

Управление идентификацией пользователей в разнородных системах

Антон Синский

Менеджер по работе с ключевыми заказчиками

Производственный отдел

Sun Microsystems CIS



Управление идентификацией. Что это?

Относится к 4 “А” безопасности



Authentication – Кто Вы?



Authorization – Что Вы можете делать?



Administration – Управление жизненным циклом пользователя



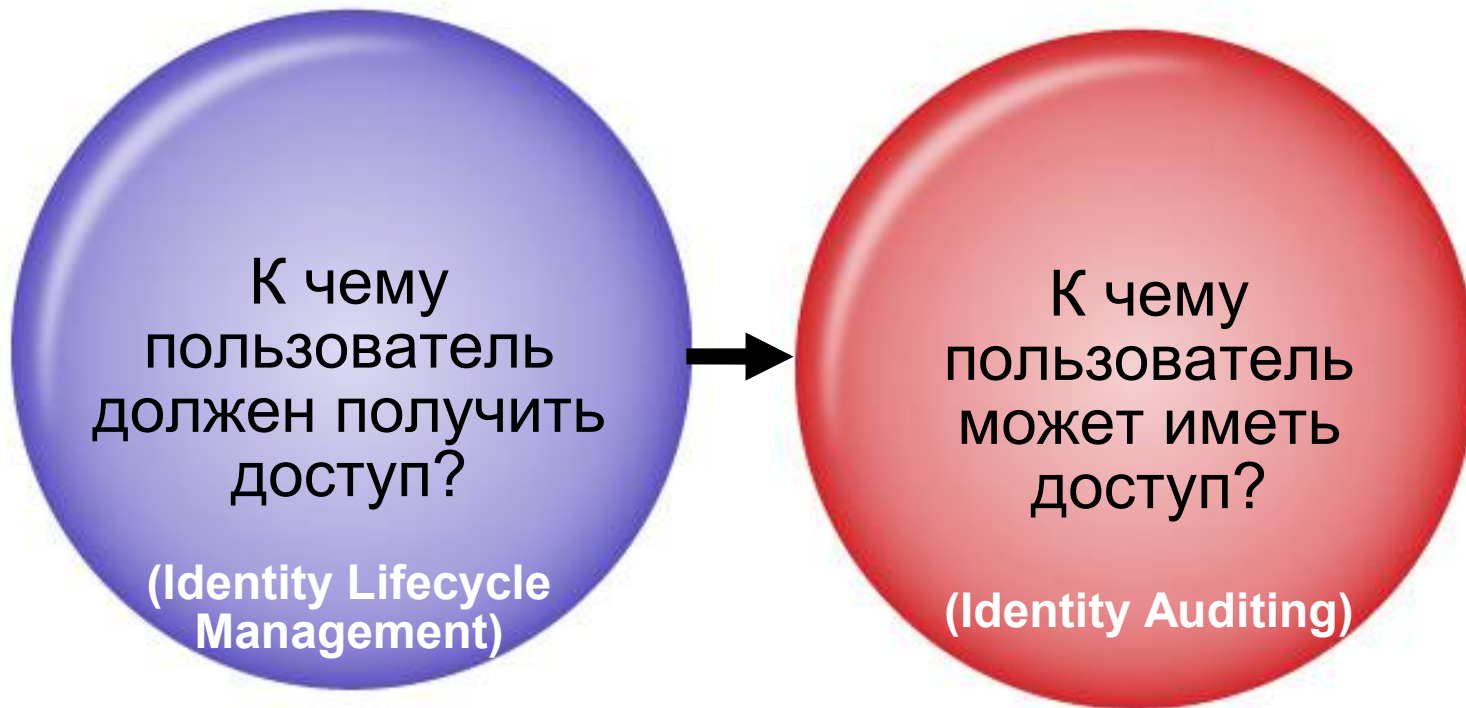
Audit – Отчет и анализ происшедшего

Топ 10 нарушений безопасности

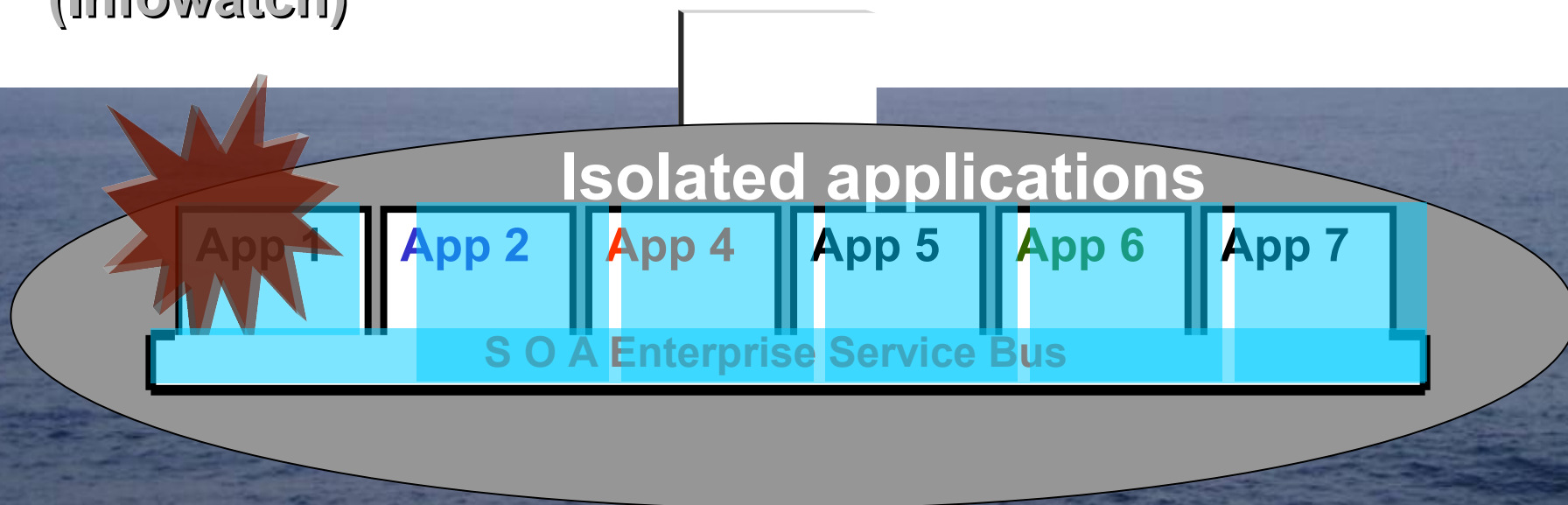
1. **Неопределенная и неразрешенная сегрегация обязанностей**
2. **Контроль доступа от ОС к финансовым приложениям или portalу небезопасен**
3. **Доступ к БД поддерживающей финансовые приложения небезопасен**
4. **Разработчики могут запускать бизнес транзакции на продуктиве**
5. **Большое количество пользователей с правами “супер пользователя”**
6. **Сотрудники/консультанты покинувшие компанию имеют доступ к системам**
7. **Время переноса записи не ограничено внутри приложения ГК**
8. **Заказные программы, таблицы и интерфейсы не защищены**
9. **Не существуют, либо не исполняются процедуры для ручных процессов**
10. **Системная документация не соответствует реальным процессам**

