



RSA

The Security Division of EMC

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 данным!

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

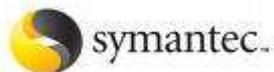
Используется для защиты:

- 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

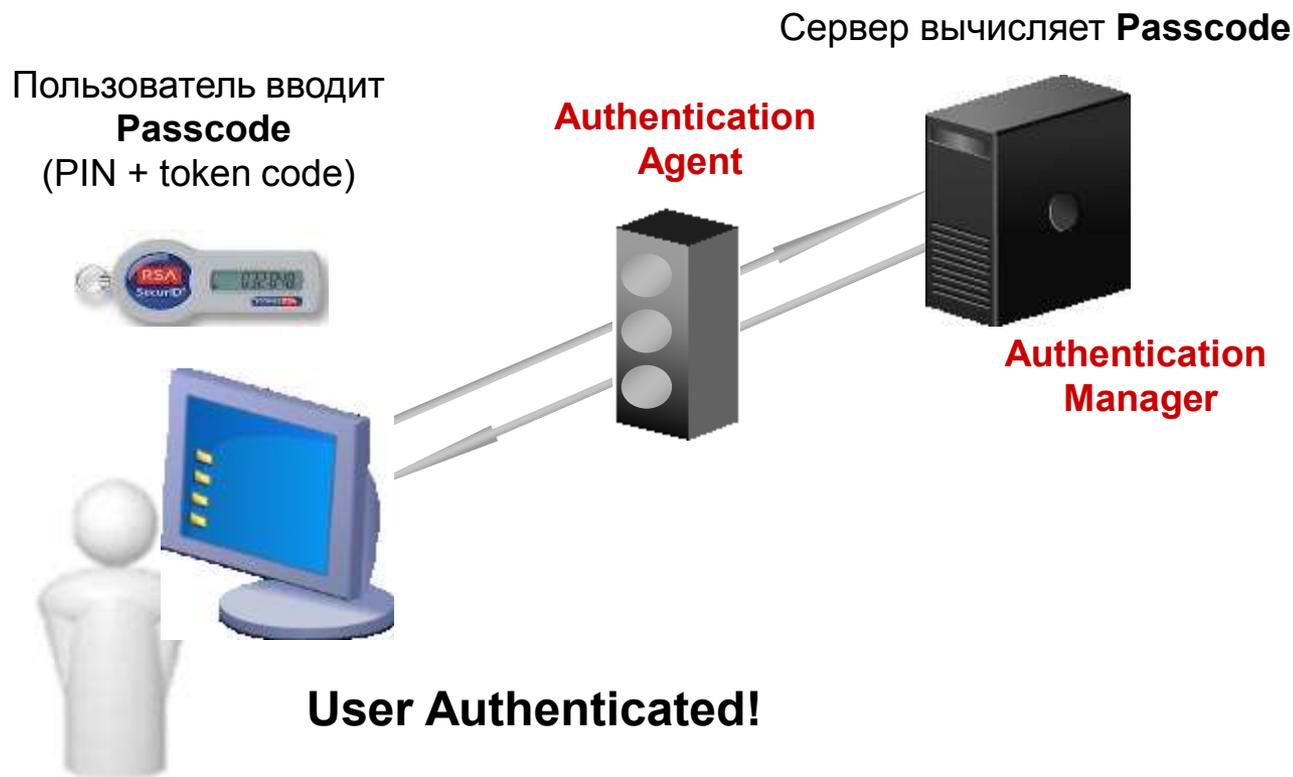


The Security Division of EMC

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.



