Новые возможности технологии двухфакторной аутентификации RSA SecurID

Решаемые проблемы

Аутентификация – способ проверить подлинность пользователя перед тем как предоставить ему доступ к корпоративной информации.

Стандартный способ аутентификации – использование паролей.

- простые пароли
  - легко взломать, подобрать, угадать
- сложные пароли
  - трудно запомнить, обычно записывают (риск перехвата)
- пароли можно передать другим пользователям и злоумышленникам – нет аутентичности
- пароли можно перехватить
- пользователи забывают пароли – нагрузка на help desk

Все это вызывает риски НСД к критичным данных!

Краткий обзор технологии

- Двухфакторная аутентификация RSA SecurID обеспечивает гораздо более надежный уровень проверки подлинности пользователя, чем обычные пароли.

Двухфакторная аутентификация

+

ПИН

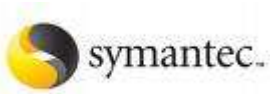
Защита доступа к критичным приложениям RSA SecurID – двухфакторная аутентификация

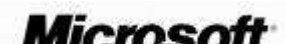
Используется для защиты:

- VPN
- Web приложений, порталов (online banking)
- терминальных серверов Citrix, Windows
- доступа привилегированных пользователей
- беспроводных сетей
- локального доступа к рабочим станциям

SecurID – совместимость

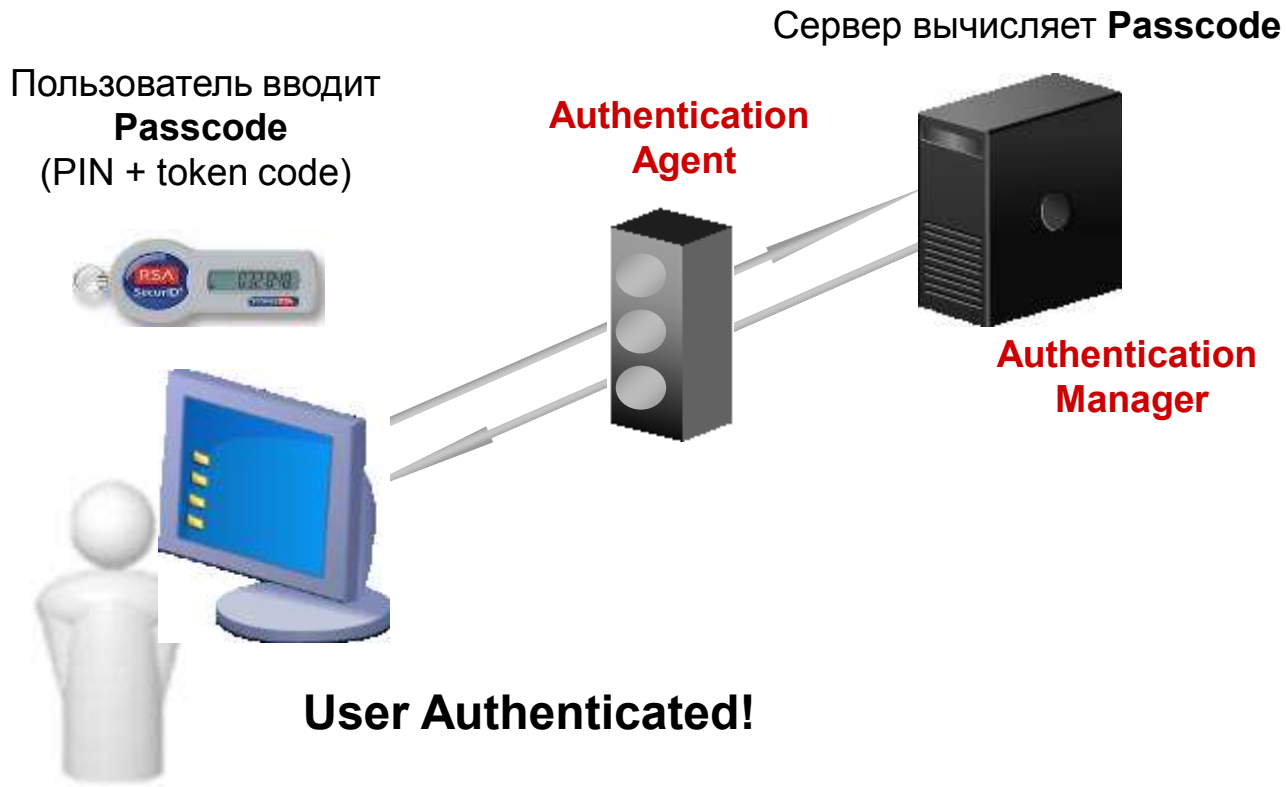
- SecurID «из коробки» работает с более чем 350 партнерскими продуктами, включая
  - Веб-серверы (Oracle Application Server, Microsoft IIS, Apache и др.)
  - VPN и прочие сетевые устройства (Cisco, CheckPoint, Microsoft и др.)
  - Терминальных серверов (Citrix, Microsoft)
  - ОС Windows
- Есть API, позволяющее встроить SecurID практически в любую систему






Технология двухфакторной аутентификации RSA (SecurID)

Secure One-Time Password
Как работает аутентификация RSA SecurID®



Аутентификатор генерирует каждый 60 сек. новый pass code

RSA SecurID

USERID: ivanov
PASSCODE: 2468 234836

PASSCODE = PIN + TOKENCODE

TOKENCODE – сменяется каждые 60 сек.

Часы, синхронизованные с UTC / GMT

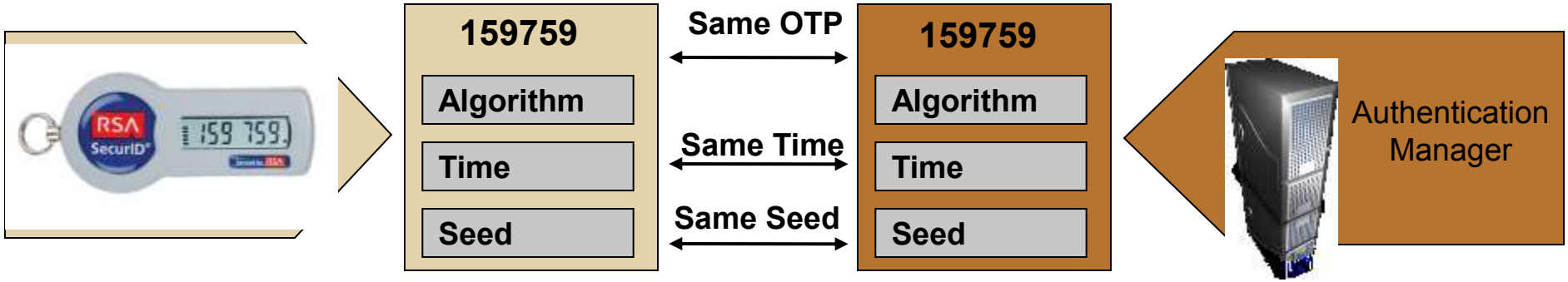
Алгорит

Уникальное число – seed – начальный вектор генерации

Батарея

RSA The Security Division of EMC

Как работают генераторы OTP (One Time Password), синхронизированные по времени?



