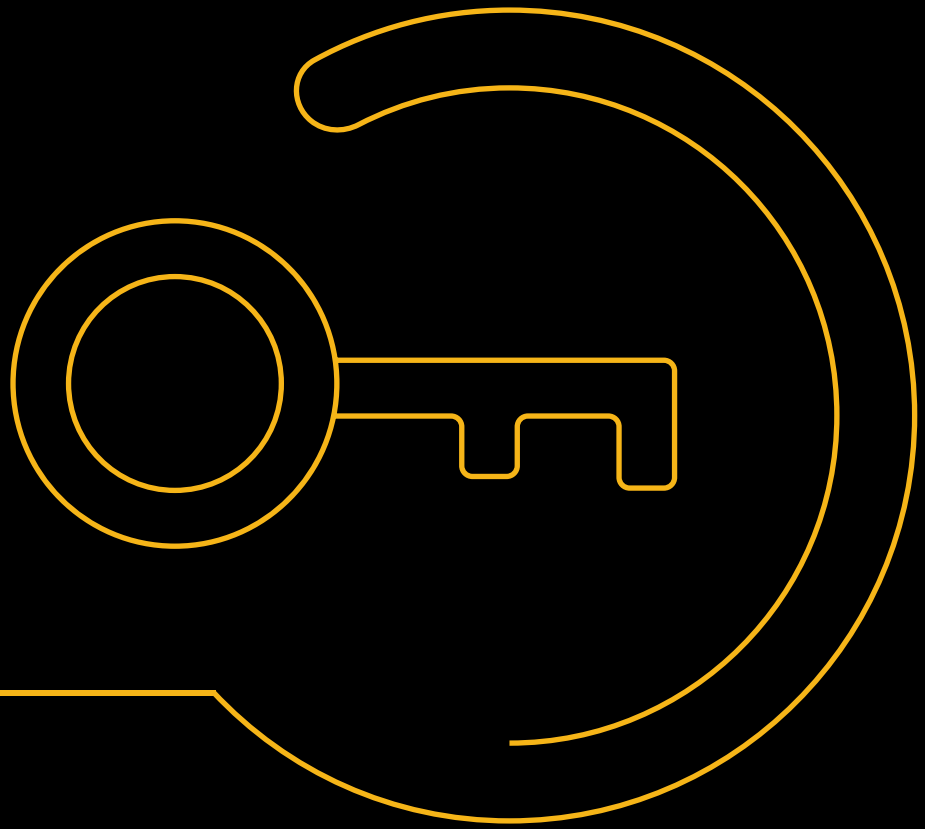
ESKA

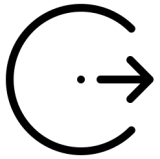
КОМПЛЕКСНОЕ УПРАВЛЕНИЕ ДОСТУПОМ



ONE IDENTITY™

Что такое IAM?

ONE IDENTITY



Аутентификация

“Who am I?

Авторизация

“What I can do?“

Администрирование

“Как все настроить правильно?”

Аудит

“Как убедиться, что все работает по правилам?”

Зачем нужно комплексное управление доступом

ONE IDENTITY

Bloomberg Our Company | Professional | Anywhere

HOME QUICK NEWS OPINION MARKET DATA PERSONAL FINANCE TECH POLITICS SUSTAINABILI

Societe Generale Reports EU4.9 Billion Trading Loss (Update8)

France's Societe Generale Reports Biggest Trading Loss Ever by a Bank — Bloomberg

Societe Generale, France's second-largest bank by market value, said unauthorized bets on stock-index futures by an unidentified employee caused a 4.9 billion-euro, or $7.2 billion trading loss, the largest in banking history.

The graphic on the right lists some the biggest and most notable losses by rogue traders.

Company (Country): Year		Cause of loss
Societe Generale (France): 2008	$7.2 billion	Stock-index futures
Amaranth Advisors (U.S.): 2006	$6.6 billion	Natural-gas futures
Sumitomo (Japan): 1996	$2.6 billion	Copper futures
Barings (U.K.): 1995	$1.8 billion	Asian futures
Allied Irish Banks (Ireland): 2002	$691 million	Currency options

By Gregory Viscusi and Anne-Sylvaine Chassany - January 24, 2008 15:20 EST

The New York Times — World Business

French Bank Says Rogue Trader Lost $7 Billion

By NICOLA CLARK and DAVID JOLLY
Published: January 25, 2008

TWITTER LINKEDIN SIGN IN TO E-MAIL PRINT SINGLE PAGE REPRINTS SHARE

BROOKLYN NOVEMBER 4 WATCH TRAILER

Correction Appended

PARIS — A French bank announced Thursday that it had lost $7.2 billion, not because of complex subprime loans, but the old-fashioned way — because a 31-year-old rogue trader made bad bets on stocks and then, in trying to cover up those losses, dug himself deeper into a hole.