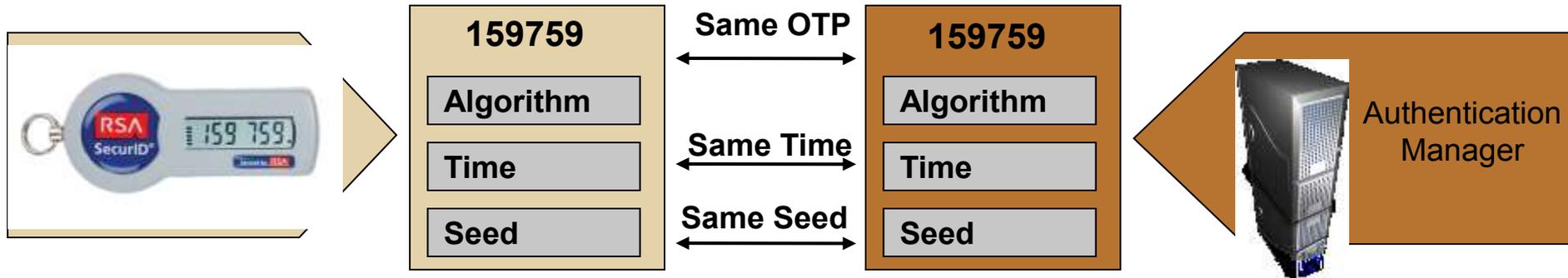
Часы,
синхронизованные
с UTC / GMT

Алгоритм

Уникальное число –
seed – начальный
вектор генерации

Батарея

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



Традиционные аппаратные SecurID аутентификаторы



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



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



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

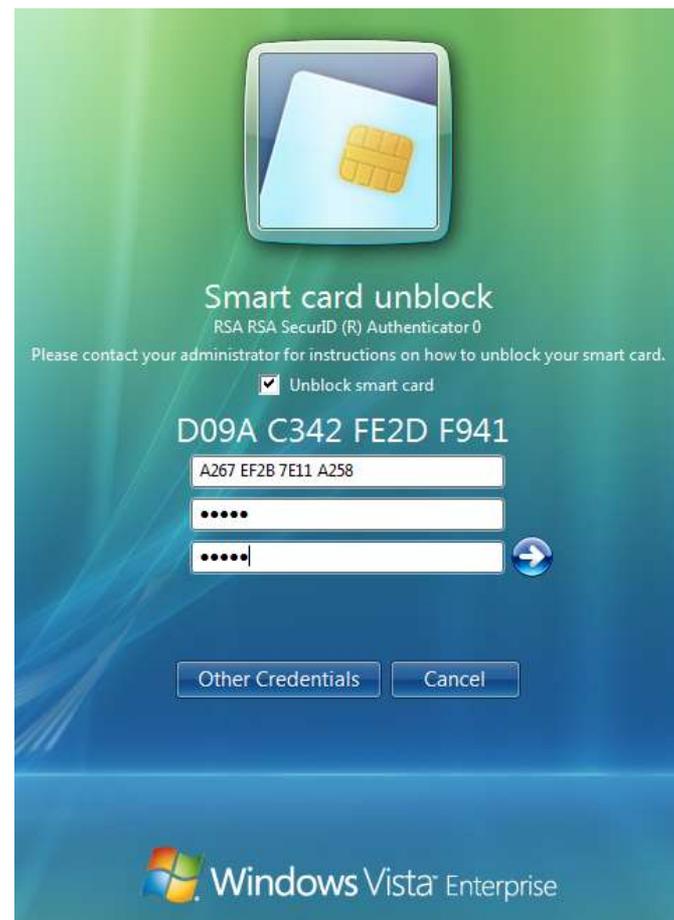
RSA Authentication Client 3.5 (SecurID 800 Client Software)



SecurID 800 “Rev D” (USB Hybrid Authenticator)

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 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



Программные токены на Mobile Devices

- ▶ Превращает мобильное устройство в SecurID аутентификатор
- ▶ 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



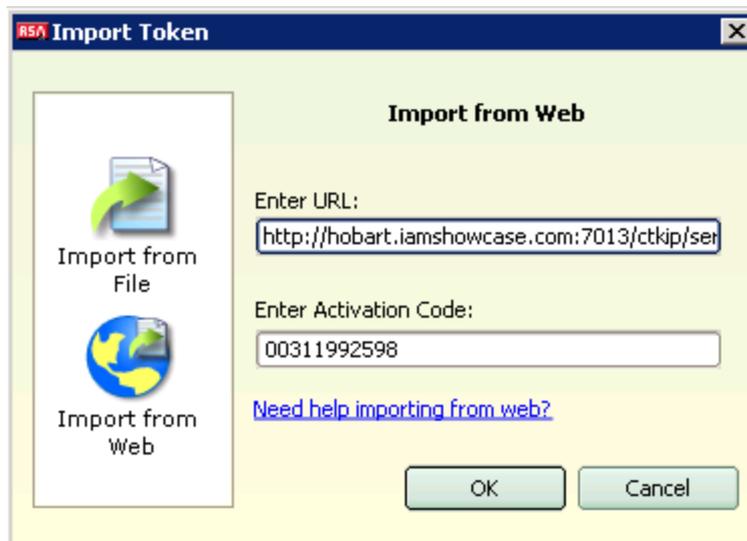


The Security Division of EMC

The Cryptographic Token Key Initialization Protocol (CT-KIP)

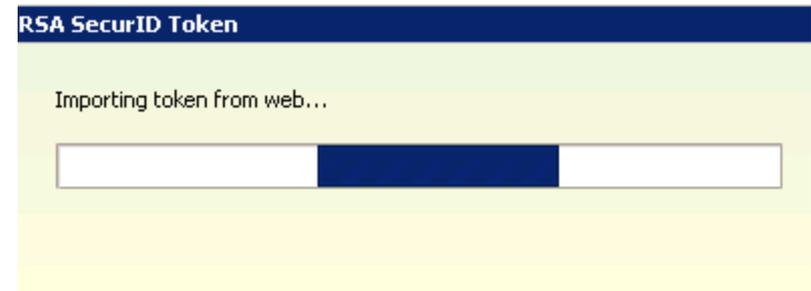
Программный токен Desktop 4.0. Динамическая активация

- ▶ 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 СТ-КIP динамической инициализации
- ▶ Если разрешено, пользователь может задать метку (название) программного токена
- ▶ Токен готов к использованию



