DB2 on System z: Meet the 12 requirements of PCI DSS compliance

Jim Pickel, STSM
DB2 for z/OS Security Architect
pickel@us.ibm.com

Disclaimer Statement

- ***The information on new product is intended to outline our general product direction and it should not be relied on in making a purchasing decision.***

- ***The information on new product is for informational purposes only and may not be incorporated into any contract. The information on the new product is not a commitment, promise, or legal obligation to deliver any material, code or functionality.***

- ***The development, release, and timing of any features or functionality described for IBM products remains at IBM's sole discretion.***

- ***It is the customer's responsibility to identify, interpret and comply with any laws or regulatory requirements that affect its business. IBM does not represent that its products or services will ensure that the customer is in compliance with the law.***

Assessing Your Data Compliance

- The Payment Card Industry Data Security Standard (PCI DSS) developed 12 requirements for securing cardholder data that is stored, processed and transmitted by merchants and other organizations
- Review these requirements as they pertain to protecting cardholder data residing in DB2 on System z
- Provide best practices in your pursuit for compliance when storing cardholder data in DB2 9 for z/OS

COMPLIANCE IS A CONTINUOUS PROCESS

PCI DSS Compliance – like most Security Initiatives is about:

- You, Your Processes, and Strong Technology

DB2 can be a PCI DSS compliant data hub

DB2 leverages mainframe policies and processes that have been developed over many years in your enterprise

z/OS and System Z provide the strongest encryption, authentication, access controls, and auditing features in the industry

PCI DSS Requirements "The Digital Dozen"

Build and Maintain a Secure Network	
1.	Install and maintain a firewall configuration to protect cardholder data
2.	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	
3.	Protect stored cardholder data
4.	Encrypt transmission of cardholder data sent across open, public networks
Maintain a Vulnerability Management Program	
5.	Use and regularly update anti-virus software
6.	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	
7.	Restrict access to cardholder data by business need-to-know
8.	Assign a unique ID to each person with computer access
9.	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	
10.	Track and monitor all access to network resources and cardholder data
11.	Regularly test security systems and processes
Maintain an Information Security Policy	
12.	Maintain a policy that addresses information security – Connected Entities and Contracts

Requirement 1: Install and maintain a firewall to protect cardholder data

RACF protects all user access to DB2

RACF authenticates all users and prevents unauthorized access from specific security zones

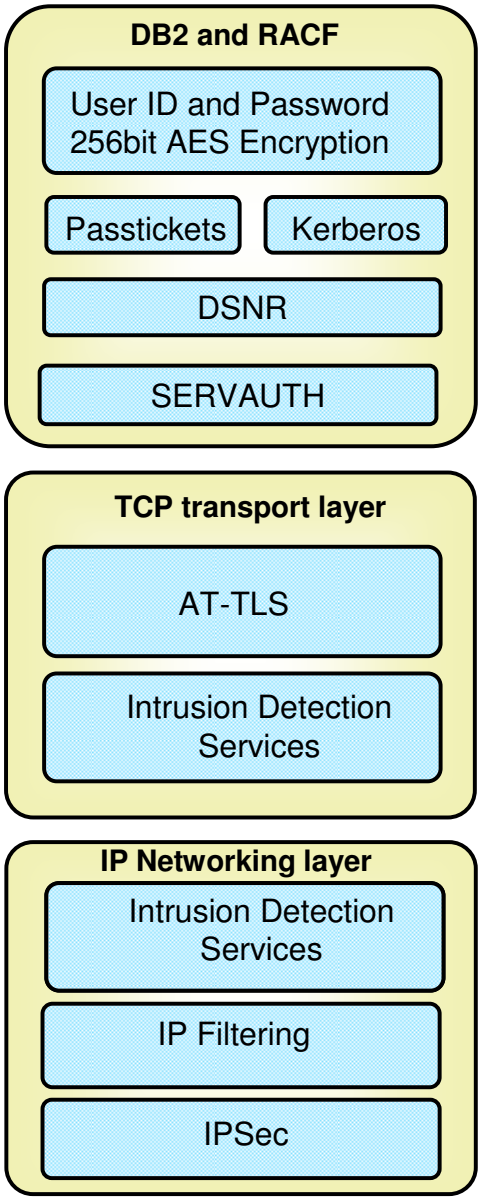
Communications Server creates a protective zone around DB2

Application Transparent -TLS is transparent to DB2

IDS protection is provided in two layers

IP packet filtering blocks out all IP traffic that the DB2 server doesn't specifically permit.