Société Générale, one of France's largest and most respected banks, said an unassuming midlevel employee who made about 100,000 euros ($147,000) a year — identified by others as Jérôme Kerviel — managed to evade multiple layers of computer controls and audits for as long as a year, stacking up 4.9 billion euros in losses for the bank.

Jérôme Kerviel, 31, was a low-level bank employee.

Unlike many of his high-level trading colleagues, Mr. Kerviel graduated not from one of France's elite

- Высокая трудоёмкость сбора данных о правах доступа сотрудников, об их согласовании и изменении
- После переводов по должности накапливаются избыточные права доступа
- Незаблокированные учётные записи уволенных сотрудников
- В информационных системах есть пользователи с несогласованными правами доступа
- Сотрудники имеют больше прав доступа, чем им необходимо
- Конфликты разделения ответственности при назначении полномочий

Зачем нужно комплексное управление доступом

ONE IDENTITY

Исследование Dimentional Reseach, опрос 100 CISO

- 70% не уверены, что отбор доступа при увольнении происходит своевременно
- Только в 14% случаев доступ к излишним ресурсам отзывается сразу после события в кадрах
- Только 9% уверены, что у них отсутствуют бесхозные учетки
- Только 1 из 4 уверен, что права и полномочия сотрудников назначены правильно
- Только 11% проводят аудит ролевой модели хотя бы раз в месяц
- 2 дня всреднем занимает отобрать доступ при увольнении

