



*Techno
Logica*

**Решения за управление на жизнения
цикъл на дигиталната идентичност**

*Николай Попов,
Решения за управление на дигитална
идентичност*

npopov@technologica.com

TechnoLogica Ltd.

3, Sofiisko Pole Str. tel: (+ 3592) 91 912 (ten lines)

e-mail: office@technologica.com, [http:// www.technologica.com](http://www.technologica.com)

- ◆ Какво е управление на жизнения цикъл на дигиталната идентичност - терминология
- ◆ Бизнес мотивация за прилагане на решения за управление на дигиталната идентичност
- ◆ Възможни решения на проблема за управление на дигиталната идентичност
- ◆ Технологични средства, с които предлагаме решения
- ◆ TL IdMS - преглед и функционални области
- ◆ Oracle Identity Management Suite - преглед
- ◆ Q&A

Терминология от областта на управление на дигиталната идентичност³

*Techno
Logica*

- ◆ Какво е дигитална идентичност? – ”Набор от атрибути, описващи дадена личност в информационна система” – бяла книга на CNET
- ◆ Какво е управление на жизнения цикъл на дигиталната идентичност? – управление на потребителските профили и процесите по провизиране/депровизиране на права, управление на заявки за провизиране и техните одобрения, управление на история на промените в атрибутите и правата на дигиталната идентичност (т.нар. identity транзакции) и пълно одитиране и проследяване на тези промени
- ◆ Какво е провизиране? - процеса на създаване на дигиталната идентичност и нейните права за достъп в множество системи, на базата на предварително конфигурирани шаблони на роли, политики

- ◆ Недопускане на изтичане, унищожаване на конфиденциална за организацията информация



- Ненавременното спиране на достъпа и не отнемане на правата е потенциална дупка в сигурността на организацията

- ◆ Оптимизация и автоматизация на процесите в ИТ отдела
 - ◆ Създаването на потребителски профили и даването на права на новопостъпили служители за ИТ ресурсите на организацията отнема твърде много време по традиционния начин
 - ◆ С промените в организацията и смяната на длъжностите на хората е много трудно да се проследи кои до какво има достъп и с какви права

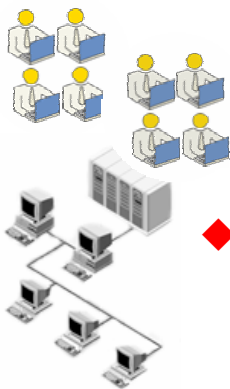
- ◆ Съвместимост с регулаторни рамки (Sarbanes – Oxley Act, Graham-Leach...) – разделение на задълженията и отчетност
 - ◆ Изключително трудно е и е свързано с много разходи да се осигурят регулярни отчети от вида “Кой има права за какво и от кога до кога?”, така както изискват нарастващите регулаторни изисквания
 - ◆ Демонстрирането на съвместимост обикновено изисква ръчни процедури
 - ◆ По данни на IDC, през 2006 водещите компании са насочили 30% от своите ИТ бюджети за съвместимост и системи за управление на дигиталната идентичност



Бизнес мотивация – нарастваща сложност на ИТ в организациите

Techno
Logica

- ◆ Нарастващата сложност и увеличаващия се брой системи в организациите усложняват нещата още повече
 - ◆ От строго централизирания модел през 60-70 години на миналия век, с един компютър на който всички служители работят с терминалите си...
 - ◆ През клиент – сървър ерата и бумът на евтиният PC хардуер през 90-те...
 - ◆ До сегашната ситуация, в която в една организация служителите работят с 10-60 ИТ системи средно, със съответния брой администратори, необходими за създаване и промяна на профилите, правата и паролите им в тях



- ◆ Синхронизационно решение – между системата за управление и една или повече управлявани системи се настройва синхронизация на атрибути на дигитални идентичности и права. Напр. синхронизация между две LDAP директории, между LDAP и база данни и т.н.

