



Zákoutí implementace IdM

Svět IdM pohledem dodavatele

Není IdM jako IdM

různé produkty

různí zákazníci

různé integrace

uživatelský self-service

pokročilé funkcionality

federated identity

ČSSZ, O2 CZ, Orange SK, ISIC,

Ministerstvo zemědělství



Jihočeská univerzita
v Českých Budějovicích
University of South Bohemia
in České Budějovice

UNIVERZITA J. E. PURKYNĚ V ÚSTÍ NAD LABEM



IBM Security Identity Manager



DirX Identity



Organisation Manager



Licence open-source IdM

Apache License v 2.0

CDDL 1.0

MIT License

GNU Lesser General Public License 2.1

GNU Lesser General Public License 3.0

Eclipse Public License - v 1.0

Common Public License Version 1.0

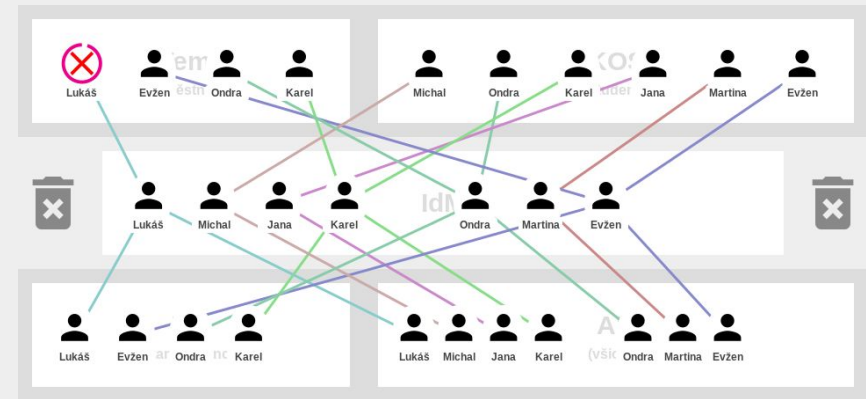
GPLv2 with classpath exception

Všechny hlavní open-source
projekty používají tento mix.



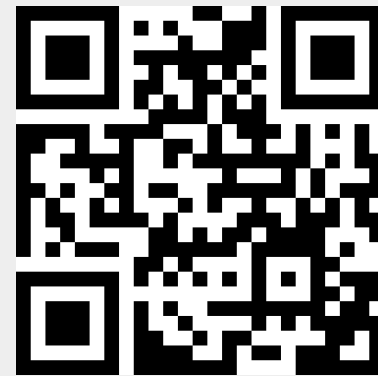
identitr

<https://idm.systems/identitr/>

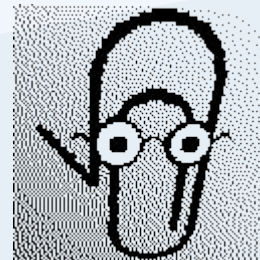


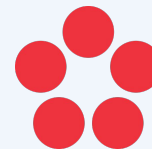
Zahrajte si na IdM.

Jak dlouho zvládnete reagovat na události ve zdrojových a cílových systémech?



Správa identit má být jednoduchý
problém.





