Multi Factor Authentication for Linux on IBM Z using a centralized z/OS LDAP infrastructure

Dr. Manfred Gnirss
Thomas Wienert
Z ATS
IBM Germany R & D

IBM Systems

Boeblingen, 18.7.2018

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States, other countries, or both.

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.

Those trademarks followed by ® are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml:

*BladeCenter®, DB2®, e business(logo)®, DataPower®, ESCON, eServer, FICON, IBM®, IBM (logo)®, MVS, OS/390®, POWER6®, POWER6+, POWER7®, Power Architecture®, PowerVM®, S/390®, System p®, System p5, System x®, System z®, System z9®, System z10®, WebSphere®, X-Architecture®, zEnterprise, z9®, z10, z/Architecture®, z/OS®, z/VM®, z/VSE®, zSeries®

The following are trademearks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

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

Microsoft, Windows, Windows NT, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the 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.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Acknowledgement

Our very best thanks belong to

Florian Warband – Fiducia & GAD IT AG
Christian Tatz – Fiducia & GAD IT AG
Pascal Meyer – Fiducia & GAD IT AG
Andreas Geiss – Fiducia & GAD IT AG
Karsten Rohrbach – ABK Systeme GmbH
Uwe Denneler – IBM
Günter Weber – IBM
Richard Young - IBM
and all the others

who contributed to this session.

Current Security Landscape

1,935

Number of security incidents in 2015 with confirmed data disclosure as a result of stolen credentials.[1]

(506 worse than prior year)

81%

Number of breaches due to stolen and/or weak passwords.[1]

(18% worse than prior year)

$4 million

The average total cost of a data breach.[2]

60%

Number of security incidents that are from insider threats. [3]

Criminals are identifying key employees at organizations and exploiting them with savvy phishing attacks to gain initial access to the employees' system and steal their account credentials. This puts emphasis on the need for tighter restrictions on access privileges to key data repositories.[1]

[1] 2017 Verizon Data Breach Investigations Report

[2] Ponemon: 2016 Cost of Data Breach Study: Global Analysis

[3] IBM X-Force 2016 Cyber Security Intelligence Index

Current Security Landscape . . .

- "81% of hacking-related breaches leveraged either stolen and/or weak passwords."

Source: Verizon Data Breach Investigations Report, 2017

- In 2014, 2 in 5 people
  - Received notice that their personal information was breached
  - Had an account hacked
  - Had a password stolen
- 73% of online accounts are guarded by duplicate passwords
- 47% of people use passwords that are at least 5 years old
- 21% of people use passwords that are over 10 years old

  Source: https://www.entrepreneur.com/article/246902

- "59% of employees steal proprietary corporate data when they quit or are fired."
- "In 93% of breaches, attackers take minutes or less to compromise."

  Source: https://www.bitsighttech.com/blog/data-breach-statistics

- According to Symantec's 2016 Internet Security Threat Report, 80% of breaches can be prevented by using multi-factor authentication.

Source https://www.lexology.com/library/detail.aspx?g=5df10dbf-54fa-40dd-9f3f-2d08d275bf75

User Authentication Today

- Users can 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
  - . . .

Compliance

PCI DSS v3.2

8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.

8.3.1 Incorporate multi-factor authentication for all non-console access into the Cardholder Data Environment (CDE) for personnel with administrative access.

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

NIST SP 800-171

3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

Note: Network access is any access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).

Note: This requirement is effective December 31, 2017.

Why MFA is needed

- We need to be sure the person logging in is you! A single factor alone is more susceptible to unauthorized use.

- To better secure your systems, application, and data, by thwarting attacks of only a single factor.

- Payment Card Industry (PCI) requires it for things such as remote access and administrative access to the card data environment

- Requirements for access to Federal Government systems

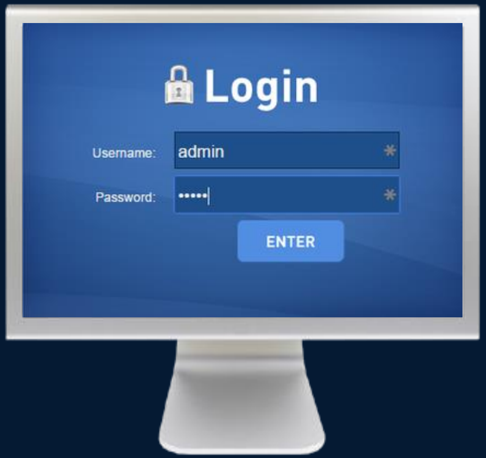
- Possibly to follow your own corporate security policy

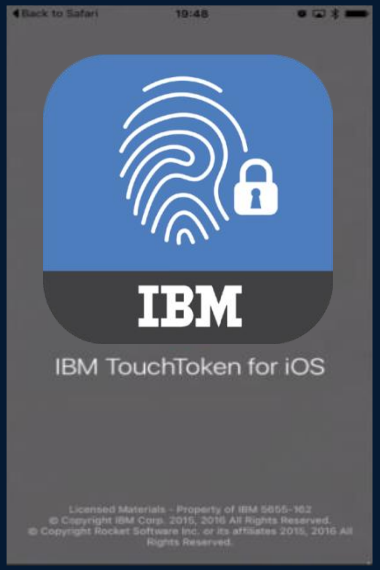
- MFA is especially important for privileged administrative accounts.

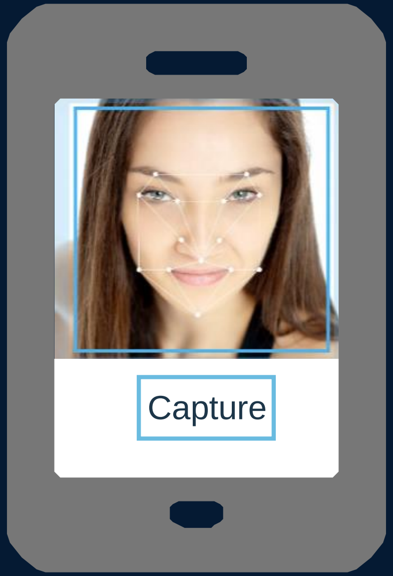
- *To be smart and secure your data!*

Authentication is a journey

Moving to stronger, easier authentication







SOMETHING THAT YOU KNOW
- Usernames and passwords
- PIN Code
- Knowledge questions

SOMETHING THAT YOU HAVE
- ID Badge
- One time passwords
  - Time-based
  - Email / SMS

SOMETHING THAT YOU ARE
- Biometrics

What is multi-factor authentication (MFA)

- Authentication with more than one factor such as a password or a key to gain access
- A factor could be something only you know (ie password), something only you have (ie key fob), or something only you are (i.e. biometrics)

- ATM Card and PIN – Something you have and something you know
- More factors generally mean more security, as if one factor is compromised such as a password, more factors are still required to successfully authentication

- There is a distinction between multi-factor authentication vs multi-step authentication.
  - Multi step could be two or more pins, two or more passwords, two or more keys, or two or more biometric identifiers, but all of the evidence or factor type (ie they are all something you know)
  - Two password or two pins might be compromised by a key stroke logger.
  - Different factors being used, but providing results of authentication before all factors have been presented is considered “multi-step”.

- PCI-DSS requires factors to be independent. Example: Userid/pw used to authenticate to the system in question can not be the same as the userid/pw for email if a one time password emailed.

What is NOT a MFA or not acceptable implementations

- Using SSH keys protected by a password. The keys could be considered something you have and the password something you know. However this can not be verified by the server. Also the use of a password to protect the ssh keys can not be enforced or audited.
- Multi-step authentication
  - Multiple of the same category of factor
  - Providing results of one of the factors independently before all factors have been presented.
- Different factors dependent on each other.
  - First factor is a password
  - Second factor is a One Time Password sent to an email account protected by the same password as the first factor
- Some consider OTP over SMS to be too insecure to be acceptable. SMS and voice calls can be intercepted.
- NIST had permitted the use of SMS, but has advised that out-of-band authentication using SMS or voice has been deprecated and may be removed from future releases of their publication
- Authentication process “out of band” from transmission of factors. For example if you enter all factors in to a web browser on your phone, but one of factors is a OTP soft token on your phone, the effectiveness of that factor is considered nullified.

Oath Standard

OATH (Initiative for Open Authentication) is an organization that specifies two open authentication standards: TOTP and HOTP https://openauthentication.org

Don’t confuse with Oauth with is something different (An open standard for access delegation).

TOTP - Time-Based One-Time Password, the user enters a 6-8 digit code that changes every 30 seconds. https://tools.ietf.org/html/rfc6238

HOTP (HMAC based One-Time Password) is similar to TOTP, except that an authentication counter is used instead of a timestamp. This means there are no time synchronization issues.