- Предимство: по-просто технически

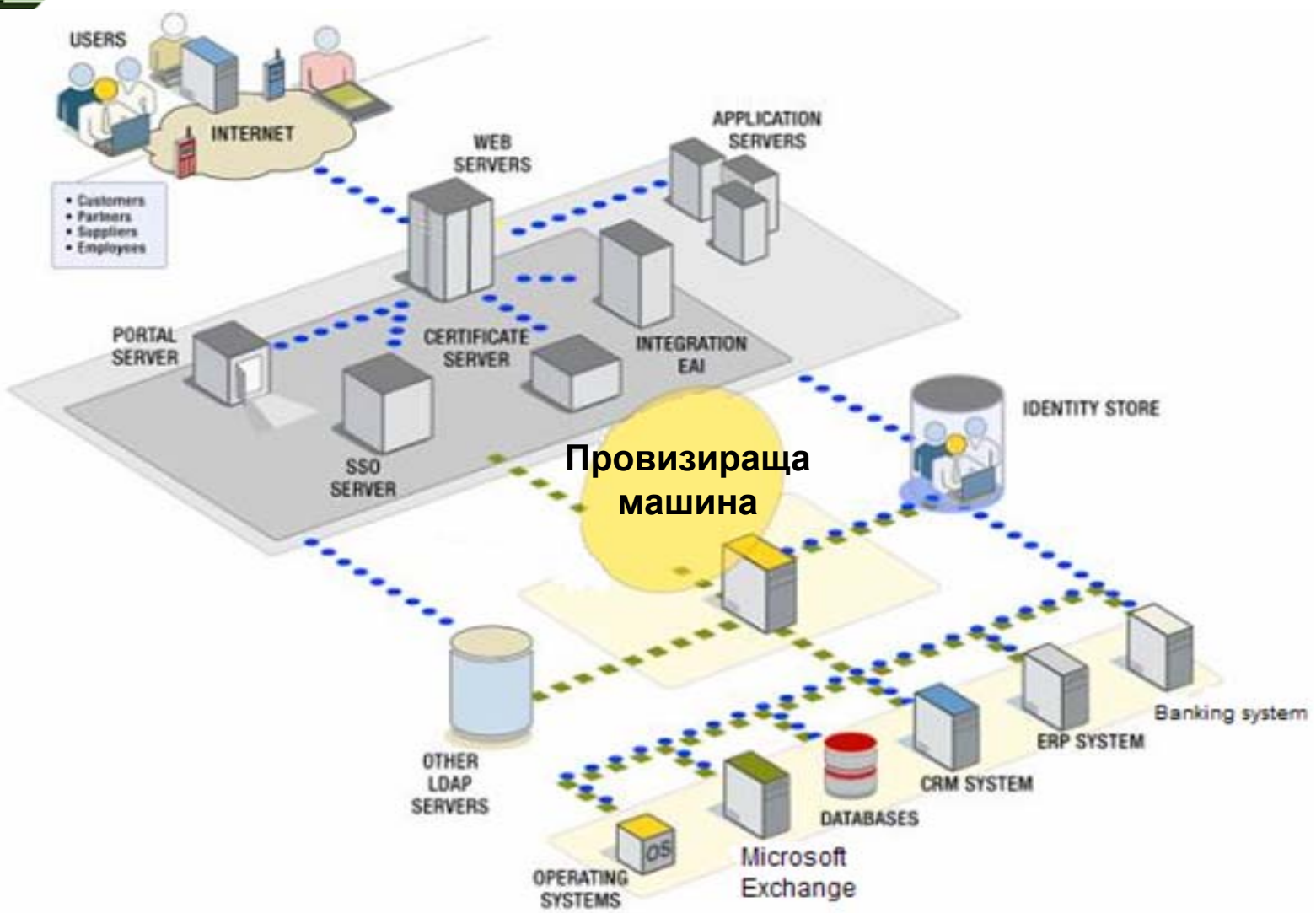


- Недостатък: с по-малка приложимост; не може да обхване и управлява бизнес процес по провизиране, включващ одобрения и координирано (управлявано) провизиране в много системи

Видове решения за управление на дигиталната идентичност – провизиране

*Techno
Logica*

- ◆ Провизиращо решение – специализирана системата за обработка на бизнес процеси за провизиране, включващи заявки за създаване на дигитални идентичности, одобрението им, стъпки от организационната практика в компанията , като напр. подписването на трудов договор и множество провизиращи действия, създаващи дигитални идентичности в множество управлявани системи.
- ◆ По същество провизиращата система е интеграционна система – за управление на различните като технологична платформа системи се използват адаптори – напр. за LDAP, Exchange, Lotus Notes, бази данни.
- ◆ Предварително настроени шаблони на роли или провизиращи политики определят в кои системи се създават профили и права



