U-Scan®
PABP (Payment Applications Best Practices) Implementation Guide

Document:	U-Scan® PABP Implementation Guide
Last Update:	May 29, 2008
Prepared by:	Fujitsu Transaction Solutions Inc.
Version:	1.7

1 Contents

2 Introduction

2.1 Intended Audience

This document describes how the U-Scan® system and the environment that it runs in should be implemented in order to be compliant with Payment Applications Best Practices (PABP) and the Payment Card Industry Data Security Standard (PCI DSS). Fujitsu strongly urges U-Scan® users to follow these implementation recommendations. This document is intended for U-Scan® customers, resellers, and integrators, and will be reviewed annually and updated as required.

2.2 Implementation Training

Fujitsu recommends that U-Scan® users, including Retailers, Resellers, and Integrators provide relevant personnel with training on how to implement U-Scan® in a PCI-compliant manner. This training should consist of an overview of the PCI DSS and related compliance requirements, and a careful review of the material presented in this document.

3 An Emphasis on Security

3.1 Retailer Responsibility for PCI Compliance

The Retailer is responsible for operating Payment Applications in an environment that minimizes the potential for breaches in security that might lead to compromises of cardholder data, resulting in fraud and other damages. PCI Compliance is therefore a Retailer responsibility. When implemented according to the recommendations of this document U-Scan® does not store or process cardholder data, but is considered to be a Payment Application because it can transmit cardholder data to the Retailer's Point of Sale (POS) system. Fujitsu has developed U-Scan® systems so that Retailers can implement U-Scan® in a PCI-compliant manner in their environments so long as the recommendations in this document are followed.

3.2 Operating System Critical Security Updates

PCI DSS requirement 6 mandates that security patches be installed to reduce the possibility of unauthorized access to Payment Application systems. Application of security updates is recommended even in systems such as U-Scan® that run only in a secure network environment. U-Scan® systems are delivered with software that includes a pre-installed operating system. While the image from which the operating system is installed is updated periodically with the latest security patches, factors such as storage, shipping delays, and others mean that these patches may not be current when the system is installed. It is the Retailer's responsibility to maintain the U-Scan® host operating system, including service packs and other relevant patches on an ongoing basis as part of their overall infrastructure support and maintenance process.

Fujitsu recommends that patches identified by Microsoft as "critical" should be applied by enabling the Windows update function on U-Scan® systems, and using Microsoft tools to push critical security updates to these systems as well as to any other Windows-based systems on the same network. Doing so will not void or impair any Retailer's active Software Maintenance Agreement, and Fujitsu recommends it as a best practice so long as the following considerations are respected:

- The Retailer should obtain Critical Security Updates directly from Microsoft and use Microsoft tools to push them to their U-Scan® systems on a periodic basis, first testing each update as described in the following points.
- The Retailer should apply and test each Update in a lab environment.
- Following successful lab testing the Retailer should apply the Updates in a single production environment and monitor the result.
- Following successful testing in a single production environment, the Retailer should apply the Updates to additional individual sites that represent different geographies or operating environments and monitor the result.
- When the above testing has been successfully completed, the Retailer can proceed to apply the Update to all of the U-Scan® systems that it operates.
- In general, Security Updates will not have any adverse affects on a U-Scan® system. If a Security Update exhibits adverse affects on U-Scan®, the Retailer should roll back the update and inform Fujitsu so that it can reproduce and remedy the problem.
- The Retailer should act upon any bulletins that Fujitsu may issue with regard to specific operating system updates that may be discovered to cause problems with U-Scan®.

3.3 U-Scan® Security Updates

U-Scan® software updates are provided by Fujitsu as full installation CDs and as ASM packages (sometimes referred to as patches). Only CDs delivered by Fujitsu and clearly identified as produced by Fujitsu are to be installed on U-Scan® systems. ASM packages can be delivered by CD, but usually are securely downloaded from a Fujitsu-controlled FTP site. The Retailer should obtain access information and instructions from their Fujitsu representative to securely download these update packages.

In addition to regular software updates, from time to time Fujitsu may issue a U-Scan® Security Update. A U-Scan® Security Update is intended to correct any weakness that may be discovered in U-Scan® software that could impair the PCI-compliant functioning of U-Scan®. All U-Scan® Security Updates will be accompanied by a bulletin that identifies the nature of the

weakness, describes the remedy provided by the Update, and identifies the Update as a Mandatory Security Update.

Fujitsu recommends that all U-Scan® Security Updates be applied as quickly as possible to all U-Scan® systems. As with the application of operating system Security Updates, the following practice should be followed:

- The Retailer should apply and test the U-Scan® Security Update in a lab environment.
- Following successful lab testing the Retailer should apply the Update in a single production environment and monitor the result.
- Following successful testing in a single production environment, the Retailer should apply the Update to additional individual sites that represent different geographies or operating environments and monitor the result.
- When the above testing has been successfully completed, the Retailer can proceed to apply the Update to all of the U-Scan® systems that it operates.
- If a U-Scan® Security Update exhibits an adverse affect on a U-Scan® system, the Retailer should roll back the Update and inform Fujitsu so that it can reproduce and remedy the problem.