IPSec is transparent to upper-layer protocols



Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

- Utilize RACF best practices to secure your system's passwords, data, and system
  - Allows centralized administration, authentication, authorization, and auditing for all access to DB2 data
  - RACF only detects failures, auditing is still needed to verify your security policies are adhered
- Utilize IBM Health Checker recommendations to improve your system configuration
- Protect from malicious users and internal administrators
  - Protect external threats by restricting data access from end users
    - Can use package authorization to restrict data access from users
    - Can use Trusted Context to restrict data access to secure applications only
  - Protect internal threats by separating security tasks from database tasks
    - Can use RACF access control to separate security tasks
    - Can use Trusted Context to control use of authorities and implicit privileges

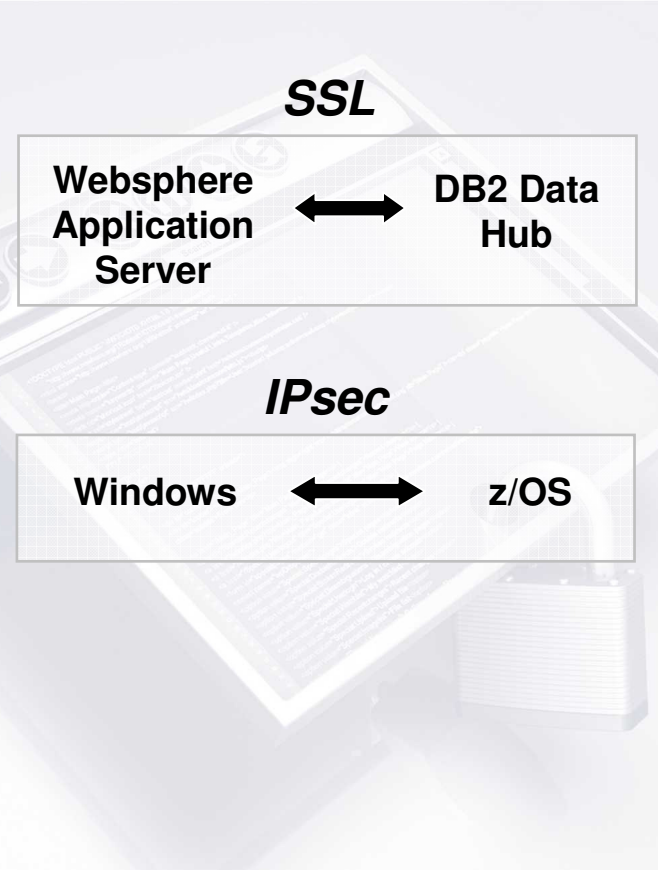
Requirement 3: Protect stored cardholder data (1 of 2)

- **Protection methods such as truncation, masking, and hashing are critical components**
  - Separate cardholder data and process using masked cardholder values
  - Use z/OS ICSF or Optim PCI Module's Payment Card masking functions to obscure cardholder data in DB2
  - Minimizes cardholder data from being exposed in DB2 indexes, DB2 logs, and DB2 traces

Requirement 3: Protect stored cardholder data (2 of 2)

- **Protection methods such as encryption are critical components**
  - Can use IBM Data Encryption for IMS and DB2 Tool
    - Protect cardholder data from intruder gaining access to datasets containing cardholder data making it unreadable
    - Cardholder data in indexes are not protected
    - Separate from the native operating systems mechanisms
  - Best practice is to use IBM Tape Encryption Solutions
    - Protects logs and traces containing cardholder data
    - Separate from the native operating systems mechanisms
  - Best practice is to use IBM Disk Encryption Solutions
    - Renders cardholder data unreadable when a disk is removed
    - Separate from the native operating systems mechanisms

Requirement 4: Encrypt transmission of cardholder data across open and public networks