3 zdrojové systémy ... 6 cílových systémů ... 3 plánované systémy

70k identit, z toho 15k aktivních

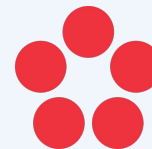
synchronizace hesel

slučování identit

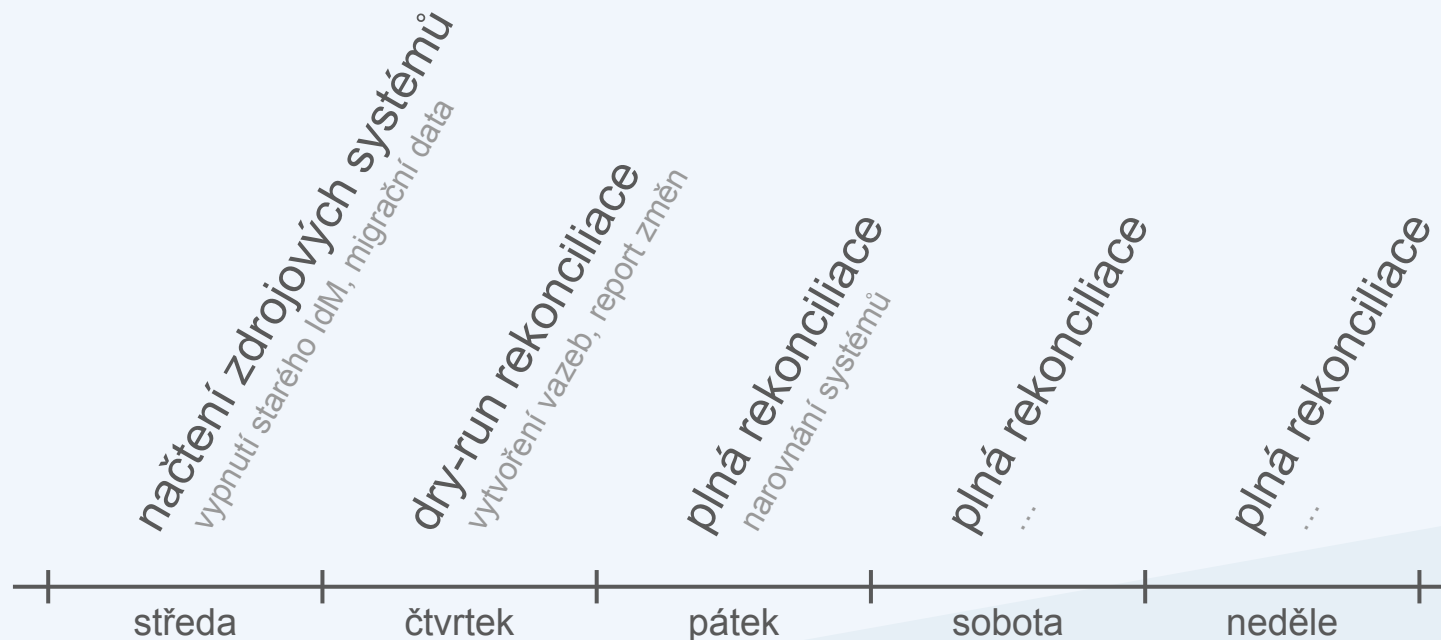
osobní e-maily

Jihočeská univerzita

přechod do produkce

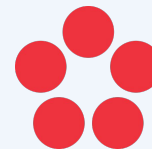


Jihočeská univerzita
v Českých Budějovicích
University of South Bohemia
in České Budějovice



Jihočeská univerzita

simulovaný zápis neboli dry-run



Jihočeská univerzita
v Českých Budějovicích
University of South Bohemia
in České Budějovice

AD

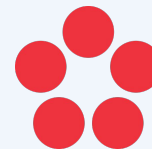
14k namapovaných
33k neoprávněných
8 chybějících
150 neidentifikovaných

RADIUS

8k namapovaných
30 neoprávněných
3 chybějící
1 neidentifikovaný



```
...9862 [department] [ null, "M4101" ]
...9862 [company] [ null, "FZE" ]
...9862 [ldapGroups] [ [ ], [ "CN=FZEAlum,OU=IDMGroups,DC=ad,DC=jcu,DC=cz" ] ]
...b14a [mail] [ "le*****@zf.jcu.cz", "le*****@jcu.cz" ]
...b14a [department] [ null, "P1601" ]
...b14a [company] [ null, "FZE" ]
...b14a [mail] [ "kn*****@ef.jcu.cz", "kn*****@jcu.cz" ]
...dbb5 [sn] [ "KNECHT", "Knecht" ]
...dbb5 [cn] [ "KNECHT *****", "Knecht *****" ]
...dbb5 [department] [ null, "B6208" ]
...dbb5 [company] [ null, "FEK" ]
...a2ef [userAccountControl] [ "546", "544" ]
```

