Vanguard

Two Factor Authentication Solutions
Legal Notice

Copyright
©2016 Vanguard Integrity Professionals, Inc. All Rights Reserved. You have a limited license to view these materials for your organization’s internal purposes. Any unauthorized reproduction, distribution, exhibition or use of these copyrighted materials is expressly prohibited.

Trademarks
The following are trademarks of Vanguard Integrity Professionals – Nevada:

- Vanguard Administrator
- Vanguard Advisor
- Vanguard Analyzer
- Vanguard Authenticator
- Vanguard SecurityCenter
- Vanguard SecurityCenter for DB2
- Vanguard Offline
- Vanguard Cleanup
- Vanguard PasswordReset
- Vanguard inCompliance
- Vanguard IAM
- Vanguard GRC
- Vanguard QuickGen
- Vanguard Active Alerts
- Vanguard Configuration Manager
- Vanguard Configuration Manager Enterprise Edition
- Vanguard Policy Manager
- Vanguard Enforcer
- Vanguard ez/Token
- Vanguard Tokenless Authentication
- Vanguard ez/PIV Card Authenticator
- Vanguard ez/Integrator
- Vanguard ez/SignOn
- Vanguard ez/Password Synchronization
- Vanguard Active Alerts
- Vanguard Security Solutions
- Vanguard Security & Compliance
- Vanguard zSecurity University
Trademarks

The following are trademarks or registered trademarks of the International Business Machines Corporation:

- CICS
- CICSPlex
- DB2
- eServer
- IBM
- IBM z
- IBM z Systems
- IBM z13
- IMS
- MQSeries
- MVS
- NetView
- OS/390
- Parallel Sysplex
- RACF
- RMF
- S/390
- System z
- System z9
- System z10
- System/390
- VTAM
- WebSphere
- z/Architecture
- z/OS
- z/VM
- z zEnterprise
- z13
- z9

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

Other company, product, and service names may be trademarks or service marks of others.
AGENDA

1. Why utilize Two Factor Authentication
2. An Industry of Terms
3. How Vanguard Addresses
   1. Vanguard ez/PivCard Authenticator™
   2. Vanguard ez/Token™
   3. Vanguard Tokenless Authentication™
4. Q/A
CYBER ATTACK
CYBER ATTACK
CYBER ATTACK
CYBER ATTACK
Why Utilize Two Factor

Source: Information is Beautiful - World's Biggest Data Breaches

©2015 Vanguard Integrity Professionals, Inc.
Why Utilize Two Factor

Source: Information is Beautiful - World's Biggest Data Breaches

Court Ventures
200,000,000

Massive American business hack
160,000,000

Sony PSN
77,000,000

Steam
35,000,000

Tianya
28,000,000

Sony Online
Entertainment

NHS

(Source: Information is Beautiful – World’s Biggest Data Breaches)
©2015 Vanguard Integrity Professionals, Inc.)
Why Utilize Two Factor

Source: Information is Beautiful - World's Biggest Data Breaches

(Photograph Source From: Information is Beautiful – World's Biggest Data Breaches)
"A year ago, cybersecurity experts were calling 2013 'the year of the data breach' only to find 2014 had far worse in store."

Atlantic Council

"100% of breaches examined included an exploitation of a user id and password that was compromised."

Mandiant 2014 Data Breach Report
Mandiant 2015 Findings

- Attackers had access to victims’ environments for 205 days before they were discovered.

- Sixty-nine percent of victims learn from a third party that they are compromised.
Mandiant 2015 Findings

- Attribution is becoming harder as the lines blur between tactics used by cyber criminals and nation-state actors.

- Over the last year, threat actors have used stealthy new tactics to move laterally and maintain a presence in victim environments.
Mandiant 2015 Findings

Weak authentication when accessing virtualized application environments was found to be a major attack vector in the retail sector, allowing hackers to gain an initial foothold into systems from which they could “roam into other parts”.

