Announce: 10/10
GA: 12/15

Enhancing Security with PowerSC Multi-Factor Authentication

Petra Bührer
Offering Manager Power Systems Software
Petra.Buehrer@de.ibm.com

October 2017

Security & Compliance – Some Facts

University of California Santa Cruz found that

- **fines of up to $500,000 per incident for security breaches when merchants are not PCI compliant**

Ponemon Institute research found in 2017 that

- **$3.62 million is the average total cost of data breach**
- **$141 is the average cost per lost or stolen records**
- **It takes companies an average of 191 days to find out about a breach**, extending the window of opportunity during which attackers covertly reside in the breached systems and harvest more data!
- **It takes an average of 66 days to contain the data breach**

➢ **The faster the data breach can be identified and contained, the lower the costs**

UCSC - Financial affairs
https://financial.ucsc.edu/pages/security_penalties.aspx#non

2017 Ponemon Cost of Data Breach Study:
https://www.ibm.com/security/data-breach/

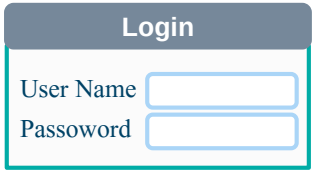
Multi-Factor Authentication - Background

What is Multi-Factor Authentication?

At least two different of the following categories are used to confirm separate pieces of evidences in order to grant access to a system.

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



Why Not just Use Passwords?

- Passwords are not handled securely by password owners
  - Written down
  - Shared
- Passwords can be brute-forced or guessed
- Good passwords are hard to remember
- Need for enhanced certainty by regulation that person performing a task is actually that person

Why is MFA important now?

Financial and Retail Industries

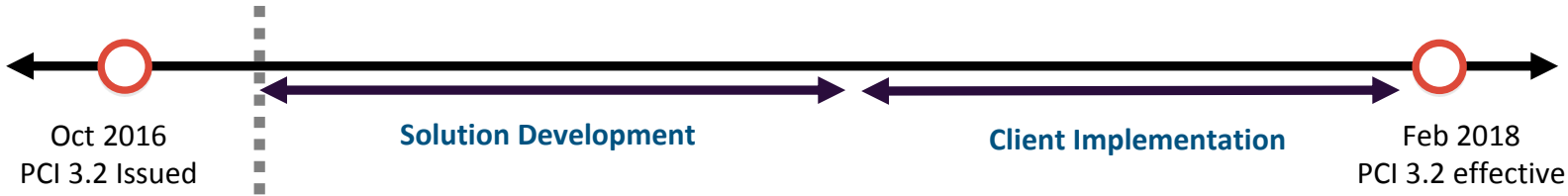
– PCI-DSS (Payment Card Industry Data Security Standard) has released version 3.2, officially replacing version 3.1 on October 31,2016

– PCI 3.2 Section 8.3 requires multi-factor authentication for any personnel with admin access to environments handling card data, whereas previously it was only for remote access from untrusted networks.

– This requirement becomes effective February 1, 2018

Federal

– US Defense is issuing confidential STIG requirements related to MFA, to be implemented by this year. Requires LOA4 (PIV/CAC)



MFA Options

Multi-factor authentication can be performed

- Upon entry to the CDE (Cardholder Data Environment) network
- Or to every CDE component throughout your network
  - Anywhere card data is stored, transmitted or viewed
  - For root, RBAC admins, SU, SUDO, DBAs, web admins, application admins, …

