Data Protection Delivery Center, s. r. o.

IDENTITY MANAGEMENT,

SPRÁVA OPRÁVNĚNÍ

a SINGLE SIGN-ON

pro Vaši bezpečnost

DPDC Identity

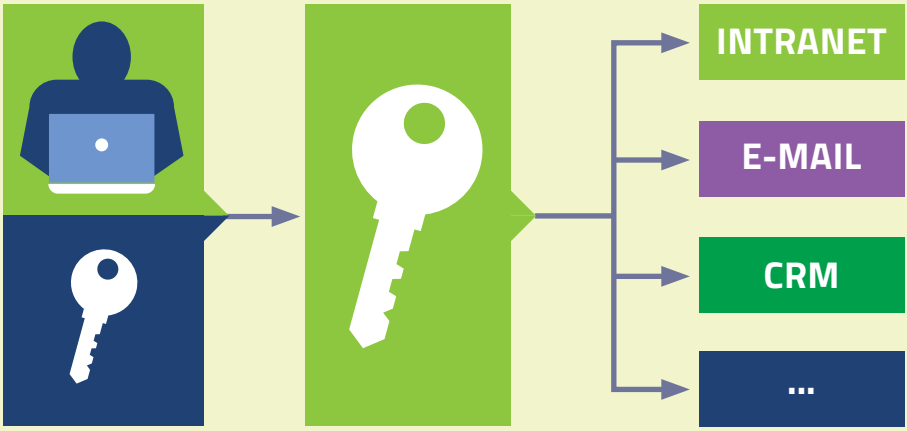
DPDC Identity

DPDC Identity je komplexním řešením pro automatizovanou správu a audit uživatelských oprávnění (IDM - Identity Management) a pro jednotné přihlašování uživatelů (SSO - Single sign-on).

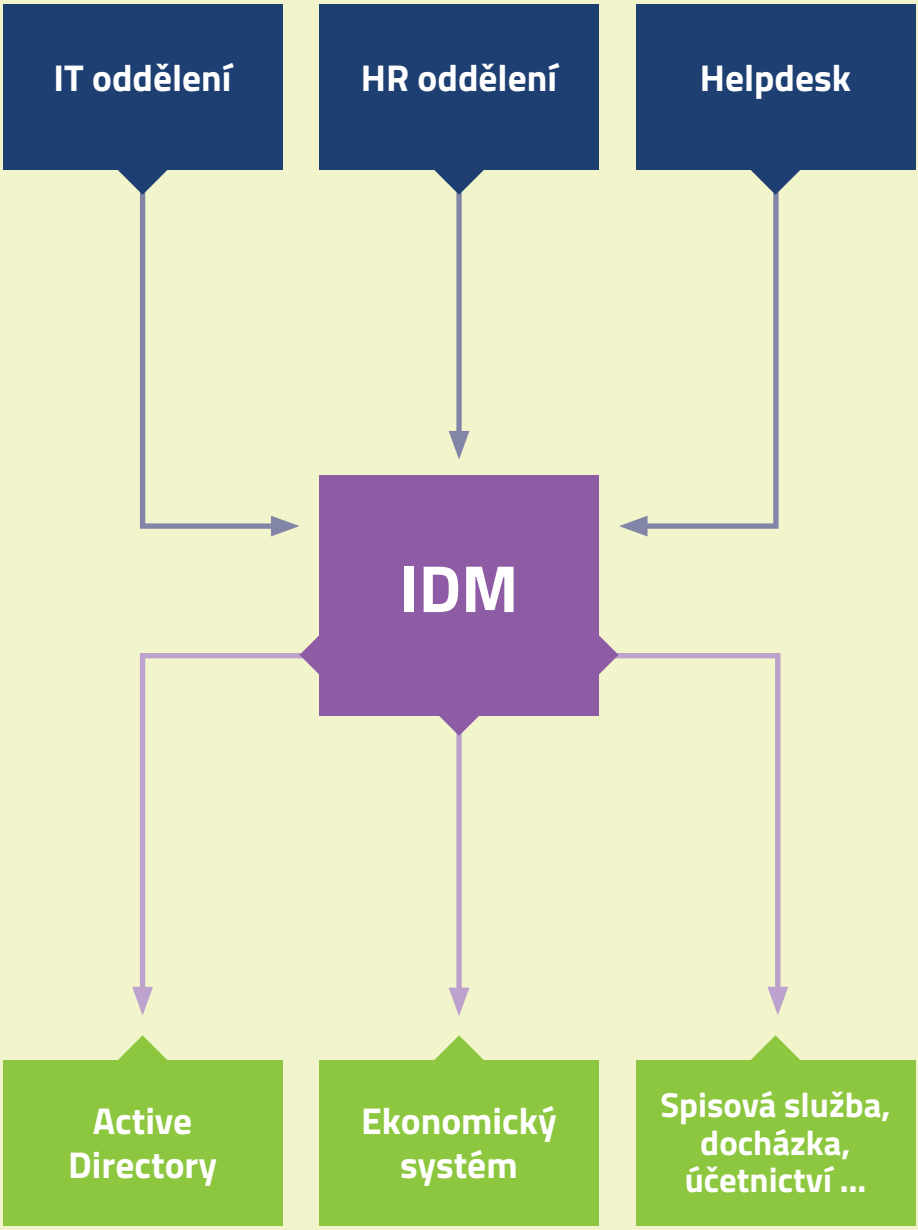
Cílem implementace služby DPDC Identity je zprovoznění integrovaného řízení přístupu k informacím, což ve výsledku vede k zefektivnění vnitrofiremních informačních toků, k eliminacím bezpečnostních rizik úniku a zneužití dat a ke zjednodušení a zprůhlednění požadavků na vytvoření, rozšíření a rušení uživatelských účtů.