“In every case we investigated that involved this attack vector, we saw the same primary security gap: remote access to the application required only a user name and a password. Two-factor authentication would have helped control this attack vector.”
The Threat is REAL

Cybercrimes now take 33% longer to resolve than 5 years ago.

The annual global cost of Cybercrime is $113 billion USD.

U.S. Government – Hackers stole data on 21.5 million federal employees.

Critical U.S. infrastructure intrusions have increased 17 times in the past 3 years.

20,000 people at the F.B.I. and 9,000 at the Department of Homeland Security hacked.

The average cost of resolving a cyber attack is now $1.6 million USD.

DOD alone experiences 41 million scans, probes and attacks per MONTH.
DATA BREACHES
DATA BREACHES
DATA BREACHES
DATA BREACHES
Impact of Most Recent Breaches

- Anthem – 80,000,000 Records (Name, DOB, SSN and Personal Records)
- Ashley Madison – 37,000,000 Records and Company Financial Records
- Voter Database – 191 million records – US Voters
- IRS – 330,000 Records – Full Personal Information
- OPM – 21,500,000 – All Military personnel with Top Secret Clearances
- Securus – 70,000,000 – Prison Service Provider – Records/Recordings
- Premera – 11,000,000 Records (Name, DOB, SSN and Personal Records)
- EBAY – 145,000,000 Records – User Records (Lowered Sales Target 200M)
- Home Depot – 56,000,000 Records – Credit Card Details - $43M pretax
- Target – 70,000,000 Records – Credit Card Details
2015 Cost of Data Breach Study: Global Analysis

The average total cost of a data breach for 350 companies participating in this research study increased from $3.5 to $3.7 million in 2015.
Per-record data breach costs vary widely across industries, with significant year-to-year increase from retail.
The Challenge today!

We have a Target on our back!

Attacks are going to continue!

We need information at the right time, so we can respond in the right way.

The largest companies and governments are faced with massive changes to their organizations.

Most changes come from creating, collecting, storing and sharing data.

All this data is extremely tempting for hackers making Cybersecurity one of the top issues for executives and business leaders today.
Vanguard

Two-Factor Authentication Solutions
An Industry of Terms

When I say "Two-Factor" I mean;

• Multifactor Authentication
  • Knowledge Factors - User KNOWS
  • Possession Factors - User HAS
  • Inherence Factors - User IS

• Two-Factor Authentication
  • A combination of two DIFFERENT factors above
An Industry of Terms

I am not referring to;

- **Two-Step Verification**
  - A type of Multi-Factor, involves two subsequent but dependent checks
  - BOTH checks can be from the same factor

- **Strong Authentication**
  - More of a "Generic Term", with multiple meanings depending on context of use
  - Is this a "Strong Authentication"? [!_Dust1nP@$w*rdIsL0ng]
How Vanguard Can Help - Overview

Two-Factor Authentication Solutions

• Vanguard ez/PivCard Authenticator™

• Vanguard ez/Token™

• Vanguard Tokenless Authentication™
Summary
Smart Card Strength using your existing infrastructure and investment

The Justification

- Real-time verification of Card (Account) Status, including centralized account de-provisioning
- Selectively determine which users require Smart Card Authentication
- Selectively determine which applications require Smart Card Authentication
- Out of Band Deployment Options, with simple "end user self-registration"
- Achieve NIST FIPS 201 Regulatory Requirements

Key Feature
Delivers Smart Card authentication capabilities to z/OS, without requirement for direct TCP/IP connectivity to your mainframe. Benefit from centralized account management including de-provisioning for lost, stolen, or terminated cards

PIV Cards
CAC Cards
JAVA Cards/SmartCards
PIV Validation Occurs and a RACF® PIV Pass is generated.
Vanguard ez/PivCard Authenticator™ – Configuration

• Key Configuration Parameters
  – PIVREG Value: $PIVCARD (New Class)
  – Controlling Profile: PIVCARD.ENABLE
  – Class Defined by: PIV_AUTH_CLASS
  – Excluding STCs: PIV_EXCL_JNAME
  – Including STCs: PIV_INCL_JNAME