- ◆ TL IdMS – разработена от ТехноЛогика провизираща машина
 - ◆ Интегрирана със системата за управление на човешки ресурси HeRMeS
 - ◆ Обработват се бизнес процеси по назначаване, преназначаване, напускане, отсъствие на служител
 - ◆ Провизиране, базирано на шаблони на роли
 - ◆ Интегрирана с Oracle Internet Directory, Oracle Single Sign On Server – компоненти на Oracle Identity Management
 - ◆ С множество технологични адаптори – Microsoft Exchange, Microsoft Active Directory, бази данни и др.
 - ◆ WEB базиран, административен интерфейс с диференциран достъп

TL IdMS функционални области

*Techno
Logica*

- ◆ Администриране на дигиталните идентичности
 - ◆ Самоуправление на паролите
 - ◆ Управлявано от заявки и шаблони на роли провизиране
 - ◆ Делегирано администриране на потребители, групи и ресурси
- ◆ Администриране на роли
 - ◆ Има възможност за управление и провизиране на групи/роли, права в TL IdMS и в управляваните системи
 - ◆ Има възможност за включване на одобрение в процеса на провизиране

- ◆ Администриране на заявки
 - ◆ Диференциран достъп до подаването на заявки
 - ◆ Заявките се обработват автоматично или задействат workflow и чакат одобрение
 - ◆ Всички провизиращи действия в системата се корелират с породилата ги заявка
 - ◆ Администраторите могат да обработват ръчни заявки
 - ◆ Всички действия и заявки записват проследяващи съобщения за осигуряване на одит и съвместимост с регулаторните рамки
 - ◆ Работните потоци на заявките и провизиращите действия могат да бъдат настроени по Вашите практики и бизнес процеси
- ◆ Администриране на шаблоните на роли
 - ◆ Шаблоните определят какви профили / достъп и права получава служителя
 - ◆ Шаблоните на роли се “закачат” към организационната йерархия

ORCLADMIN

Начало

Заявки

Потребители

Позиции

Приложения

Настройки на IAMS

* Заявки за достъп | Журнал на промените |

Избор на заявки

Търсене по текстови полета

 За обработка
 Приключени
 Всички

Създадени: всички

РЪЧНА ПРОМЯНА

АВТОМАТИЧНА ПРОМЯНА

Действия по ръчна промяна

Действия по автоматична промяна

ВСИЧКИ ЗАЯВКИ - за ръчна промяна

1 - 18

HelpDesk#	Създадена ▼	Пояснения по заявката	Статус	IAMS статус	Ефективна от	Тип	Тип заявка	Поз.роля	ДАО	Създадена от
32986	2006-08-18 11:21:15	Потребител: U41158-Иван Иванов Иванов Бележки: Za ad	performed	PROCESSED	17/08/2006	CHANGE	CHANGE_RIGHTS_MANUAL		1651	U03292 : Петя Петрова Загорова
32985	2006-08-18 11:12:37	Потребител: U41158-Иван Иванов Иванов Бележки: ABAD => REPORTS	performed	PROCESSED	18/08/2006	CHANGE	CHANGE_RIGHTS_MANUAL		1651	U03292 : Петя Петрова Загорова
32984	2006-08-17	Потребител: U35892-Надежда Енева Пеева	performed	PROCESSED	17/08/2006	CHANGE	CHANGE_RIGHTS_MANUAL		1651	U03292 : Петя



Избрана позиция

Структурна единица: ████ Пълнофункц клон Варна
 Подединица: ВСИЧКИ
 Секция: ВСИЧКИ
 Подсекция: ВСИЧКИ
 Длъжност: **ВСИЧКИ**
 Поз. поля: MAN1 - Branch Position Role

Назначени групи и права на тази позиция

Потребители в тази позиция

Потребители със шаблони от тази позиция

История на промените

Приложение	Роля	Право	Статус
APP_ABAD - ABAD SQL Server based application	REPORTS - Справки		VALID
APP_ACTIVE_DIRECTORY - Active Directory	Region 1 All Users (RG) - Active Directory Group 1		VALID
APP_APHASY_BE - APHASY BE SQL Server based application	9 - Справки(9)		VALID
APP_APHASY_RETAIL - APHASY_RETAIL SQL Server based application	2 - DAO (Клон/Въвеждащ)		VALID
APP_APHASY_SME - APHASY SME SQL Server based application	2 - CRO		VALID
APP_GLOBUS - Globus Corebanking System	NEWCRO - CUSTOMER RELATIONSHIP OFFICER M46		VALID
APP_MIS - MIS Oracle Portal based application	DAO_MANAGERS		VALID
APP_MPLS - MPLS SQL Server based application	YES		VALID
			1 - 8

