IBM Multi-Factor Authentication for z/OS

John Petreshock
z Systems Security Offering Manager
jpetres@us.ibm.com

April 2016

Notices and Disclaimers

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 according to the terms and conditions of the agreements under which they are provided.

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 is in compliance with any law

Notices and Disclaimers Con't.

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 in connection with 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 PARTICULAR PURPOSE.

The provision of the information contained h erein 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, Aspera®, Bluemix, Blueworks Live, CICS, Clearcase, Cognos®, DOORS®, Emptoris®, Enterprise Document Management System™, FASP®, FileNet®, Global Business Services ®, Global Technology Services ®, IBM ExperienceOne™, IBM SmartCloud®, IBM Social Business®, Information on Demand, ILOG, Maximo®, MQIntegrator®, MQSeries®, Netcool®, OMEGAMON, OpenPower, PureAnalytics™, PureApplication®, pureCluster™, PureCoverage®, PureData®, PureExperience®, PureFlex®, pureQuery®, pureScale®, PureSystems®, QRadar®, Rational®, Rhapsody®, Smarter Commerce®, SoDA, SPSS, Sterling Commerce®, StoredIQ, Tealeaf®, Tivoli®, Trusteer®, Unica®, urban{code}®, Watson, WebSphere®, Worklight®, X-Force® and System z® Z/OS, 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.

Multi-factor Authentication

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

- Authentication Factors:
  - Something you know
    - A password / PIN Code
  - Something you have
    - ID badge or a cryptographic key
  - Something you are
    - Fingerprint or other biometric data

- Today on z/OS, users can authentication with:
  - Passwords, Password phrases, PassTickets, Digital Certificates, or via Kerberos

- Today's problem:
  - 2014 Verizon Data Breach Investigations Report said 2 out of 3 breaches involved attackers using stolen or misused credentials.
  - In the case of an attempted breach using comprised credentials, the extra protection that MFA provides can make the difference between having a secured vs. compromised system.
  - Breaches impact clients financially, their customers, and their reputations

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 and applications / hosting environments by extending RACF to authenticate individual users:
- Support for third-party authentication systems
  - RSA® Ready supporting RSA® SecurID® Tokens (hardware & software based)
  - Direction to support the IBM TouchToken – Timed One time use Password (TOTP) generator token
  - Direction to support PIV/CAC cards - Commonly used to authenticate in the Public Sector enterprises
- Tightly integrated with SAF & RACF
  - RACF provides the configuration point to describe multi-factor authentication requirements down to a per User ID basis
  - Deep RACF integration for configuration and provisioning data stored in RACF database allowing seamless back-up and recovery

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

Achieve regulatory compliance, reduce risk to critical applications and data

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

Typical Client Use Cases:

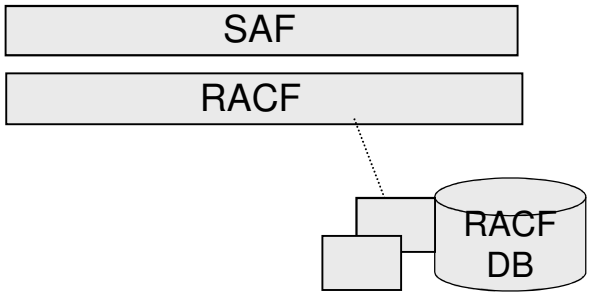
- **Enable higher-security user logins** on IBM z/OS systems that use RACF for security
- Enable strong authentication for employees that carry **iOS devices** or **RSA SecurID** tokens

RACF & MFA Services and Related Support

- RACF 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
    - Definition of authentication token types
  - Extensions to SAF programming interfaces
    - Provides new SAF services for z/OS MFA Services allowing the access to MFA data stored in the RACF database.
  - Auditing extensions
    - Tracks which factors 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
      - Related to the tokens used on a specific authentication event
- z/OS MFA Services started task
  - z/OS MFA address space which tracks state for user authentication events
  - Provides an anchor for communications for factors such as RSA SecurID