• Where: PDS Member:
  – Your Defined Class
  – HLQ.V212.VANOPTS(VIPTOKEN)
Manual Registration
• PIV card PIN Validation
• Creates a unique signature based on PIV card Certificates for each z/OS user
• Designed for when direct network communication is not available to end-users

Signature can be sent to administrator of system for entry into user profile. Or loaded manually into TSO or CICS® registration applications.
Vanguard ez/PivCard Authenticator™ – Semi-Auto Registration

- Requires RACF User id
- PIV card PIN Validation
- IP address of z/OS system
- Creates a unique signature based on PIV card Certificates and automatically enters the information into the RACF user profile correctly.
Simple user interface User provides

• RACF ID
• RACF Password
• PIV Card Pin.
If Card /PIN is validated PivPass will be generated. Enter PIV Password in the Password field of z/OS enable logon such as; TSO, CICS, DB2®, IMS™, etc.
Vanguard ez/PivCard Authenticator™ – Validation

All PIV Validation must pass from External PIV provider prior to Generating a PIVPass

Standard PIV Validation
- PIN Validation
- Card Validation
- Certificate Validation
- FASC-N Validation
- OCSP Validation
Vanguard ez/Token™

Summary
Two-factor security solution that utilizes your existing tokens investment (physical tokens or virtual tokens)

The Justification
➡️ Force users with elevated privileges to utilize two-factor authentication
➡️ Selectively determine which users require Token Authentication
➡️ Selectively determine which applications require Token Authentication
➡️ Dynamically choose your authentication solution(s)
  • RSA SecureID
  • Active Identity
  • Safe Sign
  • OAUTH HOTP/TOTP (Such as Google Authenticator)
  • YubiKey
  • Or Native RACF

Key Features
Authenticate through many different token providers to logon to the mainframe via TSO, CICS, IMS or any other application that utilizes RACF authentication.

Now with 2 new features
• Pre and Post exit processing
• No IPL required to install or remove product
• Aliasing processing in RACF
Vanguard ez/Token™ – Overview

Process Flow
1) User Starts 3270 Terminal or another ez/Token enabled application (CICS, etc)
   User enter appropriate RACF UserID and RSA Authentication
   (Either a Passcode, a TokenCode, or a Pin/Token combination depending on RSA requirements)
2) z/OS ICHRIX01 Exit delivers control Vanguard’s ICHRIX01 Process (IAMEZTSV)
3) IAMEZTSV Started Task, on z/OS determines, if the user required to utilize RSA?
   3.1) User is not required to utilize RSA, passes to RACF for normal RACF processing
       NONE access to the Grouping Class Member
   3.2) User is required two inputs (Pin/Token)
       READ access to the Grouping Class Member
   3.3) User is required one input (Either Passcode or TokenCode)
       UPDATE access to the Grouping Class Member
4) IAMEZTSV connects to Vanguard’s ez/Token Agent Host
5) Vanguard’s ez/Token Agent Host contacts RSA Server
6) RSA Server determines if the user’s authentication attempt succeeds
7) Return communication occurs back to z/OS either permitting or denying logon attempt

Notes
A) Vanguard’s VIPMAIN Started Task must be running for Vanguard datecode validation (Every 24 Hours)
B) Vanguard’s EZSTC Started Task dynamically installs Vanguard’s ICHRIX01 Exit Process (One Time)
Vanguard ez/Token™ – Configuration

- Key Configuration Parameters
  - Configuration Profile: EZTOKEN.SECUREID (Grouping)
  - Controlling Profile: EZTOKEN.SECUREID (Member)
  - Fallback Profile: EZTOKEN.BACKUP
  - Including STCs: EZTOKEN.SECUREID.INCLUDE

- Where: PDS Member:
  - Your Defined Member/Grouping Class
  - HLQ.V212.VANOPTS(VIPTOKEN)
Vanguard ez/Token™
– Use (CICS)

User enters PIN here

User enters Token Code here

Type your userid and password, then press ENTER:

UserId . . . . RSAUSER Groupid . . . .
Password . . .
Language . . .