AD – maximální délka uživatelského jména je 20 znaků

AD – sambaNTPassword je MD4 v UTF-16LE

RADIUS – single-value není tak úplně single-value

AD – speciální znaky v hesle nesmí být moc speciální

Původní IdM – diakritika v e-mailových adresách

AD – UserPasswordNotRequired

LDAP + SQL – referenční integrita



4 zdrojové systémy ... 4 cílové systémy

60k identit, z toho 12k aktivních

nový způsob evidence studentů

nový LDAP, nový způsob autentizace

hostovské identity, žádost o mailbox

Univerzita J. E. Purkyně

přechod do produkce

UNIVERZITA J. E. PURKYNĚ V ÚSTÍ NAD LABEM



akce „Kulový blesk“
přechod do produkce, změna účtů

—+—+—
středa

Univerzita J. E. Purkyně

problémy

UNIVERZITA J. E. PURKYNĚ V ÚSTÍ NAD LABEM



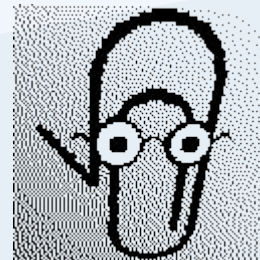
Víceméně vše vyřešeno v rámci testovacích migrací.

OpenLDAP – nestabilní při replikaci pod zatížením

UNL – chybějící objectclasses

eDirectory – datum jako INT32 (1970 ~ 2038)

Správa identit má být jednoduchý
problém.



Slučování identit I

ve zdroji jsou chyby

- zdánlivě komplexní problém

duplicity ve zdrojových systémech

duplicity mezi zdrojovými systémy

slučování konfliktních atributů

- jednoduchý use-case

dohledání duplicity a její označení

přenesení vazebních atributů

zakázání duplikátu

Business Logic © Orchitech Solutions

Slučování identit II

zdroj fyzickou osobu neřeší

- zdrojový systém to neřeší?

oddělený model pro zdrojové objekty

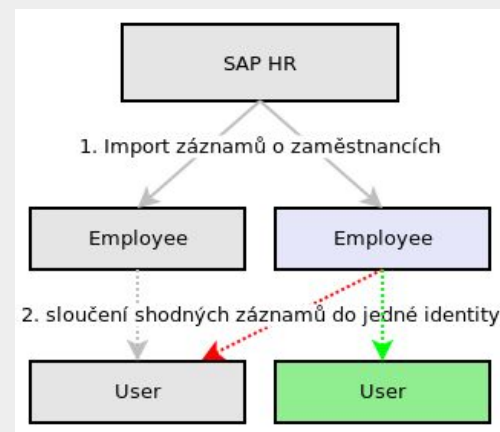
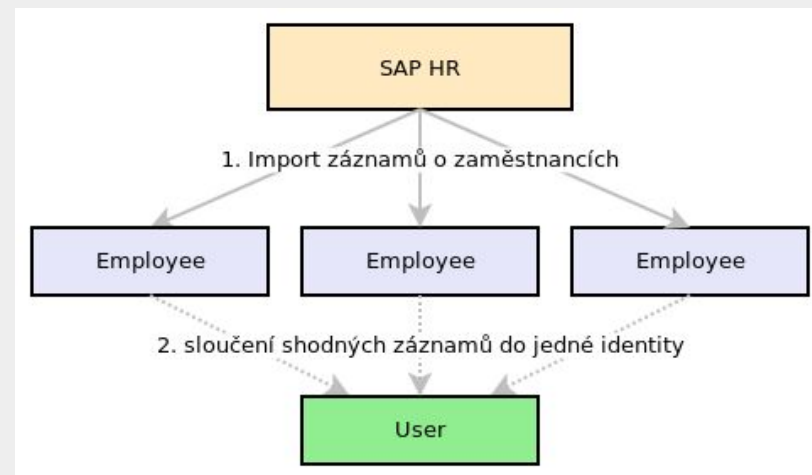
proces párování zdrojových objektů

proces mapování na identitu

- přepárování není problém

proces nebude nikdy bezchybný

změna vazby a zbytek plyne z IdM



Slučování identit III

slučujeme zákazníky

- správa zákazníků

vícenásobné mapování

aktualizace a zastarávání údajů

evidence souhlasů a jejich odvolání

marketingové využití dat

- identity provider

přihlášení a namapování účtu

Resolved Complete

First Name	David
Last Name	MALINA
Birthdate	1.1.1900
School name	Test import
School type	Vysoká škola
Field of Study	
Phone number	