- Генератор (брелок) содержит встроенные высокоточные часы, которые каждые 60 сек. используются для вычисления нового пароля
- Практически невозможно перехватить этот пароль, т.к. он уже не действителен через одну минуту
- Второй параметр, используемый для генерации одноразового пароля – вектор начальной инициализации (Seed). Он “прошивается” в генераторе при его производстве.
- Для аутентификации, сервер Authentication Manager также вычисляет текущий пароль пользователя используя показания системных часов и начальный вектор инициализации (с каждым аппаратным токеном поставляется файл с Seed, который загружается в сервер)

Аутентификаторы RSA SecurID

RSA SecurID

Устройства аутентификации

- Большое разнообразие видов устройств
  - Key fob (Токены)
  - Карты
  - Pin Pad
  - PC
  - КПК Palm
  - Мобильные телефоны
  - Смарт-карты/USB
- Аутентификация Zero-footprint
  - Не требуется инсталляции программного обеспечения (только токены)
- Просты в использовании и при обучении
- Наиболее широко применяемое решение для аутентификации

RSA
The Security Division of EMC

Традиционные аппаратные SecurID аутентификацторы

SID200

SID520

SID900

Формат – классические карточки

- RSA SecurID® SID200 – Classic Card
- RSA SecurID® SID520 – Pin Pad
- RSA SecurID® SID900 – Transaction Signing

Формат “брелков”

- RSA SecurID® SID700 – брелок
- RSA SecurID® SID800 – USB / Hybrid Smart Card

SID700

SID800

RSA The Security Division of EMC

RSA SecurID SID700 Authenticator

- Более высокое качество и надёжность
  - Усовершенствованный дизайн
- Удобство и простота использования вместе с уменьшенными размерами устройства и расширенным функциональным экраном
- Поддержка co-branding токенов – нанесение логотипа банка
- Использует Authentication Manager версии 5.1 или выше

RSA SecurID SID800 Authenticator

- Одно хранилище для множества типов удостоверений
  - Динамически изменяемые OTP,Сертификаты и Пароли
  - Смешенные среды аутентификации для Enterprise, Remote & Web доступа
  - Цифровые подписи и сложная криптография
- Защита инвестиций клиента через масштабируемость
  - Развертывайте OTP токены и выборочно задавайте другую функциональность
  - Наличие JAVA поддерживает уверенность в совместимости с будущими приложениями и расширениями
- Простота использования
  - Программный код доступа токена уменьшает количество вводимых пользователем символов

RSA
The Security Division of EMC

Новая версия RSA SecurID 800

- Четвертое поколение аппаратных аутентификаторов и программных клиентов
  - SecurID 800 “Revision D”
  - RSA Authentication Client 3.5
- Поддержка ключей 2048-bit
  - Новое требование NIST начиная с 2010
- Лучшая в своем классе производительность
- Тесная интеграция с Microsoft Windows
  - Windows 7 / Server 2008 R2
  - Microsoft Forefront Identity Manager 2010
  - BitLocker to Go
  - DirectAccess
- Новый графический интерфейс
- Централизованное управление политиками

RSA Authentication Client 3.5
(SecurID 800 Client Software)

SecurID 800 “Rev D”
(USB Hybrid Authenticator)

RSA
The Security Division of EMC

Совместимость с Microsoft Smart Card Framework и поддержка «из коробки» Microsoft environments

- Архитектура “Minidriver”
  - Нет «толстых» клиентов, не нужно заменять CSP
  - Используется существующий Microsoft Base Smart Card CSP
- Поддержка различных версия OS
  - Windows XP (32-bit)
  - Windows 2K3/2K8 (32/64-bit)
  - Vista / Windows 7 (32/64-bit)
- Совместимость с Windows Logon
  - Не нужно менять GINA (graphical identification and authentication) или Credential Provider (Vista)
  - Управление smart card PIN
  - Challenge / response PIN unblocking
- Поддержка новейших технологий Windows
  - Forefront Identity Manager 2010 (бывший ILM)
  - BitLocker-to-Go
  - DirectAccess

RSA
The Security Division of EMC

RSA Control Center

Интуитивно понятный пользовательский интерфейс и централизованное управление

RSA Control Center это опциональный компонент Authentication Client 3.x, который упрощает развертывание и предоставляет сервис «самообслуживания» когда не развернута централизованная система Card Management System (CMS).

- Графический клиент (Self-service GUI Client)
  - Импорт и управление учетными данными
  - Управление PIN кодом
  - Информация и статус устройства аутентификации (SID800)
  - Быстрый доступ к SecurID tokencodes из Control Center tray icon
- Модульность и возможность настройки
  - Деактивация\активация пунктов меню на основе централизованной ИТ политики (GPO)
- Дополнительные возможности
  - GPO-enforced (запрет на изменение конфигурации локальными администраторами)
  - Утилита для решения проблем с токенами
  - Поддержка нескольких токенов

RSA
The Security Division of EMC

Програмные токены на Mobile Devices

- Превращает мобильное устройство в SecurID аутентификацитор
- Поддержка всех распространенных мобильных платформ
- BlackBerry, Windows Mobile, Java Micro Edition, Symbian UIQ, iPhone, Android (план на этот год)
- П.о. устанавливается как приложение Software application installed и “привязывается” к устройству пользователя