Source: Ken Vander Wal, Partner, National Quality Leader, E&YISACA Sarbanes Conference, 4/6/04

Ключом к “КАК” является “КТО”



-До **70% случаев** мошенничества и воровства информационных ценностей приходится на инсайдеров (Infowatch)



- Критически важные транзакции или действия не могут быть выполнены единолично одним человеком
- Жесткие определения сфер конфликта интересов при доступе к разным финансовым системам
- Жесткие требования по ограничению единоличного накопления привилегий доступа к системам, в том числе ИТ

SEGATION OF DUTIES

Жизненный цикл Identity по SOX

Без доказательств наличия контроля
считается, что нет контроля

Basic User Provisioning не выполняет требований
SOX



Создание
учетной записи

Использование
учетной записи

Модификация
учетной записи

Удаление
учетной записи



Аудит + Segregation of Duties

HR

Доверенный
независимый
источник данных

Растущие риски ИТ безопасности от инсайдеров

1. Ответственные за ИТ безопасность в больших и географически распределенных компаниях имеют эффективные инструменты контроля
2. Информация от HR об изменениях статуса сотрудников (должности, привилегии доступа) в ИТ приходит автоматически on-line
3. Полная ликвидация увеличения накопления привилегий доступа к ресурсам и «мертвых душ»