Resolved Marketing

There are no resolved marketing data to display

Subscriptions

E-mail	Agreement Type	Status
dave.malina@seznam.cz	Mandatory	Exported to Oempro

Customer approved agreements

Name	Card number	E-mail	Birthdate	Approved until	Source System	Agreement
MALINA, David	S420300000000P	dave.malina@example.com	1.1.1900	14.10.2028	NADB	Download

Hostovské identity

rychlý přístup pro hosty

- ad-hoc identity

omezená platnost

omezená práva

- zodpovídá garant

proces prodloužení

proces převzetí

The screenshot shows the UJEP user interface. At the top, there is a dark blue header with the UJEP logo, navigation icons, and language options (EN, CS) and a power button. Below the header, the user's name 'Antonín Kulička' is displayed. The main content area is divided into two sections: 'Antonín Kulička' and 'Informace o garantovi'. Each section contains a list of user attributes in a table-like format.

Antonín Kulička	
UID	2
Uživatelské jméno	xkulicka1
Jméno	Antonín
Příjmení	Kulička
Osobní e-mail	antonin.kulicka@example.com
Datum vypršení	2016-10-16
Poznámka	Testovací identita.

Informace o garantovi	
UID	1001
Uživatelské jméno	horal
Jméno	Pavel
Příjmení	Horal
Osobní e-mail	

Business Logic © Orchitech Solutions

Licence

když přístupy nejsou zdarma

- omezení počtu přiřazení

definice licencí (účet vs. právo)

logika čerpání licencí

překročení a navázané procesy

- rezervace

rezervace počtu přiřazení

rezervace pro konkrétní účel

Jan Novák 1234

[← Zpět](#)

Licencovaný systém

Informace o systému

ID systému	cn=LICENCE,cn=Systems
Název systému	LICENCE
Popis systému	

Licencovaná práva (skupiny)

Admin

ID skupiny	cn=Admin,cn=groups,cn=LICENCE,cn=Systems
Garanti licencí	František Veslo 4295
Notifikační práh překročení licenční kvóty (%)	80.0 %
Licenční kvóta	100 Změnit kvótu
Přehled čerpaných licencí	Využité: 6 Nevyužité blokováno: 0 Nevyužité volně: 94 Rezervované: 0

Další zajímavosti

všehochuť

Viditelnost a přiřaditelnost – access control naruby

Odložená synchronizace – řešení referenční integrity

Unique value cache – generujeme unikátní hodnoty

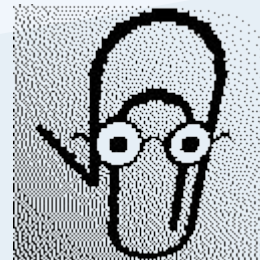
Integration profiling – kontrola počtu a délky operací

Request logging – rozšířené logování BE i FE

Nestandardní oprávnění – plnohodnotná free-text práva

Pokročilá workflow – agregace žádostí, poznámky k realizaci

Správa identit má být jednoduchý
problém.



Watchdog

tady hlídám já

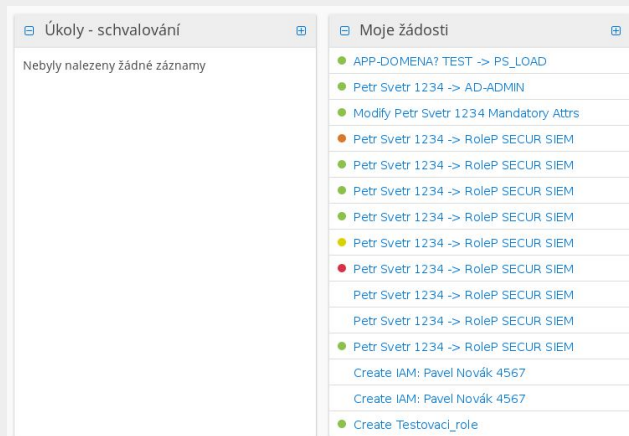
- jak a co kontrolovat
 - počet změn objektu za danou rekonciliaci
 - počet změn na objektu za daný čas (load)
- co (ne)hlídat
 - inkrementální rekonciliace (LIVE SYNC)
 - odvozené změny
- problémy
 - kdy je UPDATE skutečně UPDATE