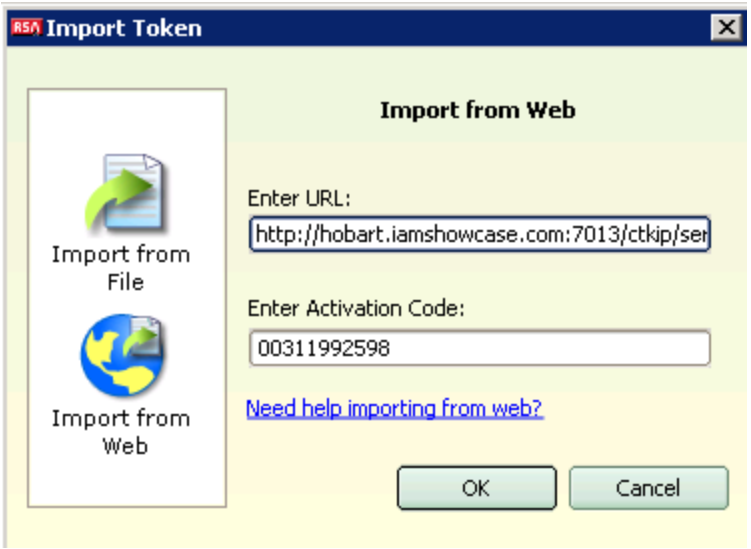
Превращает мобильное устройство в RSA SecurID Authenticator

Обеспечивает защищенный удаленный доступ с мобильного устройства

The Cryptographic Token Key Initialization Protocol (CT-KIP)

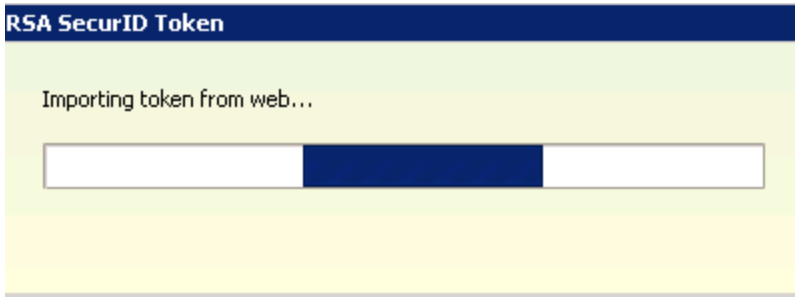
Программный токен Desktop 4.0. Динамическая активация

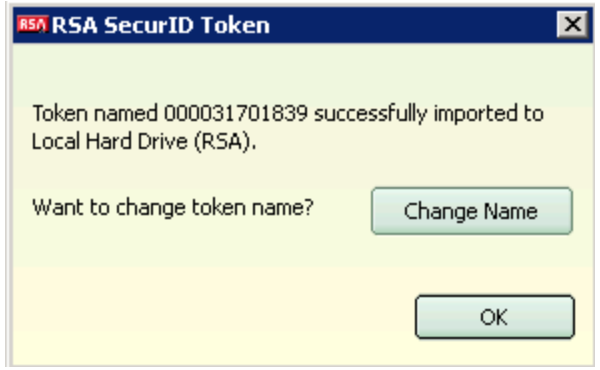
- Администратор передал пользователю CT-KIP URL и Activation Code
- Пользователь запускает приложение и выбирает “Import Token” и “Import from Web”
- Пользователь вводит CT-KIP URL и Activation Code



Программный токен Desktop 4.0. Динамическая активация

- Запускается процесс CT-KIP динамической инициализации
- Если разрешено, пользователь может задать метку (название) программного токена
- Токен готов к использованию





RSA
The Security Division of EMC

Пример активация на мобильных платформах

- Java ME 2.3
- BlackBerry 3.0

RSA
The Security Division of EMC

Виртуальные токены (onDemand Authenticators)

Дополнительные возможности – аутентификация по запросу - On-demand Authentication

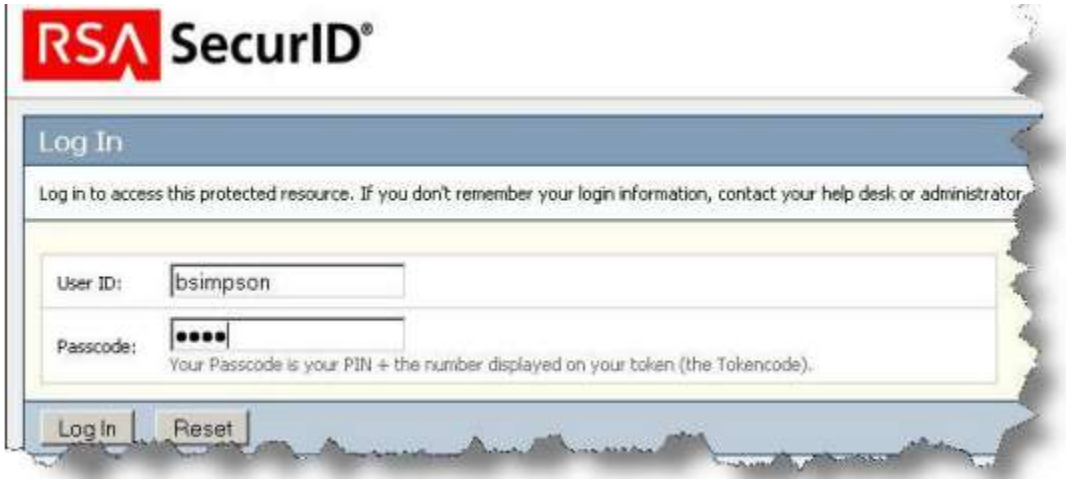
- Не требует аппаратных и программных устройств аутентификации
  - Передает одноразовый пароль (One Time Password – OTP) через SMS или по электронной почте
  - Легитимный пользователь может сам инициализировать запрос на генерацию OTP

Extended Authentication Options

On-Demand Authentication – аутентификация по запросу

- Аутентификация без использования дополнительных устройств
- Пользователь запрашивает доступ через web-сайт или получает автоматически через In-Line запрос
  - 8-разрядный одноразовый пароль (OTP) доставляется на мобильный телефон пользователя через SMS или email
- Время жизни OTP настраивается в пределах 1-70 минут