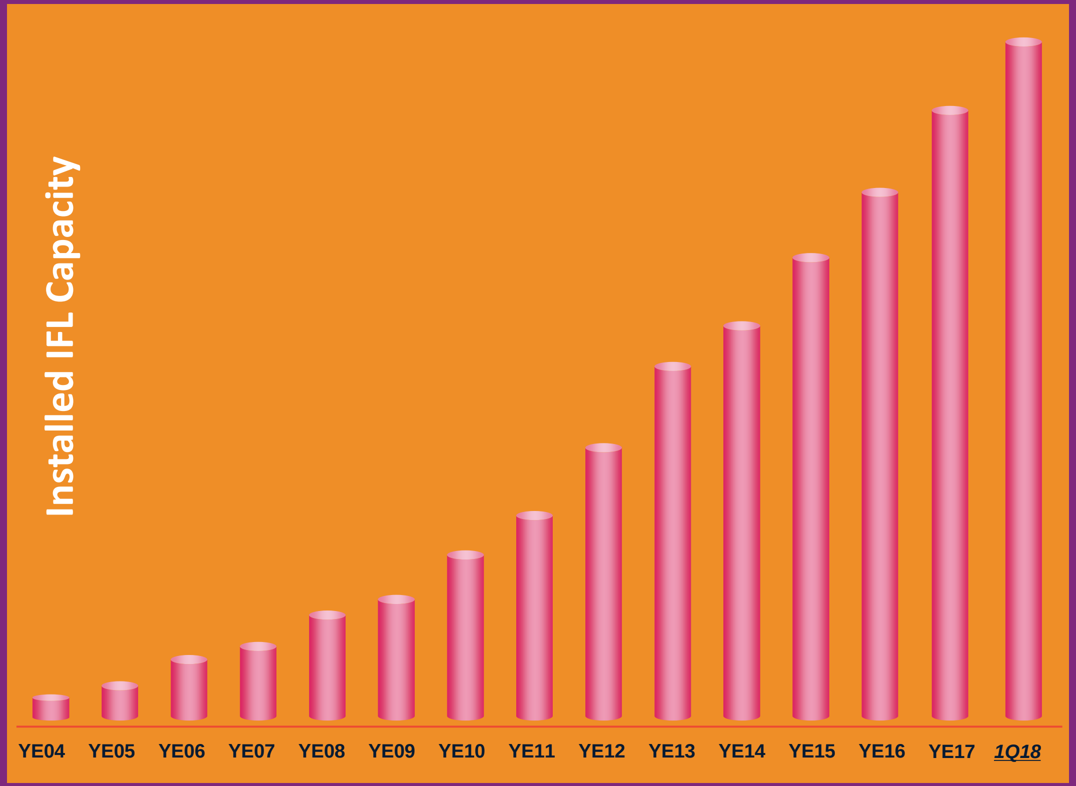
https://tools.ietf.org/html/rfc4226

Linux on IBM Z in 1Q2018

*Installed Linux MIPS at 38% CAGR**

- 29.1% of Total installed MIPS run Linux as of 1Q18
- Installed IFL MIPS increased by 20% YTY from 1Q17 to 1Q18
- 50% of IBM Z Enterprises have IFL’s installed as of 1Q18
- 91 of the top 100 IBM Z Enterprises are running Linux on Z as of 1Q18 **
- 38% of all IBM Z servers have IFLs
- 56% of new FIE/FIC IBM Z Accounts run Linux

Installed Capacity Over Time



** Based on YE 2003 to YE 2017* ***Top 100 is based on total installed MIPS*

IBM Multi-Factor Authentication for z/OS

Higher assurance authentication for IBM z/OS systems that use RACF

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

- Support for third-party authentication systems
  - RSA SecurID® Tokens (hardware & software based)
  - IBM TouchToken – Timed One Time use Password (TOTP) generator token
  - PIV/CAC and Smart cards – Commonly used to authenticate in Public Sector enterprises
  - RADIUS-based factors
  - High Availability MFA Web Services

- Tightly integrated with SAF & RACF

TECHNOLOGY RSA READY PARTNER

gemalto security to be free

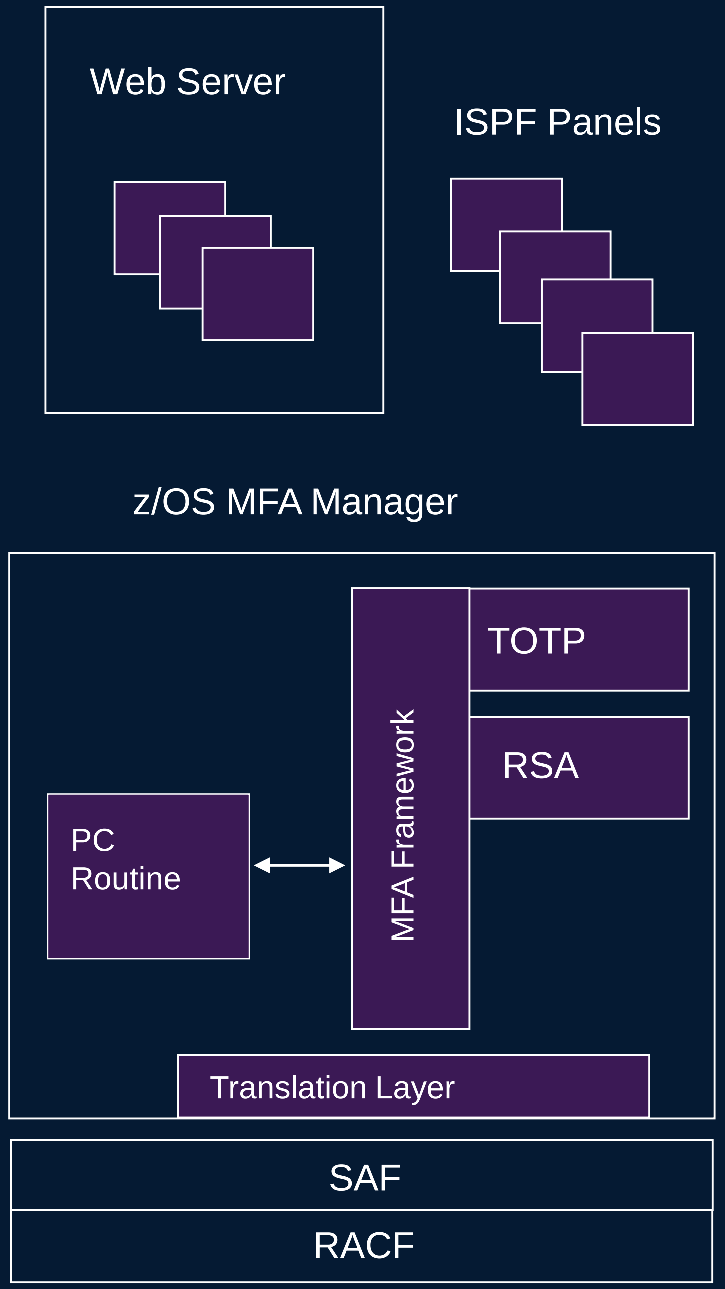
Fast, flexible, deeply integrated, easy to deploy, easy to manage, and easy to use

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/OS

- MFA Manager Web Interface
  - – User Interface – supports factors such as smartphone apps and serves as web interface for registration – depending on factor type
- MFA ISPF panels for management of authentication tokens
- 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
  - – Common MFA processing
- Translation Layer
  - – Allows MFA components to invoke RACF callable services
    - "Wrap" SAF/RACF database access APIs



RSA SecurID Tokens Support

RSA READY

- Requires RSA SecurID server configured to the MFA Server
- Since the use of RSA SecurID requires an external configured server instance – this could represent a point of failure
- Supports both hard and soft RSA SecurID tokens

000147678169 Options

Tokencode:
6760 2680

Re-enter PIN Copy

RSA SecurID

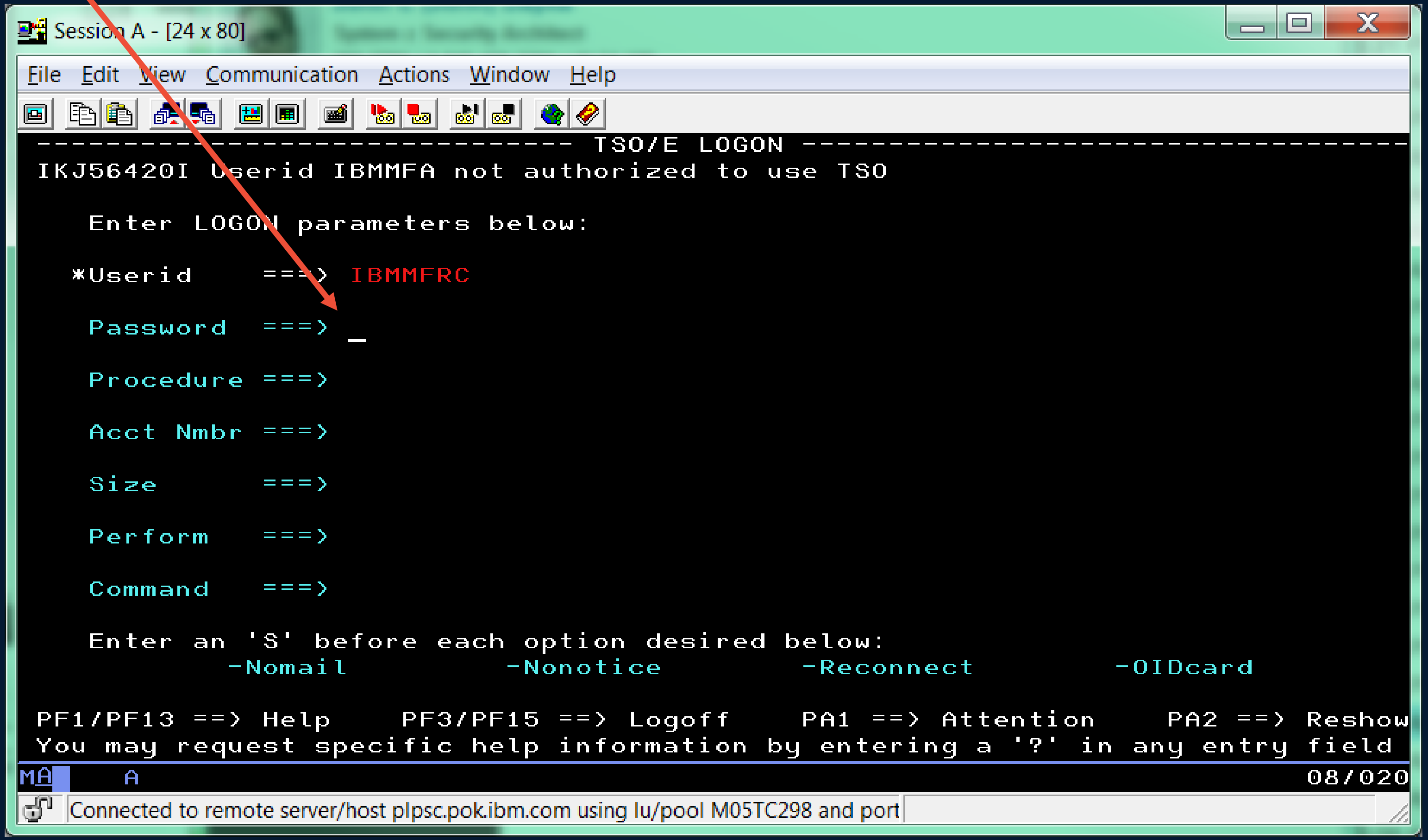
Requires RSA Authentication Manager 8.1 or later for RSA® SecurID® exploitation