- **Can use Application-based encryption**
  using SSL and Transport Layer Security
  - DB2 9 server added explicit AT-TLS support
  - All DB2 9 drivers exploit SSL encryption
  - Encryption acceleration in the System z server
- **Can use End-to-end network encryption**
  using IP security
  - Can create a secure tunnel for selected network traffic (Virtual Private Network)
  - Enabled without application changes
  - More compelling on System z with zIIP support

Simpler and consistent configuration with

Configuration Assistant for z/OS Communications Server

Requirement 5: Use and regularly update anti-viruses software and programs

- **Built-in protection**
  - Enforced Isolation
    - Separate address space
    - Supervisor state & system programs protection
  - Authorized Program Facility (APF)
    - Executables only accessible to authorized users
    - Identifies programs that use system functions
  - Storage Protection Keys
    - Controls access to protected storage
    - Cross memory services prevent unauthorized data access

Ensures business approved activities are protected from current and evolving malicious software threads

Can help prevent intrusion from malware, viruses and worms

Proven over 40 years of secured operations!

Requirement 6: Develop and maintain secure systems (1 of 3)

- **Ensure all system components and software have latest vendor-supplied security patches installed**
  - SMP/E manages the installation of software products and components on z/OS
  - SMP/E tracks all modifications you make to your system and software
  - All z/OS and DB2 security patches are identified as an security APAR
- **Establish a process to identify newly discovered security vulnerabilities**
  - DB2 and z/OS will investigate, accept, and resolve, any security exposures as a high-severity problem
  - Security fixes are always noted in the APAR and fixing PTF
- **Develop software based on industry best practices and incorporate information security throughout the software development life cycle**
  - DB2 and z/OS Common Criteria certifications are proof points in addressing IBM practices of incorporating security throughout the development life cycle

Requirement 6: Develop and maintain secure systems (2 of 3)

- DB2 is designed from top to bottom to help protect your system, data, transactions, and applications from accidental or malicious modification
- DB2 is committed to prevent unauthorized application programs and users from gaining access, circumventing, disabling, altering, or obtaining access to data under DB2 control unless allowed by the installation
- IBM will always take action to resolve if a case is found where the above can be circumvented

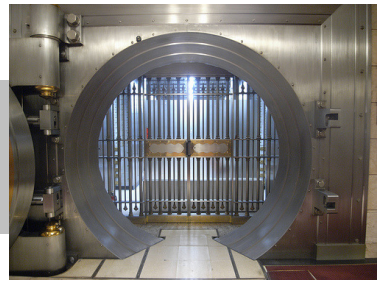
DB2 and z/OS integrity statement and the Common Criteria certifications can be helpful proof points in addressing compliance requirements.

ibm.com/servers/eserver/zseries/zos/racf/zos_integrity_statement.html

Requirement 6: Develop and maintain secure applications (3 of 3)

- **SQL Injection is most common vulnerability to cardholder data**
  - Use static SQL when accessing any cardholder data
  - SQL injection happens because the database cannot effectively distinguish between static portion of the SQL statement and the user input
  - If there is a way you can tell the database - this is static SQL statement and this is user input, SQL injection could be stopped

Last year, SQL injection jumped 134 percent and replaced cross-site scripting as the predominant type of Web application vulnerability.



Requirement 6: Separate test and development environments

- The IBM Optim Data Privacy Solution provides a comprehensive set of data masking techniques that can be used to de-identify cardholder data
  - Masked data are in the appropriate context and respect the application logic
  - Test data management capabilities provide an efficient and compliant alternative to database cloning, allowing you to create development and testing environments that are sized appropriately

Requirement 7: Restrict Access to cardholder data by business need to know

- Restrict access to privileged user IDs to least privileges
  - Granular access controls can be established using DB2 authorities and privileges
- Assign privileges based on individual job classification and function
  - Can use RACF groups or DB2 roles to assign privileges or authorities to individual job responsibilities
- Establish access control system based on user's need to know
  - Can use Trusted context to prevent user from accessing cardholder data outside applications that contain your company security policies
  - Can use MLS security labels to provide mandatory access control to tables with cardholder data