In-Line On-Demand Token Authentication

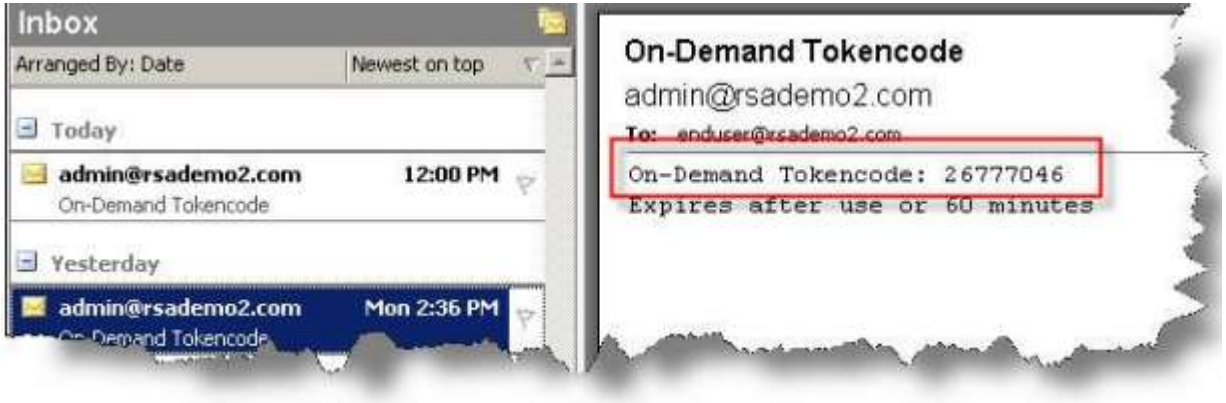


Пользователь вводит User Name и PIN в поле Passcode Длина PINa от 4 до 8 символов, что позволяет Authentication Manager отличит его от Passcode (PIN + Tokencode > 8 символов) и перейти в режим onDemand

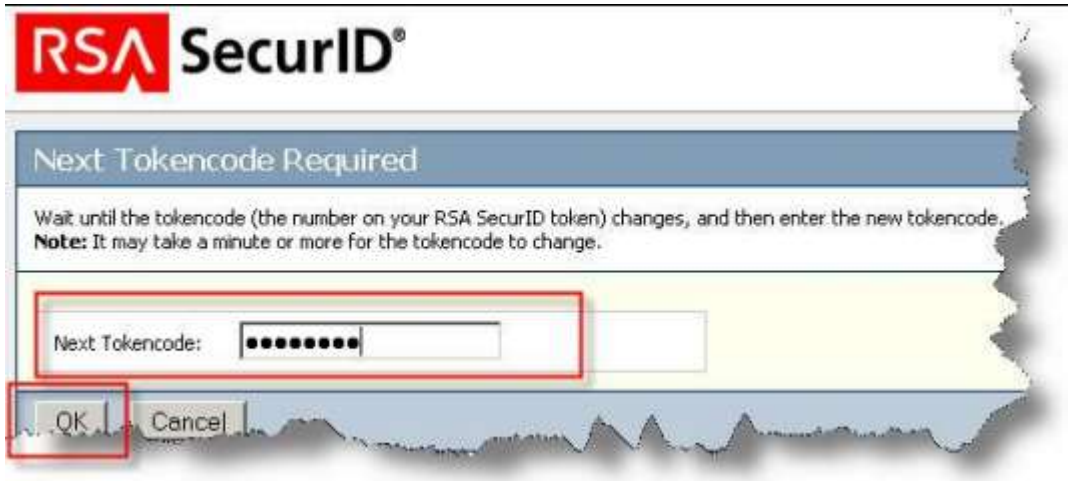
Система показывает поле Next Tokecode

RSA
The Security Division of EMC

In-Line On-Demand Token Authentication



Пользователь получает onDemand Tokencode по eMail или SMS



Пользователь в водит его в поле New Tokencode

RSA
The Security Division of EMC

Серверная часть

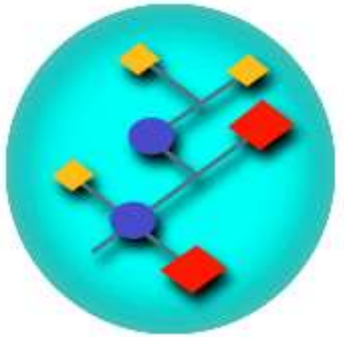
RSA Authentication Manager

- Функции AM сервер
  - Выдать аутентификаторы доверенным лицам
  - Установить и внедрить предписания политики безопасности, защищая доступ к корпоративной сети, файлам и приложениям
  - Контроль и протоколирование регистрации пользователей
  - Наиболее универсальное (всестороннее) решение на рынке аутентификации

RSA Authentication Manager

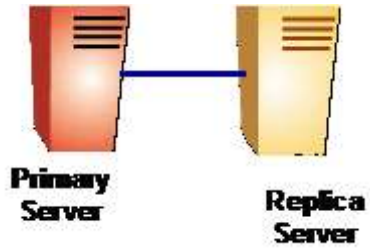
Основные моменты

- Простое решение с низкой общей стоимостью владения
  - Репликация Баз Данных
  - Прямая поддержка LDAP (Sun One, AD)
  - Web-Based Management
- Улучшенная масштабируемость и производительность
  - Балансировка сетевой нагрузки и репликация базы данных
- Снижение трудозатрат и уменьшение риска
  - Реализация высокой доступности устройств
  - Восстановление данных после сбоев
- Сохранение Инвестиций
  - Поддержка RSA Authentication Agents v5.x и выше



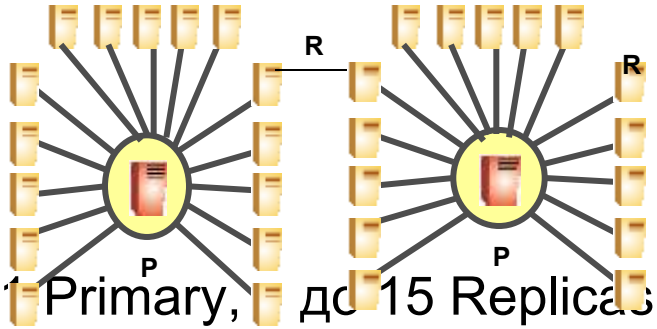
Базовая и Корпоративная версии

Base Edition



- 1 Primary, 1 Replica
- Только один Realm
- Включен модуль RSA Credential Manager ***Self Service***

Enterprise Edition



- 1 Primary, до 15 Replicas
- До 6 realms
- Кластеризация
- Высокая готовность
- Включены модули RSA Credential Manager ***Self Service*** и ***Workflow Provisioning***

Web-Based Management

- Полностью обновленный web интерфейс
- Расширенные возможности поиска
- Контекстное меню
- Манипуляция одновременно несколькими объектами
- Ролевое администрирование
- Есть интерфейс командной строки
- Java и C# API's