Using Hard RSA SecurID Tokens

Pin Code: **1234**

159759

1234159759



```
------------------------------- TSO/E LOGON ---------------------------------------
IKJ56420I Userid IBMMFA not authorized to use TSO

   Enter LOGON parameters below:

  *Userid    ===> IBMMFRC

   Password  ===> _

   Procedure ===>

   Acct Nmbr ===>

   Size      ===>

   Perform   ===>

   Command   ===>

   Enter an 'S' before each option desired below:
           -Nomail          -Nonotice         -Reconnect         -OIDcard

PF1/PF13 ==> Help    PF3/PF15 ==> Logoff    PA1 ==> Attention    PA2 ==> Reshow
You may request specific help information by entering a '?' in any entry field
MA      A                                                                08/020
```

Connected to remote server/host plpsc.pok.ibm.com using lu/pool M05TC298 and port

Something you know: RSA PIN Code

Something you have: RSA SecurID FOB with your specific cryptographic key

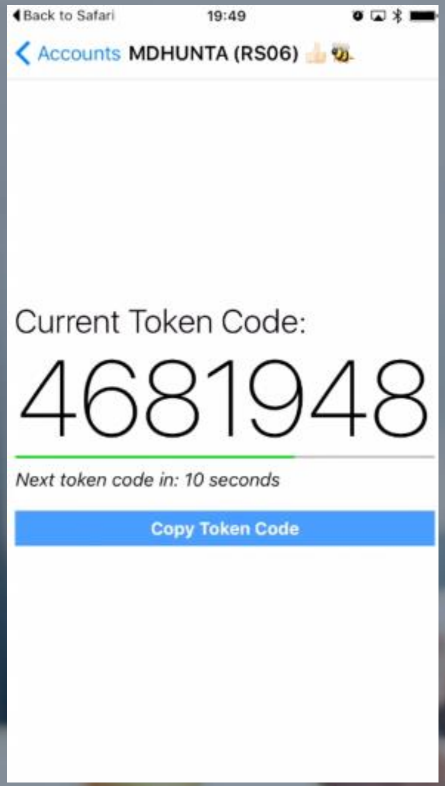
Note: Applications must be configured to support password phrases.

IBM TouchToken – Timed One Time use Password generator

- Authentication factor that can be directly evaluated on z/OS to ensure that there is always a means of enforcing 2 factor authentication for users

- Provisioned with a shared secret key into the iOS key chain

- Does not rely on an external server, eliminates an external point of failure


Back to Safari 19:49

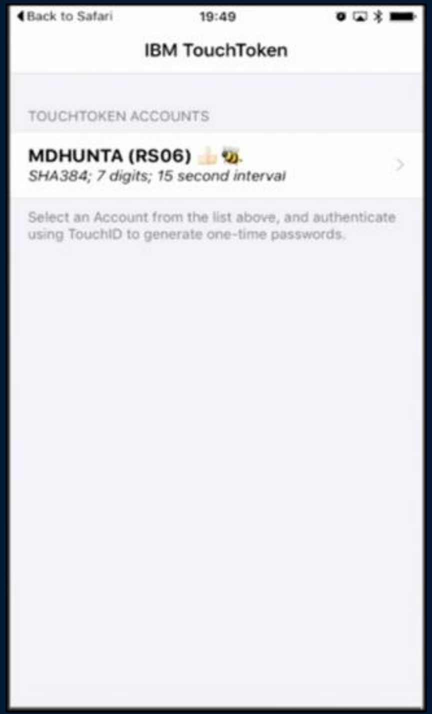
Accounts MDHUNTA (RS06)

Current Token Code:

4681948

Next token code in: 10 seconds

Using IBM TouchToken for iOS – Logon to TSO



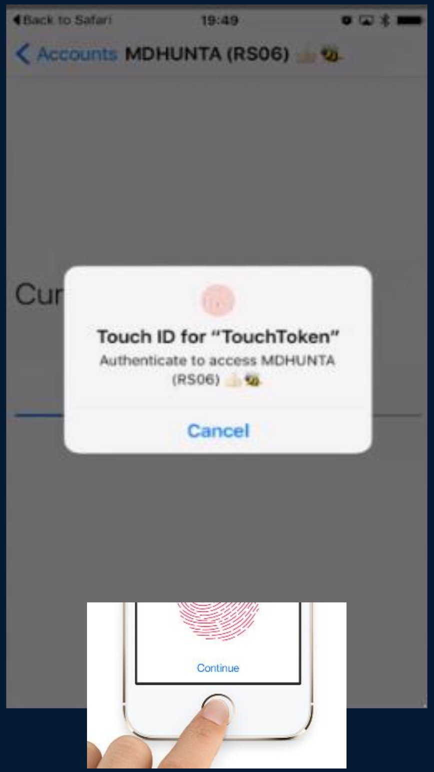
◀Back to Safari 19:49

IBM TouchToken

TOUCHTOKEN ACCOUNTS

MDHUNTA (RS06) 👍🐝
SHA384; 7 digits; 15 second interval

Select an Account from the list above, and authenticate using TouchID to generate one-time passwords.



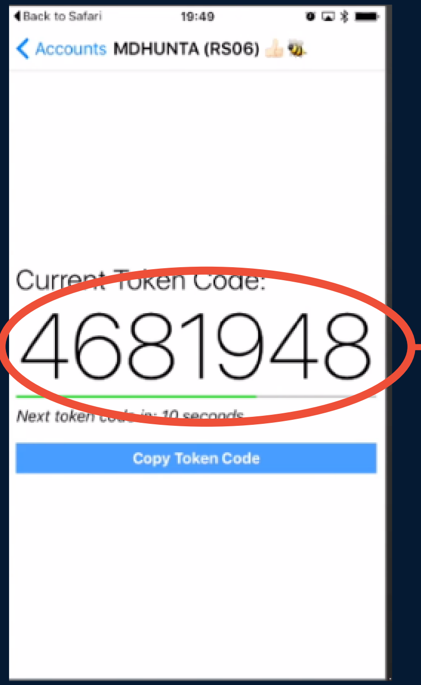
◀Back to Safari 19:49

< Accounts MDHUNTA (RS06) 👍🐝

Cur

Touch ID for "TouchToken"
Authenticate to access MDHUNTA (RS06) 👍🐝

Cancel



◀Back to Safari 19:49

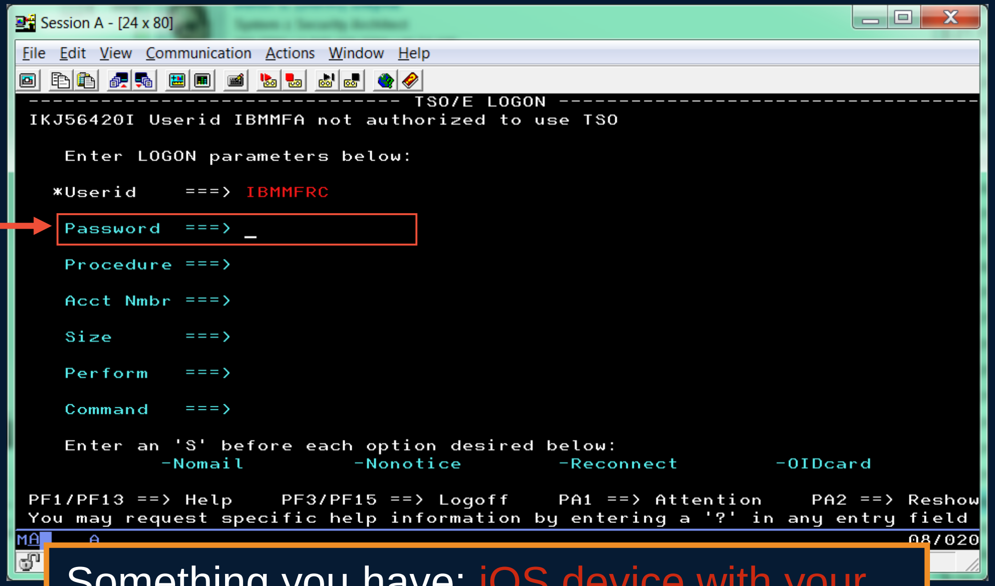
< Accounts MDHUNTA (RS06) 👍🐝

Current Token Code:

4681948

Next token code in: 10 seconds

Copy Token Code



```
------------------------------- TSO/E LOGON -----------------------------------
IKJ56420I Userid IBMMFA not authorized to use TSO

   Enter LOGON parameters below:

  *Userid    ===> IBMMFRC

   Password  ===> _

   Procedure ===>

   Acct Nmbr ===>

   Size      ===>

   Perform   ===>

   Command   ===>

   Enter an 'S' before each option desired below:
           -Nomail         -Nonotice         -Reconnect         -OIDcard

PF1/PF13 ==> Help    PF3/PF15 ==> Logoff    PA1 ==> Attention    PA2 ==> Reshow
You may request specific help information by entering a '?' in any entry field
MA    a                                                                 08/020
```