Пример активация на мобильных платформах

- ▶ Java ME 2.3
- ▶ BlackBerry 3.0



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

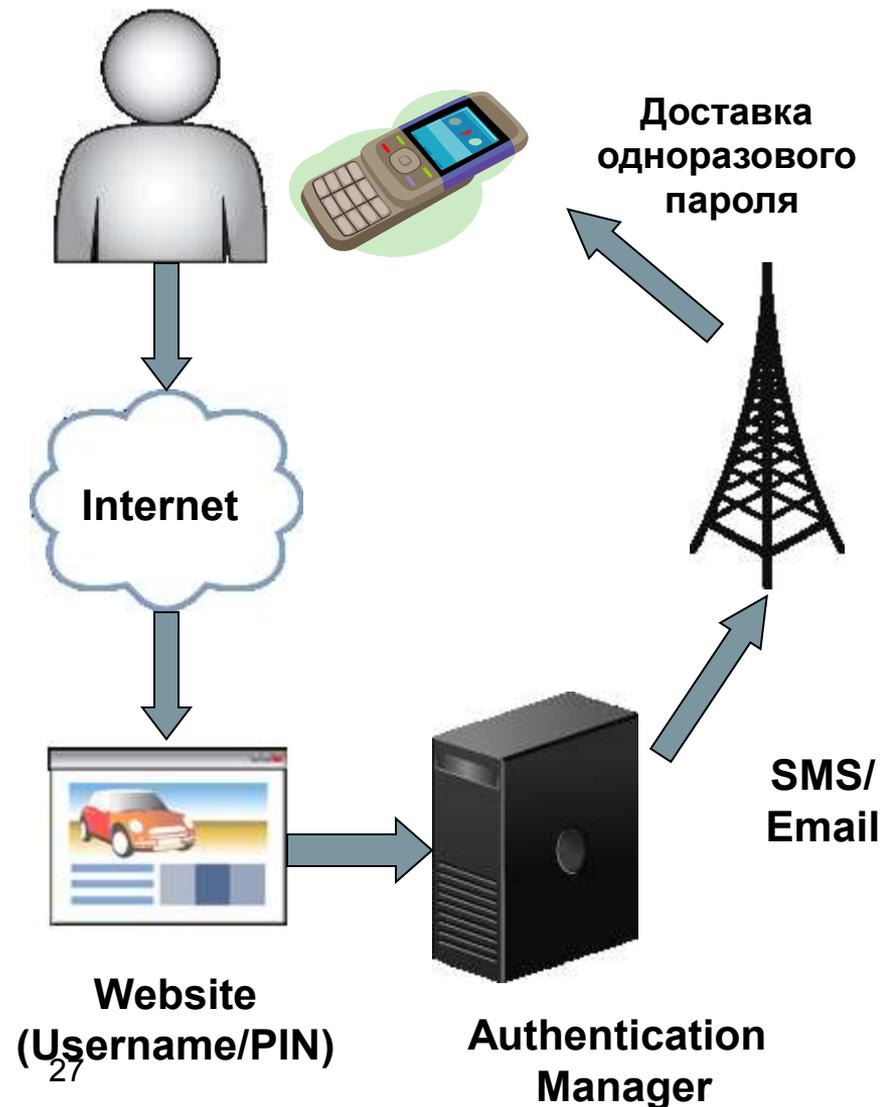




Extended Authentication Options

On-Demand Authentication – аутентификация по запросу

Пользователь



- ▶ 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



The image shows the RSA SecurID Log In interface. At the top left is the RSA SecurID logo. Below it is a blue header bar with the text "Log In". Underneath is a light blue box containing the text: "Log in to access this protected resource. If you don't remember your login information, contact your help desk or administrator". Below this is a yellow box with two input fields. The first is labeled "User ID:" and contains the text "bsimpson". The second is labeled "Passcode:" and contains four black dots. Below the passcode field is the text: "Your Passcode is your PIN + the number displayed on your token (the Tokencode)". At the bottom of the yellow box are two buttons: "Log In" and "Reset".

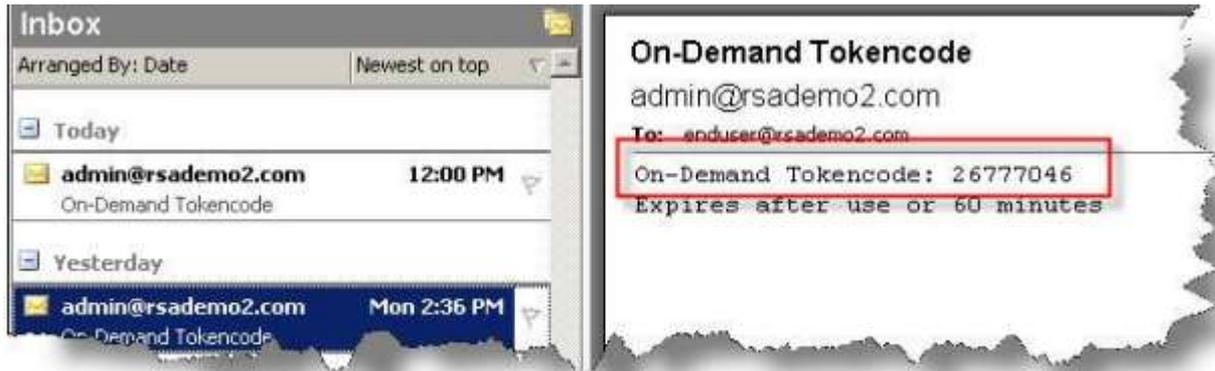
Пользователь вводит User Name и PIN в поле Passcode
Длина PINa от 4 до 8 символов, что позволяет Authentication Manager отличить его от Passcode (PIN + Tokencode > 8 символов) и перейти в режим onDemand



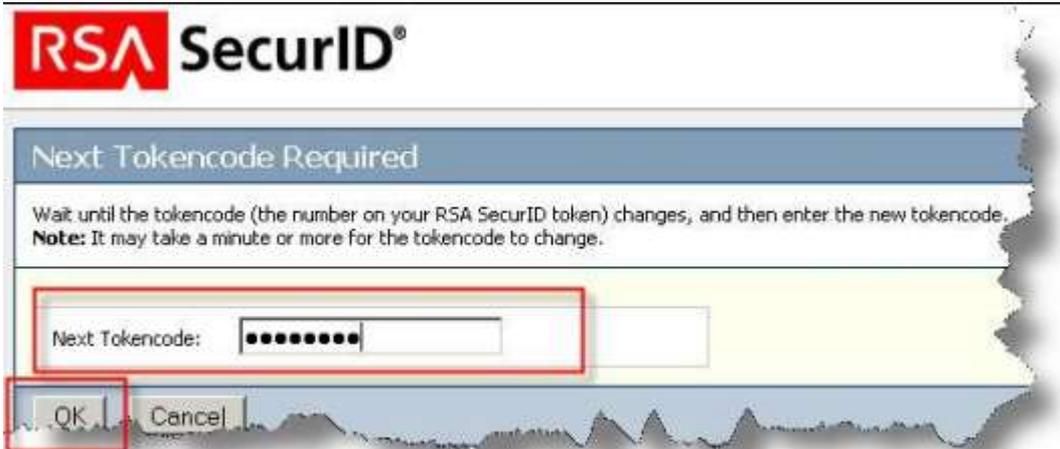
The image shows a dialog box titled "Next Tokencode Required". It has a blue header bar with the title. Below the header is a light blue box with the text: "Wait until the tokencode (the number on your RSA SecurID token) changes, and then enter the new tokencode". Below this is a yellow box with a single input field labeled "Next Tokencode:". The input field is highlighted with a red border. At the bottom of the yellow box are two buttons: "OK" and "Cancel".