- **Итог: Облегченное администрирование**

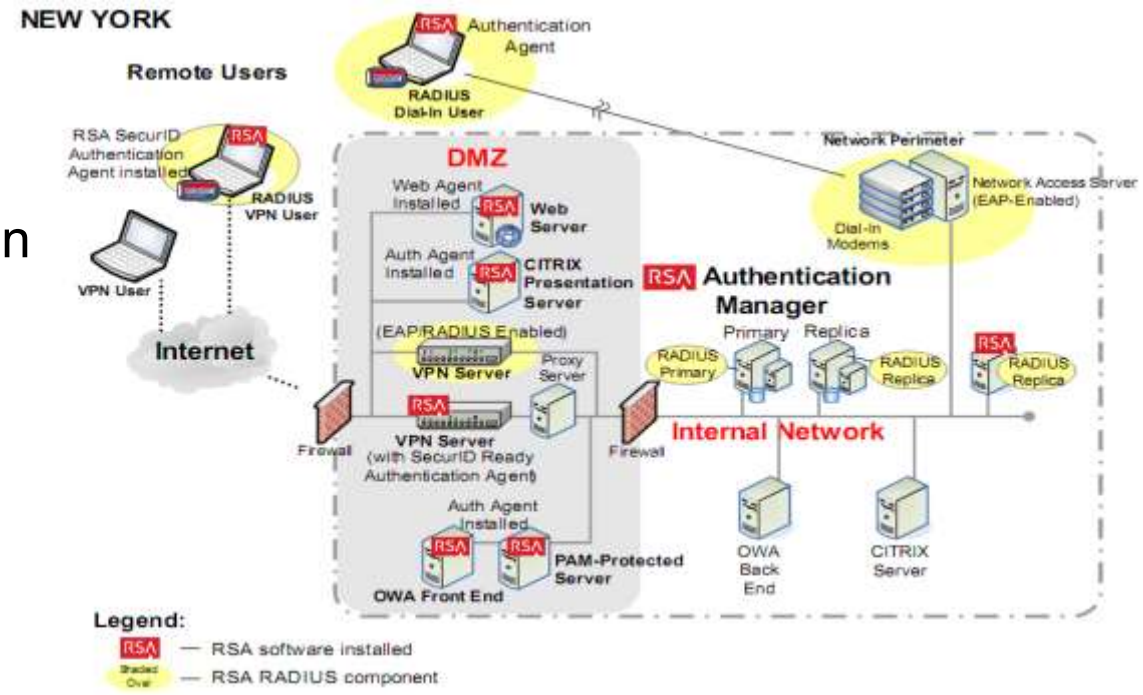
Локализация

- Возможность полной локализации как административного интерфейса, так и интерфейса пользователей (SelfService Console)
- Локализация сводится просто к переводу тегов с текстовом файле ресурсов.

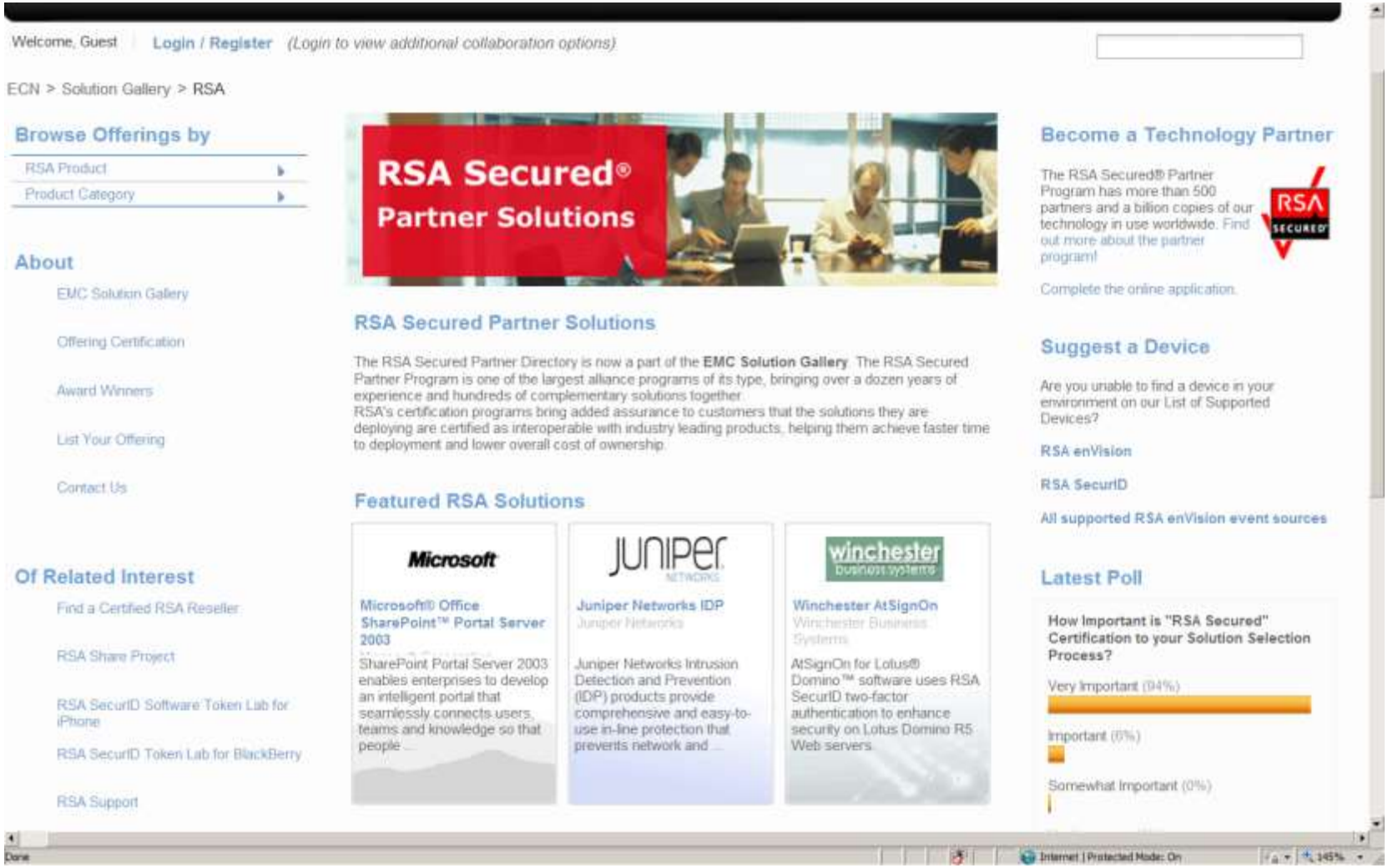
Документация

Подробное описание технологии, процедуры инсталляции, администрирования и планирования

