

Enterprise Authentication and Passwordless Security



Anton Niemand

Cybersecurity Specialist
zSecure and MFA

March 24, 2021

Top 10 Breaches of 2020

- 10. Microsoft – 250 million records
- 9. Wattpad – 268 million records
- 8. Broadvoice – 350 million records
- 7. Estée Lauder – 440 million records
- 6. Sina Weibo – 538 million records
- 5. Whisper – 900 million records
- 4. BlueKai – billions of records
- 3. Keepnet Labs – 5 billion records
- 2. Advanced Info Service (AIS) – 8.3 billion records
- 1. CAM4 – 10.88 billion records

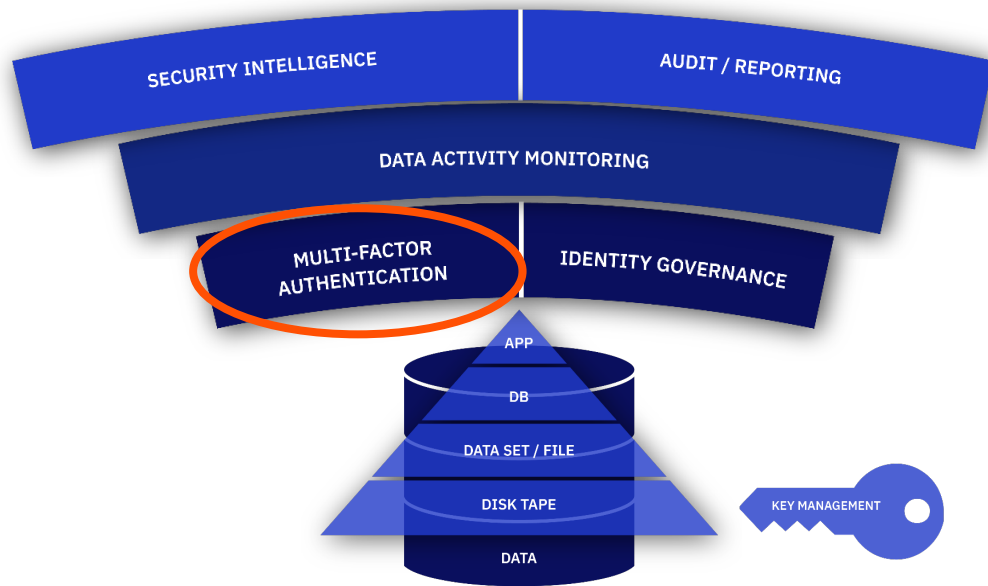
Security Magazine: <https://ibm.biz/BdfZpY>

zSecurity considerations

- Complacency
- Insider Threat Report – CyberSecurity Insiders
- Does Zero Trust apply to the Mainframe?
- By Default, the mainframe is NOT the most secure platform
- The mainframe is your most securable platform!
- Just because you can still do something doesn't mean you should...
- GITHUB

Protecting data at the core of the enterprise

Encryption is the solid foundation of a layered cybersecurity strategy



Relevant IBM Security Solutions:

- Enterprise Key Management Foundation
- IBM Multi-Factor Authentication for z/OS
- IBM Security Identity Governance
- IBM Security Guardium Family
- IBM Security zSecure Suite
- IBM Security QRadar

The State of Passwordless Security

Key Findings

- Passwordless MFA Secures Users and Reduces Costs
- User Experience and Security Are Interdependent
- Passwordless Solutions Reduce Complexity

Why is it Important

- Stop Credential Theft and Phishing
- User Experience
- Achieve Digital Experience
- Cost Savings

Observations

- Most 'Passwordless' Solutions Still Rely on Passwords
- Smartphones Lead the Way for Passwordless Adoption
- Remote Work is the #1 Use Case for Passwordless Adoption
- Ease of Use and Integration are Top Deciding Factors
- Password Managers