Modularita řešení umožňuje víceúrovňové napojování koncových systémů, kdy se k základu, tvořenému systémem Identity Managementu, postupně připojují nové aplikace.

Single sign-on - jednotné přihlášení



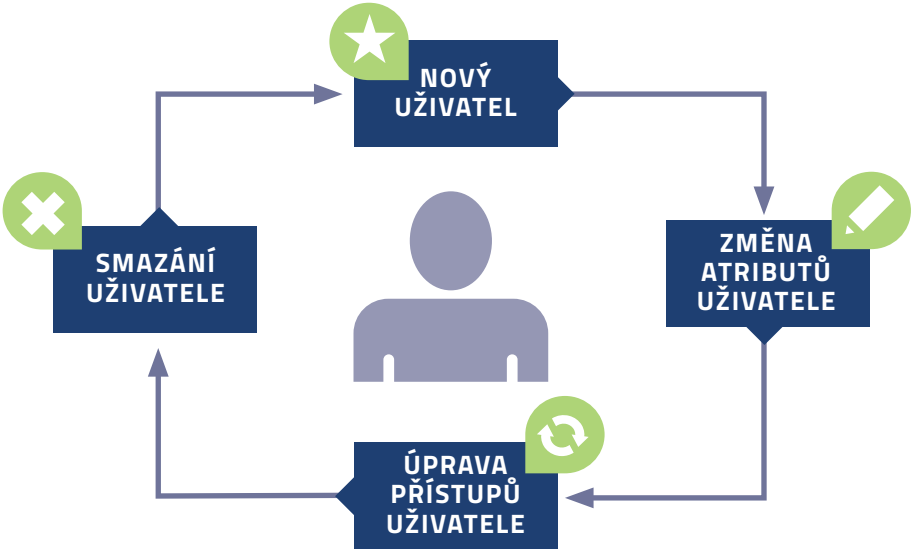
Identity Management



Realizační fáze v implementaci IDM DPDC Identity

1/ Externí audit aktuálního stavu.