- ❑Getting Started
- ❑Planning Guide
- ❑Migration Guide
- ❑Installation and Configuration Guide
- ❑Administrator’s Guide
- ❑RADIUS Reference Guide



Каталог решений RSA SecurID



RSA
The Security Division of EMC

RSA Authentication Manager 8.x

Что нового

AM 8.0 поддерживает новый метод аутентификации RBA

RBA можно использовать для следующих приложений:

- SSL-VPN
- OWA
- SharePoint
- Citrix
- Web portals

Улучшений интерфейс управления

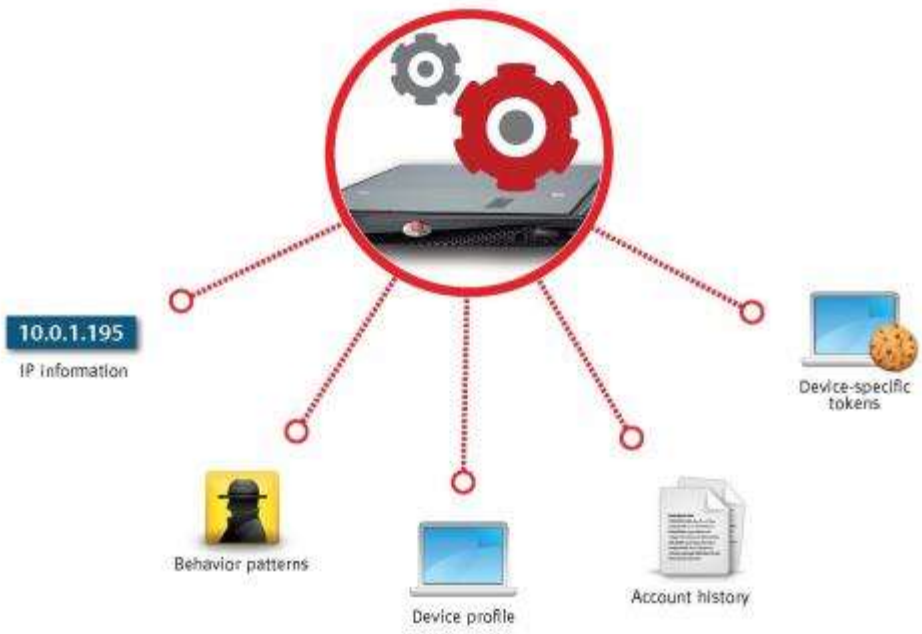
Возможность выноса сервисов, с которыми взаимодействуют пользователи в DMZ:

- RBA
- Self-Service
- CT-KIP

Распространяется как готовый к использованию продукт - аппаратный или виртуальный апплайнс

RSA Risk Engine

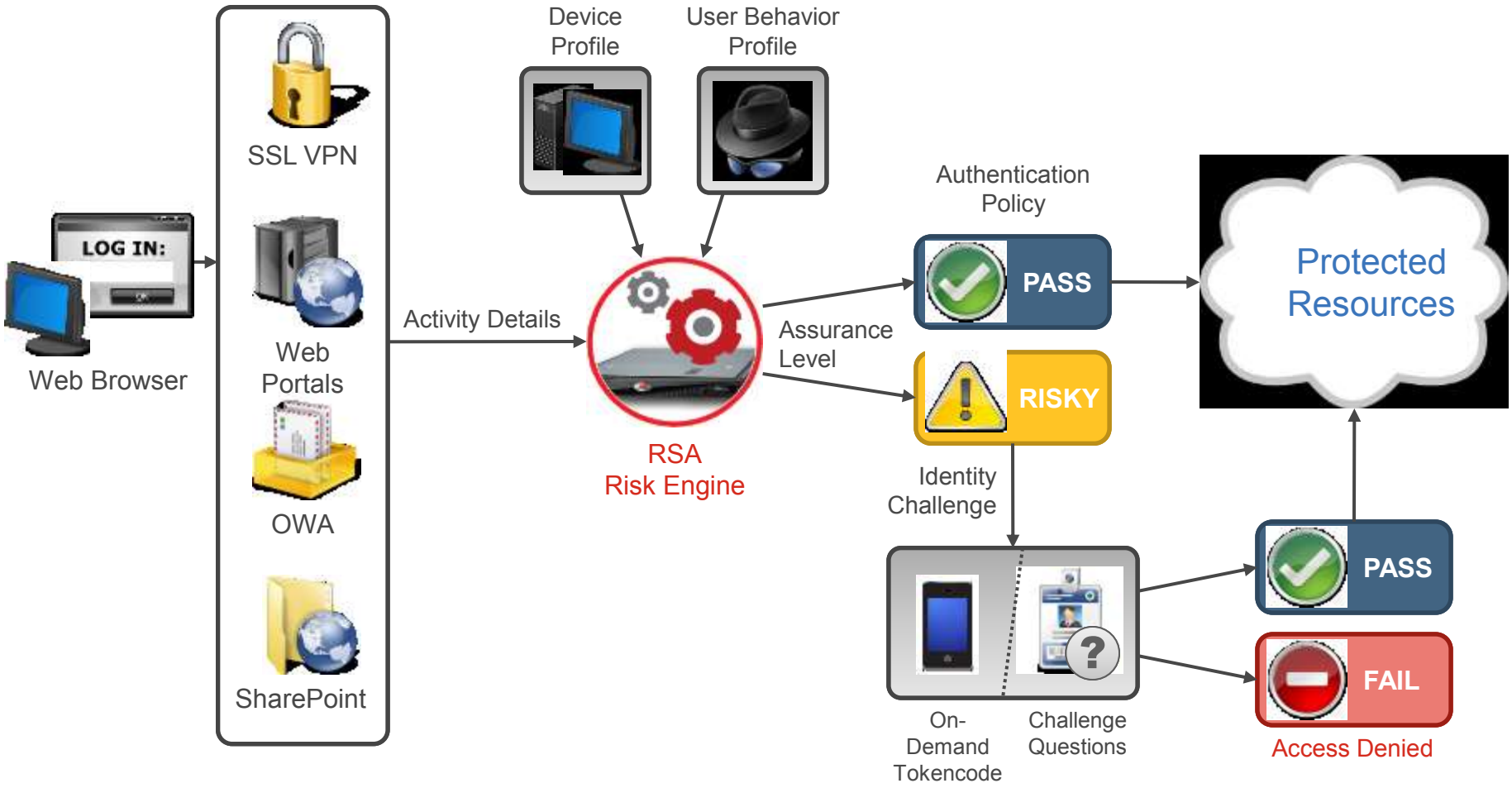
Главной отличительной особенностью AM 8.0 является механизм аутентификации с учетом факторов риска (RBA), который распознает и удостоверяет подлинность пользователей на основе информации об устройстве и профиле поведения пользователя.