Зачем нужно комплексное управление доступом

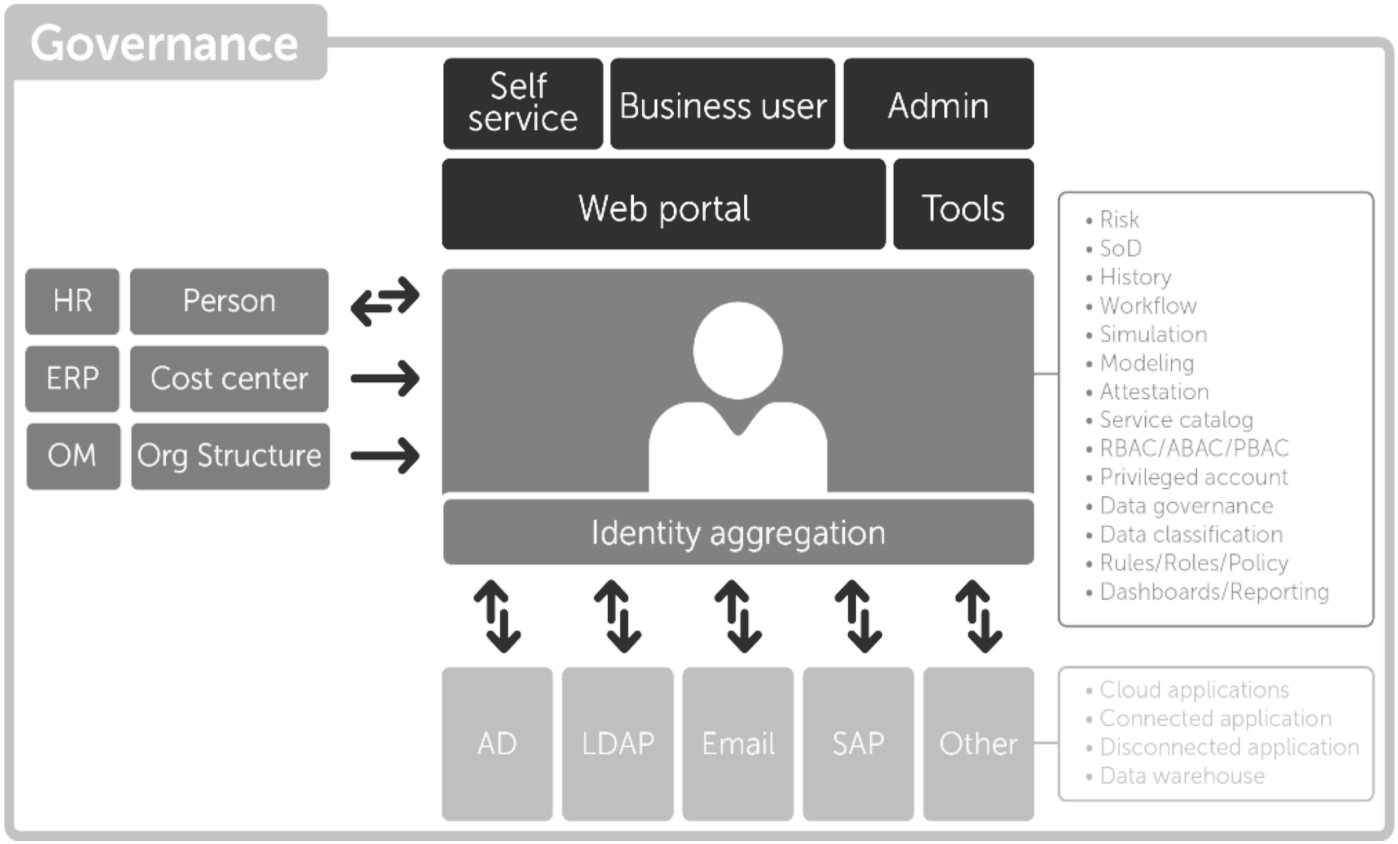
ONE IDENTITY

PCI Security Standards Council

Information Security Management ISO 27001 Certified

- Должно контролироваться создание, изменение и удаление идентификационных данных (PCI DSS п.8.5.1)
- Предоставление полномочий должно быть согласованным, контролируемым (PCI DSS п.7.1.3, ISO 27001 п.11.2.2)
- Права доступа должны незамедлительно отзываться при увольнении сотрудника, пересматриваться при переводе по должности (PCI DSS п.8.5.4)
- Руководство должно осуществлять периодически пересмотр прав доступа пользователей, используя формальный процесс (ISO 27001 п.11.2.4)
- Обязанности и области ответственности должны быть разграничены (ISO 27001 п.10.1.3)

Комплексное управление доступом, построенное как единое решение – One Identity Manager (1IM)



- Жизненный цикл информации о сотруднике и доступе
- Ролевая модель доступа
- Заявки и согласование доступа
- Сертификация доступа
- Контроль доступа и анализ рисков
- Разделение полномочий
- Отчетность и аналитика

Жизненный цикл сотрудника компании

ONE IDENTITY™

Комплексный контроль доступа

One Identity Manager (1IM) – Комплексная система управления правами доступа уровня предприятия. Раздача прав при приеме/переводе/увольнении, организация ролевой модели, конструктор ролей, аттестация доступа, коннекторы к HR и целевым системам, конструктор коннекторов, портал для запроса доступа, цепочки согласования, делегирование, рисковая модель, контроль конфликтного доступа и разделение полномочий - SoD, обзор доступа на 360, отчетность и интерактивные панели управления и тд.

One Identity Manager – Data Governance Edition (1IM –DGE) - расширение 1IM для неструктрированных данных на файловых серверах

Эффективность доступа

Active Roles – автоматизация рутиных процессов в AD, Exchange. «Облегченный» вариант IDM для MS среды

Password Manager – Самостоятельный сброс паролей и разблокировка учетных записей пользователями.

Defender – двухфакторная аутентификация. Soft и Hard токены.

Cloud Access Manager – система единой точки входа для Web-приложений. Технология Reverse proxy.