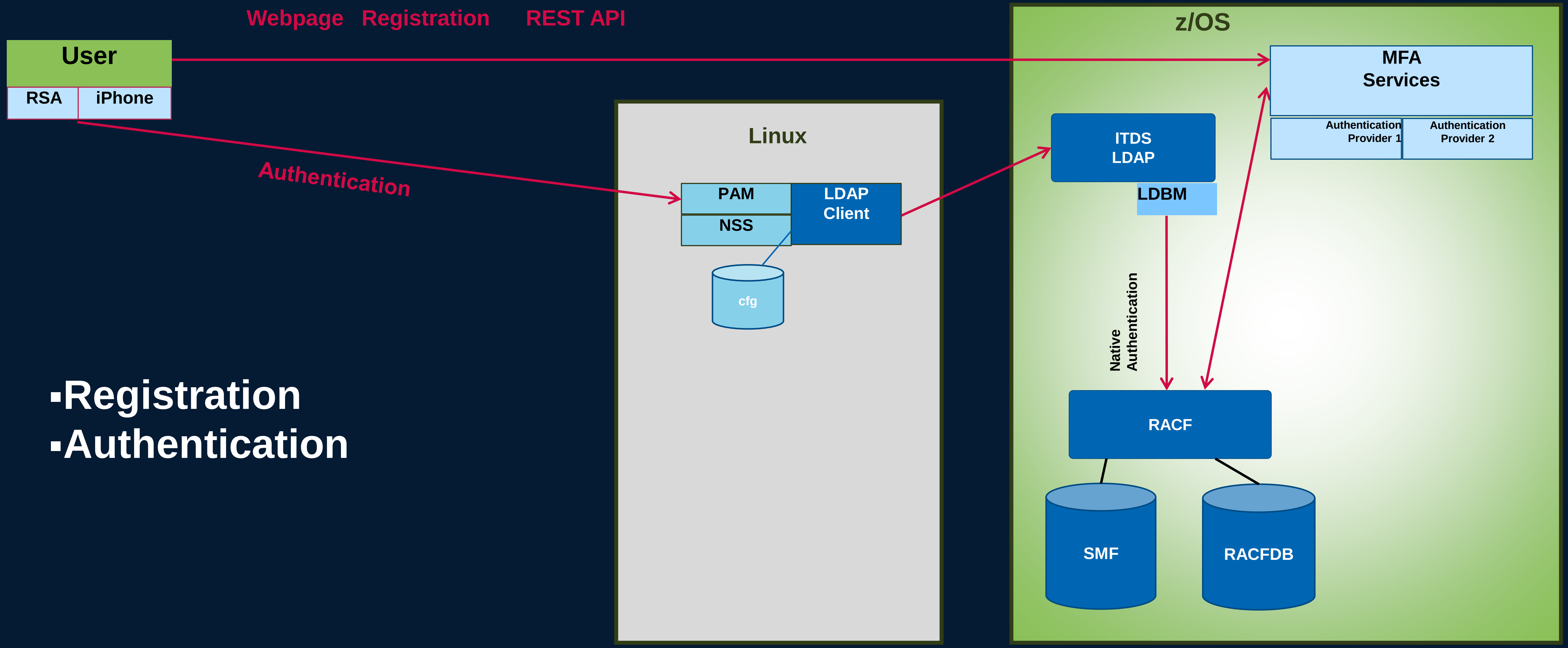
Something you have: iOS device with your specific cryptographic key inside.

Something you are: Fingerprint

1. User selects the account that a IBM TouchToken will be used for Authentication
2. Authenticates with Touch ID, scan fingerprint.
3. IBM TouchToken app access the iOS key chain to generate a TouchToken code
4. User enter TSO user ID and current token

Centralized MFA authentication for Linux with z/OS

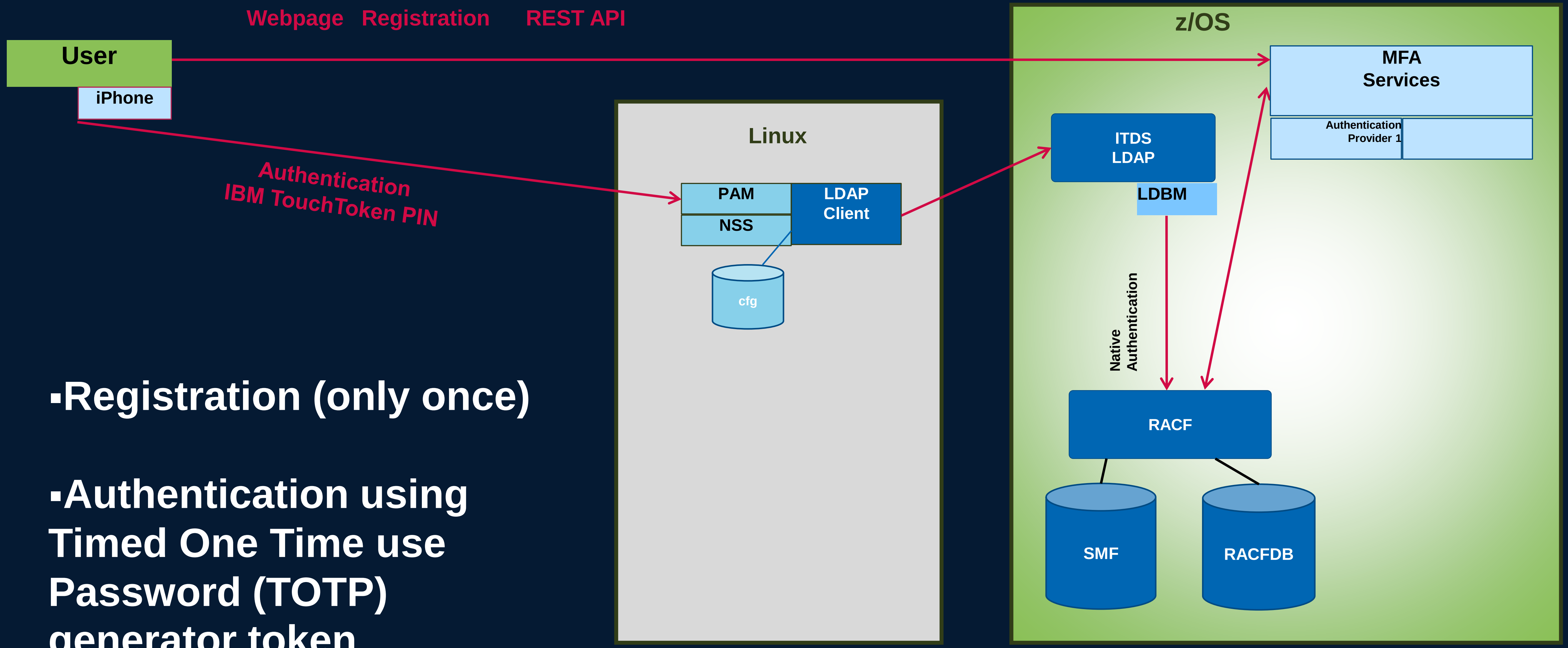
Centralized authentication using ITDS / RACF / MFA infrastructure of z/OS - General



- Registration
- Authentication

Centralized MFA authentication for Linux with z/OS . . .

Centralized authentication using ITDS / RACF / MFA infrastructure of z/OS
- IBM Touch Token

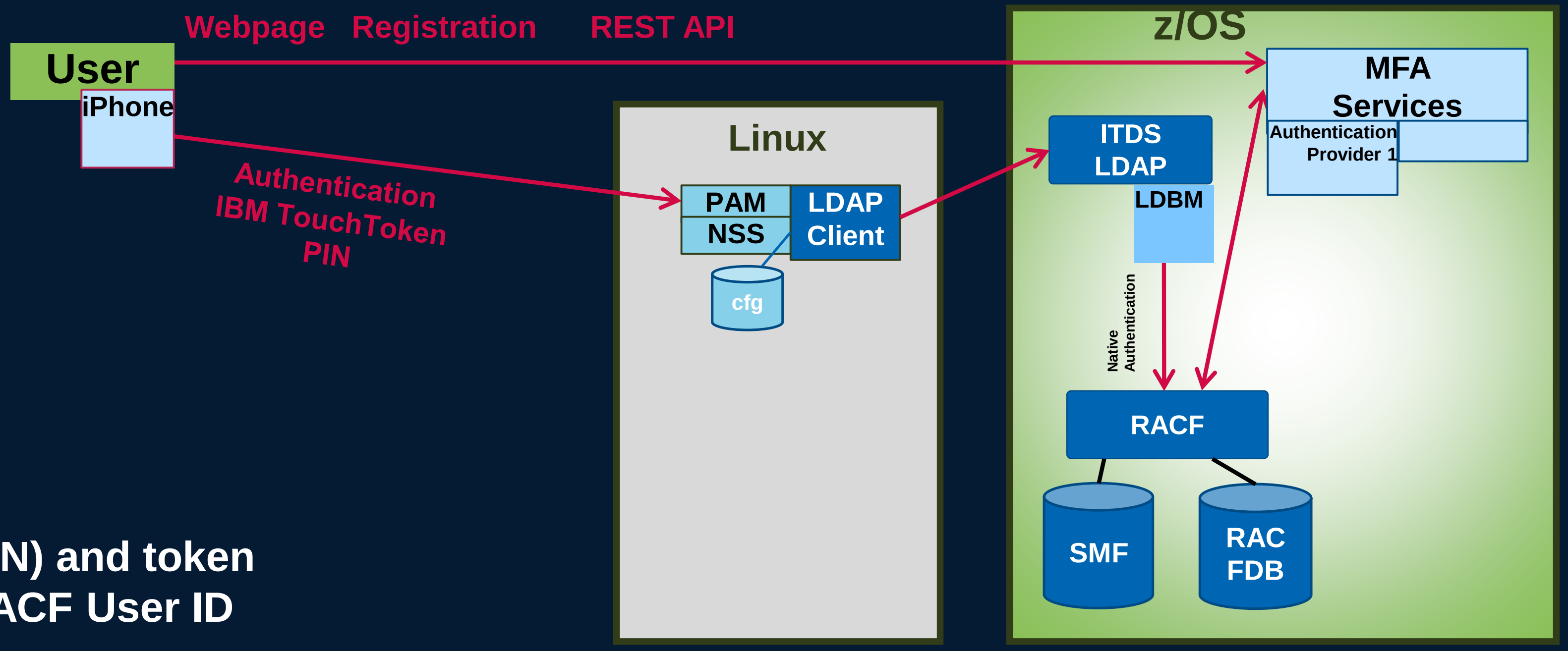


- Registration (only once)

- Authentication using Timed One Time use Password (TOTP) generator token

Centralized MFA authentication for Linux with z/OS . . .

