globalscape™
securely connected

Whitepaper

Facilitating Enterprise Compliance

With Globalscape® EFT™ and the High-Security Module

Globalscape's Enhanced File Transfer™ (EFT™) High Security module (HSM), with the Auditing and Reporting module (ARM), helps achieve or exceed security practices mandated by the most rigorous standards, including PCI DSS, FIPS 140-2 Validation, HIPAA, and Sarbanes-Oxley. This whitepaper discusses how EFT, the HSM, and ARM can help you achieve compliance and stay compliant with the PCI DSS.

The Case for Compliance

Throughout history, people have sought to protect their valuable possessions. In today's world, credit card numbers are among the most valuable assets we have. To ensure their protection, the Payment Card Industry Security Standards Council has created their Data Security Standard (PCI DSS).

For any organization that stores, processes, or transmits Primary Account Number (PAN) data, failure to comply can have serious consequences: up to US$500,000 per incident, increased fees, restrictions and even removal of processing privileges. Yet, even these fines look insignificant compared to the consequences of sensitive data being compromised. Apart from externally imposed penalties, the organization will also face irate customers, possible lawsuits, heavy regulatory oversight, costly repairs to their system, lost goodwill, and lost business. The true cost of a breach is estimated at $90+ per record. At that level of cost, an ounce of prevention is indeed worth a pound of cure.knowing that the data was properly processed, reported, and analyzed. The right MFT solution must do all of this.

4500 Lockhill-Selma Road, Suite 150; San Antonio TX 78249; 1-800-290-5054 (USA & Canada); 1-210-308-8267 (Worldwide)

The PCI DSS as a Security Standard

The PCI DSS is at the forefront of the drive toward cutting-edge security best practices, while companies are taking a heightened interest in security guidelines for their sensitive data, whether credit card related or not. Even for companies that are not obligated to comply, the PCI DSS offers an authoritative road map for high security systems and processes that can help guard a company's data.

Failure to comply can have serious consequences: up to US$500,000 per incident, increased fees, restrictions and even removal of processing privileges.

The Origin of the Standard

With the advent of the Internet and the explosion of e-commerce, the payment card industry faces an unprecedented level of security risk. As PAN data is transmitted across an increasingly wide range of electronic networks, industry leaders realized they had to collaborate on how to address security risks to cardholder data.

The PCI Security Standards Council created the PCI DSS—an authoritative roadmap for implementing high security systems and processes. The PCI DSS is a multifaceted security standard developed as a collaborative effort among six industry-leading companies: Visa, MasterCard, American Express, Diner's Club, Discover, and JCB USA, as well as many major merchants. Comprised of twelve major requirements, each with several individual categories, the PCI DSS is a comprehensive standard that covers security management, policies, procedures, network architecture, software design and other hardened security measures.

The Challenge of Compliance

Technology solutions have simplified much of modern business operations. However, enterprise compliance to any standard, including the PCI DSS, involves far more than a technology solution. Compliance is a doctrine that must be integrated into your IT procedures. With so many tasks from implementation to enforcement of the standard, where can you find the resources to comply?

The HSM is designed to facilitate this integration. By providing security measures for data storage, access, and transmission, the HSM supports the technology requirements of the PCI DSS. In addition, the HSM also assists you with procedure and policy enforcement by monitoring and reporting on PCI DSS compliance by using prompts and warnings, while also permitting flexibility by allowing non-compliant settings—provided a compensating control is described. A compensating control can be specified when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

Who Must Comply?

Any organization that stores, processes, or transmits Primary Account Number (PAN) data is required to comply with the PCI DSS. They are broken down into four levels of risk. These levels are driven by the transaction volume of the company. The levels range from Level 1, companies handling over 6,000,000 transactions per year, to Level 4, companies handling fewer than 20,000 transactions per year. Compliance at all levels is mandatory, but reporting and scanning requirements differ depending upon transaction volume.

The table below describes the measure that you must take to validate compliance within your organization.

Level	Transactions/Year	Validation Required
1	*6,000,000 or more*	*Annual on-site review by a QSA and quarterly scans by an ASV*
2	*150,000 to 6,000,000*	*Quarterly self-assessment and quarterly scans by an ASV*
3	*20,000 to 150,000*	*Quarterly self-assessment and quarterly scans by an ASV*
4	*All others*	*Quarterly self-assessment and quarterly scans by an ASV*

QSA = Qualified Security Assessor; ASV = Approved Scanning Vendor

A Qualified Security Assessors (QSA) is certified by the PCI to validate compliance. Only Level 1 merchants have to use a QSA; the other levels are required to self assess their compliance and have the option to bring in a QSA. An Approved Scanning Vendor (ASV) is certified to run the required network scans for vulnerabilities.

