

**2009**



The Egyptian Bureau For  
Engineering

# **PCI DSS REQUIREMENTS AND EBE SOLUTIONS**





## PCI DSS REQUIREMENTS AND EBE SOLUTIONS

### EBE

EBE is the leading company in Egypt which provides Banking systems solutions and services including personalization smart cards software, POS and ATM services and Internet Security. Besides that EBE provides complete solutions for RFID, VoIP and Smart Card applications. We provide many security solutions for difference purposes.

We are a leading provider of card personalization, secure identity solutions, wafer handling & embedding solutions, and point of sale transaction devices and services for financial institutions. EBE has a card centre for printing cards and our printing systems solutions are installed on most banks in Egypt for printing credit and debit, magnetic and smart cards.

In addition, we provide complete security systems not just for the data but also for locations. Our solutions include access control and time attendance systems, CCTV systems, X-ray and metal detection systems.

### PCI DSS

The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

The PCI Security Standards Council will enhance the PCI DSS as needed to ensure that the standard includes any new or modified requirements necessary to mitigate emerging payment security risks, while continuing to foster wide-scale adoption.

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized. EBE is a leading company in banking and security systems provides many solutions to cover all PCI DSS requirements. The list of the requirements and EBE solutions will present next section.



## PCI DSS REQUIREMENTS

### **Requirement 1: Install and maintain a firewall and router configuration to protect cardholder data**

The input file which contains the card holder data will transfer from the remote sites or from the CMS to the card issuing room before printing process so the local network of the card centre should be protected. EBE provides a strong firewall solution for the LANs from PHION; **netfence sectorwall**.

Netfence sectorwall appliances present the optimum solution for internal firewalling and LAN zoning. They allow efficient implementation of security policies right across the organisation.

Features & Benefits:

- Internal LAN zoning.
- Protection of corporate assets against internal threats and misuse
- ARP Security
- IP Spoofing detection
- Local and central management

If there are PCs inside the card centre connected direct to the Internet, based on PCI DSS requirements a personal firewall should be installed on these PCs. EBE provides a security solution to protect the desktops; **netfence entegra**.

Netfence entegra adding powerful and effective endpoint security and network access control functionality to protect endpoint inside and outside the perimeter.

Features & Benefits:

- Network access policy enforcement.
- VPN and office LAN security
- Centrally managed personal firewall
- Powerful policy framework
- Wireless and 3G adapter control
- Auto-remediation and virtual quarantine
- Endpoint state tracking
- Enforces endpoint policy compliance
- Protects office clients and roaming clients

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

The Bank should change all default password and settings for any network devices before installing it on the network. This includes the wireless networks and systems connected to the card holder data environment or used to transfer or process these data. All non-console administrative access should be encrypted like web management tools. All of the above are Bank responsibility. EBE changes all default passwords of their printing systems before bank issues the cards.

**Requirement 3: Protect stored cardholder data**

After finalizing the printing processes, the card holder data does not store in any place inside the Card Centre. No need to implement any storage policy inside card printing centre. But it is mandatory to encrypt the input file which contains the card holder embossing and encoding data so it will be unreadable outside the card printing room. EBE provides a very good solution to encrypt the files; **SafeNet ProtectDrive TM**. This application is 100% hard drive encryption of: local and remote servers, network drivers, workstations, laptops, user data, system files and registry settings.

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

IF the bank downloads the credit cards input files from outside the Bank site, it should use a VPN connection to access the ftp server. The bank should use a strong encryption protocol like SSL/TLS to protect the card holder data when ever it transmits through any open or public network. EBE provides an ftp server authentication solution; **Gemalto OTP (Protiva)**. This will help bank to grantee the encryption and the authentication for files transmission over ftp server's connections.

**Requirement 5: Use and regularly update anti-virus software or programs**

Antivirus software should be installed on all PCs and servers. It is a bank responsibility. EBE provides a security solution to check all the updates for the antivirus and windows operating systems, **netfence entegra** from PHION. We mentioned it in requirement 1.



### **Requirement 6: Develop and maintain secure systems and applications**

EBE provides a new card printing application **SmartSys** from Ubiq Corp. The application is compatible with PCI DSS requirements. Different Level of privileges for the users is embedded in the system, and more secure techniques for securing card holder data. The application produce a log file for all printing process and has an auto printing feature so every card personalises in the system will appears in the log and in the hardcopy printed papers. This software should be installed in each PC connected to Embosser machine.