Система показывает поле Next Tokencode

In-Line On-Demand Token Authentication



Пользователь получает onDemand Tokencode по eMail или SMS



Пользователь вводит его в поле New Tokencode

Серверная часть

RSA Authentication Manager

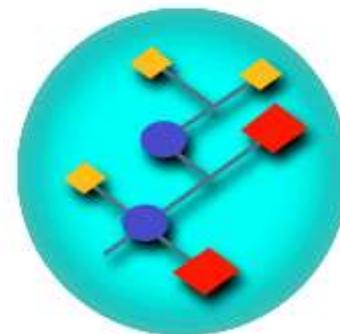
▶ Функции АМ сервер

- 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

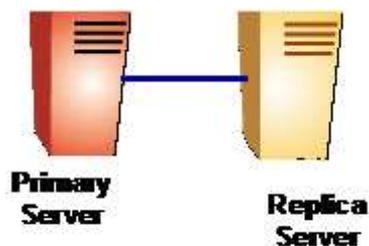
Основные моменты

- ▶ 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



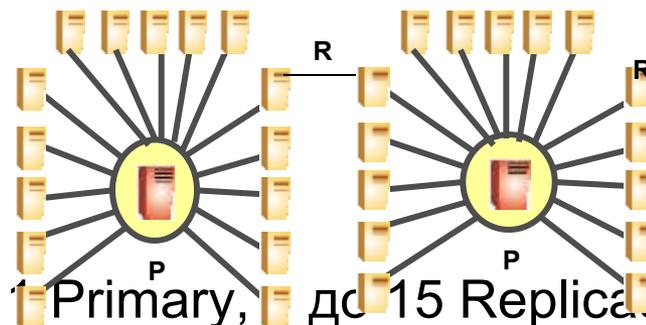
Базовая и Корпоративная версии

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

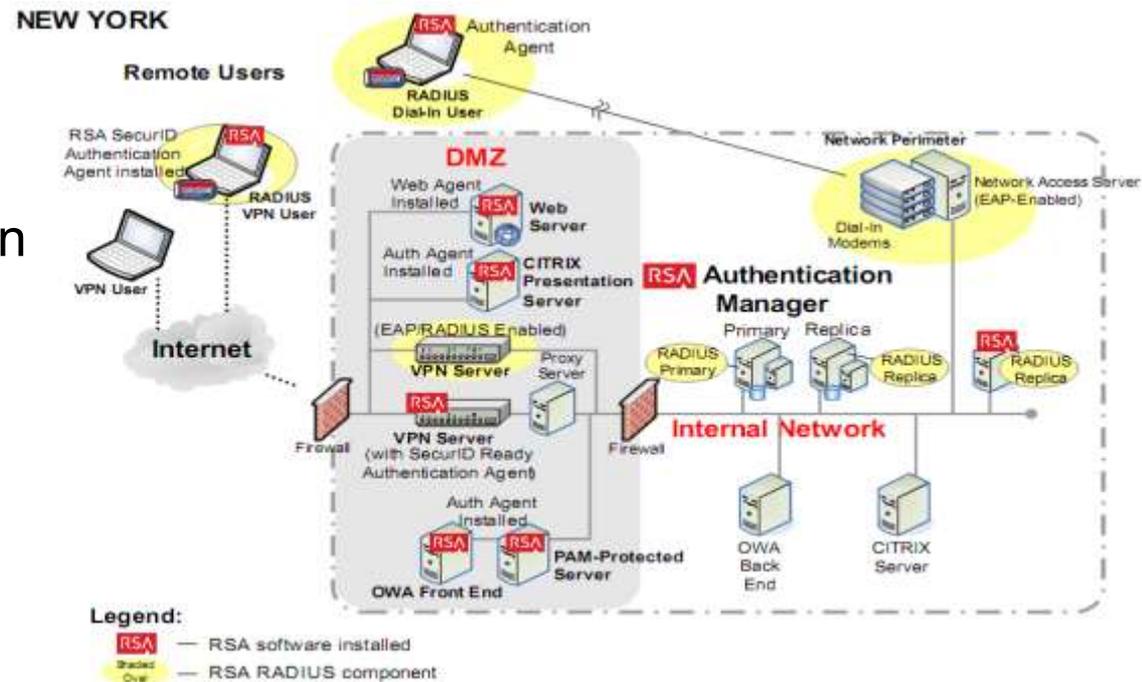
- ▶ Возможность полной локализации как административного интерфейса, так и интерфейса пользователей (SelfService Console)
- ▶ Локализация сводится просто к переводу тегов с текстовом файле ресурсов.