Facilitating Compliance

Implementing and enforcing compliance in any organization requires extensive time and resources. The HSM provides a comprehensive mechanism to quickly bring your organization into compliance with key requirements. After implementing the HSM, reports and monitoring features help to facilitate ongoing compliance.

Protecting Data at Rest

Data must be protected in storage. The HSM ensures that data is stored using repository encryption and never resides in the DMZ. Even deleted data is securely sanitized so that it cannot be reconstituted.

Protecting Data in Transit

Cardholder data must be secure during the transfer process. The HSM enforces the use of secure protocols, strong ciphers, and encryption keys that strictly follow PCI DSS guidelines.

Controlling Access to Data

User access and password policies are also strictly enforced according to the PCI DSS guidelines. A wide range of secure user authentication sources, including Active Directory, NTLM, LDAP, or ODBC-compatible databases, are supported to simplify integration with your existing structure. Alternatively, you can choose EFT's built-in Globalscape authentication manager to isolate users from your domain.

For added control, the HSM also captures all user activity in a relational database for reporting or individual user activity review.

Facilitating Ongoing Compliance

Your organization's ongoing compliance is a key focus of the HSM. Policies set according to the PCI DSS are enforced using prompts and warnings; however, ultimate control and flexibility remain in your hands, because non-compliant settings can be accepted by providing a corresponding compensating control.
How can you track your compliance with all the various requirements? The HSM supplies daily compliance reports (using ARM) with explanations of all compensating controls to help you maintain compliance. These reports can also facilitate cooperation with a QSA and ASV.

A Comprehensive Approach

This PCI DSS has a wide range of requirements. While many of these requirements involve technology solutions that are addressed directly by the HSM, some require external measures to ensure compliance.

Secure and Compliant Data Exchange

This whitepaper focused specifically on the PCI DSS; however, no matter which security regulations you need to follow, EFT with the HSM and ARM can help you get and stay in compliance and generate reports to facilitate reviews and audits.

4500 Lockhill-Selma Road, Suite 150; San Antonio TX 78249; 1-800-290-5054 (USA & Canada); 1-210-308-8267 (Worldwide)

Appendix 1: Quick Reference to the PCI DSS Requirements

The table below is a quick reference guide to which requirements are addressed with EFT/ HSM and which are external to EFT.

= EFT/HSM facilitates a significant portion of that section's requirements.
= EFT/HSM doesn't hamper compliance; it provides capabilities that augment/support what you might already have in place to comply.
= The requirements in this section require measures external to EFT.

Install and maintain a firewall configuration to protect cardholder data	1.1	1.2	1.3	1.4	1.5					
Do not use vendor-supplied defaults for system passwords and other security parameters	2.1	2.2	2.3	2.4	2.5	2.6				
Protect stored cardholder data	3.1	3.2	3.3	3.4	3.5	3.6	3.7			
Encrypt transmission of cardholder data across open, public networks	4.1	4.2	4.3							
Protect all systems against malware and regularly update anti-virus software or programs	5.1	5.2	5.3	5.4						
Develop and maintain secure systems and applications	6.1	6.2	6.3	6.4	6.5	6.6	6.7			
Restrict access to cardholder data by business need to know	7.1	7.2	7.3							
Identify and authenticate access to system components	8.1	8.2	8.3	8.4	8.5	8.6	8.7	8.8		
Restrict physical access to cardholder data	9.1	9.2	9.3	9.4	9.5	9.6	9.7	9.8	9.9	9.10
Track and monitor all access to network resources and cardholder data	10.1	10.2	10.3	10.4	10.5	10.6	10.7	10.8		
Regularly test security systems and processes	11.1	11.2	11.3	11.4	11.5	11.6				
Maintain a policy that addresses information security for all personnel	12.1	12.2	12.3	12.4	12.5	12.6	12.7	12.8	12.9	12.10

Appendix 2: PCI DSS Requirements Addressed with EFT™ and the High Security Module

The tables below list each requirement and a description of how the HSM helps comply with the requirement.

Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

PCI DSS Requirement	How Requirement is Addressed with EFT
1.1 Establish and implement firewall and router configuration standards.	Requires measures external to EFT.
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	Requires measures external to EFT; however EFT also provides a robust set of IP access filters to control access to EFT and/or the DMZ Gateway.
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	Storing cardholder in the DMZ or other untrusted network is expressly prohibited by PCI DSS (1.3.7). And for security best practices you should now allow inbound connections to originate from untrusted into trusted zones. EFT's optional DMZ Gateway module solves both of these problems. Refer to http://www.globalscape.com/mft/dmz-gateway.aspx for details of DMZ Gateway.
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	EFT in combination with the DMZ Gateway module facilitates compliance with this requirement.
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	When EFT is used in combination with the DMZ Gateway, no internal inbound ports need be opened into the trusted network, hence all inbound traffic will be restricted to IP addresses within the DMZ.
1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.	The need for inbound connections between the DMZ and the internal network is eliminated when using EFT in combination with the DMZ Gateway module.
1.3.4 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.	Requires measures external to EFT.
1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	EFT can be configured* to use the DMZ Gateway as a SOCKS5 proxy for outbound traffic. Offloading files using EFT though the DMZ Gateway means your internal IP address won't be exposed (1.3.48). Additional steps may be required to fulfill this requirement, such as DLP and deep content inspection tools, before files are submitted to EFT for offloading. *Requires DMZ Gateway.
1.3.6 Implement stateful inspection, also known as dynamic packet filtering.	Requires measures external to EFT.

1.3.7 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	EFT, when combined with the DMZ Gateway, eliminates the need to store data in the DMZ.
1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties.	Your internal IP addressing scheme is never exposed when EFT is used in combination with the DMZ Gateway .
1.4 Install personal firewall software on any mobile and/or employee-owned computers	Requires measures external to EFT.
1.5 Document policies and procedures	Requires measures external to EFT.

Requirement 2: Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

PCI DSS Requirement	How Requirement is Addressed with EFT
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	With the HSM and a high security-enabled Site, EFT detects whether any default values are specified for Admin login port (1100), DMZ Gateway port (44500), FTP banner message, or SFTP banner message, and will prompt you to change them. No default passwords, usernames, certificates, or keys are used.
2.2 Develop configuration standards for all system components.	Refer to the specific sub-requirements below.
2.2.1 Implement only one primary function per server	EFT's primary function is File Transfer. It is up to the administrator to segregate servers.
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	It is up to the administrator to determine whether an enabled protocol is necessary. No protocol is enabled by default.
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.	Any unsecure protocols such as plaintext FTP or HTTP are automatically detected* and you are prompted to change them or present a compensating control. *Requires HSM and creation of a PCI DSS Site.
2.2.4 Configure system security parameters to prevent misuse.	With the HSM and a PCI DSS Site, EFT monitors and warns when ○ User login credentials not-persisted in memory beyond the absolute minimum time necessary (some configurations require this when reusing credentials for secondary connections) ○ Flood and DoS prevention settings set too low ○ FTP Anti-timeout prevention scheme disabled or FXP (site-to-site) permitted

2.2.5 Remove all unnecessary functionality	It is up to the administrator to remove any scripts, custom commands, AWE workflows or similar user-created files that are no longer in use.
2.3 Encrypt all non-console administrative access using strong cryptography.	The status of non-console (remote) access settings are monitored* and you are warned if SSL is not enabled and given the option to either disable remote administration or enable SSL. *Requires HSM and creation of a PCI DSS Site
2.4 - 2.6 Inventory maintenance, policy documentation and enforcement, and shared hosting requirements	Requires measures external to EFT.