Существующие проблемы

Ручные процессы неадекватны требованиям бизнеса

1. Запросы бизнес-подразделений на доступ к ИТ ресурсу (s) обрабатываются on-line и без ошибок (опечатки, неполная информация невозможны)
3. Прекращены Helpdesk штормы по понедельникам (Я забыл свой пароль)
4. Автоматизирован процесс делегирования полномочий, если ответственный за ресурс отсутствует (отпуск, болезнь, командировка)

Почему это было так сложно

NT	Exchange	LDAP	AD	SecurID	ERP
Jberry	Bbanks	A49320	Cooperl	Skeeti	Sequensh
Esiegel	Lsullej	A39943	Tinleyj	Frenetc	Welchj
Jrowland	Lbitmore	A49454	Harrisd	Smileys	Pettyr
Mfriedel	Ltimble	A93934	wooc	Entrald	Robertsj
Sbenson	Aboyle	A39485	Rowlandr	Novacho	Julianr
Thanks	Bcoldwel	A49382	Bensons	Alvarag	Nantpre
Jwayne	Dparis	A48382	Quinleys	Narlersh	Enaget
Tcarrol	Clriot	A49382	Harminb	Woodst	Jhancock
Sharris	Etear	A39485	Travolta	Nicklausj	Johnh
Bwhite	Smackay	A29483	Francek	Hoganb	Hanwayv
Ddailey	Mturner	A49583	Lipperd	Palmera	Composi
Eheiden	Mmclain	A49382	Skatee	Dimarcoc	Initialialy
Lball	Mcpasch	A49302	Marinoe	Perryk	cwooc
Hwiggins	Jpasch	A42845	Flamingo	Beards	Stickler
Cjohnson	claytonw	A20184	Russiak	cw33	Bourne
Cwillis	Tdean	A49284	Crowd	Fusar	Fusar
c_woo	Jtorville	A49248	Pazzaz	Poli	Margoliao
Mthomas	Cdean	A50824	Daoudc	Margaglio	Navka
Browland	Nreagan	A42948	Louf	Lithowan	Koskoma
Mprehn	Rnixon	A49274	Peizerat	Vanagas	Hackinsa
Ggoodnow	Gbush	A37520	Anissina	Lightes	Newjers
Slake	Jvance	A49294	Ferrisb	Naugano	Shara
Bblake	Jcarpent	A03749	Lupers	Footman	Alexander
Fjohnson	Mstewart	A49274	Lobach	Figureas	Sasha
Galonso	Lchristia	A33993	Frenchj	Lupesh	Reuben
Slippes	Jbenley	A38288	Navratol	Arganish	Struedl
salger	jmackay	A48228	dellm	Delegant	tangor



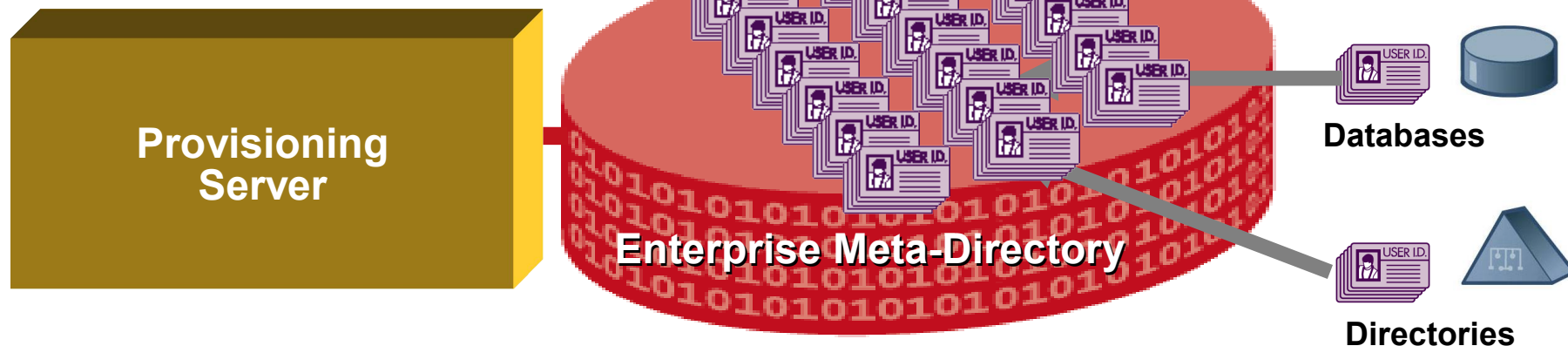
Clayton Woo

NT: c_woo
Exchange: claytonw
LDAP: A49382
AD: wooc
ERP: cwoo
SecurID: cw33

Три нерешенные проблемы

1. Узкое место , единая точка отказа и атак DOS
2. Большой объем синхронизации данных
3. Сосредоточение в одном месте полных атрибутов данных всех пользователей организации