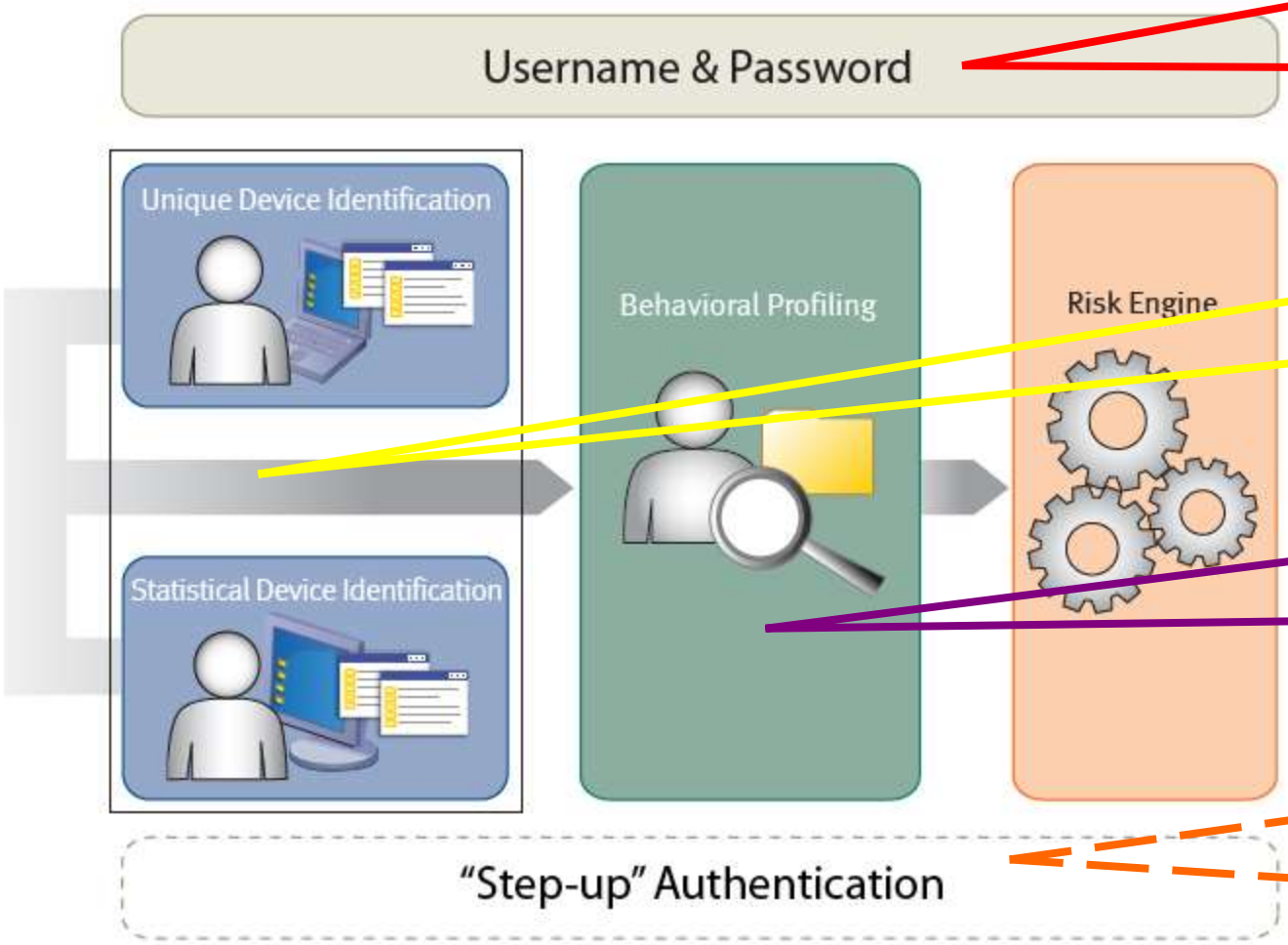
RSA
The Security Division of EMC

RBA - Risk-Based Authentication

Как это работает ?



Multi-factor Risk-based Authentication (RBA)