Pozorované chyby I

nevhodné UI požadavky

- přehnané barvičky
- nekonceptčnost
- vše na jedné obrazovce
- prohřešky proti UX
WCAG, WAI-ARIA, ...



Je nutné specifikovat konvence pro UI a neporušovat best practices.



Pozorované chyby II

projekt nepodléhá verzování

- nejasná verze projektu

implementace klikáním

ad-hoc změny

ruční přenos do produkce

- chyby a jejich odstraňování

neodstraňování starých částí

důvod implementační změny

Projekt by měl být v SCM a podléhat release managementu.

```
276be16 CUA mapping changes. See RM #26143.
24e53eb Next dev cycle.
64cbc96 1.0.6
be87bba Fixed incorrect version in master branch.
5e46195 LDAP contactVisible rules changed. See RM #25961.
3ae0ad0 E-mail change detection with disconnected mailboxes. See RM #25438.
c9c153e Next development cycle.
b66a9ae 1.0.4
01bbdf3 Better upgrade instructions. NOREF
a51c02b Manager can be NULL. See RM #25182
e9f94bc Notification dispatcher can handle non-existing template. NOREF
207dec0 Workaround for PostgreSQL audit record logging error. See RM #24045.
a4b29c5 Fixed MailboxSearch result size limitation. See RM #24910.
e3ac8d5 Mapping Building attr from HR export. See RM #24910.
c1a0df3 Next release cycle.
82fa206 1.0.3
fc63300 Default value for empty managers in AD. See RM #24910.
```



Pozorované chyby IV

kontrolujeme změnu nebo stav

- změnové vs. stavové chování
velmi odlišný způsob implementace
funkcionality jako reakce na události
události spouštějící kontrolu stavu
- když událost nezpracujeme
nekonzistentní stav
rollback



**Synchronizace by měla přenášet raději stav
než změny.**

Best practices

software development

- release management
projekt, dokumentace, konfigurace
- sestavování konfigurace
kompilace, transpilace
- zero-configuration
okamžitý start
- unit testy
skripty, konfigurace, UI