Requirement 3: Protect Stored Cardholder Data

PCI DSS Requirement	How Requirement is Addressed with EFT
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes.	EFT provides a scheduled, automatic Clean-up Action*. Deleted files can be purged** by writing over the initial data using encrypted and/or pseudorandom data (PCI DSS 9.8). Disk quotas can be set to limit data storage. *Requires EFT Enterprise. **Requires HSM
3.2 Do not store sensitive authentication data after authorization (even if encrypted).	3.2.1-3 Refers to card sensitive authentication data (SAD), which should never be stored on the server. Use a third-party DLP or similar tool to detect and prevent SAD storage.
3.3 Mask PAN when displayed	Not applicable to EFT, because EFT cannot display that data.
3.4 Render PAN, at minimum, unreadable anywhere it is stored.	Encrypt PAN or other sensitive data using EFT's optional OpenPGP encryption module or third-party encryption utilities.
3.4.1 If disk encryption is used, logical access must be managed independently of native operating system authentication and access control mechanisms.	EFT will detect and warn if Microsoft Encrypting File System (EFS) is being used. (Requires HSM and creation of a PCI DSS Site.)
3.5 Document and implement procedures to protect keys	Mostly requires measures external to EFT; however access to keys through the administrator interface is limited to administrator roles with Site or Server access only.
3.6 Fully document and implement all key management processes and procedures	Mostly requires measures external to EFT; however, per 3.6.1 EFT will disallow creation of 512 or lesser certificate/key bit lengths. Default bit-length is set to 2048 bits for new keys. When importing SSL or SFTP keys, a warning will appear if a weak key is imported. *Requires HSM and creation of a PCI DSS Site
3.7 Document policies and procedures	Requires measures external to EFT.

Requirement 4: Encrypt Transmission of Cardholder Data across Open, Public Networks

PCI DSS Requirement	How Requirement is Addressed with EFT
4.1 Use strong cryptography and security protocols	Secure protocols such as SSL, TLS, and SFTP (SSH2) are provided for data transmission. For high security-enabled sites, SSL is restricted* to versions v3 or higher, and ciphers to minimum of 128 bits. Secure data transmission is enforced* by automatically redirecting incoming HTTP traffic to HTTPS. *Requires HSM
4.2 - 4.3 Never send unprotected PANs by end-user messaging technologies; document security policies and procedures	Requires measures external to EFT.

Requirement 5: Use and Regularly Update Anti-Virus Software

PCI DSS Requirement	How Requirement is Addressed with EFT
5.1 - 5.4 Anti-virus requirements.	Requires measures external to EFT

Requirement 6: Develop and Maintain Secure Systems and Applications

PCI DSS Requirement	How Requirement is Addressed with EFT
6.1 Establish a process to identify security vulnerabilities	Globalscape has formal processes for dealing with potential security vulnerabilities discovered in EFT, including an escalation process, a risk assessment that includes Common Vulnerability Scoring System (CVSS) risk ranking, and a process for notifying customers of critical patches or workarounds.
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	The latest version of EFT is always available from the Globalscape website. Customers are automatically notified upon critical patch availability. It is up to the customer to install the patch within the designated one-month window.
6.3 Develop internal and external software applications securely.	Globalscape takes a number steps to develop secure software, as documented here: http://kb.globalscape.com/KnowledgebaseArticle11061.aspx.
6.3.1 Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers	Only applies to Professional Services engagements and should be verified prior to deployment.
6.3.2 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability.	Only applies to Professional Services engagements and should be verified prior to deployment.
6.4 Follow change control procedures for all changes to system components.	Requires measures external to EFT.
6.5 Address common coding vulnerabilities in software-development processes	Globalscape takes a number steps to develop secure software, as documented here: http://kb.globalscape.com/KnowledgebaseArticle11061.aspx.

6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis.	Requires customer to run a security scan. However, Globalscape also performs routine third-party security scans of EFT's public-facing web interfaces as part of its quality assurance process.
6.7 Document policies and procedures	Requires measures external to EFT.

Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know

PCI DSS Requirement	How Requirement is Addressed with EFT
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	EFT provides complete control administrator and user access to resources, with administrator accounts completely segregated from user accounts.
7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	Segregation and control of user access is achieved using unique accounts, permission groups, virtual folders, and settings templates. Segregation and control of administrator access is accomplished via delegated, role-based administrator accounts
7.3 Document policies and procedures.	Requires measures external to EFT.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

PCI DSS Requirement	How Requirement is Addressed with EFT
8.1 Define and implement policies and procedures to ensure proper user identification management	EFT enforces unique usernames for both users and administrators (8.1.1), provides granular administrative controls over user provisioning and authorization (8.1.2), allows user and admin account revocation (8.1.3), provides automatic removal of inactive users after 90 days (8.1.4), includes controls for temporarily enabling/disabling users (8.1.5), auto-locks users after six failed login attempts (8.1.6), either for a period of time or permanently until the admin unbans (8.1.7), and automatically expires sessions after 15 minutes of inactivity (8.1.8)
8.2 In addition to assigning a unique ID, ensure proper user authentication.	EFT supports various combinations of password, certificate, two-factor, and public-key authentication mechanisms (8.2), secures passwords during transmission (assumes SSL or SSH), and storage (with a one way [uniquely salted] hash)(8.2.1), verifies identify before allowing password reset or lost username retrieval according to OWASP guidelines (8.2.2), includes minimum length and a number of complexity options (8.2.3), expires and forces password change after 90 days (8.2.4), disallows password re-use, internal dictionary match, or username match (8.2.5), and can force first time use password reset (8.2.6).
8.3 Incorporate two-factor authentication for remote network access.	Although EFT supports 2FA, this requirement is about *network access*, such as what is normally done over a VPN.
8.4 Document and communicate authentication procedures and policies	Requires measures external to EFT.