Увеличение рисков безопасности

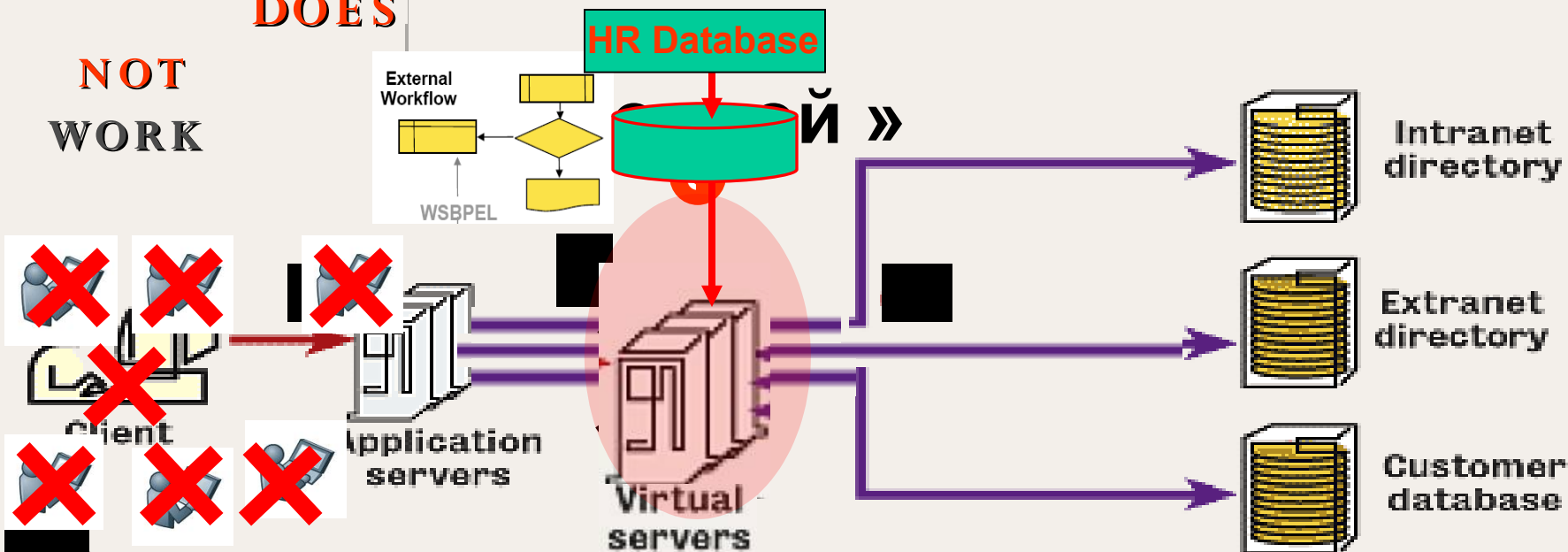


Identity and Access manager

«Виртуальный вахтер единой

■ **HOW IT WORKS**
DOES

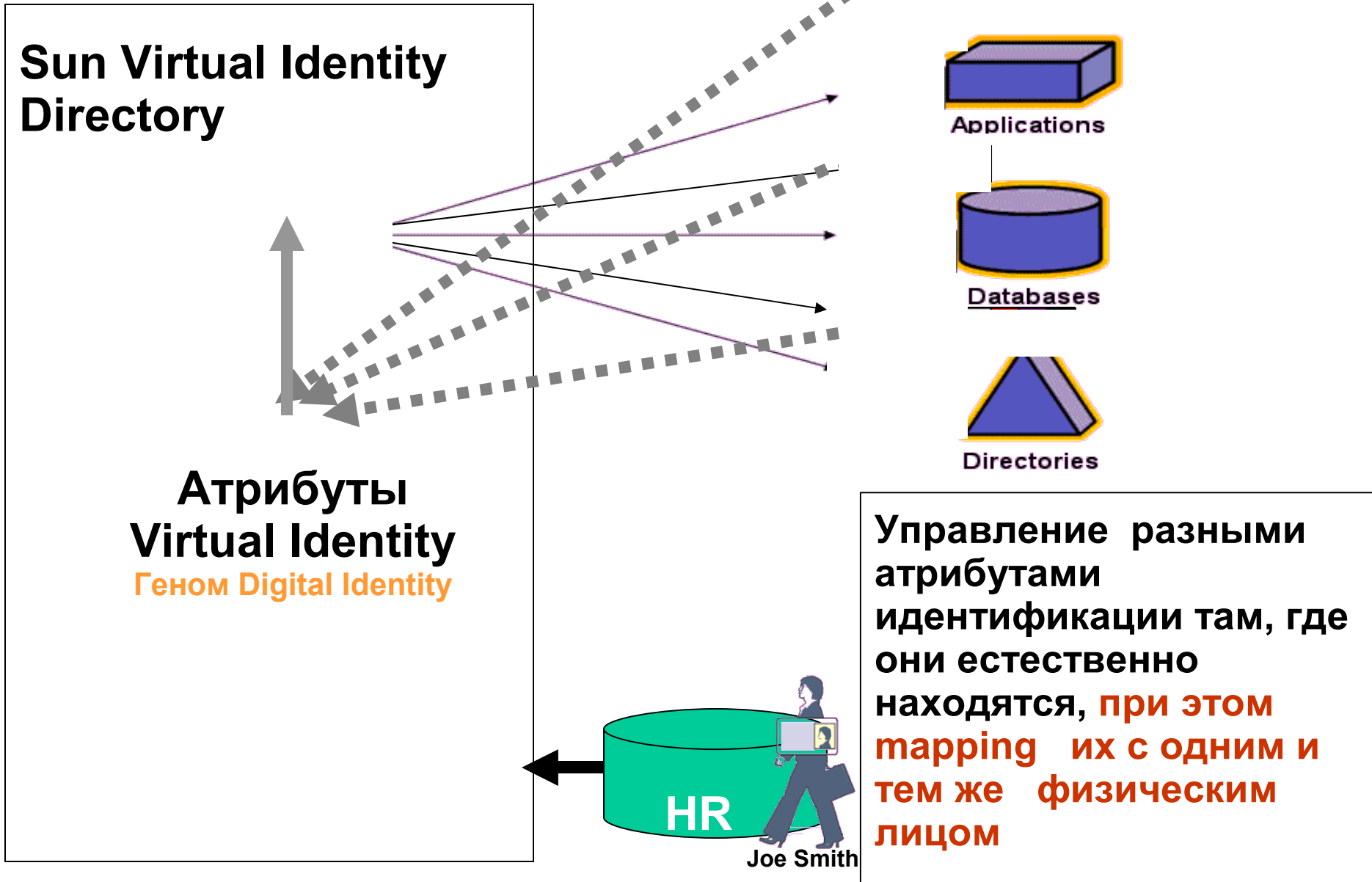
**NOT
WORK**



Проблема

**Для ВСЕХ пользователей ВСЕЙ
организации разом!**