Enterprise Single Sign-on - система единой точки входа для любых приложений

Привилегированный доступ

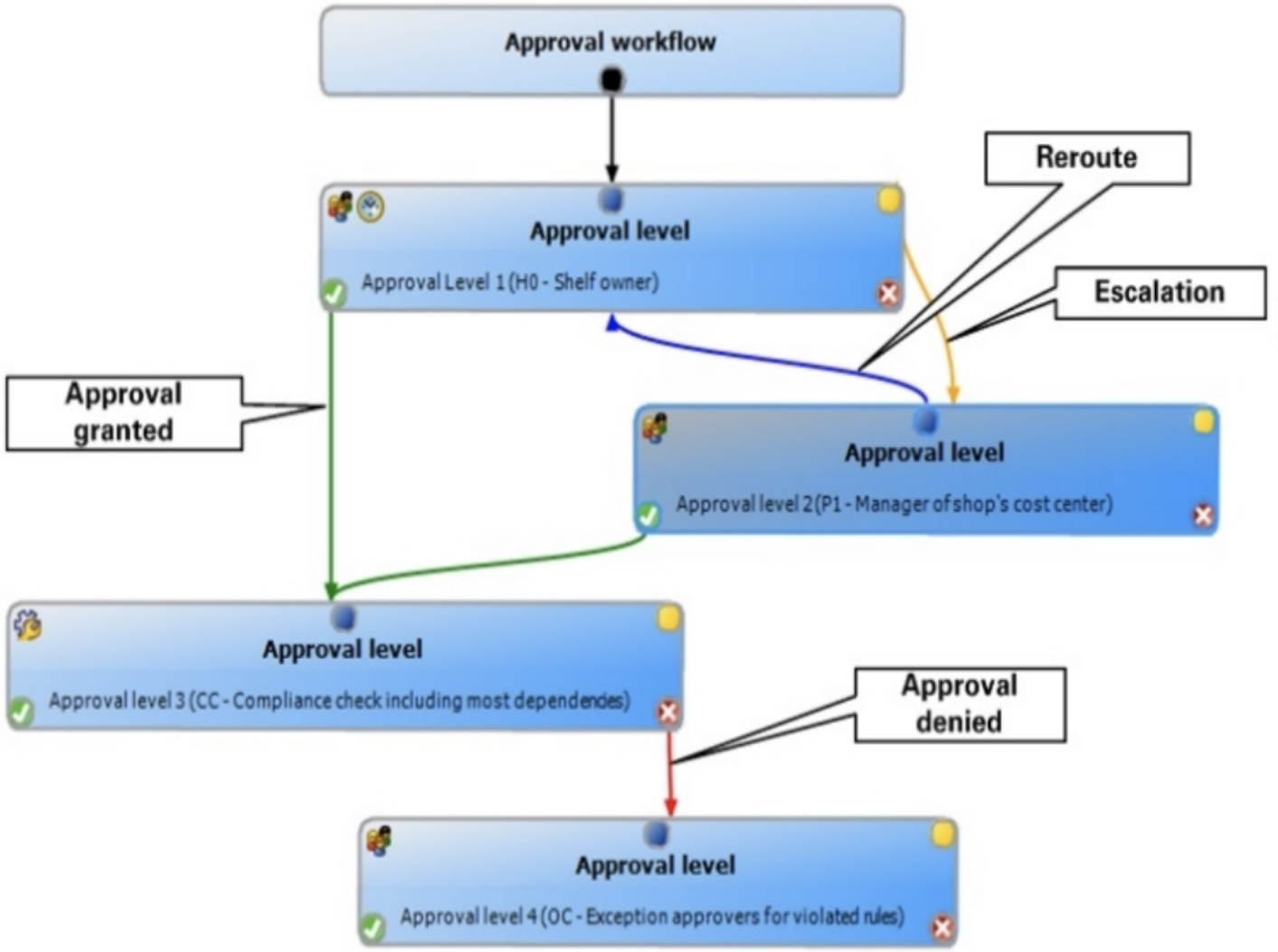
Safeguard for Privileged Passwords – Решение для выдачи административных паролей. Защищенный аплаенс.

Safeguard for Privileged Sessions – выдача и запись административных сессий. Защищенный аплаенс.

Privileged Access Suite for Unix - Аутентификация в UNIX/Linux через AD, управление Unix/Linux через групповые политики AD, делегирование полномочий, Расширение SUDO, контроль доступа, логирование ввода с клавиатуры.

Цепочки согласований настраиваются в удобном графическом интерфейсе

ONE IDENTITY



Более 40 шаблонов утверждения доступны «из коробки»

- Делегирование
- Предоставление прав с условием
- Эскалация
- Напоминания
- Передача прав доступа последовательная и параллельная
- На основе корпоративной иерархии

ESKA

One Identity Manager – коннекторы к системам

ONE IDENTITY

Любое другое облачное приложение

servicenow · CONCUR · salesforce · SAP SuccessFactors · Taleo

Подключение к облаку One Identity

Azure Active Directory · Office 365 · Google apps

1IM

Базовые коннекторы

CSV · SCIM · Web Services · Powershell · ADO .Net

Готовые коннекторы

Active Directory · Exchange · SharePoint · SAP R/3 · IBM Notes · LDAP Lightweight Directory Access Protocol · UNIX · ORACLE e-businesssuite · IBM Mainframe · AS/400

eska.global