©2021 Cybersecurity Insiders : <https://ibm.biz/BdfZpX>

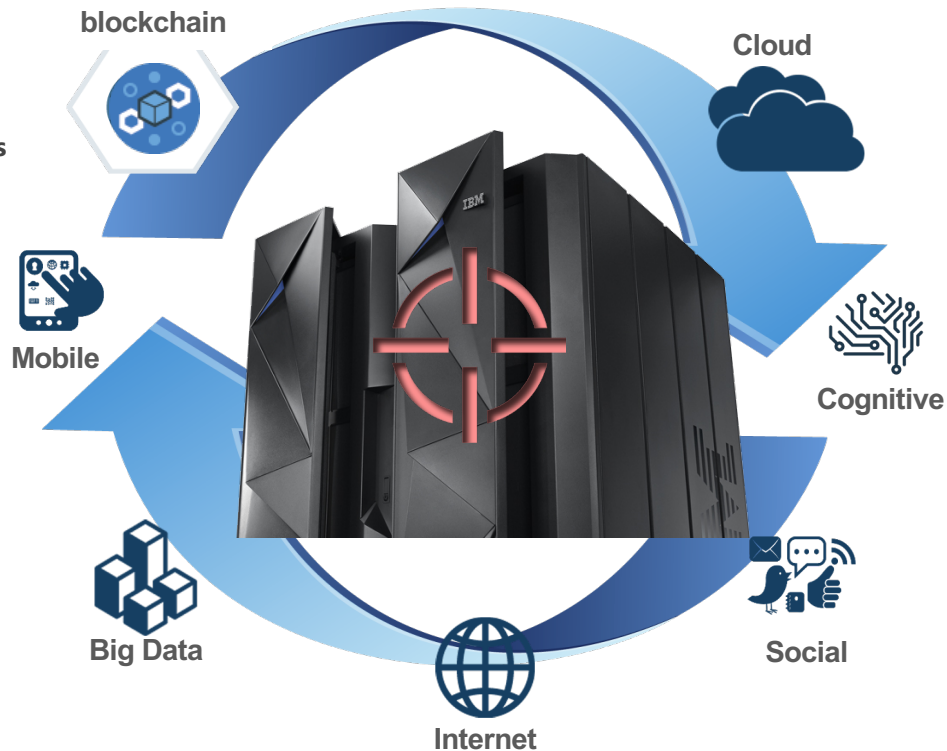


Why is a Multi-Factor
Authentication solution needed?

IBM Z is an increasingly desirable target

Today's technologies have eliminated "mainframe isolation"

Mainframes are increasingly closer to the Internet and mobile platforms and this has made them more vulnerable to outside threats.



Compliance

PCI DSS v3.2

*Note: This is a best practice until **January 31, 2018**, after which it became a requirement.*

DFS 23 NYCRR 500

*Note: Effective March 1, 2017, reporting required as of **February 15, 2018***

NIST SP 800-171

*Note: This requirement is effective **December 31, 2017**.*

Using multi-factor authentication on IBM Z is considered a security **Best Practice**.

How are users authenticating without MFA?

Users authenticate with:

- Passwords
- Password phrases
- Digital Certificates
- via Kerberos

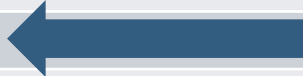
Problems with passwords:

- Common passwords
- Employees are selling their passwords
- Password reuse
- People write down passwords
- Malware
- Key log
- Password cracking



History of Authentication

Year	Event
1976	User identification/verification
1981	Password processing support
1984	DES password encryption option
1994	DES as password default
1999	PROTECTED user IDs
2004	Password enveloping and LDAP change log support
2005	Mixed case passwords and Detect or prevent password recycling
2006	Password phrases from 14 to 100 characters in length
2007	Password phrases from 9 to 13 characters in length
2008	Password phrase exploitation and more granularity on password reset
2013	RACF_ENCRYPTION_ALGORITHM health check (Rolled back)
2014	KDFAES password support, Additional special characters, Password phrase only users
2015	Elimination of the need for an ICHDEX01 exit to eliminate the RACF masking algorithm, ADDUSER will no longer assign a default password, RACLINK support of password phrase
2016	Multi-factor Authentication



Majority of mainframe environments are using 35+ year old technology to protect their critical assets!

IBM Multi-Factor Authentication for Z

Higher assurance authentication for IBM Z systems that use RACF



IBM Multi-Factor Authentication on Z provides a way to **raise the assurance level** of Z, applications, and hosting environments by extending RACF to authenticate users with multiple factors.