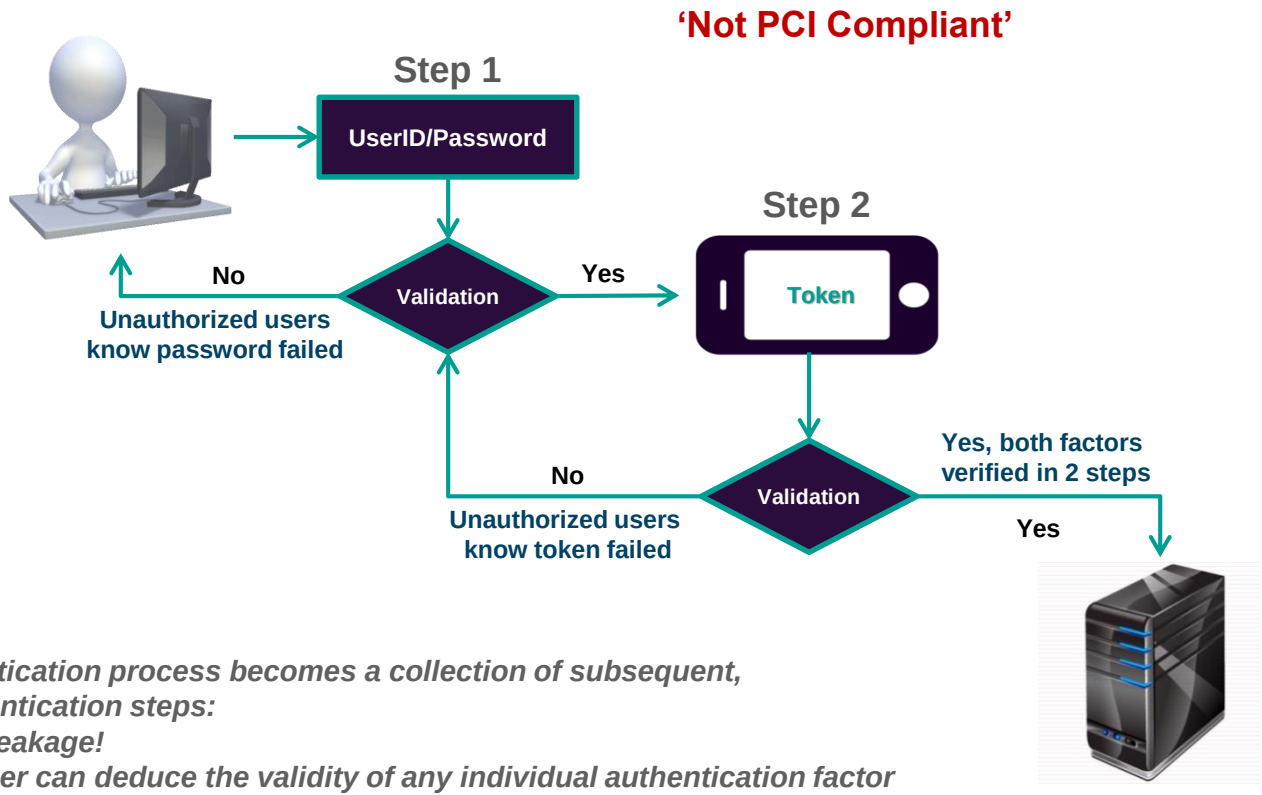
- Examples of CDE components, requiring MFA, include
  - Servers, Firewall, Routers, Switches, Hypervisors, SAN, Tape, Console access, …
  - For Servers, this means every client/server interface needs to support MFA

MFA, 2FA and Multi-Step Authentication

- **Multi-factor authentication** - method of computer access control in which a user is granted access only after successfully presenting **several separate pieces of evidence** to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are).
- **Two-factor authentication** - (also known as 2FA) is a method of confirming a user's claimed identity by utilizing **a combination of two different components**. Two-factor authentication is a type of multi-factor authentication.

- **Multi-Step Authentication** - **collection of subsequent, single-factor authentication steps**, such as the submission of credentials (e.g., username/password) that, once successfully validated, lead to the presentation of a second factor for validation (e.g., biometric or token).