Continuous Integration
Continuous Delivery

```
it("employee short", function() {
  expect(generateUsername(openidmMock, {
    givenName: 'Ab',
    surname: 'Cd',
    workforceId: 1
  })).toBe('acd');
});

it("employee long", function() {
  expect(generateUsername(openidmMock, {
    givenName: 'Karel',
    surname: 'TesterTestovitý',
    workforceId: 1
  })).toBe('ktestertestovit');
});

it("employee two names", function() {
  expect(generateUsername(openidmMock, {
    givenName: 'Hana',
    surname: 'Vorlová Görglová',
    workforceId: 1
  })).toBe('hvorlovagorglov');
});

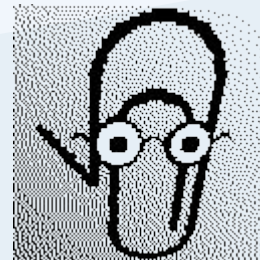
it("student", function() {
  expect(generateUsername(openidmMock, {
    givenName: 'Petr',
    surname: 'Svetr'
  })).toBe('svetrp00');
});

it("student conflict", function() {
  expect(generateUsername(openidmMock, {
    givenName: 'Jan',
    surname: 'Novák'
  })).toBe('novakj02');
});

it("accents", function() {
  expect(generateUsername(openidmMock, {
    givenName: 'Žlababa',
    surname: 'Řhážová'
  })).toBe('řnazoz00');
  expect(generateUsername(openidmMock, {
    givenName: 'Nikola',
    surname: 'Mojzyszková',
    workforceId: 1
  })).toBe('nmojzyszkova');
});
```

```
[14:15:26] Using gulpfile ~/Documents/repository/mze/
[14:15:26] Starting 'clean'...
[14:15:26] Finished 'clean' after 34 ms
[14:15:26] Starting 'default'...
[14:15:26] Starting 'build:vendor'...
[14:15:26] Starting 'build:conf:json'...
[14:15:26] Starting 'build:conf:other'...
[14:15:26] Starting 'build:data'...
[14:15:26] Starting 'build:doc'...
[14:15:26] Starting 'build:ui'...
[14:15:26] Starting 'build:script:js'...
[14:15:26] Starting 'build:script:other'...
[14:15:26] Finished 'default' after 56 ms
[14:15:26] Finished 'build:doc' after 43 ms
[14:15:26] Finished 'build:vendor' after 170 ms
[14:15:26] Starting 'test'...
[14:15:26] Finished 'build:ui' after 195 ms
[14:15:26] Finished 'build:conf:other' after 212 ms
.....
36 specs, 0 failures
Finished in 0 seconds
[14:15:26] Finished 'test' after 202 ms
[14:15:26] Finished 'build:data' after 354 ms
[14:15:26] Finished 'build:script:other' after 480 ms
[14:15:26] Finished 'build:script:js' after 533 ms
[14:15:26] Starting 'build:script'...
[14:15:26] Finished 'build:script' after 2.95 us
[14:15:26] Finished 'build:conf:json' after 553 ms
[14:15:26] Starting 'build:conf'...
[14:15:26] Finished 'build:conf' after 1.99 us
[14:15:26] Starting 'build'...
[14:15:26] Finished 'build' after 1.76 us
[14:15:26] Starting 'default:build'...
[14:15:26] Finished 'default:build' after 1.68 us
```

Správa identit má být jednoduchý
problém.



Správný návrh UI

Vyberte prostředí **Vyberte aplikaci**

Produkční

Odeslat ke schválení

Zrušit změny

ESS - Elektronická spisová služba + 1 1

Nesmíte vybrat více než 2 výjimky.

Role Sekretářka

Výjimky Mělník (123456)

Petr Svetr 1234

Přirazení oprávnění uživatelům

Uživatelé

Novák Jan 4567

Oprávnění

TEST_ENV_ACCESS

PORTAL_ACCESS

Platnost do

2016-10-15

Zdůvodnění žádosti

Odeslat žádost

Last name *

Username *

E-mail *

Phone

Active Yes No

Organisation

Roles

Card issuer
Has privilege to update cards for assigned card ranges.

Email notifications

Email notifications for unsuccessful location geocodings

Email notifications for import problems

Import reports

New password

Leave blank to keep the existing password

Několik ukázek UI

The screenshot displays a web application interface for user activities. At the top, there is a navigation bar with tabs: Přístupy, Aktivity, Žadosti, Delegace, Správa, Reporty, and Helpdesk. The user's name, Kenobi Karel 123456, is shown in the top right corner. The main heading is "Aktivity uživatele: Kenobi Karel 123456".

The primary section is titled "Úkoly - schvalování" and contains a search bar labeled "Hledat". Below it is a table with the following columns: Stav, Název úkolu, Uživatel přístupů, Autor žádosti, Čas zadání, and Obsah žádosti. Two tasks are listed:

Stav	Název úkolu	Uživatel přístupů	Autor žádosti	Čas zadání	Obsah žádosti
<input type="checkbox"/>	Novak Jan 654321 -> LDAP-ADMIN Přřazení oprávnění uživateli / účtu - schválení nadřizeným	Novák Jan 654321	Novák Jan 654321	14.09.2016 09:04:30	Novák Jan 654321 (1111) LDAP-ADMIN
<input type="checkbox"/>	Icha Petr 123654 -> DOMAIN-AUTH Přřazení oprávnění uživateli / účtu - schválení nadřizeným	Icha Petr 123654	Icha Petr 123654	11.10.2016 12:01:57	Icha Petr 123654 (1111) DOMAIN-AUTH

Below the table is a text area for "Důvod schválení / zamítnutí" and two buttons: "Schválit" (green) and "Zamítnout" (red).