Fast, flexible, deeply integrated, easy to deploy, easy to manage, and easy to use

*PCI-DSS
Achieve regulatory compliance, reduce risk to critical applications and data*

Architecture supports multiple third-party authentication systems at the same time

IBM Multi-Factor Authentication for Z (5655-MA1)
IBM Multi-Factor Authentication for Z S&S (5655-MA2)

What is multi-factor authentication?

SOMETHING THAT YOU KNOW

- Usernames and passwords
- PIN Code



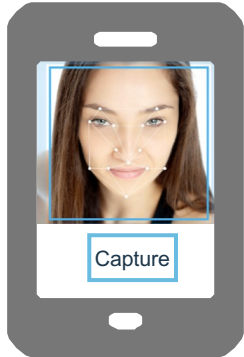
SOMETHING THAT YOU HAVE

- ID Badge
- One time passwords
- Time-based



SOMETHING THAT YOU ARE

- Biometrics



What works with IBM MFA?

IBM Z MFA supports a wide range of authentication systems!**

Proprietary Protocol:



RADIUS Based Factors:



TOTP Support:



Certificate Authentication:



Password/Passphrase:

RACF Password/Passphrase can be used in conjunction with all in-band authentication methods.



Disclaimer: Not everything above has been fully tested, but they *should* work, if not we will investigate.

**Not an all-inclusive list

Target Personas for MFA

Question: Who should be covered with MFA?

Answer: Everyone



Employees that work with personally identifiable info.

- Human Resources
- Healthcare workers
- Law Clerks
- DMV Clerks



Employees that have authority over managing money

- Brokers, Traders, Analysts
- Tellers
- Payroll
- Credit Card Processing



Users that have knowledge of Corporate Intellectual Property

- Executives
- Engineers



Business Partners – that access YOUR data

- Agents – Travel, Insurance
- Contract organization – Outsourcers



Users managing key IT assets

- Systems Programmers
- Security Administrators
- Database Admins, Developers

Target personas for IBM MFA include anyone with access to data a client would *not* want released to the public

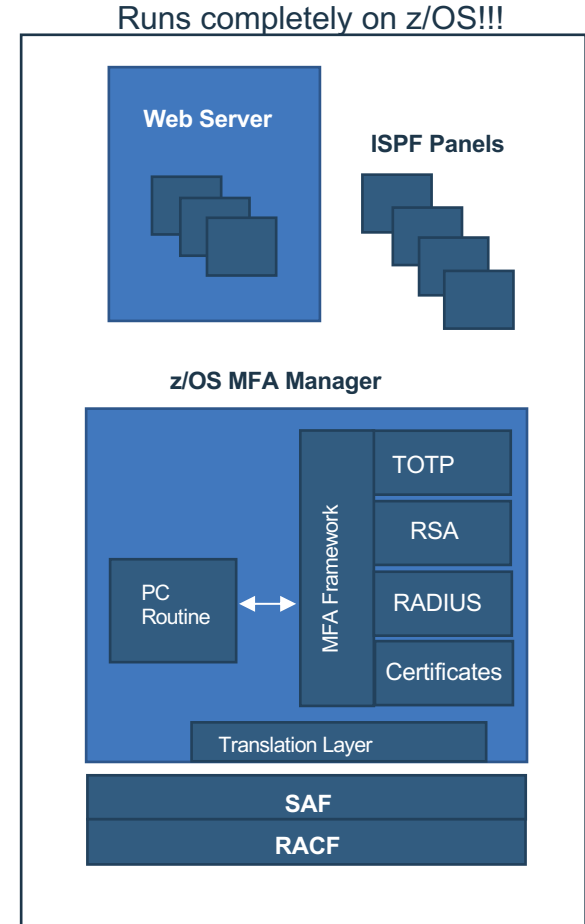
RACF Support

- RACF's MFA support introduces extensions to a variety of components of RACF
 - User related commands
 - Allow the provisioning and definition of the acceptable MFA tokens for a user
 - Extensions to authentication processing
 - Allows supported tokens to be used by any z/OS application
 - Extensions to SAF programming interfaces
 - Provides a new SAF service for IBM MFA allowing access to MFA data stored in the RACF database
 - Auditing extensions
 - Tracks that MFA was used during the authentication process for a given user
 - Utilities
 - RACF Database unload non-sensitive fields added to the RACF database used by MFA processing
 - SMF Unload – unloads additional relocate sections added to SMF records