Centralized authentication using ITDS / RACF / MFA infrastructure of z/OS - IBM Touch Token



- Linux user MFA registration
- Linux user authentication:
  - Linux userid is mapped to RACF User ID
- Linux user then authenticates to Linux via token
- PAM module invokes ITDS to validate Linux User ID (LDAP CN) and token
  - Using Native Authentication LDAP CN is mapped to a RACF User ID
    - Token evaluation performed by RACF
  - RACF uses policy to determine if Two Factor Authentication is required – if so, invokes MFA services to validate the token
  - If token is valid, authentication is successful.
  - ITDS returns the result of the authentication to the Linux PAM

RACF and IBM MFA can leverage *Two Factor Authentication* for Linux users.

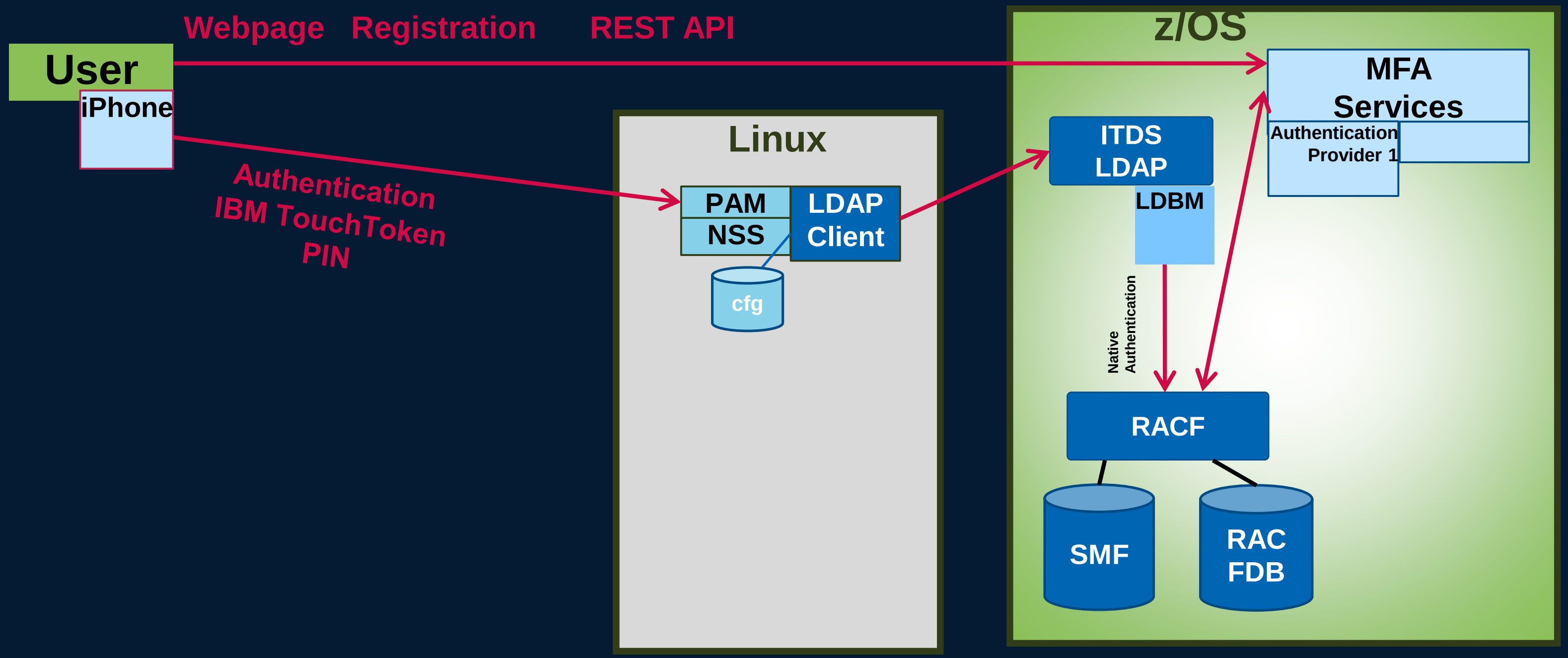
Centralized MFA authentication for Linux with z/OS . . .

Centralized authentication using ITDS / RACF / MFA infrastructure of z/OS with IBM Touch Token

- An approach for implementation and test

- If not yet available:
  Setup and configure MFA on z/OS

- Decide which Linux users will be enabled for MFA
  Note: These users need also a RACF userid!



Centralized MFA authentication for Linux with z/OS . . .

Centralized authentication using ITDS / RACF / MFA infrastructure of z/OS with IBM Touch Token

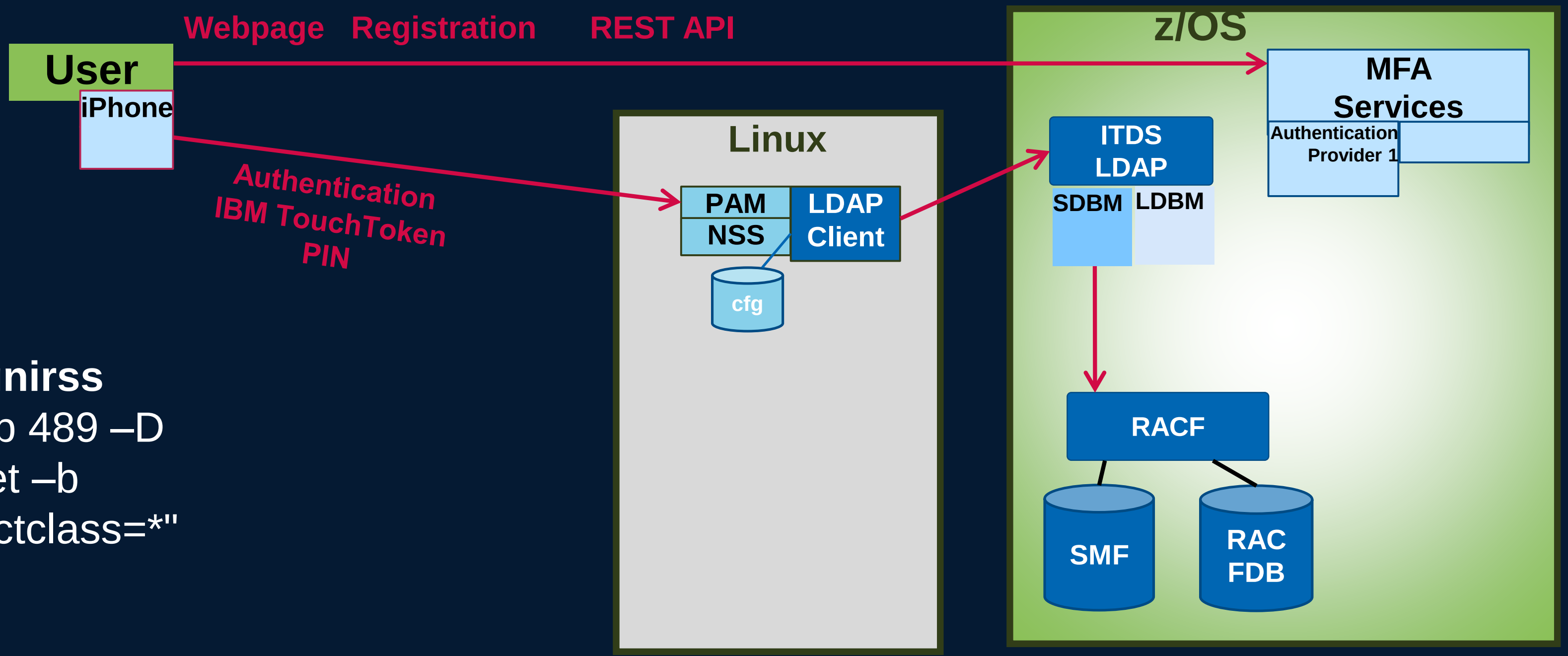
- An approach for implementation and test

- Setup / configure LDAP Server on z/OS
  - SDBM for verification only (optional step)
    - Example LDAP Configuration:

      ```
      database SDBM GLDBSD31/GLDBSD64
      suffix "sysplex=CC11"
      ```
    - Example: Test with ldapsearch command for userid mgnirss