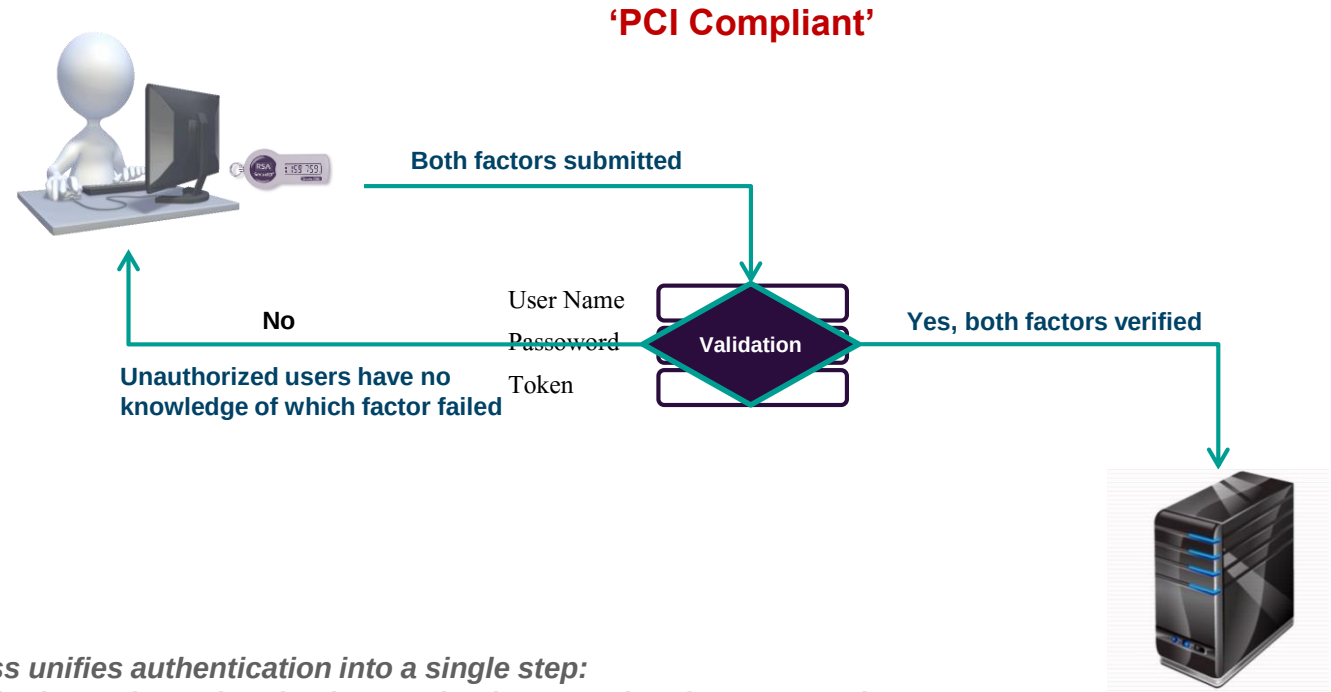
Example of Multi-Step Authentication



The overall authentication process becomes a collection of subsequent, single-factor authentication steps:

- *Potential Data Leakage!*
  Unauthorized user can deduce the validity of any individual authentication factor

Example of Multi-Factor Authentication



The overall process unifies authentication into a single step:
All factors verified prior to the authentication mechanism granting the requested access.

- *No Data Leakage!*
  No prior knowledge of the success or failure of any single factor provided.

IBM PowerSC MFA

What are important points to be considered?

Authentication Method

Level of Assurance	Example
LOA-1	Username/ Password
LOA-2	One Time Password
LOA-3	RSA w/PIN, Biometrics
LOA-4	PIV/CAC