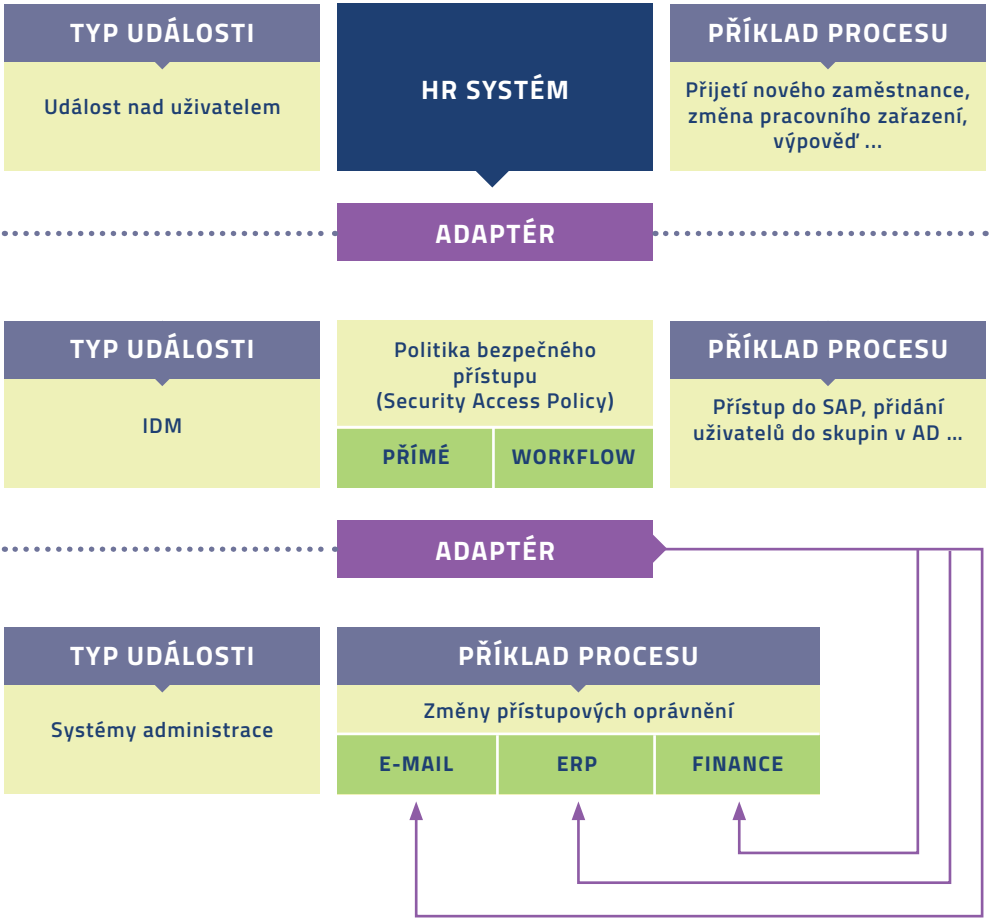
ŽIVOTNÍ CYKLUS UŽIVATELSKÉ IDENTITY
(IDENTITY LIFECYCLE)



2/ Implementace Proof of Concept IDM v testovacím prostředí pro ověření a vyzkoušení nabízených vlastností.

3/ Dodávka licencí a převod do produkčního prostředí.

Architektura IDM



Příklad workflow: zaměstnanec zažádá o přístup do určitého modulu systému SAP. Na základě předchozí analýzy vnitropodnikových procesů a nastavených pravidel se spustí proces schvalování, který může mít různý počet kroků (schválení nadřízeného, schválení správce systému, schválení licenčního správce ...).

Rekonciliace (zpětná kontrola)

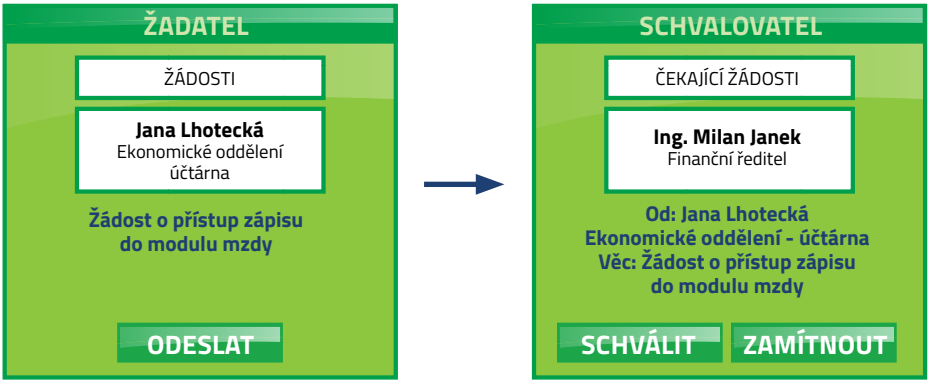
Srovnání nastavené bezpečnostní politiky se skutečností.