8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods	The "Anonymous" password type is disallowed on a high-security-enabled Site (Requires HSM). To comply with 8.5.1 you will need to create unique accounts for service provider access, should there ever be a need to provide such access.
8.6 Requirements for unique and controlled access using non-standard authentication mechanisms.	Requires measures external to EFT as most of these are physically provisioned to the user.
8.7 All access to any database containing cardholder data is restricted.	EFT provides granular controls over which administrators can access EFT's reports from within the EFT Server console; however controls over access to the database (including the data) itself requires measures external to EFT.
8.8 Document policies and procedures.	Requires measures external to EFT

Requirement 9: Restrict Physical Access to Cardholder Data

PCI DSS Requirement	How Requirement is Addressed with EFT
9.1 - 9.7 Requirements related to *physical* access to the cardholder environment.	Requires measures external to EFT.
9.8 Cardholder data on electronic media must be rendered unrecoverable via a secure wipe program	EFT includes a data-wiping algorithm for sanitizing deleted data on disk. (Requires HSM.)
9.9 Protect devices that capture payment card data via direct physical interaction	Requires measures external to EFT
9.10 Document policies and procedures.	Requires measures external to EFT

Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data

PCI DSS Requirement	How Requirement is Addressed with EFT
10.1 Implement audit trails to link all access to system components to each individual user	Preconfigured reports of all activity (including administrator actions*) within EFT can be generated on demand with the Auditing and Reporting Module (ARM) *Requires ARM and HSM.
10.2 Implement automated audit trails for all system components	EFT will audit* all user access to data (10.2.1), and all administrator changes** to configuration settings (10.2.2). Access to audit trails, invalid logical access, authentication mechanisms, object creation, and initialization of audit logs (10.2.3-2.7) is managed at the database server. *Requires ARM and HSM
10.3 Record audit trail entries for all system components	EFT audits* user identity (10.3.1), type of transaction (10.3.2), date and time of transaction (10.3.3), transaction result (10.3.4), remote and local IP (10.3.5), and objects affected (10.3.6). *Requires ARM
10.4 Synchronize critical system clocks and times	Requires measures external to EFT.
10.5 Secure audit trails so that they cannot be altered.	Audited data integrity depends on the chosen database solution and authentication architecture. EFT supports auditing* to a central SQL or Oracle** server. *Requires ARM **Requires EFT Enterprise

10.6 Review log sand security events for all system components (10.6.1) at least daily	A daily PCI DSS Compliance report can be generated by EFT and sent via email to the appropriate recipient(s). Administrators can also attach any other canned or administrator created report to the daily email. (Requires both ARM and HSM.)
10.7 Retain audit trail history for at least one year	Requires measures external to EFT.
10.8 Document policies and procedures	Requires measures external to EFT

Requirement 11: Regularly Test Security Systems and Processes

PCI DSS Requirement	How Requirement is Addressed with EFT
11.1 - 11.6 Requirements relating to regular testing of security systems and processes.	Requires measures external to EFT.

Requirement 12: Maintain a Policy that Addresses Information Security

PCI DSS Requirement	How Requirement is Addressed with EFT
12.1 - 12.10 Maintain a policy that addresses information security for all personnel	Requires measures external to EFT

About Globalscape

Globalscape ensures the reliability of mission-critical operations by securing sensitive data and intellectual property. Globalscape's suite of solutions features Enhanced File Transfer™, the industry-leading enterprise file transfer platform that delivers military-grade security and a customizable solution for achieving best-in-class control and visibility of data in motion or at rest, across multiple locations. Founded in 1996, Globalscape is a leading enterprise solution provider of secure information exchange software and services to thousands of customers, including global enterprises, governments, and small businesses.

4500 Lockhill-Selma Road, Suite 150; San Antonio TX 78249; 1-800-290-5054 (USA & Canada); 1-210-308-8267 (Worldwide)