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

Welcome, Guest | [Login / Register](#) (Login to view additional collaboration options)

ECN > Solution Gallery > RSA

Browse Offerings by

- RSA Product
- Product Category

About

- EMC Solution Gallery
- Offering Certification
- Award Winners
- List Your Offering
- Contact Us

Of Related Interest

- Find a Certified RSA Reseller
- RSA Share Project
- RSA SecurID Software Token Lab for iPhone
- RSA SecurID Token Lab for BlackBerry
- RSA Support

RSA Secured® Partner Solutions

RSA Secured Partner Solutions

The RSA Secured Partner Directory is now a part of the **EMC Solution Gallery**. The RSA Secured Partner Program is one of the largest alliance programs of its type, bringing over a dozen years of experience and hundreds of complementary solutions together. RSA's certification programs bring added assurance to customers that the solutions they are deploying are certified as interoperable with industry leading products, helping them achieve faster time to deployment and lower overall cost of ownership.

Featured RSA Solutions

<p>Microsoft® Office SharePoint™ Portal Server 2003</p> <p>SharePoint Portal Server 2003 enables enterprises to develop an intelligent portal that seamlessly connects users, teams and knowledge so that people...</p>	<p>Juniper Networks IDP Juniper Networks</p> <p>Juniper Networks Intrusion Detection and Prevention (IDP) products provide comprehensive and easy-to-use in-line protection that prevents network and...</p>	<p>Winchester AtSignOn Winchester Business Systems</p> <p>AtSignOn for Lotus® Domino™ software uses RSA SecurID two-factor authentication to enhance security on Lotus Domino R5 Web servers.</p>
--	---	--

Become a Technology Partner

The RSA Secured® Partner Program has more than 500 partners and a billion copies of our technology in use worldwide. Find out more about the partner program!



Complete the online application.

Suggest a Device

Are you unable to find a device in your environment on our List of Supported Devices?

RSA enVision

RSA SecurID

All supported RSA enVision event sources

Latest Poll

How Important is "RSA Secured" Certification to your Solution Selection Process?

Very Important (94%)	94%
Important (0%)	0%
Somewhat Important (0%)	0%

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

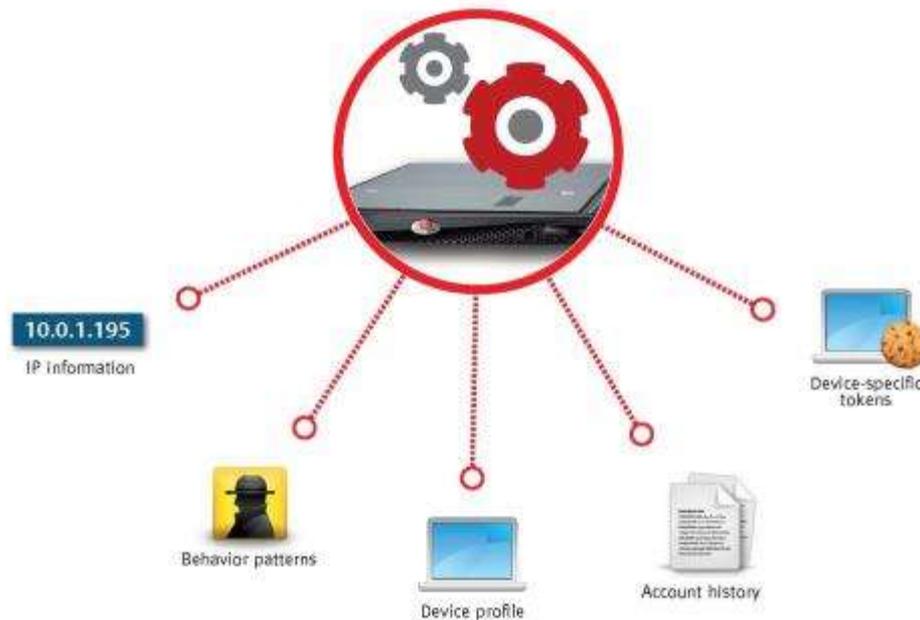
Возможность выноса сервисов, с которыми взаимодействуют пользователи в DMZ:

- RBA
- Self-Service
- CT-KIP

Распространяется как готовый к использованию продукт - аппаратный или виртуальный апплайнс