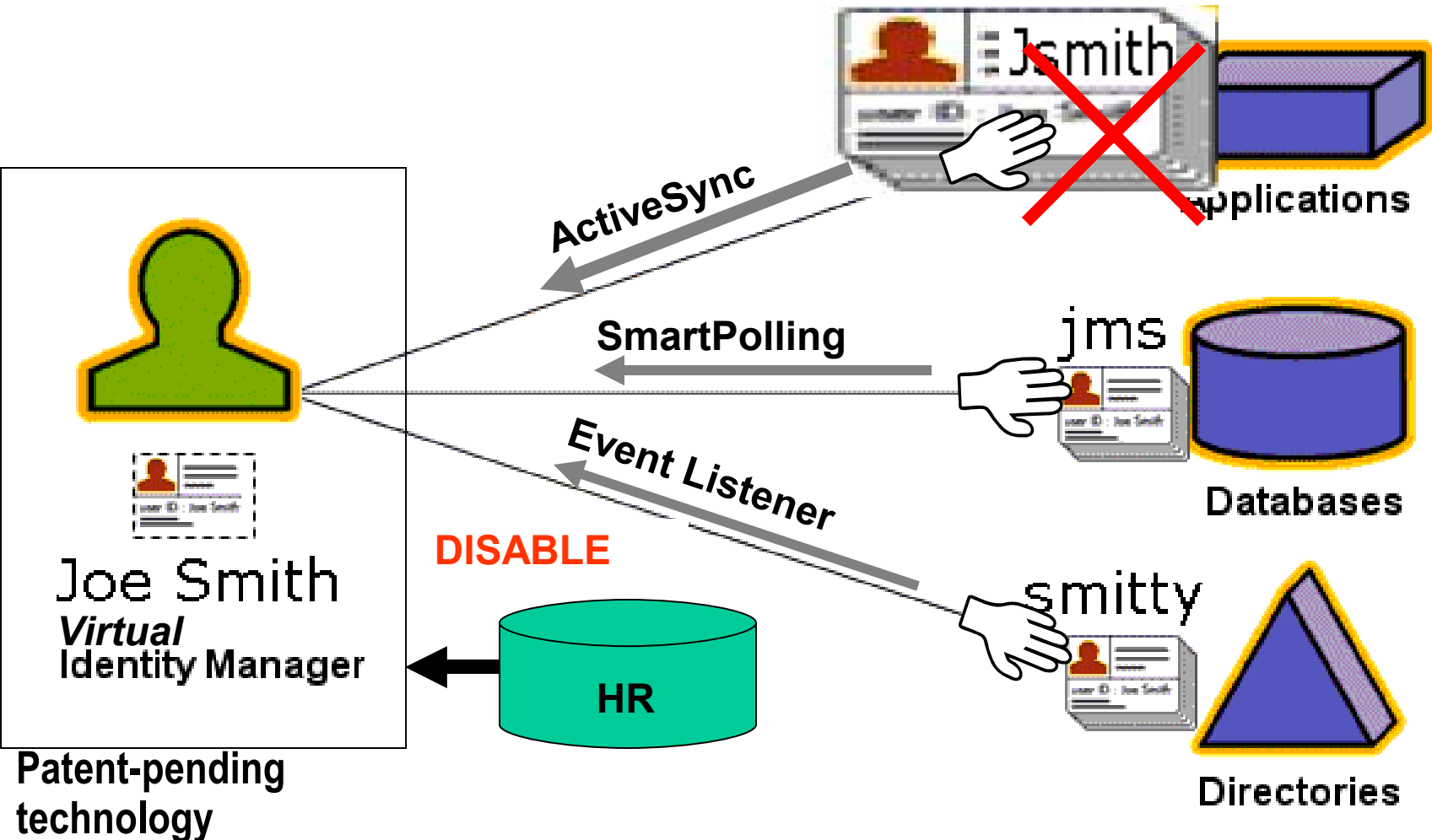
Patent-pending technology



Sun Virtual IdM

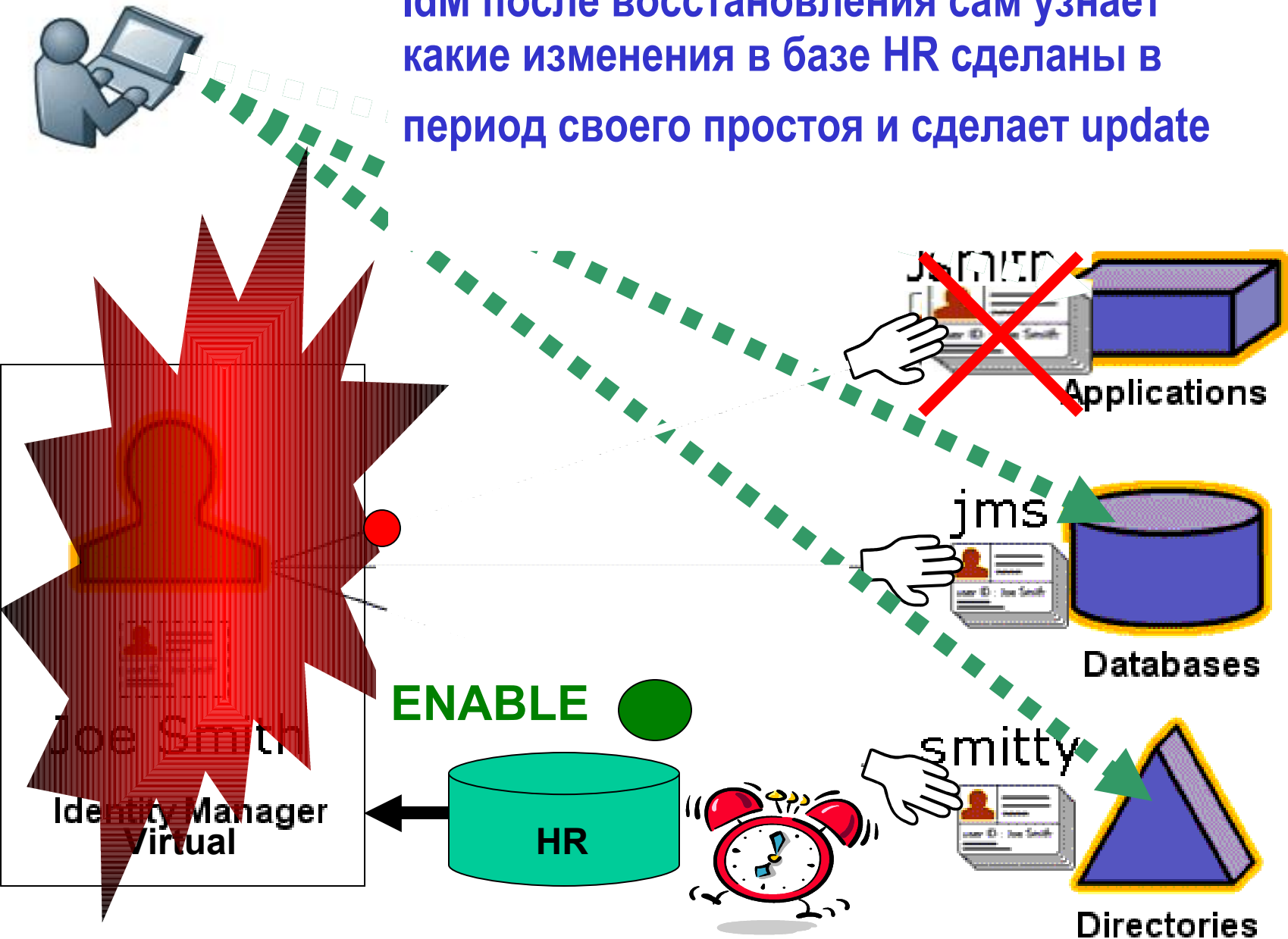


Многофункциональный **интерактивный** адаптер *create, update, delete, enable, disable, passwords*