EBE provides a solution for the Web application for the bank. It protects the web application against the attacks. **AIRLOCK** from PHION. As the only web application firewall on the market PHION Airlock covers the entire spectrum for protecting and optimising complete web environments. The combination of the web applications security, single sign on and SSL-VPN access provides the best possible flexibility at the highest security level. Besides this, EBE provides another web security solution; **Barracuda**, which is email and web filtering.

For E-Commerce, EBE has a perfect solution to secure e-commerce applications; **Identikey Server** from VASCO. It is offering you strong user authentication for remote access to web-based in-house business applications. In Addition, Identikey Server 3.0's is an electronic signature system to secure your bank's financial transactions

### **Requirement 7: Restrict access to cardholder data by business need-to-know**

The new card printing application **SmartSys** (mentioned in requirement 6) has a facility to manage the access of the software. It limit access to system components to only those individuals whose job requires such access and restricts access based on a user's need-to-know. The operating systems should configure to be compatible with this requirement and this is bank responsibility.

### **Requirement 8: assign a unique ID to each person with computer access**

In the new card printing application **SmartSys** (mentioned in requirement 6) there are password for each username assigned for each operator inside card printing centre. There is no need to exist a remote access to any PC inside the card printing centre. In case there is a remote access connection from outside card centre, EBE provides a strong authentication devices (token) **Gemalto**. Gemalto is on-time password, PKI (digital signing) and windows PKI compatibility.



### **Requirement 9: Restrict physical access to cardholder data**

EBE has a complete solution for the physical access control and mentoring. Access control Model:-T1B (finger, proximity, pin code) and IP cameras with web management software and motion detection.

### **Requirement 10: Track and monitor all access to network resources and cardholder data**

Bank should implement automated audit for all operating systems using Microsoft windows event log. EBE can help bank to achieve this requirement inside the card printing center.

### **Requirement 11: Regularly test security systems and processes**

EBE provides IPS (Intrusion prevention System) **TippingPoint**, the number one in the Gartner report for last three years. TippingPoint provides the IPS-Secure Network, which deliver attack control, access control and application control.

EBE has a very good solution for securing the ATM machines, **Checker**. This is a file integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files or contents files. Another solution for physical securing the ATM machines is **ATMeye**. ATMeye System is a video security complex for ATMs surveillance, exposure of a fraud and resolution of conflicts and transaction problems at the ATMs.

In addition, EBE provides very strong Network Scan software, **QualysGuard** PCI Compliance from **Qualys**. QualysGuard PCI can complete an annual PCI DSS self-assessment questionnaire, pass a network security scan, maintain secure web applications according to PCI Requirement 6.6 and it is from Qualys which is approved scanning vender (ASV).

### **Requirement 12: Maintain a policy that addresses information security for employees and contractors**

The bank should implement all sub requirements of this requirement. This includes: establish, publish and maintain a security policy that address all PCI DSS requirements. Another important issue, if the bank share the card holder data with service providers, then bank should require them to implement PCI DSS policies and procedures for cardholder data security.



## **List of the products:**

### **a) For Card Printing Center\*\*:**

- **netfence sectorwall** (for secure LANs)
- **netfence entegra** (for endpoint security and network access control)
- **SafeNet ProtectDrive** (for encrypt/decrypt any data in any storage media)
- **Gemalto OTP** (for securing transmission through ftp server)
- **SmartSys** (cards printing s/w to satisfy PCI DSS applications requirements)
- **Access control Model:-T1B and IP cameras** (for physical security)

### **b) For Bank:**

- **AIRLOCK** (for WEB application security)
- **TippingPoint** (Intrusion Prevention System IPS)
- **Barracuda** (for WEB/Email filtering security solution)
- **Identikey Server** (for e-commerce authentication and transactions validation solutions)
- **QualysGuard** (PCI DSS self-assessment questionnaire, pass a network security scan, maintain secure web applications) (ASV) \*\*
- **ATMeye** (a video security complex for ATMs)
- **Checker** ( for high-security environment for ATMs PCs)

\*All products listed as solutions for card printing centre could be used for whole bank with exclude SmartSys.

\*\* EBE corporate with ControlCase Co. to provides a security scan service to the external PCs of the bank. ControlCase is also ASV.