At the bottom, there are four panels for request management:

- Moje Žadosti**: Lists "Create LDAP: Kenobi Karel 123456" and "Create LDAP: User".
- Žadosti o mé přístupy**: Lists "Create LDAP: Kenobi Karel 123456".
- Seznam vrácených SP**: Displays "Nebyly nalezeny žádné záznamy".
- SD požadavky**: Displays "Nebyly nalezeny žádné záznamy".

The footer contains the copyright information: © 2009 - 2016, Orchitech Solutions, s.r.o.

Několik ukázek UI

The screenshot shows a user management interface. At the top is a navigation bar with tabs: Přístup, Aktivita, Žadosti, Delegace, Správa, Reporty, Helpdesk. The user's name 'Kenobi Karel 123456' is displayed in the top right. Below the navigation bar are two main sections: 'Uživatel' and 'Přiznání/odebrání práv'. The 'Uživatel' section contains buttons for 'Kontakt', 'Reset hesla', 'Aktivita uživatele', 'Změna mandatorních atributů', and 'Změna uživatele'. The 'Přiznání/odebrání práv' section contains buttons for '+ Přidat role', '+ Přidat oprávnění', '- Odebrat role', and '- Odebrat oprávnění'. Below these is the 'Detail uživatele: Kenobi Karel 123456' section, which is divided into several panels: 'Uživatel' (User details), 'Mandatorní atributy' (Mandatory attributes), 'Sady a role' (Groups and roles), 'Oprávnění' (Permissions), 'Uživatelské účty' (User accounts), and 'Technologické účty' (Technical accounts).

Uživatel

Jméno	Karel
Příjmení	Kenobi
Stav	Aktivní
Typ uživatele	Externí
Primární pozice	Externí pracovník 987654
Útvar	IT oddělení - externisté 12345
Nadřazený útvaru	Sláma Pavel 1111
Odpovědná osoba	Sláma Pavel 1111
ID	cn=Kenobi Karel 123456,cn=Users,cn=IDM

Mandatorní atributy

Sady a role

IDM-EXT

Oprávnění

IDM-Admin	Domain-Auth
LDAP-Admin	AD-User

Uživatelské účty

LDAP: x123456	!SAP: x123456	Domain: x123456
AD: x123456@idm.cz	AUTENTIZACE: x123456	

Technologické účty

© 2009 – 2016, Orchitech Solutions, s.r.o.

Několik ukázek UI

The screenshot displays a web application interface with a dark blue header. The header contains several icons on the left (gears, person, group, document) and language/branding options on the right (EN, CS, jnovak, power icon). Below the header, the main content area is titled 'Detail úkolu' with a list icon. The content is divided into two columns. The left column, titled 'Informace o žádosti', contains a table with details for request ID 1601. The right column, titled 'Schválení síťovým administrátorem', contains a table for approval ID 1613, a justification section with a red border and a character count of 0/1024, and two buttons: 'SCHVÁLIT ÚKOL' and 'ZAMÍTNOUT ÚKOL'. The footer of the page reads 'Business Logic © Orchitech Solutions'.

EN CS jnovak

> Detail úkolu

Informace o žádosti	
ID	1601
Název žádosti	Přiřazení univerzitního e-mailu
Datum vzniku	2016-08-12 15:03:27
Iniciátor	[711] Kenobi Karel
Subjekt	[711] Kenobi Karel
Typ	Univerzitní alias
Emailová adresa k přeměrování	karel@kenobi.cz
Text žádosti	Prosím o redirect emailů na zadanou adresu

Schválení síťovým administrátorem	
ID	1613
Datum vzniku	2016-08-12 15:03:27
Zdůvodnění	
Text zdůvodnění nesmí být prázdný. 0/1024	
<input type="button" value="SCHVÁLIT ÚKOL"/> <input type="button" value="ZAMÍTNOUT ÚKOL"/>	

Business Logic © Orchitech Solutions

Děkujeme za pozornost.