- neoprávněné přístupové možnosti
- duplicitní účty
- účty bez přiřazené identity
- mrtvé duše (např. účty bývalých zaměstnanců)

Audit

Reporty pro interní i externí audit.

Příklady rozhraní v modulech IDM



a SINGLE SIGN-ON

Výsledné vlastnosti implementace IDM

Provozní benefity:

- Automatizace a standardizace životního cyklu uživatelského účtu napříč napojenými systémy podle definovaných politik. Součástí je také automatické vytváření nových uživatelů a jejich mazání po odchodu ze společnosti. Tato administrativa představovala zátěž pro IT a odchody byly opomíjeny.
- Změny oprávnění uživatelů jsou automatické na základě žádosti a schválení (bez IDM řešeno přes IT a „papírovou" cestou).
- Reset zablokovaných účtů a hesel přes samoobsluhu uživatele v centrálním portálu (bez IDM řešeno přes IT).
- Flexibilita změn, díky které má nastupující zaměstnanec agendu ihned připravenou.

Bezpečnostní benefity:

- Jednoznačná identifikace (personifikace) účtů zaměstnance na koncových systémech – vazba přístupových oprávnění na konkrétního zaměstnance.
- Každý přístupový účet na systémech má identitu – tj. svého konkrétního člověka.
- Přístupy k citlivým informacím mají jen pověřené osoby.
- Neautorizované změny v nastavení oprávnění jsou identifikovány a blokovány dříve, než dojde ke zneužití dat.
- Přístupy přiděluje management, nikoliv IT.

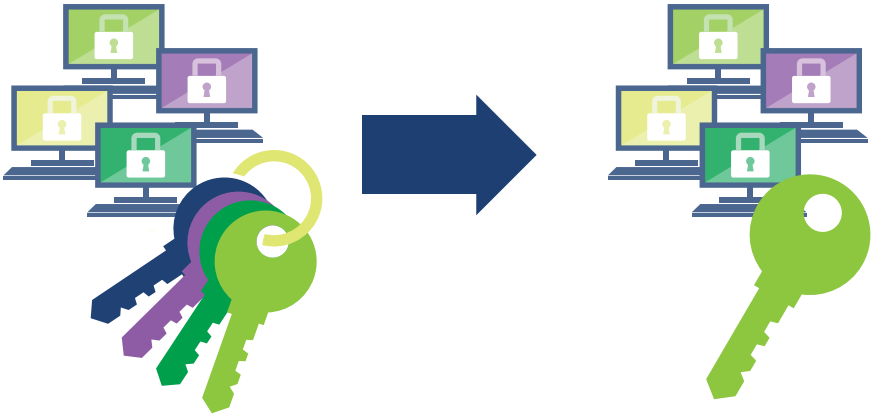
Benefity auditu:

- Centrální místo pro audit a logování operací nad uživatelskými oprávněními.
- Dohledatelnost přístupu k dílčím informacím.
- Dohledatelnost schválení přístupu.
- Doložení všech změn v oprávněních uživatelů.
- Reporty nesrovnalostí oproti organizační bezpečnostní politice.

pro Vaši bezpečnost

PROPOJENÍ Identity Managementu a Single sign-on

Systém jednotného přihlášení je vhodným rozšířením IDM. SSO zajistí uživateli automatické přihlášení do aplikace, aniž by musel opětovně zadávat přihlašovací údaje. Uživatel si tak pamatuje pouze jedno uživatelské jméno a heslo.



DPDC Identity

rychle ▪ kompletně ▪ jednoduše ▪ bezpečně

Cena

Cena je závislá na rozsahu implementace a navržených a zprovozněných řešeních. Implementace je rozdělena technicky i nákladově do tří realizačních fází a cenová kalkulace zohledňuje konkrétní personální a technické prostředí Vašeho subjektu.

www.dpdc.cz
Rybkova 1016/31
602 00 Brno
+420 602 663 351
obchod@dpdc.cz