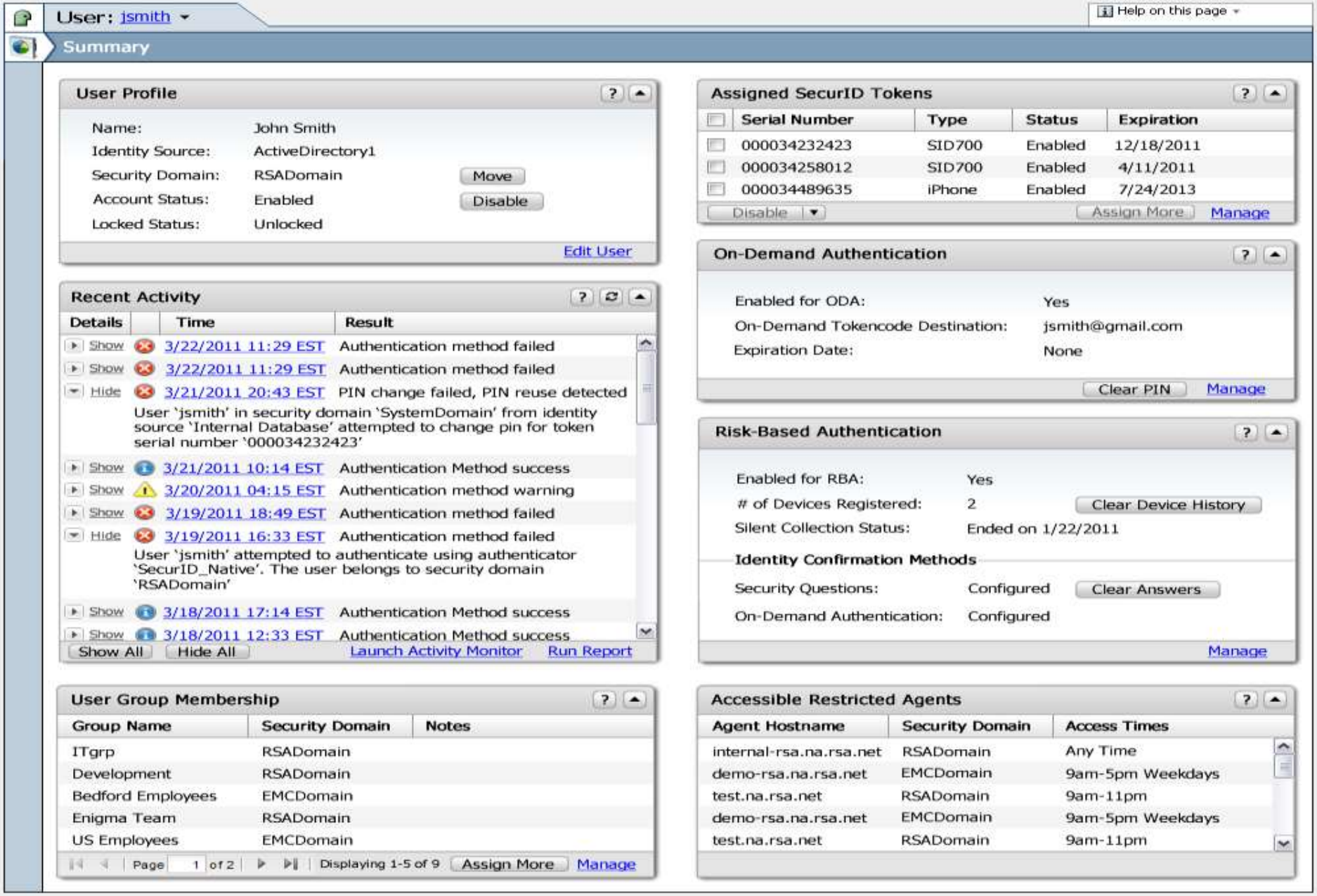
Factor #1: Something You **KNOW**

Factor #2: Something You **HAVE**

Factor #3: Something You **DO**

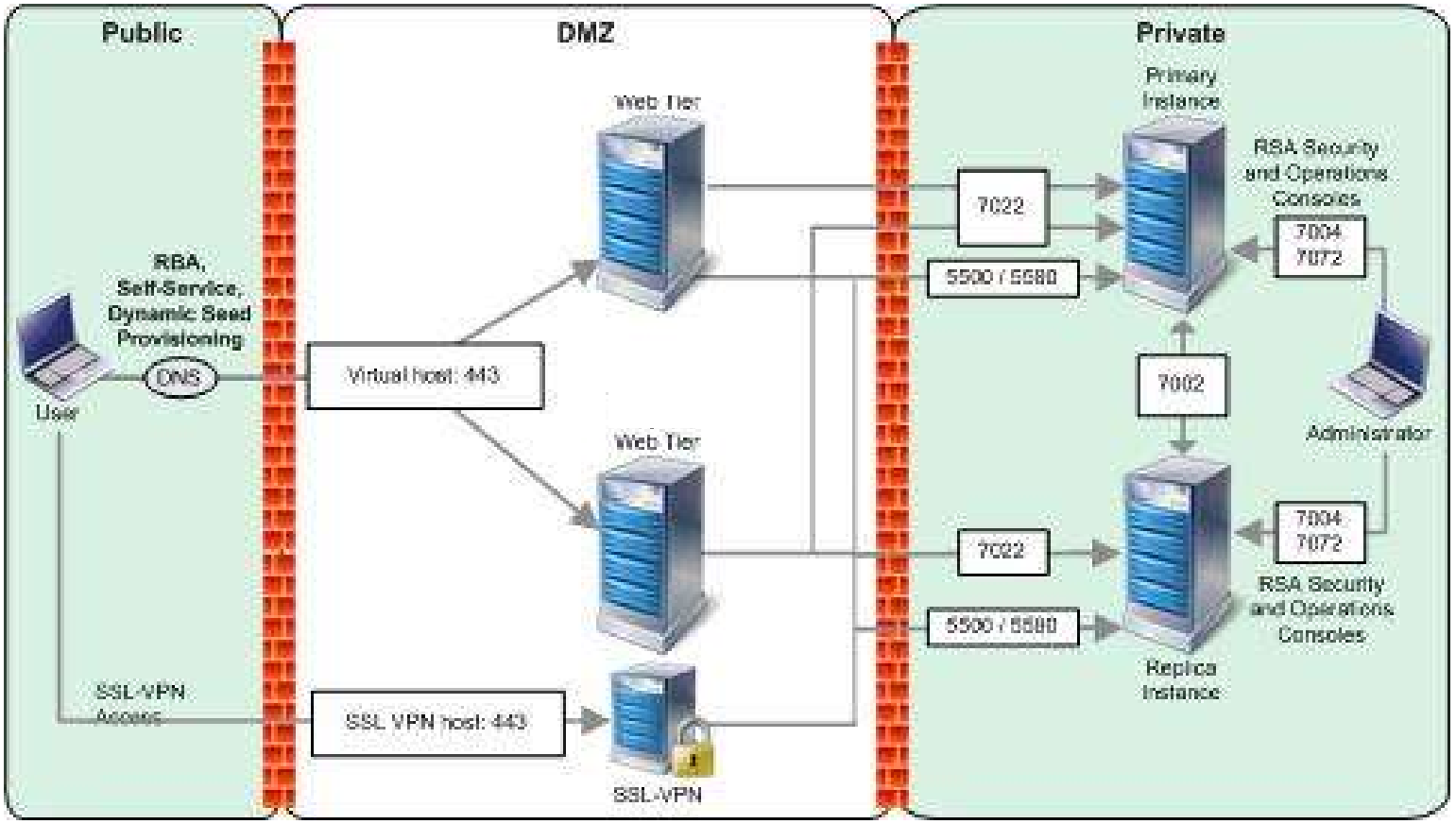
Step Up: Something You **KNOW** or **HAVE**

RSA
The Security Division of EMC



RSA
The Security Division of EMC

Web Tier Server Deployment



The Security Division of EMC

Thank you!

Резюме

Преимущества RSA SecurID

- Лидер на рынке двухфакторной OTP аутентификации (63% рынка, 20 лет)
- Поддержка большого количества систем и приложений «из коробки»
- Масштабируемость серверной части
- Разнообразие удобных и надежных аутентификаторов (hard, soft, sms)

RSA
The Security Division of EMC

Резюме

RSA SecurID:

- повышает защищенность информационных ресурсов, устраняя риски, связанные с паролями
- снижает затраты на обращения в help desk по поводу забытых паролей
- повышает удобство использования ресурсов
- создает доверенную среду для электронного бизнеса, повышая доверие клиентов и партнеров

The Security Division of EMC

Thank you!