New Password . .

DFHCE3520 Please type your userid.
F3=Exit
Vanguard Tokenless Authentication™

Summary
Strength and security of two-factor authentication for corporations which do not have an existing two-factor solution

The Justification

- Most cost-effective and convenient way to add a higher level of security to corporate networks and data
- Selectively determine which users require Token Authentication
- No need to deploy and administer expensive physical tokens
- Generates a one-time, one-use password to a “virtual token,” the user’s cell phone, each time a signon is attempted
- Cryptographically generated passcodes that expire within a short specified period of time

Key Feature
Delivers strong authentication capabilities by generating and sending a one-time, one-use, time sensitive passcode to a communication device that a user already possesses: user’s cell phone, PDA, and more.
Vanguard Tokenless Authentication™ – Configuration

• Key Configuration Parameters
  – Configuration Profile: EZTOKEN.SECUREID (Grouping)
  – Controlling Profile: EZTOKEN.SECUREID (Member)
  – SSIGNON Value: VTTFA in Class(PTKTDATA)

• Where: PDS Member:
  – Your Defined Member/Grouping Class
  – HLQ.V212.VANOPTS(VIPTOKEN)
Vanguard Tokenless Authentication™ – Overview

Process Flow
1) User starts 3270 Terminal or another Vanguard Tokenless Authentication™ enabled application (CICS, etc)
   - User enter appropriate RACF UserID and RACF Password
2) z/OS ICHRX01 Exit delivers control Vanguard’s ICHRX01 Process (IAMEZT SV)
3) IAMEZT SV Started Task, on z/OS determines, if the user required to utilize Tokenless?
   3.1 User is not required to utilize Tokenless Authentication
      - NONE access to the Grouping Class Member
   3.2 User is required Two-Factor Authentication (RACF Password & Passcode)
      - READ access to the Grouping Class Member
   3.3 User is required to utilize Vanguard PasswordReset™ to retrieve a valid Passcode
      - UPDATE access to the Grouping Class Member
4) IAMEZT SV connects to Vanguard Tokenless Agent
5) Vanguard Tokenless Agent generates Token/Code and delivers using either:
   5.1 SMTP Mail Server (to any e-mail enabled device)
   5.2 Cell Phone SMS via Cellular Modem

Notes
A) Vanguard’s VIPMAIN Started Task must be running for Vanguard datecode validation (Every 24 Hours)
B) Vanguard's EZSTC Started Task dynamically installs Vanguard's ICHRX01 Exit Process (One Time)
Vanguard Tokenless Authentication™ – Administration

Simple Web Based Admin Interface

- Setup users to use Vanguard Tokenless Authentication™
- Change Tokenless Type (Password + Token or Token Only)
- Change Deliver Address (Cell Phone / E-Mail)
Vanguard Tokenless Authentication™ – Use (E-Mail/SMS)

- Enter UserID
- Enter Password
- Receive E-Mail/SMS
- Enter Tokenless Code
Vanguard Tokenless Authentication™
– Use Vanguard PasswordReset™
(Multi Factor Authentication)

- Open Website
- Click [Send Token]
- Enter RACF User & Password
- Answer Vanguard PasswordReset Questions
- Receive Tokenless Code to use as Password
Vanguard Tokenless Authentication™ – Use Vanguard PasswordReset™ (Two Step Authentication)

- Open Website
- Click [Get Token]
- Enter RACF User & Password
- Answer Vanguard PasswordReset Questions
- Receive Tokenless Code to use as Password
Vanguard ez/Token™ - Now with OAUTH Support And...
– Overview