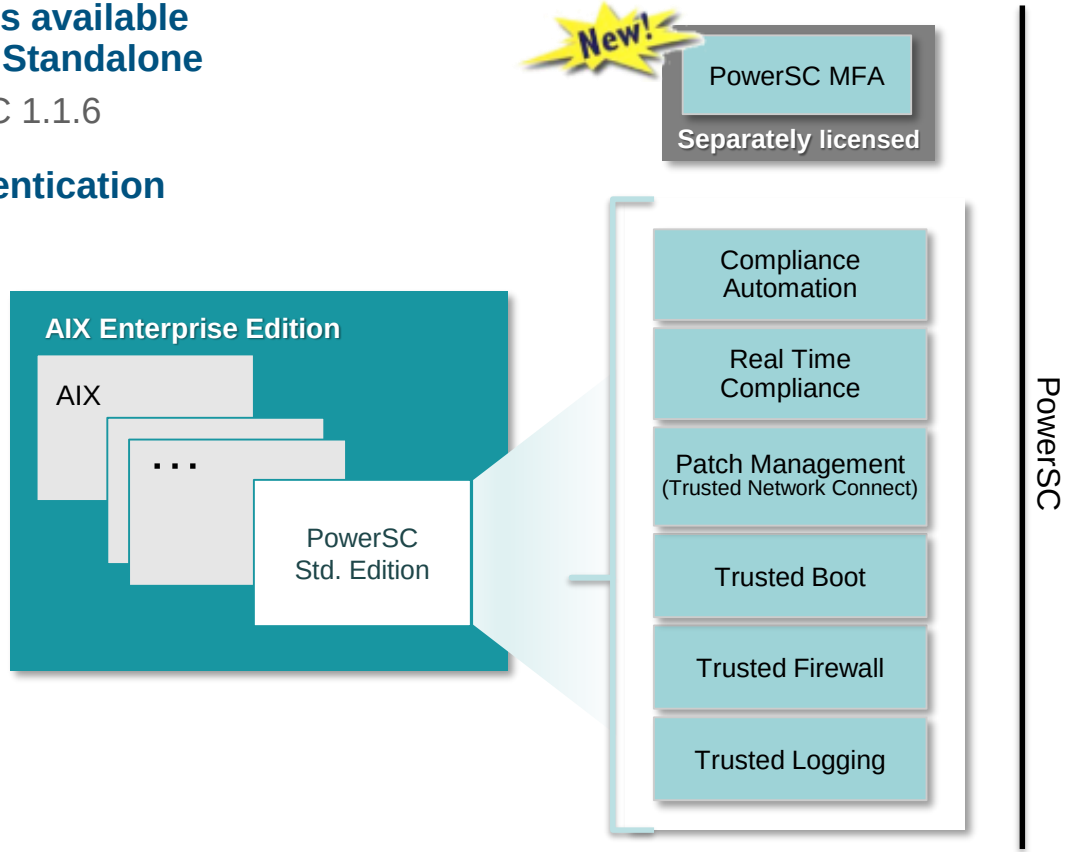
Infrastructure Requirements

- Native
- Appliance (Virtual or Physical)
- SaaS

Native on Power providing LOA-4

PowerSC Packaging

- **PowerSC Standard Edition is available in AIX Enterprise Edition or Standalone**
  - Current version is PowerSC 1.1.6
- **PowerSC Multi-Factor Authentication will be available standalone**
  - First version will be PowerSC MFA 1.1.0



PowerSC MFA - Solution Concepts

- **Factor**
  - An authentication technology – generally sourced from something you know, something you have, or something you are
- **Policy**
  - Rules that govern which factor credentials must be supplied for an authentication and define the lifetime of the generated Cache Token Credentials and their re-usability
  - Philosophy of policy-driven MFA
- **Cache Token Credential (CTC)**
  - An 16-character credential returned after a successful Out-of-band authentication

PowerSC MFA - Factors

- **RSA SecurID**
  - Prereq: RSA Authentication Manager v8.1 or later
  - Prereq: Active RSA SecurID Tokens for MFA Users

- **PIN-protected certificates on PIV/CAC smart cards**
  - Prereq: Current PIV/CAC cards derived from a CA that is accessible from client and TLS configuration

PowerSC MFA - Options

- **In-band Authentication via PAM**
  - An authentication mechanism where MFA credentials are supplied through the same channel/stream being used to access the target service – e.g. ssh login process