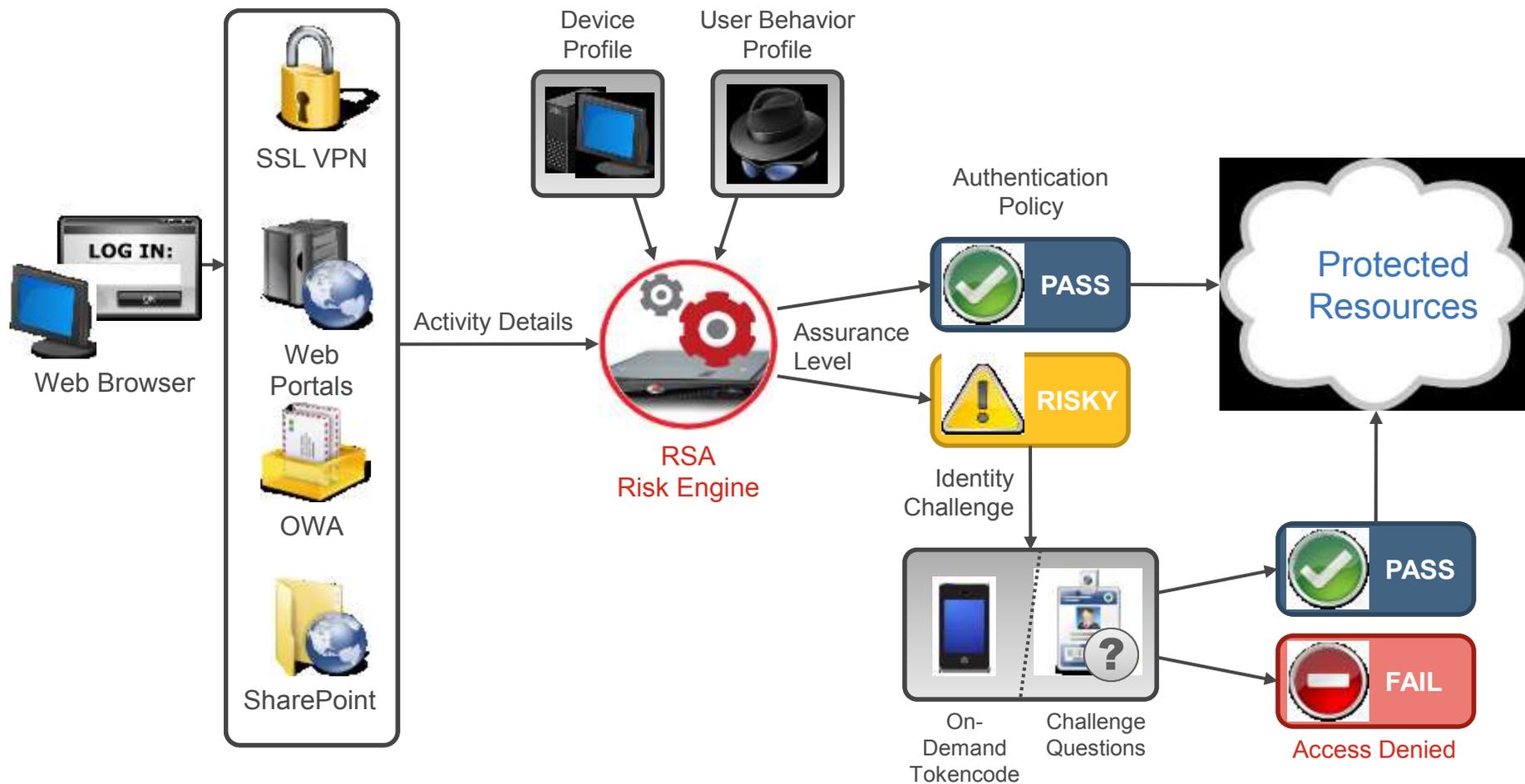
RSA Risk Engine

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.

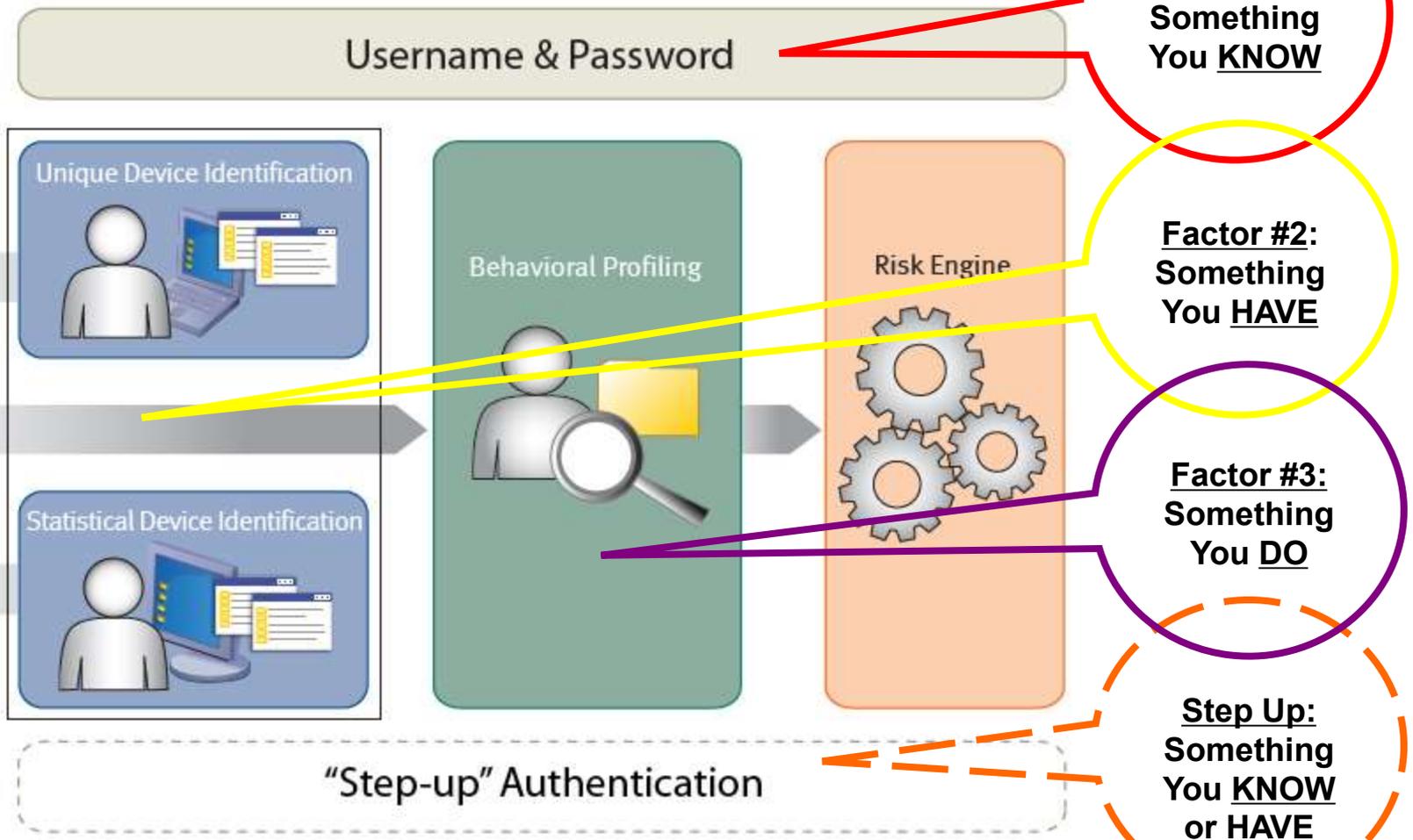


RBA - Risk-Based Authentication

Как это работает ?



