ami.cz | Web: www.ami.cz