Sun Virtual IdM

IdM после восстановления сам узнает
какие изменения в базе HR сделаны в
период своего простоя и сделает update

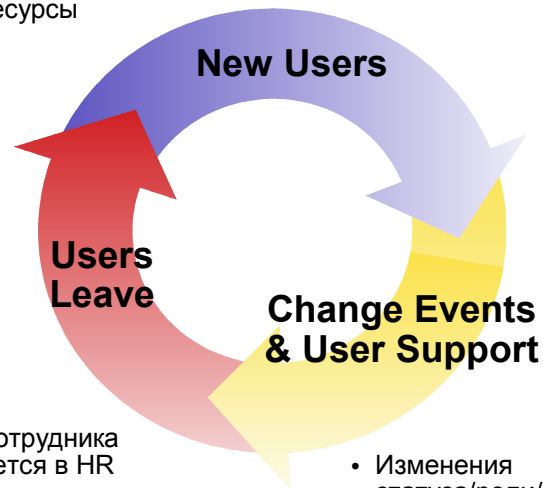


Identity Lifecycle Mgmt и Identity Auditing

Identity Lifecycle Management

(к чему пользователь **должен** иметь доступ)

- Информация пользователя внесена в HR или пользовательский регистр самообслуживания
- Эккаунты инициализированы в системах предприятия, приложениях и директориях
- Назначены и /или инициализированы нецифровые ресурсы