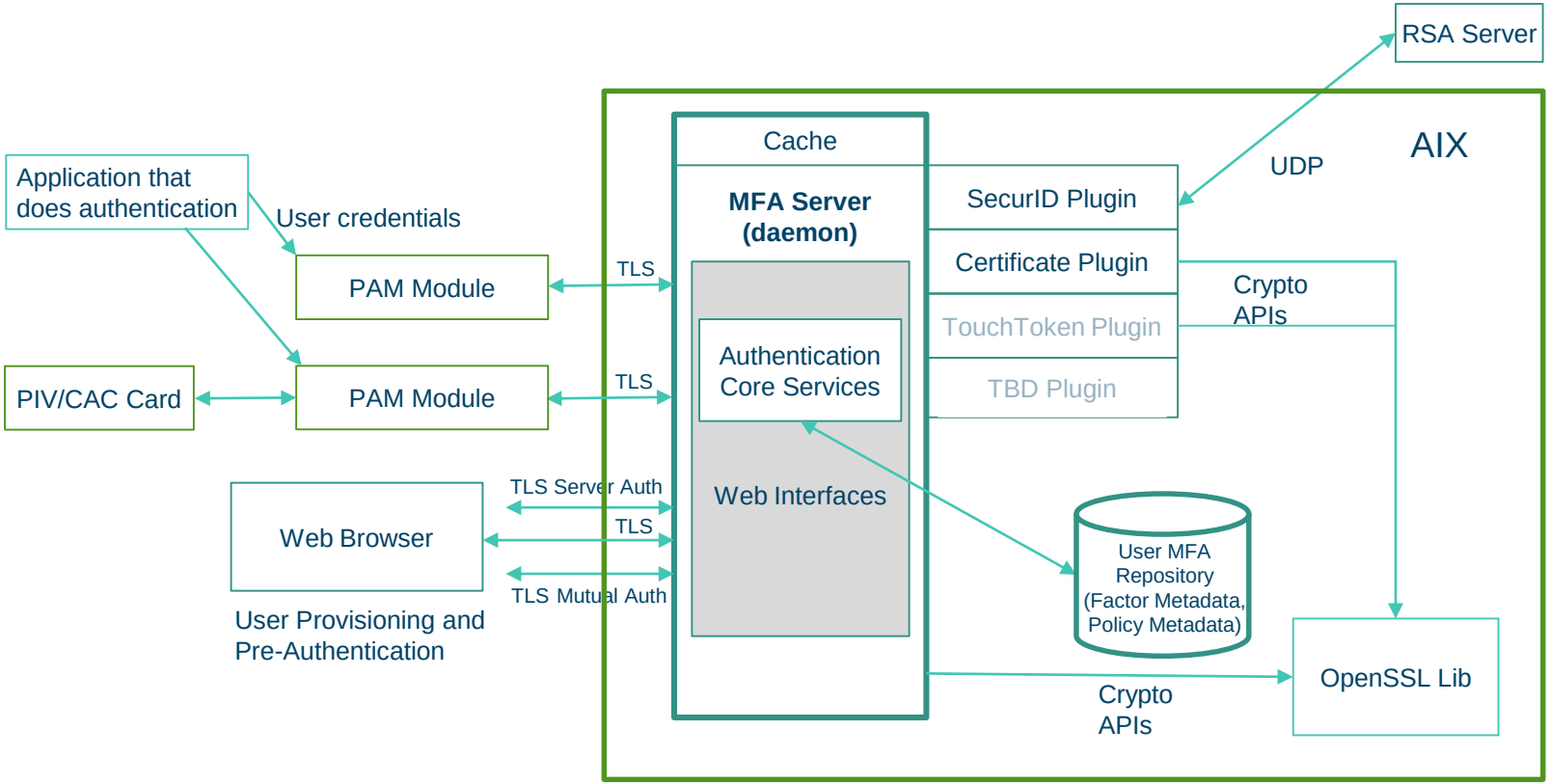
- **Out-of-band Authentication (Pre-Authentication)**
  - An authentication mechanism where MFA credentials are supplied on a web form according to a selected policy where after a successful authentication a Cache Token Credential (CTC) is obtained which is then used to authenticate to an application

PowerSC MFA - Features

- Multiple concurrent logins
- Fast path for subsequent AIX logins
- All Client-server communication encrypted; TCP/IP with TLS
- Centrally administer different factors for different user populations