Requirement 8: Assign a unique ID to each person with computer access

- **Assign a unique ID before allowing access**
  - All access requires an authenticated RACF User ID
  - Can use client info APIs to provide end user ID
  - Best practices is to use trusted context to propagate end user ID
- **Authenticate using strong password**
  - Kerberos authentication
  - Mixed-case passwords support
  - Password phrases (coming soon)
- **Incorporate two-factor authentication**
  - Best practice is to use authenticate using a password and a digital certificate

Requirement 8: Assign a unique ID to each person with computer access

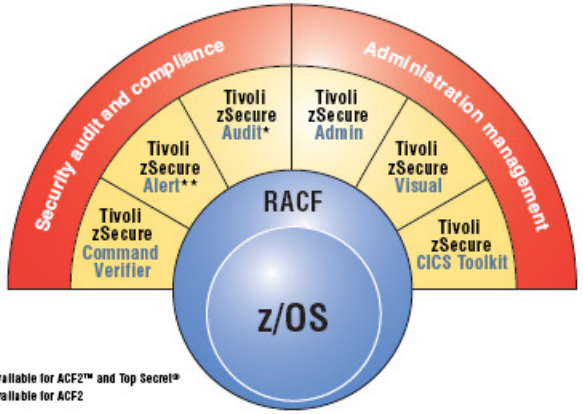
PCI DSS Requirements	RACF enforced	DB2 enforced
Render all passwords unreadable during transmission and storage using strong cryptography	RACF encrypts passwords stored in RACF database using one-way encryption protected by z/OS	Can use 256 bit AES encryption (default in 9) to obscure user ID and password during transmission
Control addition, deletion, modification of user IDs	RACF enforced –manages all DB2 IDs	
Require first-time passwords to be change on first use	RACF enforced – ADDUSER (PASSWORD) is always expired	
Immediately revoke access from terminated users	RACF enforced - DELUSER prevents user connecting to DB2	
Disable inactive user IDs every 90 days	RACF enforced - SETROPTS INACTIVE(90)	
Require user passwords to be changed every 90 days	RACF enforced - SETROPTS PASSWORD(INTERVAL(90))	
Require minimum password length to at least 7 characters	RACF enforced - SETROPTS PASSWORD(RULE1(LENGTH(7))	
Require passwords to contain numeric and alphabetic characters	RACF enforced - PASSWORD (RULE1 MIXEDNUM(1:8))	
Limit repeated access attempts after more than six attempts	RACF enforced - SETROPTS PASSWORD(REVOKE(6))	
Force a new logon after connection is idle for more than 15 minutes		DB2 enforced - IDLE THREAD TIMEOUT(IDTHTOIN) subsystem parameter and abend s0522
Require user ID authentication for any access to any object containing cardholder data		DB2 enforced – An authenticated user ID is always associated with a DB2 process

Requirement 9: Destroy media containing card data when no longer needed

- IBM tape encryption encrypts the data at near native tape drive speeds on the tape device itself after compressing the data
- In February 2009, IBM delivered full disk encryption which provides seamless data encryption of all data at rest within the DS8000, without requiring any external or internal appliance or impacting performance
- Renders cardholder data unreadable when a disk or tape is removed

Requirement 10: Regularly Monitor and Test Networks (1 of 2)

- DB2 Audit Management Expert
  - Collects and correlates information from DB2 resources
  - Processes audit trace data
  - Drill down possible breaches using detailed log analysis
- Tivoli zSecure Suite
  - Security Management and Administration for z/OS and RACF
- IBM Tivoli OMEGAMON XE for DB2 Performance Expert
  - Authorization exception event reporting



Requirement 10: Regularly Monitor and Test Networks (2 of 2)

- Retain your audit trail history and logs for a period that is consistent with its effective use, as well as legal regulations
- DB2 logs provide change data activity per authorization ID
- DB2 audit trace enabled against any table allows Auditors to review:
  - SELECT, INSERT, UPDATE, and DELETE activity by user against an audited table
  - CREATE, ALTER, and DROP operations against an audited object
  - SQL Text used against audited table
  - Row count that SQL statement affects an audited table
  - Utility access to an audited object
  - Assignment or modification of an authorization ID
  - Connection attributes such as client and role information

Requirement 11: Regularly test security systems and processes.