• Initiative for Open Authentication – OATH
  http://www.openauthentication.org/
  – HOTP - HMAC-Based One-Time Password Algorithm (RFC 4226)
    Also known as EOTP - Event-based One-time Password Algorithm
  – TOTP – Time-based One-time Password Algorithm (RFC 6238)
• YubiKey Cloud (or Onsite) Authentication
• Provided though LinOTP Linux Server – By LSE
  – Open Source Edition is Free
  – Enterprise Subscriptions Available
  https://lsexperts.de
• Key Configuration Parameters
  • Configuration Class: LINOTP_AUTH_CLASS=
  • Controlling Profile: EZTOKEN.LINOTP
  • CS Data Field Name: LINOTP_CSDATA_FLDNAME=
  • Excluding STCs: PIV_EXCL_JNAME
  • Including STCs: PIV_INCL_JNAME
Vanguard ez/Token™ - Now with OAUTH Support And... – Continued

- All OAUTH methods require both RACF Password AND OTP Code
- Utilizes the Passphrase Interfaces to simplify end user use
  - But still authenticates using the RACF Password
- Examples of Authentication String

- OATH

```
My12R@CF844622
```

<table>
<thead>
<tr>
<th>RACF Password</th>
<th>OTP Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-8 Characters</td>
<td>6 Characters</td>
</tr>
</tbody>
</table>

- YubiKey

```
My12R@CFccccccccceiicnhhlklknihnieihjejctenfevkbidbbbbfnf
```

<table>
<thead>
<tr>
<th>RACF Password</th>
<th>YubiKey Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-8 Characters</td>
<td>44 Characters</td>
</tr>
</tbody>
</table>
Vanguard ez/Token™ - OAUTH Support And...
– Supported Tokens

• Just some of your options

• More? ...Just contact us and let us know what do you have today
<table>
<thead>
<tr>
<th>Date Range</th>
<th>Course Title</th>
<th>CPE</th>
<th>Days</th>
<th>Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 23 – May 26</td>
<td>Basics of RACF Administration</td>
<td>24</td>
<td>4</td>
<td>Online</td>
</tr>
<tr>
<td>June 1 – June 3</td>
<td>RACF Security for z/OS Applications – ALL MODULES</td>
<td>18</td>
<td>3</td>
<td>Online</td>
</tr>
<tr>
<td>June 1</td>
<td>RACF Security for z/OS Applications – MODULE 1 – RACF for DB2</td>
<td>6</td>
<td>1</td>
<td>Online</td>
</tr>
<tr>
<td>June 2 – June 3</td>
<td>RACF Security for z/OS Applications – MODULE 2 – RACF for CICS</td>
<td>12</td>
<td>2</td>
<td>Online</td>
</tr>
<tr>
<td>June 6 – June 9</td>
<td>Beyond RACF Basics</td>
<td>24</td>
<td>4</td>
<td>Online</td>
</tr>
<tr>
<td>June 13 – June 15</td>
<td>Auditing z/OS and RACF</td>
<td>18</td>
<td>3</td>
<td>Online</td>
</tr>
<tr>
<td>June 21 – June 24</td>
<td>Beyond RACF Basics</td>
<td>24</td>
<td>4</td>
<td>Jacksonville, FL</td>
</tr>
<tr>
<td>June 27 – June 30</td>
<td>Basics of RACF Administration</td>
<td>24</td>
<td>4</td>
<td>Online</td>
</tr>
</tbody>
</table>

Register to attend a course, or to get more information: [http://www.go2vanguard.com/training](http://www.go2vanguard.com/training)

Don’t forget that all of the Vanguard zSecurity University™ courses are eligible for CPE Credits.

To register for a webinar or training course:
go2vanguard.com

Select - Training

Register to attend a course, or to get more information: http://www.go2vanguard.com/training

Don’t forget that all of the Vanguard zSecurity University™ courses are eligible for CPE Credits.

Customer Savings: Special Discounts for Software Customers and VSC 2016 Attendees
Vanguard Security & Compliance
November 14-17, 2016
Knowledge is The Best Defense

Proudly Celebrating 30 Years

The Westin Las Vegas Hotel
Thank You
If you need us contact
Vanguard on International@go2vanguard.com