      ```
      CC11:MGNIRSS:/u/mgnirss>ldapsearch -h 9.152.87.89 -p 489 –D
      racfid=mgnirss,profiletype=USER,sysplex=CC11 -w secret –b
      racfid=MGNIRSS,profiletype=USER,sysplex=CC11 "objectclass=*"

      racfid=MGNIRSS,profiletype=USER,sysplex=CC11
      racfid=MGNIRSS
      ...
      racfpasswordchangedate=03/29/18
      racfprogrammername=GNIRSS MANFRED
      ...
      ```

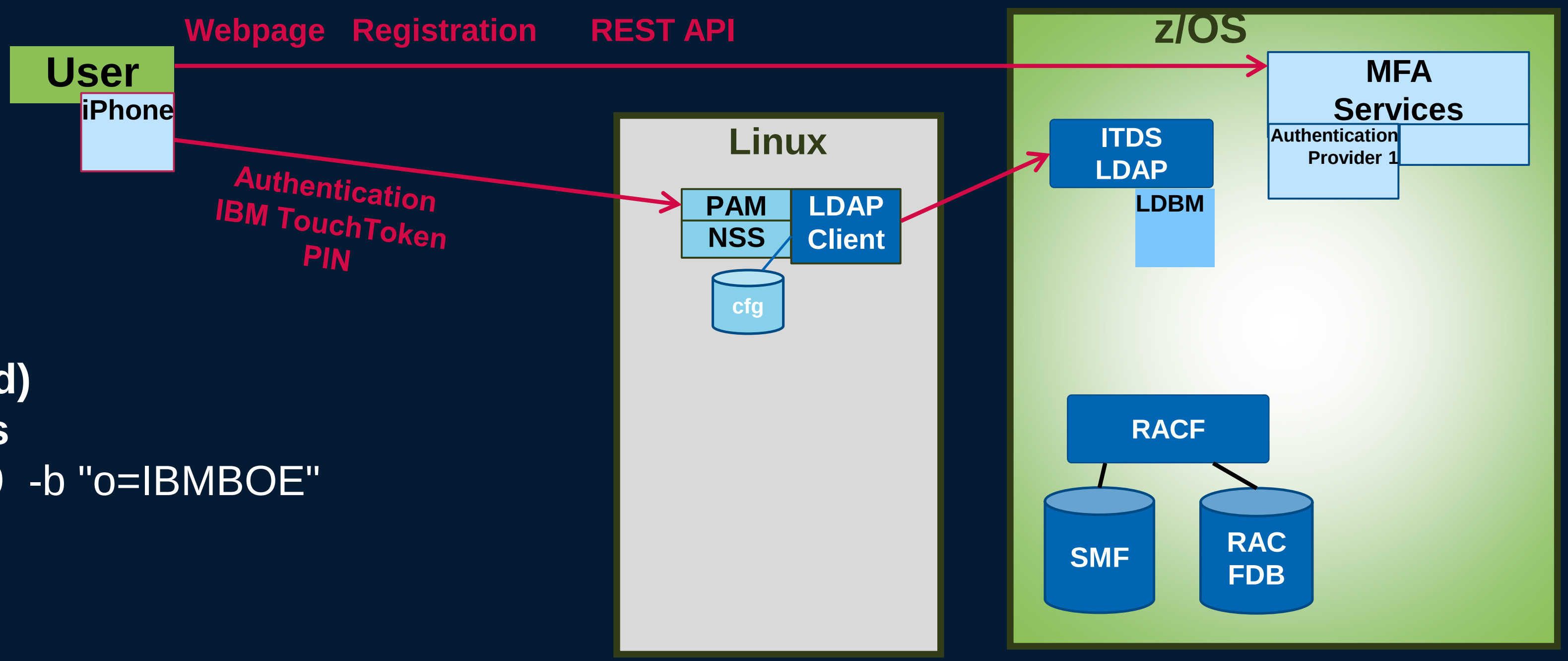


Notes:

- **In our example we have only minimal information in LDBM for authentication purpose.**
- **If ITDS/LDBM would be used for authentication without RACF / MFA , also attribute userPassword would be necessary.**
- **Depending on configuration also attribute IBM-nativeID is usefull.**

Centralized MFA authentication for Linux with z/OS . . .

Centralized authentication using ITDS / RACF / MFA infrastructure of z/OS with IBM Touch Token
- An approach for implementation and test



- **Setup / configure LDAP Server on z/OS . . .**
  - **LDBM (or TDBM) to contain user to be authenticated**
  - **Example LDAP Configuration:**

    ```
    database LDBM GLDBSD31/GLDBSD64
    suffix “o=IBMBOE"
    ```

  - **Add schema and user information (via ldapmodify command)**
  - **Example: Test with ldapsearch command for userid mgnirss**

    ```
    CC11:MGNIRSS:/u/mgnirss>ldapsearch -h 9.152.87.89 -p 489  -b "o=IBMBOE"
    "(cn=Manfred Gnirss)"

    cn=Manfred Gnirss, o=IBMBOE
    givenname=Manfred
    objectclass=top
    objectclass=person
    objectclass=inetOrgPerson
    objectclass=organizationalPerson
    uid=mgnirss
    cn=Manfred Gnirss
    sn=Gnirss
    ```

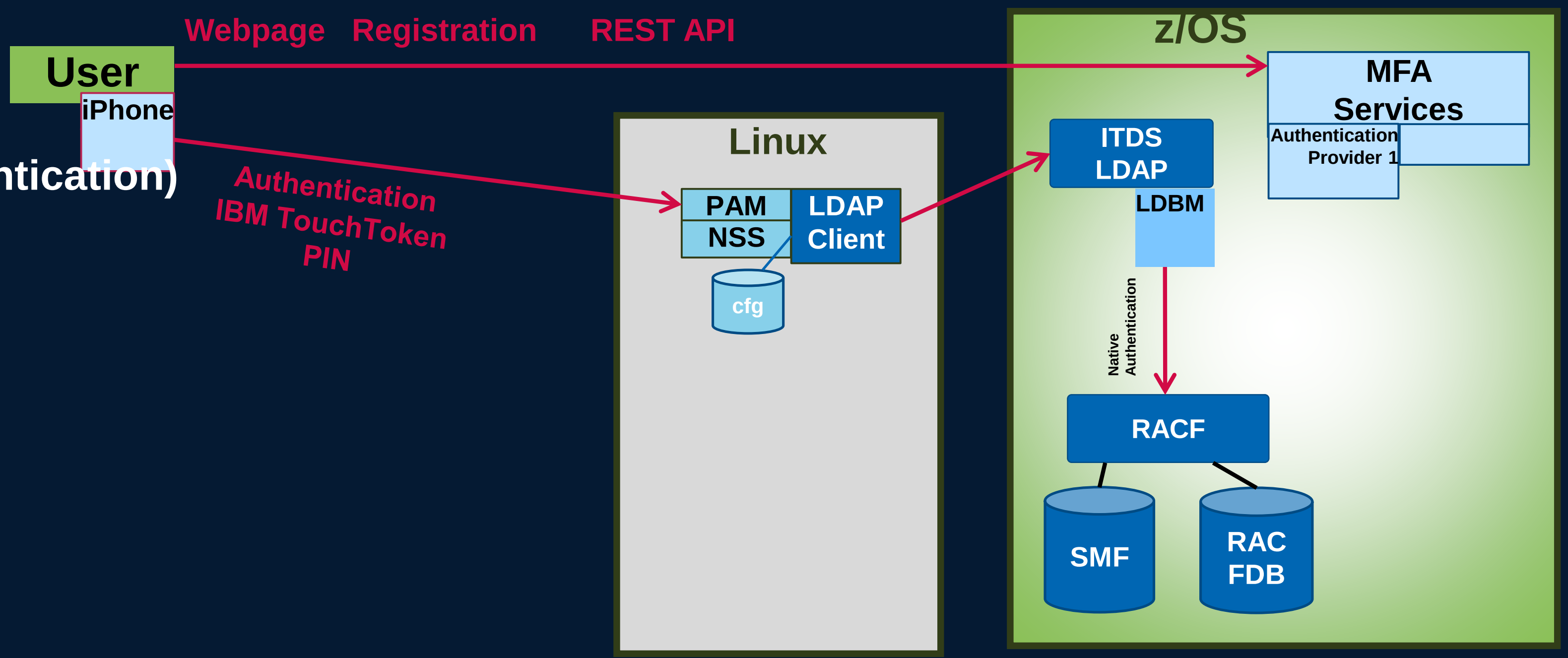
Notes:

- In our example we have only minimal information in LDBM for authentication purpose.
- If ITDS/LDBM would be used for authentication without RACF / MFA , also attribute userPassword would be necessary.
- Depending on configuration also attribute IBM-nativeID is usefull.

Centralized MFA authentication for Linux with z/OS . . .