Multi-factor Risk-based Authentication (RBA)



Summary

User Profile

Name: John Smith
 Identity Source: ActiveDirectory1
 Security Domain: RSADomain [Move](#)
 Account Status: Enabled [Disable](#)
 Locked Status: Unlocked

[Edit User](#)

Recent Activity

Details	Time	Result
Show	3/22/2011 11:29 EST	Authentication method failed
Show	3/22/2011 11:29 EST	Authentication method failed
Hide	3/21/2011 20:43 EST	PIN change failed, PIN reuse detected User 'jsmith' in security domain 'SystemDomain' from identity source 'Internal Database' attempted to change pin for token serial number '000034232423'
Show	3/21/2011 10:14 EST	Authentication Method success
Show	3/20/2011 04:15 EST	Authentication method warning
Show	3/19/2011 18:49 EST	Authentication method failed
Hide	3/19/2011 16:33 EST	Authentication method failed User 'jsmith' attempted to authenticate using authenticator 'SecurID_Native'. The user belongs to security domain 'RSADomain'
Show	3/18/2011 17:14 EST	Authentication Method success
Show	3/18/2011 12:33 EST	Authentication Method success

[Show All](#) [Hide All](#) [Launch Activity Monitor](#) [Run Report](#)

User Group Membership

Group Name	Security Domain	Notes
ITgrp	RSADomain	
Development	RSADomain	
Bedford Employees	EMCDomain	
Enigma Team	RSADomain	
US Employees	EMCDomain	

Page 1 of 2 | Displaying 1-5 of 9 [Assign More](#) [Manage](#)

Assigned SecurID Tokens

<input type="checkbox"/>	Serial Number	Type	Status	Expiration
<input type="checkbox"/>	000034232423	SID700	Enabled	12/18/2011
<input type="checkbox"/>	000034258012	SID700	Enabled	4/11/2011
<input type="checkbox"/>	000034489635	iPhone	Enabled	7/24/2013

[Disable](#) [Assign More](#) [Manage](#)

On-Demand Authentication

Enabled for ODA: Yes
 On-Demand Tokencode Destination: jsmith@gmail.com
 Expiration Date: None

[Clear PIN](#) [Manage](#)

Risk-Based Authentication

Enabled for RBA: Yes
 # of Devices Registered: 2 [Clear Device History](#)
 Silent Collection Status: Ended on 1/22/2011

Identity Confirmation Methods

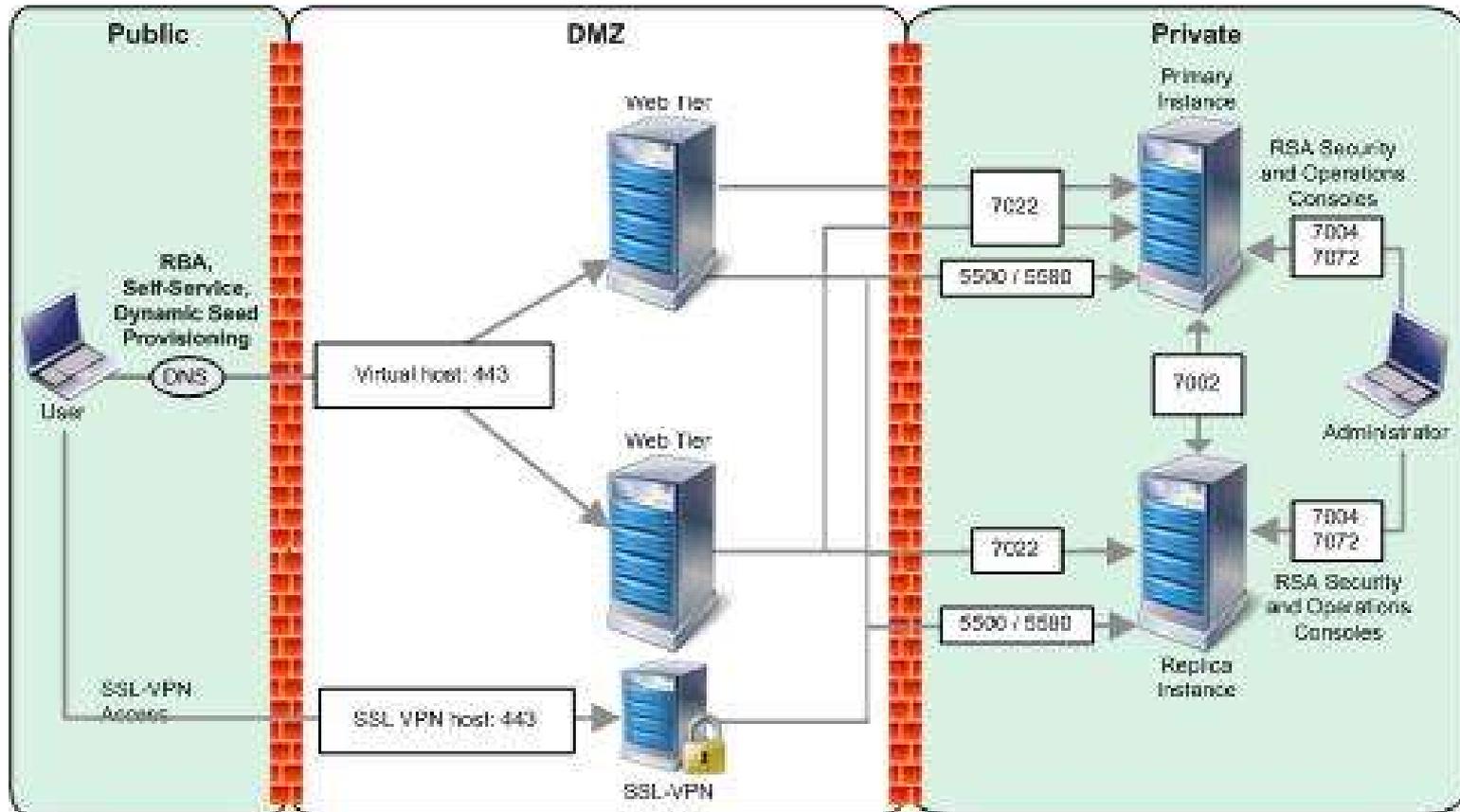
Security Questions: Configured [Clear Answers](#)
 On-Demand Authentication: Configured