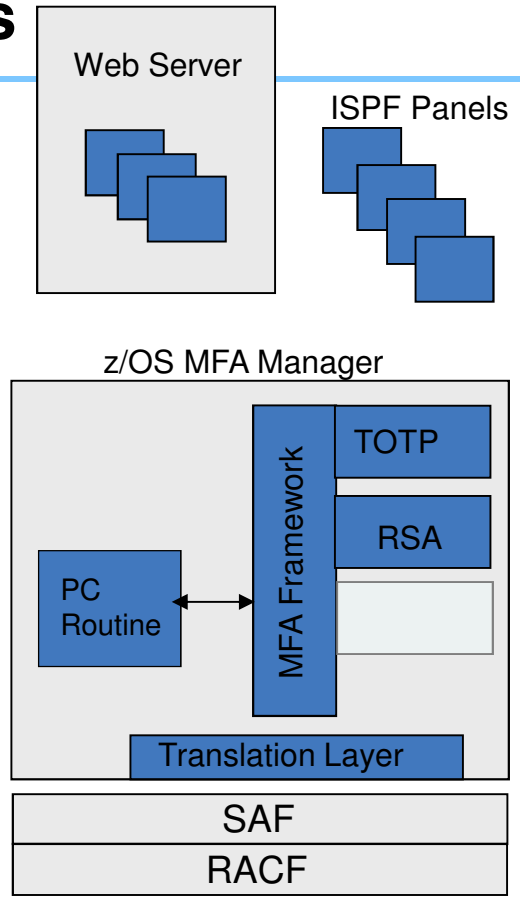
Base RACF Support for MFA Services

- RACF Database extensions
  - Store MFA information in RACF:
    - New MFA fields in the User profile
    - New MFA segment and General Resource profile class
- RACF Commands
  - Administration of MFA information in RACF
    - ALTUSER & RDEFINE / RALTER & RLIST
- RACF Logon processing
  - New MFA processing:
    - RACINIT SVC -- Calls MFA Manger during authentication processing to evaluate authentication factors
    - VLF Updates – Use MFA data in VLF object for fast ACEE access for MFA users
    - INIT_ACEE – Update ACEE cache
- SAF/RACF Database API
  Programmatic Access to RACF MFA data from the MFA Services started task:
  R_FACTOR – Access & update MFA data in RACF profiles
- Utilities
  - Support for new MFA segment data:
    - DBUNLOAD -- Report on MFA data
    - IRRADU00 – RACF SMF Unload