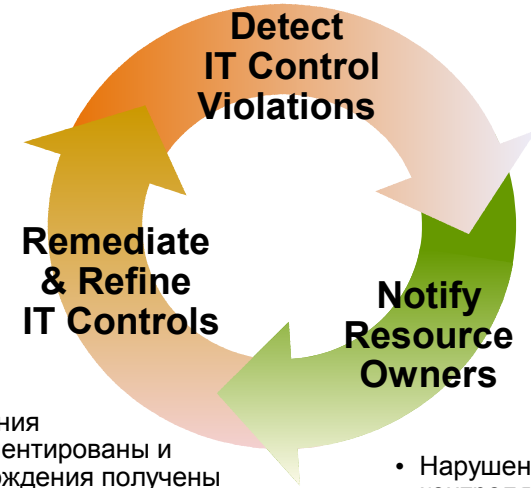
- Статус сотрудника обновляется в HR
- Изменения партнерского контакта
- Клиент закрывает эккаунт
- Эккаунт закрыт и удален
- Нецифровые ресурсы удалены

- Изменения статуса/роли/работы
- Изменение и переустановка паролей
- Изменение профайла
- Дополнительный запрос на открытие нового эккаунта или выделение ресурса

Identity Auditing

(К чему пользователь **может** иметь доступ)

- Определение функций ИТ контроля в соответствии с правилами (e.g. Sarbox, HIPAA, GLBA)
- Запланированы периодические проверки доступа
- Системы проверены на соответствие с правилами ИТ контроля



- Изменения задокументированы и подтверждения получены
- Другие нарушения ИТ контроля исправлены путем удаления эккаунтов
- Функции ИТ контроля изменены и включены в процесс инициализации эккаунта пользователя

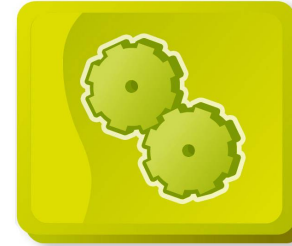
- Нарушения ИТ контроля зафиксированы на нескольких приложениях
- Владелец приложений отвечающие за соответствие правилам уведомлены о нарушениях

Порфолио Sun Identity



- Инициализация пользователей
- Управление паролями
- Синхронизация

Identity Manager



- Обзор политик аудита
- Автоматизированное подтверждение
- SEM identity services

Identity Auditor



- Контроль доступа
- Single sign-on
- Federation

Access Manager



- Администрирование идентификаций
- Услуги по синхронизации
- Интегрированная инициализация
- Carrier-grade scalability

Identity Manager SPE



- Directory services
- Безопасность/отказоустойчивость
- AD synch services

Directory Server Enterprise Edition



- Partner single sign-on
- соединение эക്കാунтов
- Global log-out

Federation Manager

Функция	Описание
Политики ИТ-безопасности и аудита	<ul style="list-style-type: none">• Преконфигурированные /best practices/ наиболее часто используемые политики контроля• Кастомизированные политики
Гибкое обнаружение нарушения выполнения политик	<ul style="list-style-type: none">• Авто-скан ресурсов: регулярный автоматический (по расписанию) или по особому случаю• Автоматическое определение нарушений, извещение о них и устранение нарушений
Суммарные отчеты высокого уровня	<ul style="list-style-type: none">• Суммарные сводные отчеты о нарушениях• Гибкое конфигурирование(фильтрование) нарушений: по политике, по ресурсам, по департаментам, пользователям и т.д.
Отчеты о нарушениях	<ul style="list-style-type: none">• Преконфигурированные отчеты по аудиту (SOX), требуемые законодательно• Кастомизированные отчеты (по внутреннему корпоративному кодексу)
Сервис "Identity for SEM"	<ul style="list-style-type: none">• Интеграция с системой оповещения Security Event Management
Интеграция с системами мониторинга доступа	<ul style="list-style-type: none">• Срочное блокирование доступа пользователя при грубых (по заранее введенным критериям) нарушениях правил

User Access Report

Показывает список ресурсов (доступов), предоставленных отдельному пользователю

Access Review Detail Report

Данные на соответствие списков доступа пользователя политике безопасности

Organization Violation History

Гистограмма случаев нарушений политики безопасности в каждом ресурсе или подразделении

ДОСКА ПОЧЕТА - КЛИЕНТЫ Sun:



Customer Reference Database



СПАСИБО!

anton.sinsky@sun.com