PowerSC MFA - Architecture

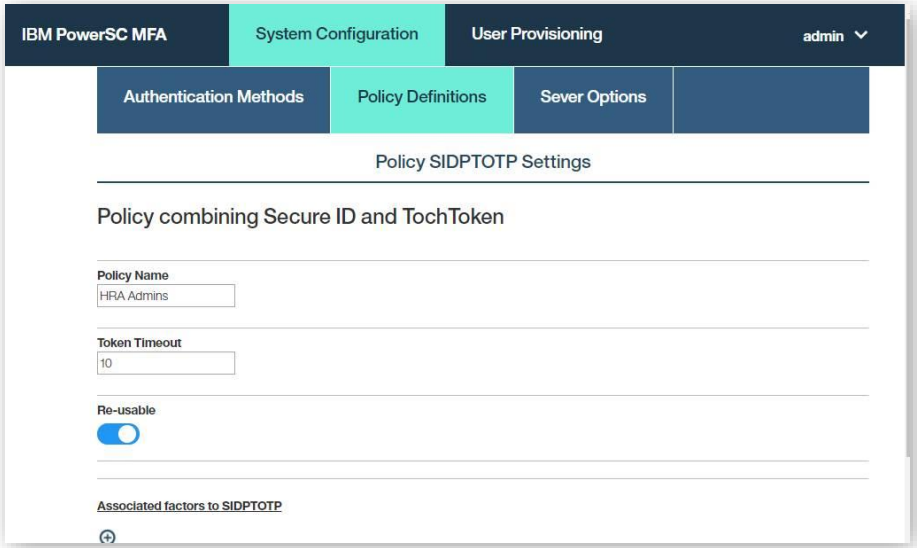
PowerSC MFA - Architecture



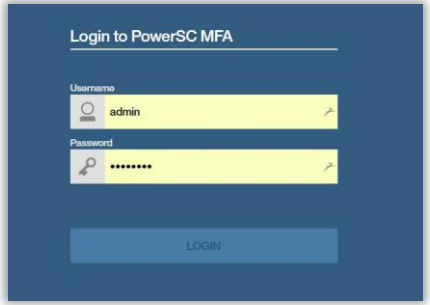
PowerSC MFA - GUIs

PowerSC MFA - Administrative GUI

- System Configuration
  - e.g. port specs, trace levels, enabling/disabling factors,…
- Policies
  - One or more factors and token settings
- Factors
  - Authentication mechanisms
- Users
  - Bulk Provisioning / Ingest
  - Groups - e.g. geographic, corporate departments, functions,…



PowerSC MFA - Operational GUI
Logging On with a Cache Token Credential (CTC)



1. User navigates to MFA Web Services site by entering https://host:port/mfa in URL field of the browser
   - Note: If server certificate not derived from a well-known Certificate Authority root certificate, the Root certificate must be installed as trusted root certificate in user's browser
2. User enters User ID and Password and clicks the Login button
3. If the credentials are valid, the user is provisioned for MFA, and has one or more satisfiable policies THEN → MFA Web Services returns a page with a list of the valid policies (normally just one)
4. User selects policy to use and enters factor credential data, one factor at a time
5. When all factors are satisfied, system displays an 16-character CTC
6. User enters (copy/paste) CTC in Password field of application authentication dialog
7. Policy governs lifetime and reusability of CTC

Reference Links

- **Check out the PowerSC WebSite**
  - *https://www-03.ibm.com/systems/power/software/security/*
- **Review the new IBM PowerSC MFA Datasheet**
  - *https://www.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=POD03139USEN&*
- **Visit the IBM Knowledge Center for information about how to install, maintain, and use IBM PowerSC MFA**
  - **PowerSC MFA 1.1.0** (link to be added as soon as available)

Legal Notices

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements and/or changes in the product(s) and/or program(s) described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. 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. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectually property rights, may be used instead.

THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER OR IMPLIED. IBM LY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (e.g., IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. 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. IBM makes no representations or warranties, end or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 1 0504- 785
U.S.A.