[Manage](#)

Accessible Restricted Agents

Agent Hostname	Security Domain	Access Times
internal-rsa.na.rsa.net	RSADomain	Any Time
demo-rsa.na.rsa.net	EMCDomain	9am-5pm Weekdays
test.na.rsa.net	RSADomain	9am-11pm
demo-rsa.na.rsa.net	EMCDomain	9am-5pm Weekdays
test.na.rsa.net	RSADomain	9am-11pm

Web Tier Server Deployment





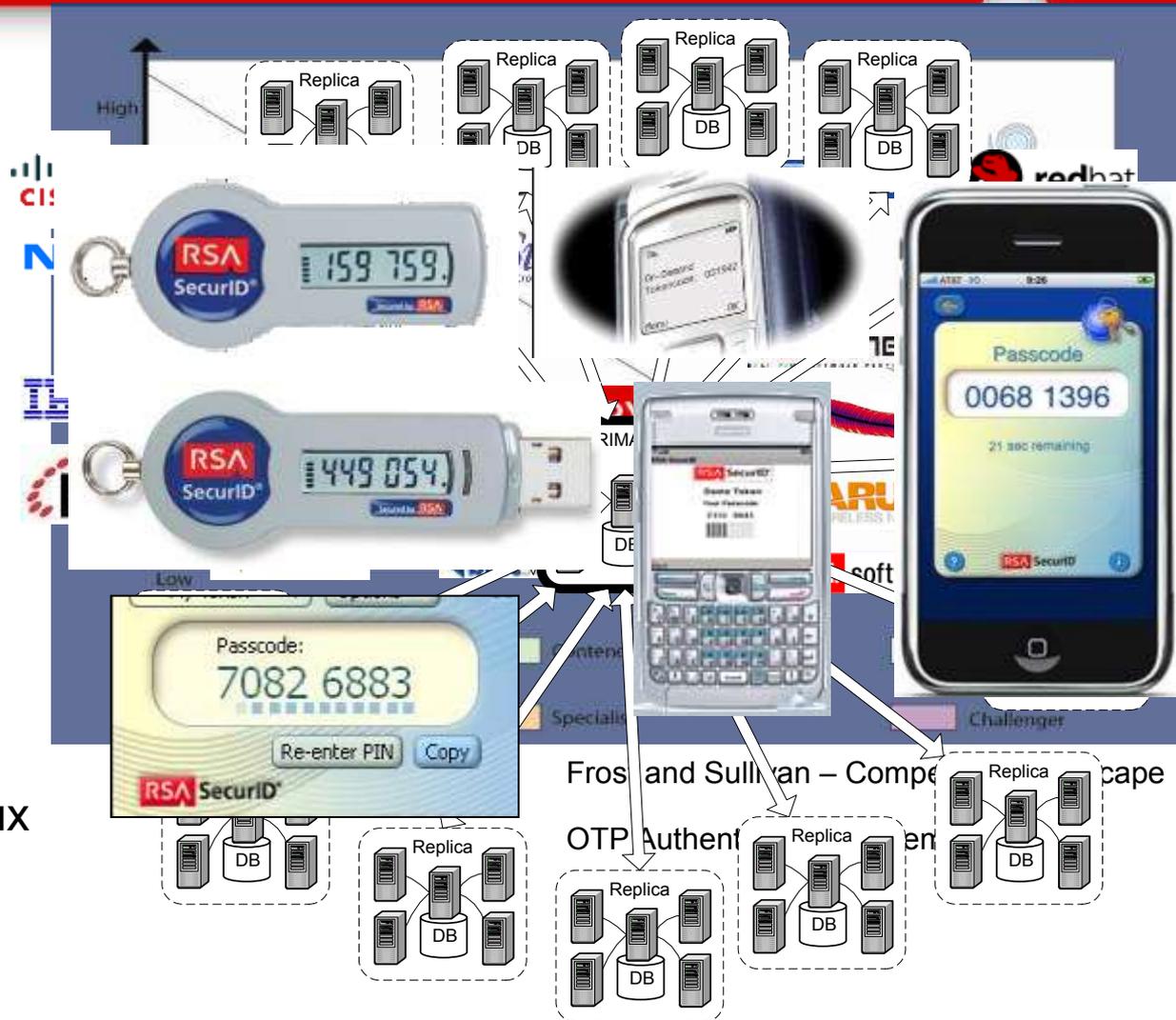
The Security Division of EMC

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 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!