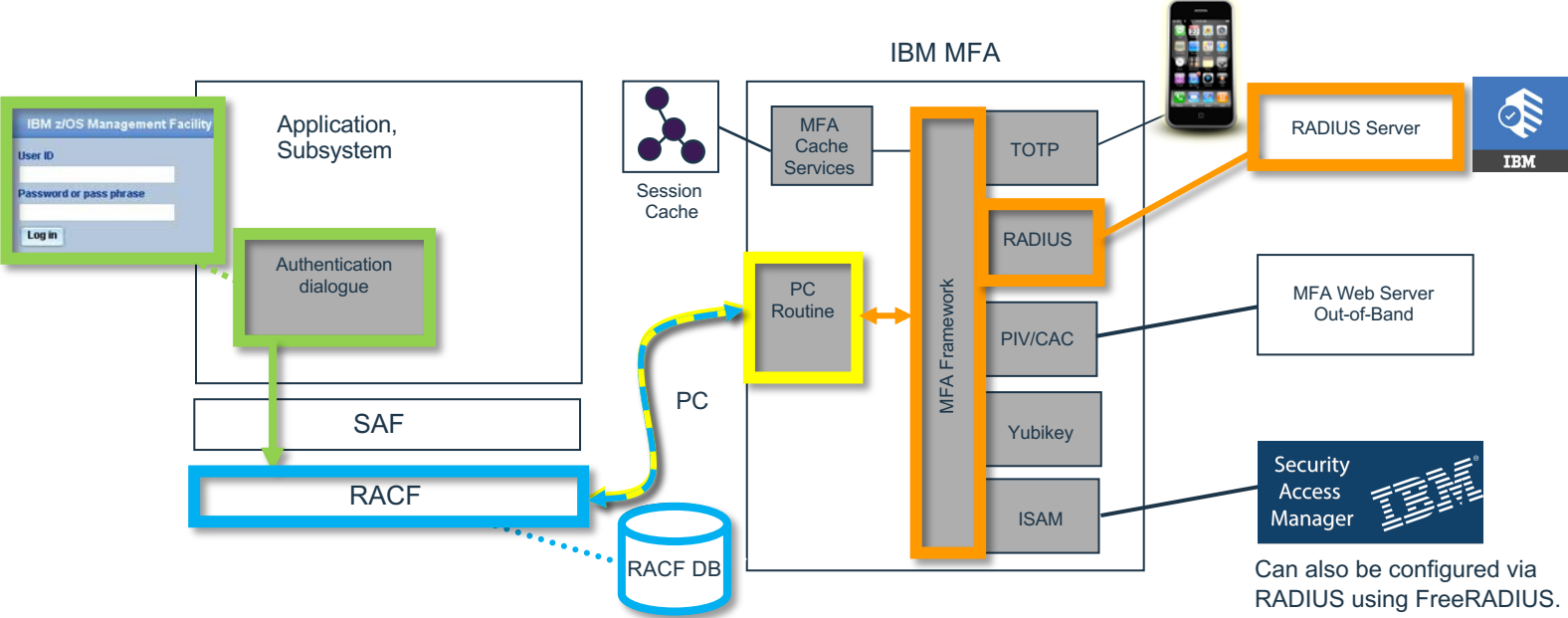


IBM Multi-Factor Authentication for Z

- MFA ISPF panels for configuration and management of authentication tokens
- MFA Web Interface
 - User Interface supports factors such as Smart Cards and serves as web interface for registration – depending on factor type
- MFA Manager Services
 - Provides MFA main logic
 - Register MFA Factor Data for a z/OS user
 - Validates a user provided factor against RACF MFA Data
 - Accesses MFA Data via SAF/RACF via callable services



Architecture Review: Logging on with MFA credentials



Logon with RADIUS Token:

- A) User logs on with User ID & Token
- B) RACF determines if the user is an MFA user & calls the IBM MFA
- C) IBM MFA calls RACF to retrieve user's MFA factor details
- D) IBM MFA validates the users authentication factors calls the Authentication Server, gets OK/Fail back
- E) RACF uses IBM MFA status to allow or deny the logon

User Provisioning with RACF

- **Activate the MFADEF class:**

```
SETR CLASSACT (MFADEF)
```

- MFADEF Class must be active for MFA authentication processing to occur

- **Define the factor profile:**

```
RDEFINE MFADEF FACTOR.AZFSIDP1
```

- **Add the factor to a RACF user:**

```
ALU JOEUSER MFA (FACTOR (AZFSIDP1) ACTIVE TAGS (SIDUSERID:JOE1))
```

- Adds factor to the user
- Activates the factor – JOEUSER is now required to authenticate to RACF with MFA credentials
- Adds a factor specific tag – SIDUSERID – Associates RSA SecurID user ID with z/OS user ID

- **User is provisioned:**

- JOEUSER must now authenticate to RACF with an RSA SecurID token and PIN

What if something doesn't work?