Centralized authentication using ITDS / RACF / MFA infrastructure of z/OS with IBM Touch Token

- An approach for implementation and test



- **Setup / configure LDAP Server on z/OS . . .**
  - **Map user to be authenticated with RACF user (Native authentication)**
    - **Example LDAP Configuration:**

```
useNativeAuth all
nativeAuthSubtree all
```

  - **Configure Linux to use LDAP server for authentication**
    - **Example for LDAP client configuration**

```
URI ldap://boecc11.boeblingen.de.ibm.com:489
BASE o=IBMBOE
```

    - **Example for pam.d/SSHD configuration**

```
account sufficient pam_ldap.so
account required        pam_unix.so use_first_pass
. . .
auth sufficient pam_ldap.so
auth   required        pam_unix.so use_first_pass
. . .
password sufficient pam_ldap.so
password required pam_unix.so use_first_pass
```

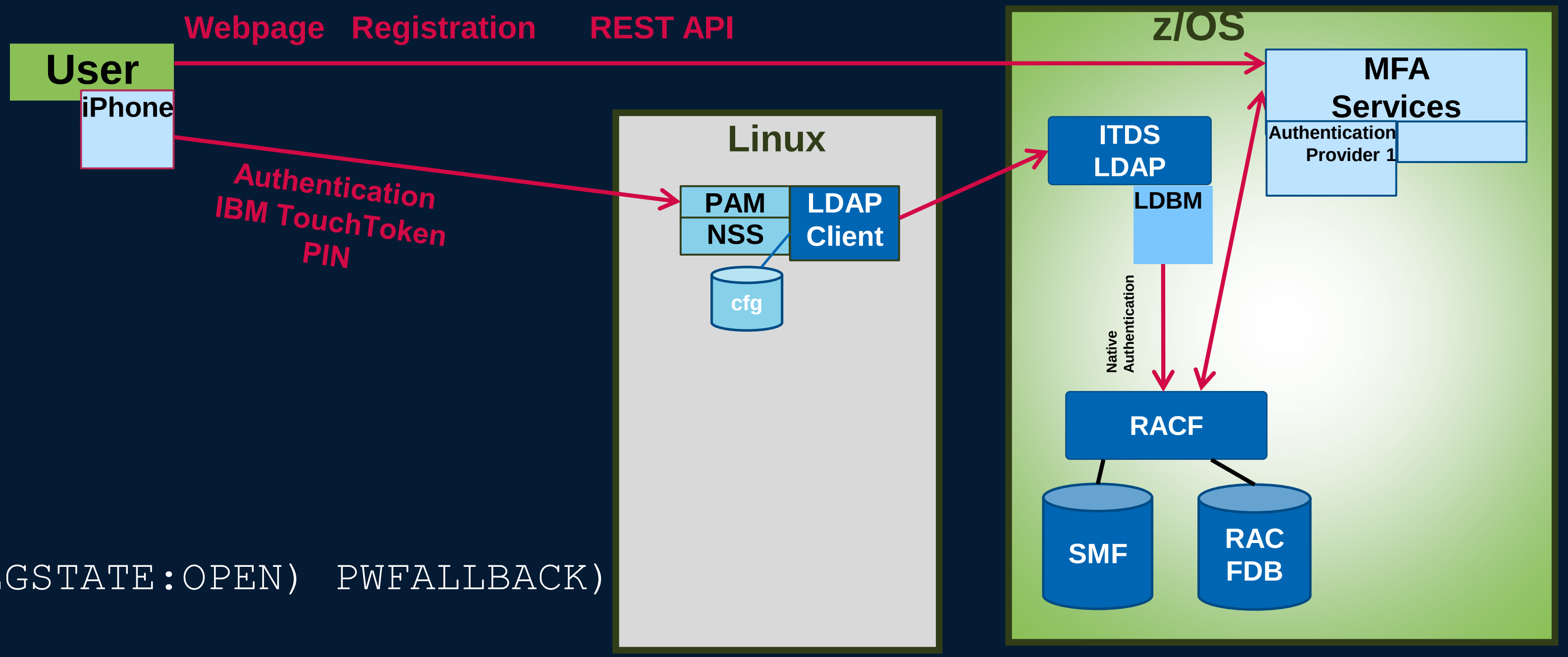
- **Test ssh login in Linux using RACF password**

Note: We strongly recommend, to protect the connection between LDAP client and LDAP server with SSL/TLS

Centralized MFA authentication for Linux with z/OS . . .

Centralized authentication using ITDS / RACF / MFA infrastructure of z/OS with IBM Touch Token

- An approach for implementation and test



- Enable user to be authenticated via MFA:
  - Activate the MFADEF class:

    ```
    SETR CLASSACT(MFADEF)
    ```

  - Define the factor profile:

    ```
    RDEFINE MFADEF FACTOR.AZFTOP1
    ```

  - Add the factor to a RACF user:

    ```
    ALU MGNIRSS MFA(FACTOR(AZFTOP1) ACTIVE TAGS(REGSTATE:OPEN) PWFALLBACK)
    ```

    Adds factor to the user
    Activates the factor – MGNIRSS is now required to authenticate to RACF with MFA credentials
    Password fallback – when MFA is unavailable, user can logon with password / phrase

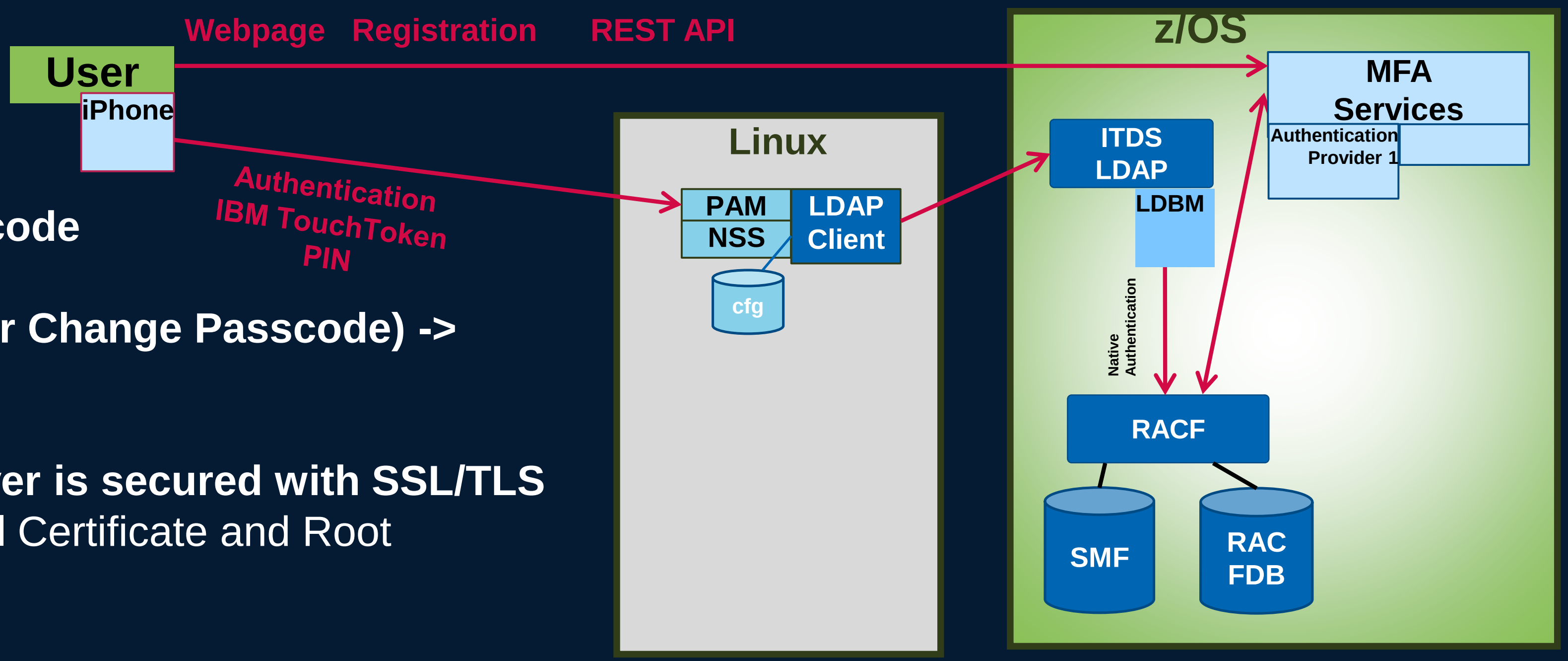
User is provisioned:

- MGNIRSS must now authenticate to RACF with token

Centralized MFA authentication for Linux with z/OS . . .

Centralized authentication using ITDS / RACF / MFA infrastructure of z/OS with IBM Touch Token

- An approach for implementation and test



- **Prepare iOS device for IBM Touch Token**
  - **Ensure that iOS device uses a complex alphanumeric passcode**

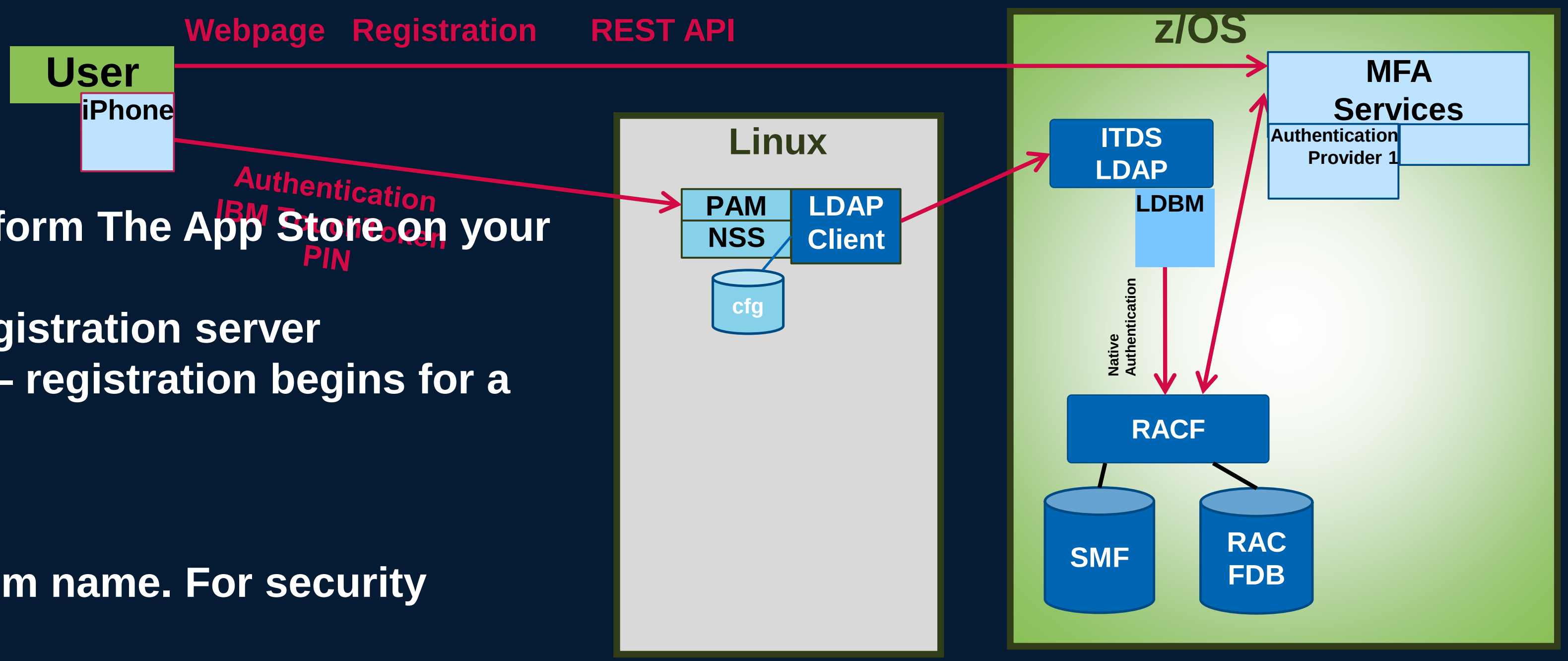
    Settings->Touch ID and Passcode -> Turn Passcode On (or Change Passcode) -> Passcode Options -> Custom Alphanumeric Code