- Verify use of Communications Server network Intrusion Detection Systems
- Verify use of Communications Server AT-TLS or IPSEC for all traffic that contains cardholder data
- Verify use of SERVAUTH and DSNR authorization classes to protect cardholder data from unauthorized access to DB2
- Verify who has privileges on tables with cardholder data
- Verify who has privileges on the underlying data sets of tables with cardholder data
- Verify cardholder data is contained in an audited and encrypted

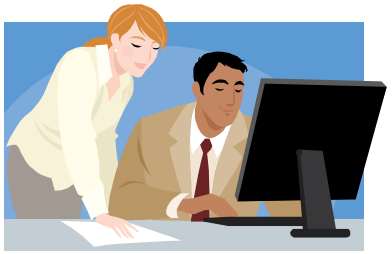
Best practices in your pursuit for compliance (1 of 2)

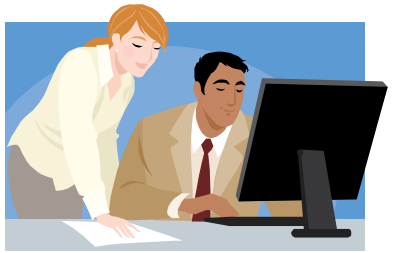
	Columns
Protected Cardholder Data	Primary Account Number
	Cardholder Name
	Service Code
	Expiration Data
Used as Index	Masked Cardholder Data
	Security Label

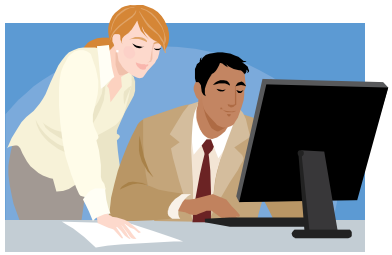
Protecting Cardholder Data in DB2

- Cardholder data stored in encrypted audited table using encrypted storage and encrypted tape for logs
- All other processing based on masked cardholder data

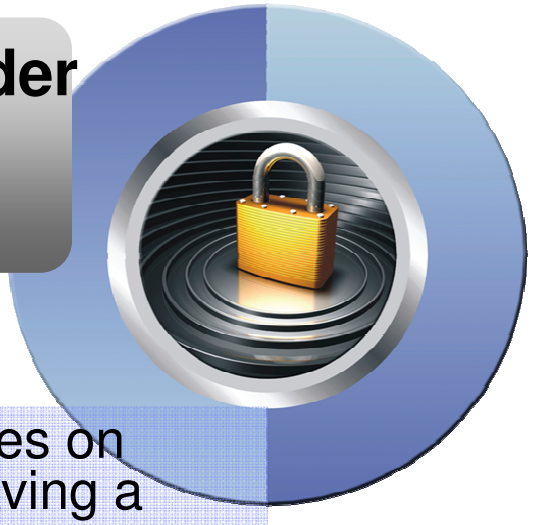
Best practices in your pursuit for compliance (2 of 2)







Protecting Cardholder Data using Strong Access Controls



- Eliminate implicit privileges on cardholder data table by having a ROLE own table
- Require strong encryption when accessing cardholder data
- Use Security Labels to control who can read or update cardholder data
- Use Identity Propagation providing end to end auditing

Fully Integrated Security Elements of DB2 on System z

Crypto Express 2 Crypto Cards

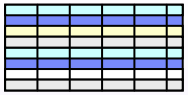
Disk and Tape encryption

DB2 Encryption Tool

TS1120

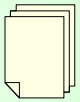
Secured Key Storage & management

Multilevel security



IBM Tivoli Security Compliance Insight Manager

IBM Tivoli zSecure Suite



System z SMF

Compliance and Audit

Data Privacy

Platform Infrastructure

Extended Enterprise

Tivoli Identity Manager

Tivoli Federated Identity Mgr

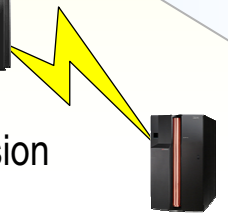
DB2 Encryption and Audit Management Expert

RACF

ICSF

z/OS Communications Server

IPSEC and AT/TLS



Network intrusion detection

Network Authentication Service

Common Criteria Ratings

PKI services

Pursing PCI DSS Compliance with DB2 9 for z/OS

Thank You

Questions?