Some applications have authentication properties which can prevent MFA from working properly:

- **Length of password field** – Some MFA credentials are longer than 8 characters
- **Replaying of passwords** – MFA credentials are one time use

IBM MFA for z/OS was architected with this in mind and provides a variety of accommodation mechanisms.

1. Selective Application Exclusion

- Exempting MFA processing for certain applications:
 - Allows a Security Administrator to mark certain applications as excluded from MFA
 - Allows a user to logon to that application using their non-MFA credentials

2. PassTicket Support

- Allows the Security Administrator to indicate that an MFA user can authenticate with a PassTicket instead of an ACTIVE MFA factor. New special MFA PassTicket Factor

3. Out-of-Band Support

- Allows users to authenticate with multiple factors directly to IBM MFA and receive a logon token
- The pre-authentication logon tokens behavior can be customized as needed
 - Controls to allow tokens to be single use or re-useable and how long a token is valid

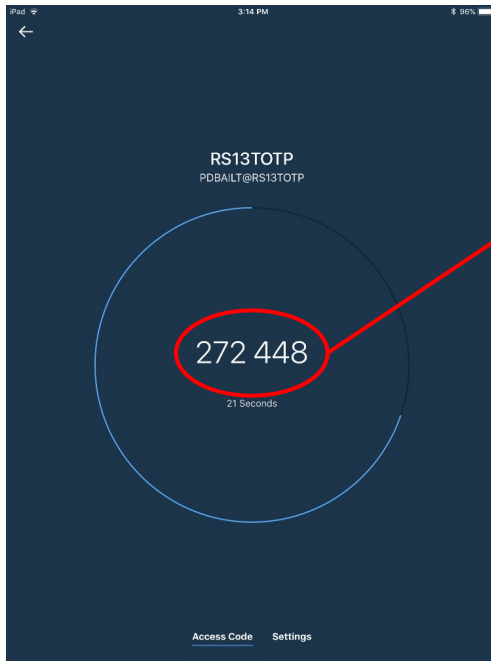
Session Managers

Provides a nice single sign-on experience on the mainframe

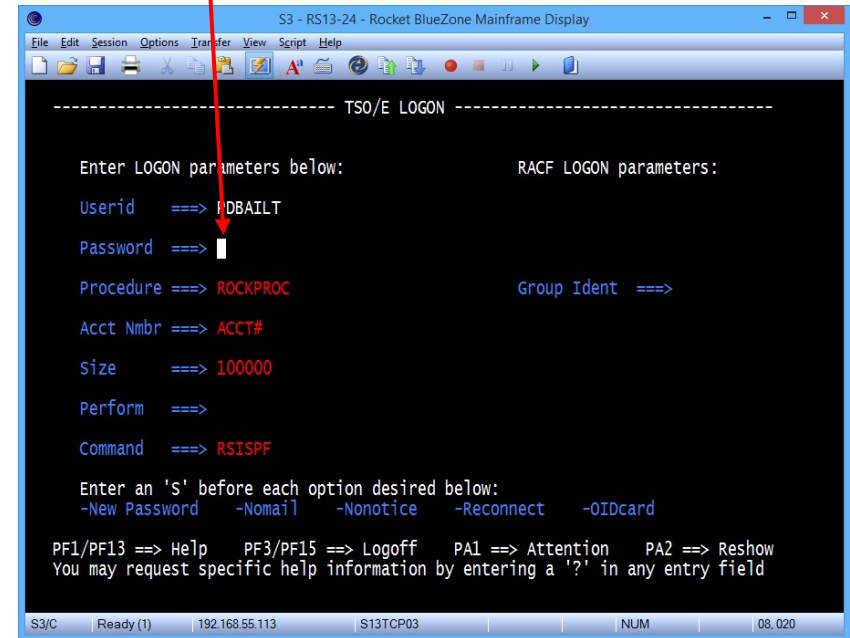
- Session Manager needs to be configured to work with PassTickets
- User logs on to the Session Manager with MFA credentials
- Subsequent calls to other applications, Session Manager will generate a PassTicket to authenticate
- Requires an additional factor for the user: AZFPTKT1