  - **Connection iOS device to IBM TouchToken registration server is secured with SSL/TLS**
    Security administrator may instruct you to download and install Certificate and Root certificates to a configuration profile in the iOS device
    Settings->General->Profile

Centralized MFA authentication for Linux with z/OS . . .

Centralized authentication using ITDS / RACF / MFA infrastructure of z/OS with IBM Touch Token

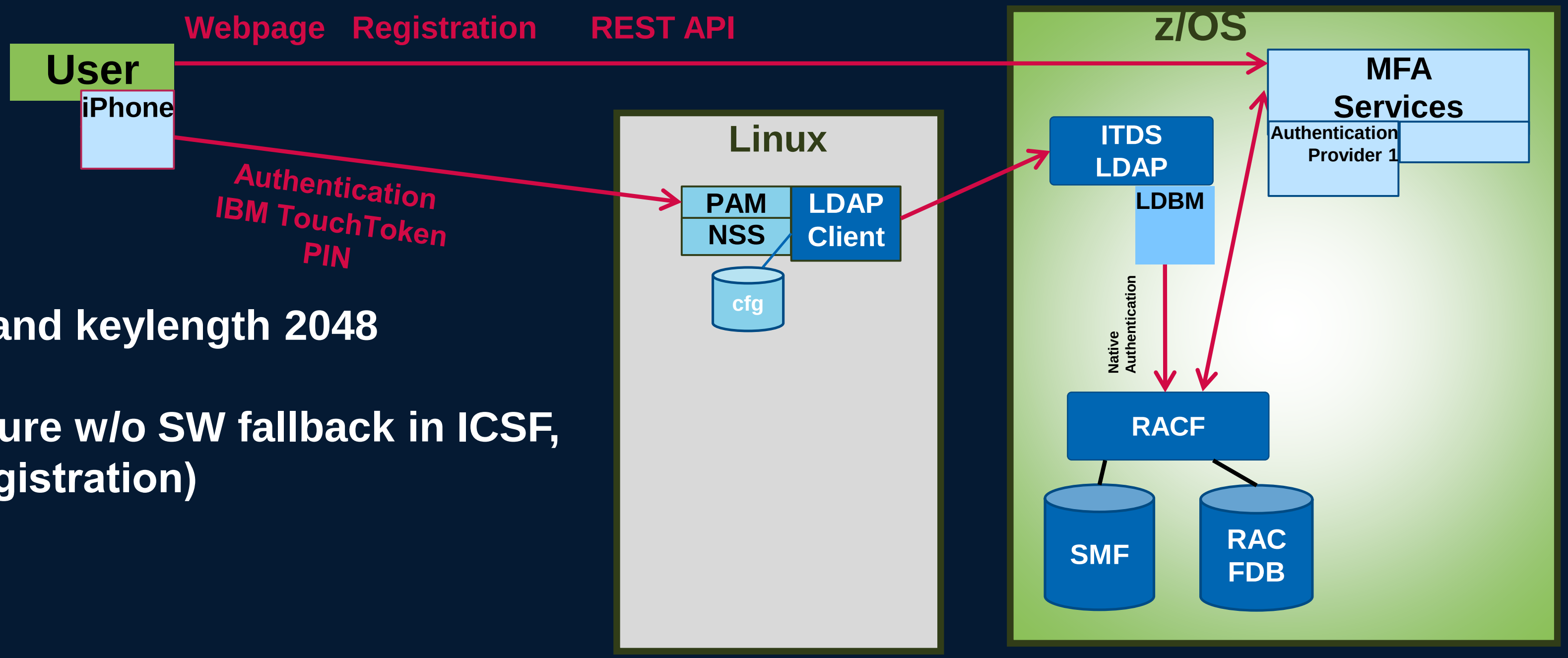
- An approach for implementation and test



- Register iOS device for IBM Touch Token
  - Download and install IBM TouchToken for iOS allplicaation form The App Store on your Apple Touch ID device
  - Use Mobile Safari to invoke URL for the IBM TouchToken registration server
  - Scan QR code with iOS camera and tap “Launch URL” link – registration begins for a new TouchToken account
  - “Begin Account Registration”
  - Enter RACF userid and password/passphrase
  - Set Token Alias screen contains user ID and touch token relm name. For security purose enter an alias (not required, but Best Practise)
  - Tap Done on Account Added screen
  - On IBM TouchToken screen tap account name you have just created
  - When prompted, enter your touch ID fingerprint
  - The application negotiates with the IBM TouchToken registration server and creates an OTP token
  - Use this OTP token to logon

Centralized MFA authentication for Linux with z/OS . . .

Centralized authentication using ITDS / RACF / MFA infrastructure of z/OS with IBM Touch Token
- An approach for implementation and test



- **Some pitfalls:**

- Webserver (SSL/TLS connection)
  - Certificates for secure connection are important
  - Need complete chain of certificates (incl. CA) with SHA256 and keylength 2048
  - May be difficulties with self-signed certificates
  - May be old/solved: For elliptic curve and activated CEX feature w/o SW fallback in ICSF, there might be SSL/TLS errors … (deactivate CEX during registration)

- iOS device
  - Easy if crypto parameters are correct.
  - In webbrowser link/launch to Webserver – in app connection for touch token registration is established.
  - Certificate on iOS device must be found in Zertifikatsvertrauenseinstellungen (Einstellungen->allgemein->info->Zertifikatsvertrauenseinstellung (CA Certificate must appear)

Summary 1

- **Linux on Z can be easily configured for using an existing z/OS MFA infrastructure.**

MFA authentication for Linux w/o z/OS services

Centralized authentication with MFA using RADIUS (using LDAP / Active Directory):

It works!

- **Example FreeRADIUS with Google Authentication PAMS**
  - **Example configuration:**

```
/etc/pam.d/radiusd

#@include common-auth

#@include common-account

#@include common-password

#@include common-session

auth requisite pam_google_authenticator.so forward_pass

auth required pam_unix.so use_first_pass
```

  - **There are also other …**

MFA authentication for Linux w/o z/OS services . . .

Some open source MFA solutions

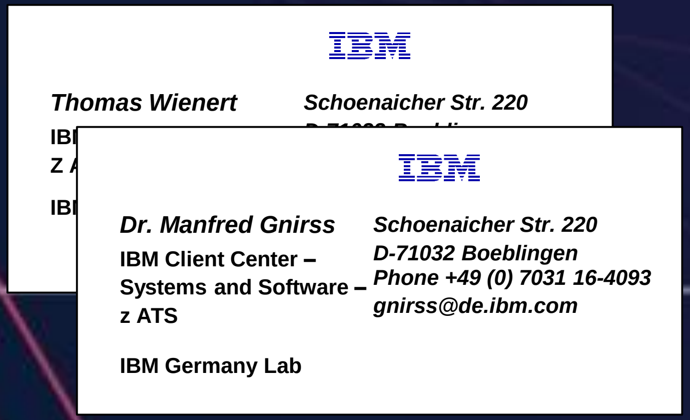
- Google Authenticator
- LinOTP
- Oath Toolkit (not to be confused with oauth or oauth2)
- OTPW
- FreeIPA
- FreeOTP
- PrivacyIDEA

Summary

- Sooner or later, MFA is mandatory
- If you have already, or if you consider to establish a z/OS MFA infrastructure, you can also use it for Linux
- Linux on Z can be easily configured for using an existing z/OS MFA infrastructure
- Linux can be configured to use MFA independent from z/OS
- You might consider to establish an enterprise wide MFA solution for (critical) users

- Consider also user management processes

Thank you



IBM

Thomas Wienert

IB

Z A

IB

Schoenaicher Str. 220

IBM

Dr. Manfred Gnirss

IBM Client Center –
Systems and Software –
z ATS

IBM Germany Lab

Schoenaicher Str. 220
D-71032 Boeblingen
Phone +49 (0) 7031 16-4093
gnirss@de.ibm.com

Misc.

- In the meantime, there is also support available for Android Smartphones (Note: not with biometric factor).

Please note

- IBM’s statements regarding its plans, directions, and intent are subject to change or withdrawal without notice and at IBM’s sole discretion.
- Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.
- The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.
- The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.
- Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user’s job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

Notices and disclaimers

- © 2018 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.
- .