◆ Identity Transactions History Data

ORCLADMIN

Начало

Заявки

Потребители

Позиции

Приложения

Настройки

* Потребители | Профили на потребители | Добавени и отсъстващи роли и права

Потребител: **U41157 - Васил Василев Василев**

Списък: U41157 - Васил Василев Василев

Покажи

Позиция на потребителя

Стр. единица	Пълнофункц.клон Добрич
Подединица	-
Секция	Масови продукти и услуги
Подсекция	-
Длъжност	Банков служител [3411]
Поз. роля	MAN2

Включени роли и права

История на промените

Добавени и отсъстващи роли и права

Лични данни

1 - 18

Дата ▲	чч:мм:сс	A	Приложение	Достъп от шаблон	Роля	Право	Статус	Потребител
2006-08-17	19:10:03	✓	APP_GLOBUS	Роля:NEWCSM			VALID	SYSTEM
	19:10:03	✓	APP_MIS	Роля:DAO_MANAGERS			VALID	SYSTEM
	19:10:03	✓	APP_APHASY_SME	Роля:5			VALID	SYSTEM
	19:10:03	✓	APP_APHASY_BE	Роля:5			VALID	SYSTEM
	19:10:03	✓	APP_ACTIVE_DIRECTORY	Роля:Region 1 All Users (RG)			VALID	SYSTEM
	19:10:03	✓	APP_ABAD	Роля:REPORTS			VALID	SYSTEM
	19:10:04	✗	APP_GLOBUS	Роля:NEWCSM			VALID	SYSTEM
	19:10:04	✗	APP_APHASY_SME	Роля:5			VALID	SYSTEM

ORCLADMIN

Начало

Заявки

Потребители

Позиции

Приложения

Настройки на AD

* Заявки за достъп | Журнал на промените

Търсене

Задача: 33002: CHANGE_RIGHTS_AUTO - Заявка №33002 за |

Създадени: всички

Филтрирай

Журнал на промените

1 - 14

Задача	#	Грешка	Текст	Статус	IDMS потребител	OS потребител	Дата създаване
40720 CHANGE_RIGHTS_AUTO: Заявка №33002 за Гергана Гогова Томова	33002		Успешно завършило изпълнение на функцията ldap_pkg.Ident_Up... детайли	FINISHED			15.09.2006 15:45:48
CHANGE_RIGHTS_AUTO: Заявка №33002 за Гергана Гогова Томова	33002		Успешно завършило изпълнение на Отдалечена LDAP операция за... детайли	FINISHED			15.09.2006 15:45:48
CHANGE_RIGHTS_AUTO: Заявка №33002 за Гергана Гогова Томова	33002		Стартирана автоматична обработка на всички действия за даден... детайли	FINISHED			15.09.2006 15:45:47
CHANGE_RIGHTS_AUTO: Заявка №33002 за Гергана Гогова Томова	33002		Завършена автоматична обработка на всички действия за дадена... детайли	FINISHED			15.09.2006 15:45:48

- ◆ LDAP директории
 - ◆ MS Active directory
 - ◆ Oracle Internet Directory
 - ◆ LDAP v3.0 съвместим сървър
- ◆ Collaboration & Messaging – Exchange Server
- ◆ Portals – Oracle Application Server Portal
- ◆ Custom Apps – MS SQL Server 2000/2005, Oracle, OleDB & ODBC datasource
- ◆ Line of Business/ ERP – Themenos Globus Core Banking
- ◆ Generic Secure Connectivity – SSH Protocol

- ◆ СУБД – Oracle
- ◆ User Interface – Oracle Application Express
- ◆ Oracle Single Sign On Server authentication
- ◆ TL IdMS е интеграционна система:
 - ◆ java libraries and java stored procedures
 - ◆ External C++ procedures
 - ◆ Heterogeneous Services (OleDB, ODBC)

- ◆ Настройка и транзакционни особености на използване на Oracle Heterogeneous Services за достъп до релационни бази данни извън Oracle – MS SQL Server 2000/2005 (Използвани материали от Петьо Зафиров, Р.Русинов и Н.Попов)
- ◆ Logging and code instrumentation PL/SQL API (Р.Русинов)
- ◆ Настройка на Oracle Sreams м/у два Oracle Instances за репликация на данни , DDL, DML и PL/SQL код (реализиран е нещо като stand by за отделна схема) (Р.Русинов)
- ◆ Настройка и писане на PL/SQL API за интегриране и управление на Oracle Job Scheduler API в нашето решение (Р.Русинов, малко Н.Николов)
- ◆ Oracle Агрегатна SQL функция , която конкатенира колони с разделител в GROUP BY заявки (Ина Найденова)
- ◆ Настройка на автентикация от UNIX (AIX) в Oracle Internet Directory (Н.Попов, Венци от ОББ)