NOTE: Session Manager must support PassTickets

Example – User log in w/ IBM Verify and RACF password



Password: `passw0rd`
`272448` } → `272448:passw0rd`



- User authenticates with compound in-band by entering:
 - The IBM Verify token code (or other TOTP App)
 - A colon (configurable separator character)
 - Their RACF password / password phrase
- All together in the password phrase field

MFA for z/VM - Overview

Runs on Linux for Z

- “Bring your own Linux” with initial support for RHEL and SLES
- Installed using RPM
- Prereqs: postgres, pkcs#11, OpenSSL

Administered and configured separately from z/OS

- Web GUI, also scripts and command-line tools

End-user flow is out-of-band

- User obtains CTC from MFA, specifies CTC when logging on to RACF or VM:Secure

1. Sign in with your IBM id
community.ibm.com/security

Contact Us

Sign In or Join

Home Groups Local Groups Events Participate Resources All Communities

Global Security Forum

AppSec

BigFix

Guardium/Data Protection

i2

IAM

MaaS360

QRadar

QRadar Windows Event Collection

Resilient

Trusteer

zSecurity

Learn

Bringing s
greatest c

Join the

er to tackle one of the

2. Join the zSecurity Community

Ask a
one –
conve

ork locally and
ect globally

Read up on the latest
tips, tricks, and
techniques

Develop your security
skills and access training
courses

Discussions →

Events →

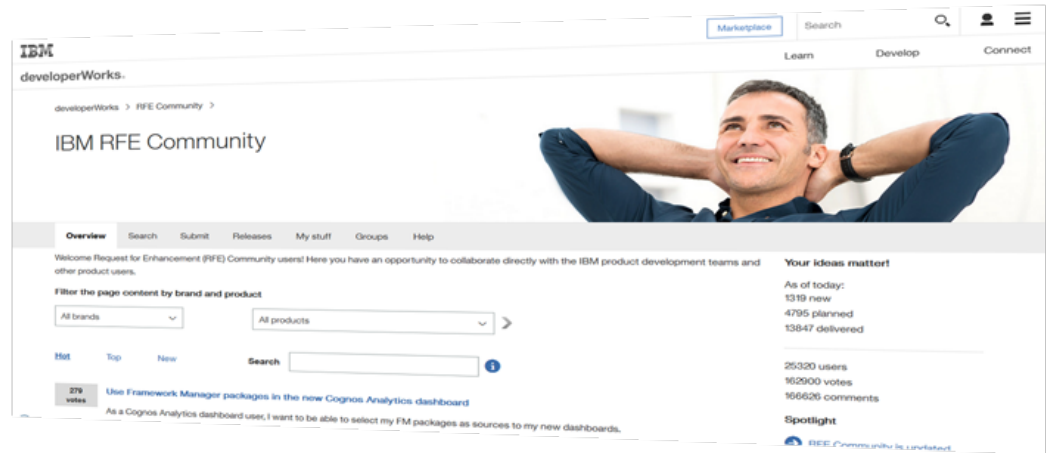
Blogs →

Resources →

Requests For Enhancements (RFE)

It is strongly recommended that clients identify their requirements for IBM MFA through this channel.

In particular, please open RFEs for additional authentication tokens that are used in your shop that would provide value if supported by IBM MFA for z/OS.



Link: <https://www.ibm.com/developerworks/rfe>

QUESTIONS



Notices and disclaimers

- © 2019 International Business Machines Corporation. No part of this document may be reproduced or transmitted in any form without written permission from IBM.
- **U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.**
- Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed “as is” without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.
- IBM products are manufactured from new parts or new and used parts.
In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply.”
- **Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.**
- Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those
- customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.
- References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.
- Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.
- It is the customer’s responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer’s business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.



Notices and disclaimers continued

- Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**
- The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.
- IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml