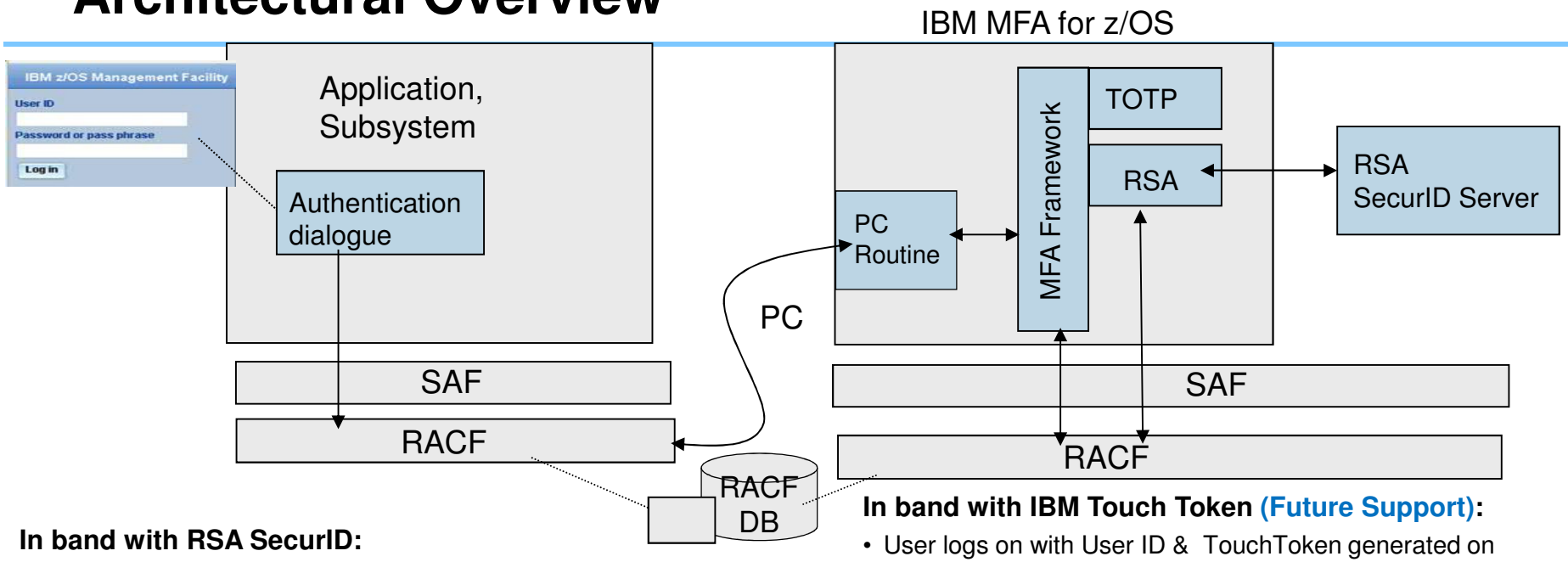


z/OS MFA Services Manager -- Components

- MFA Manager Web Interface
  - User Interface – supports factors such as smartphone apps and serves webpages 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 Data base access APIs



Architectural Overview



In band with RSA SecurID:

- User logs on with User ID & RSA SecurID Token and PIN
- RACF determines if the user is an MFA user & calls the MFA Services
- MFA Services calls RACF to retrieve user's MFA factor details
- MFA Server validates the users authentication factors and calls RSA Server
- RACF uses MFA Services status to allow or deny the logon

In band with IBM Touch Token (Future Support):

- User logs on with User ID & TouchToken generated on provisioned iOS device
- RACF Determines if the user is an MFA user & calls MFA Services
- MFA Server calls RACF to retrieve user's MFA factor details
- MFA Server validates the users authentication factors in this case the IBM TouchToken code
- RACF uses MFA Services status to allow or deny the logon

Authentication Factor Data Stored in RACF Profiles

- The RACF database will serve as the data repository for MFA data.
- MFA data will be accessed via RACF commands and via a SAF/RACF callable service.
- MFA User Specific Data contains general MFA user policy information and factor specific data for the user.
- Authentication Factor Definition
  - Defines an authentication factor and contains factor configuration – used by MFA Services
    - New RACF general resource class: **`MFADEF`**
    - Profile naming conventions: **`FACTOR.<factorName>`**

MFA RACF User Profile Management

- MFA Factor fields is stored in the RACF user profile
- Defined by a RACF Administrator via ALTUSER command

  - Example ALTUSER Syntax:

```
[ MFA(
        [ PWFALLBACK | NOPWFALLBACK ]
        [ FACTOR(factor-name) | DELFACTOR(factor-name) ]
        [ ACTIVE | NOACTIVE ]
        [ TAGS(tag-name:value …) ]
           | DELTAGS(tag-name … )
           | NOTAGS ]
)
| NOMFA ]
```

- RACF will call the MFA Services Task to validate the factor specific information that is specified on the ALTUSER command TAGS keyword
  - If a syntax error or unknown name value pair is supplied MFA Services will reflect an error to RACF
    - RACF issues a message and a MFA Services provided message which indicates the nature of the syntax error

Sample LISTUSER Output

```
ALTUSER JOEUSER MFA(PWFALLBACK(Y))
ALTUSER JOEUSER MFA(FACTOR(RSASecurID) TAGS(SIDUSERID:RSAJOE))
LISTUSER joeuser MFA
...

MULTIFACTOR AUTHENTICATION INFORMATION:
---------------------------------------
  PASSWORD FALLBACK IS ALLOWED
  FACTOR = RSASECURID
    STATUS = ACTIVE
    FACTOR TAGS =
      SIDUSERID:RSAJOE
```

z/OS MFA Services Started Task

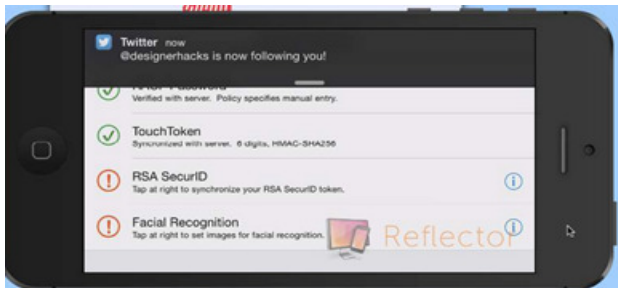
- The MFA Services started task contains the main logic supporting main flows:
  - MFA User Registration
  - MFA User Logon – factor evaluation

- MFA services will perform the following actions:
  - Get / set of data within RACF database used for user authentication
    - Logon policy data
    - Plugin data
    - Specific MFA field data (timeouts and such)
    - MFA metadata
  - Determination of whether or not a user has satisfied the MFA policy.
    - Called by SAF RACROUTE REQUEST=VERIFY or initACEE during logon processing
  - Update last-access and revoke count at each user factor attempt
- MFA Services is the focal point for evaluating the factor data while RACF is used to manage and maintain the factor data as set by the Security Administrator

Planned Initial MFA Authentication Factors

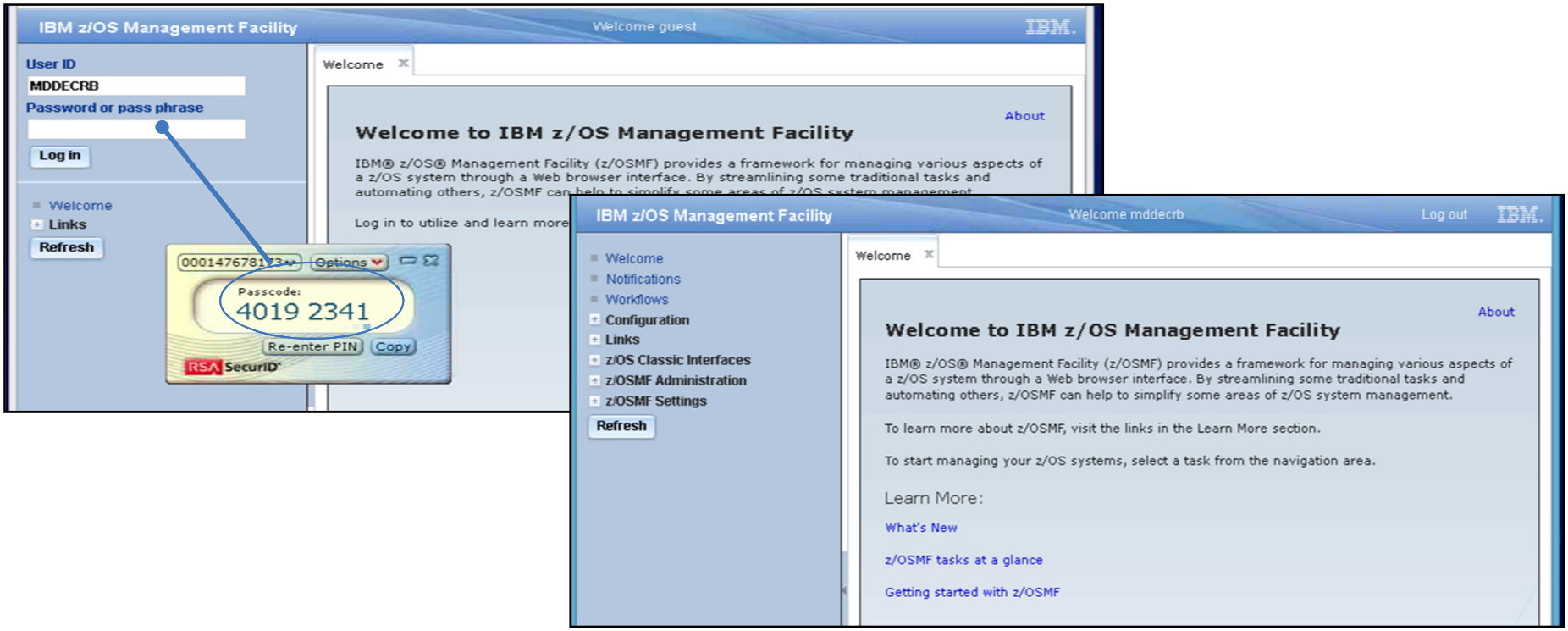
- RSA SecurID Tokens
  - Requires RSA SecurID server configured to the MFA Server
  - Since in the case of RSA SecurID requires an external configured server instance – this could represent a point of failure.
  - Supports both hard and soft RSA SecurID tokens

- IBM TouchToken – Timed One Time use Password generator token – Post GA deliverable
  - Authentication factor that can be directly evaluated on z/OS
    - Helps to ensure that there is always a means of enforcing two factor authentication for users
  - Provisioned with a shared secret key into the iOS key ring from z/OS



Sample Logon Interaction with z/OSMF
Using Soft RSA SecurID Tokens

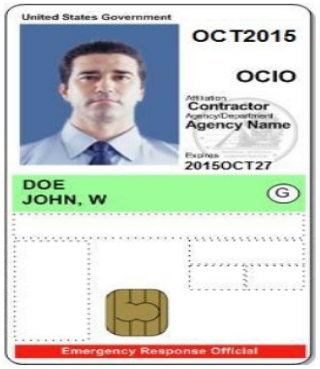
- User enters their User ID and token generated code in the password field.
  - The User's pin is not entered during logon processing

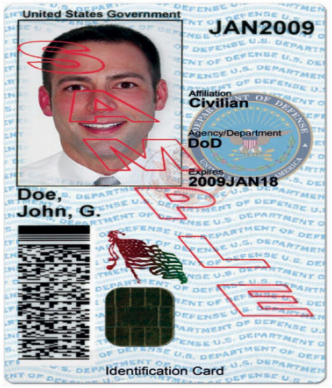


Statement of Direction for MFA Additional Authentication Factors

PIV/CAC

- A personal identity verification (*PIV*) or Common Access Card (CAC) is a United States Federal Government smart card
- Contains the necessary data for the cardholder to be granted to Federal facilities and information systems
- They are standard identification for active duty uniformed service personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel.





zSecure Support

- Support is intended to simplify administration by helping to enforce authentication policy, providing alert notifications, and reporting on authentication audit events and compliance.

More Information and Links

- z Systems - http://www-03.ibm.com/systems/z/
- z13s Announce - http://www-03.ibm.com/systems/z/hardware/z13s.html
- z/OS - http://www-03.ibm.com/systems/z/os/zos/
- IBM Enterprise Security -

  http://www-03.ibm.com/systems/z/solutions/enterprise-security.html
- Techdocs: http://www-03.ibm.com/support/techdocs/atsmastr.nsf/Web/TechDocs

  –Keywords: Crypto, TKE, ICSF
- Redbooks - http://www.redbooks.ibm.com/

16

Thank You