- ◆ Exec SSH Shell (with opening shell, executing logon scripts, or just single shell command) commands from PL/SQL code , through java stored procedure and java ssh library (Ganymed) loaded in Oracle (Н.Попов)
- ◆ C++ library for Creating, Moving, Deleting MS Exchange Server Mailboxes and Administrative Password Reset for Active Directory Domain Accounts, deployed as External Procedure in Oracle for calling the functions of the library through PL/SQL code (Н.Попов)
- ◆ PL/SQL Пакет за LDAP операции в директорийни сървъри (MS Active Directory, Oracle Internet Directory) – за създаване, триене, модифициране, търсене на LDAP entries. Написана като надстройка на DBMS_LDAP Oracle пакет (Н.Попов)
- ◆ HTMLDB чудеса от Ч.Калоянов като javascript for auto postback of a page, custom PL/SQL Renderers с Apex API и bach insert/update от една страница и много други.
- ◆ Настройка на автентикация и авторизация в Apex от Oracle Single Sign On Server и Oracle Internet Directory. (Ганчо Колев, И.Алеков,Н.Попов)
- ◆ Send SMTP e-mail PL/SQL процедура с поддръжка на кирилица за body на съобщението. (И.Алеков и Митко Димитров)
- ◆ PL/SQL пакет за криптиране /декриптиране/хеширане на параметри, пароли в таблица с настойки, с използване DBMS_Crypto (Р.Русинов)

Технологични средства, с които предлагаме решения...

*Techno
Logica*

- ◆ Oracle Identity Manager – провизиращо решение от най-висок клас
 - ◆ Много богат набор от провизиращи адаптори за ERP системи, операционни системи, LDAP сървъри...
 - ◆ Провизиране на базата на политики и правила
 - ◆ Гъвкави инструменти за настройка на провизиращите процеси
 - ◆ WEB базиран административен интерфейс с делегирана администрация
 - ◆ Адаптер фактори – инструмент за създаване на адаптори

OIM Key Features

XELLERATE USER INTERFACES



User
Self Service



Delegated
Admin



System
Admin

XELLERATE SERVICES



Reporting
Auditing



Password
Management



Task
Queues



Scheduler



Security



Permissions



Views

Who/What

- User Profiles
- Resources
- Access Policies
- Business Workflow Processes
- Rule Builder
- Form and Process Designer

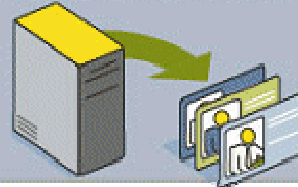
PROVISIONMANAGER



How

- Automation Engine
- Business Process Engine
- Request Manager
- State Machine
- Rollback/Recovery Processor

PROVISIONSERVER



ADAPTER FACTORY

Integration of:

- Enterprise Business Rules
- Enterprise Target Resources

RECONCILIATION ENGINE

- Real-time or Scheduled
- Bulk Imports
- External Data Monitoring
- Consistency Checking

XELLERATE API

- ◆ Reconciliation with multiple trusted sources
- ◆ Intelligent user profile definition
- ◆ Delegated administration
- ◆ Role & rule-based determination of access privileges
- ◆ Supports complex workflow requirements
- ◆ Stateful & dynamic workflow processing
- ◆ Ease of integration with Adapter Factory®
- ◆ Extensive reporting, analysis, auditing and attestation capabilities

Продукти от Oracle Identity Management Suite

*Techno
Logica*

- ◆ Oracle Access Manager – решение за контрол на достъпа, SelfService, Delegated Admin, Single Sign On за WEB приложения в/у различни платформи
- ◆ Oracle Virtual Directory – без да променя оригиналните хранилища на информация за дигитална идентичност, показва консолидиран поглед върху данните, като от един единствен източник
- ◆ Oracle Identity Management Infrastructure
 - ◆ Oracle Internet Directory (DIP)
 - ◆ Oracle Single Sign On Server
- ◆ Oracle Enterprise Single Sign On

Какво Ви предлагаме?

- ◆ Услуги по проектиране и внедряване на провизиращи решения.
- ◆ Услуги по разработка на провизиращи адаптори за Вашата специфична информационна система
- ◆ Опитът от проектиране и внедряване на решение за управление на дигиталната идентичност в организация с над 2500 служители, над 170 клона и 12 управлявани системи