3.4 Retailer Provided Test Data or Confidential Information

Fujitsu will rarely if ever require a Retailer to provide test data, diagnostic results, or any other content that contains cardholder data or other sensitive information. In the event that Fujitsu does require sensitive information, the Retailer is advised never to send email that contains unencrypted cardholder data or any other sensitive information. The Retailer is further advised to ensure that if the need arises to recover any sensitive cardholder data for testing or debugging, the data is stored in encrypted form, access to any files containing cardholder data is restricted, and the data files are securely wiped when no longer needed.

4 U-Scan® Configuration

4.1 User IDs and Passwords

Fujitsu recommends that default passwords provided when a U-Scan® system is installed should be changed, and that PCI DSS compliant user IDs and complex passwords be used to access the U-Scan® application as described in PCI Data Security Standard requirements 8.5.8 through 8.5.15. These requirements include the following:

- Do not use group, shared, or generic accounts and passwords [PCI DSS 8.5.8].
- Change user passwords at least every 90 days [PCI DSS 8.5.9].
- Require a minimum password length of at least seven characters [PCI DSS 8.5.10].
- Use passwords containing both numeric and alphabetic characters [PCI DSS 8.5.11].
- When changing passwords, do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used [PCI DSS 8.5.12].
- Lock the user's ID if more than six unsuccessful attempts have been made to access the system [PCI DSS 8.5.13].

- Set the lockout duration to 30 minutes or until administrator enables the user ID [PCI DSS 8.5.14].
- If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal [PCI DSS 8.5.15].
- Employ strong application and system passwords whenever possible.

The PCI requirements apply to operating system passwords and all U-Scan application passwords that allow access to cardholder data. The PCI requirements also apply to U-Scan application passwords, such as manager or maintenance passwords, which allow users to access the operating system

Accounts that will not be used should be given strong passwords and then disabled.

On installation the System Administrator (SA) account for the U-Scan® SQL databases does not have a default password, and Fujitsu recommends that a password be set. The SA account is not used by the U-Scan® software, so any strong password can be chosen. It should be noted that the U-Scan® databases do not contain any cardholder data, nor do they contain sensitive data of any kind at all; nevertheless as part of a consistent approach to security, Fujitsu recommends that the steps described in this paragraph should be followed.

4.2 Virus Scanners

PCI DSS requirements 5.1 and 5.2 mandate that anti-virus software should be deployed on all systems commonly affected by viruses.

Fujitsu does not recommend any specific virus scanner to be used with a U-Scan® system. Fujitsu recommends that Retailers carefully evaluate the use of anti-virus software in their environments before installing it on U-Scan® systems.

When implementing a virus scanner, the folder with U-Scan® diagnostic trace logs must be excluded from virus scans; because these files are updated constantly, system performance is seriously degraded if they are not excluded from virus scans. Fujitsu is not aware of other exclusions that may be required or recommended, but recommends that Retailers carefully evaluate which files and folders should be excluded from scanning with their selected tool in order to function successfully in their specific environments.

4.3 Application Logging

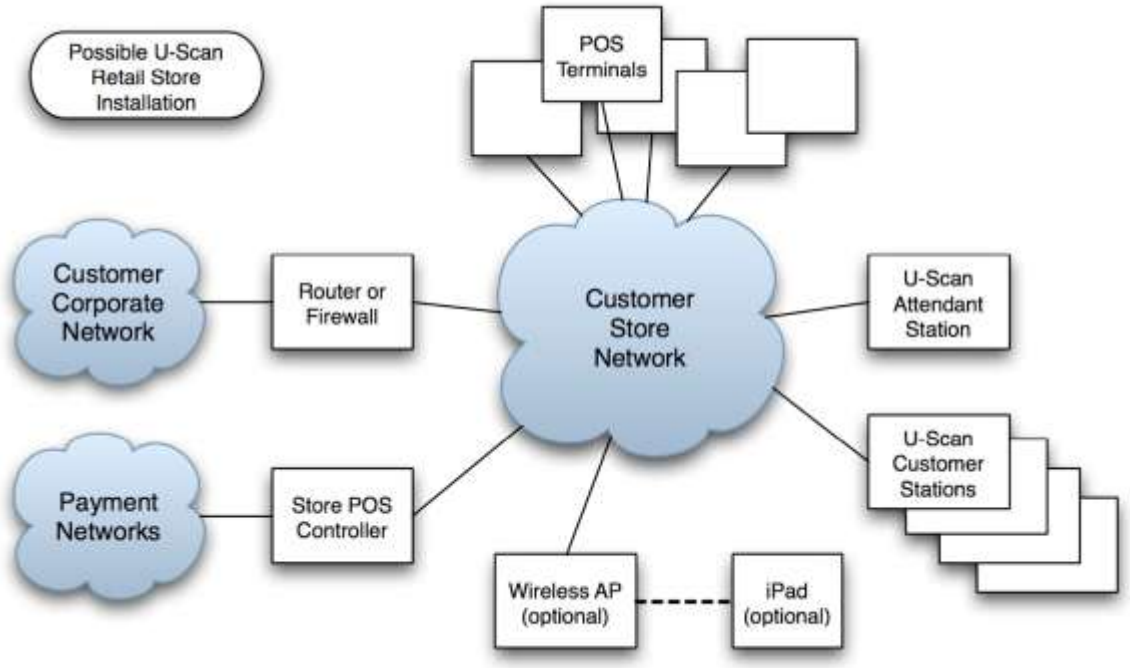
In normal operation U-Scan® generates trace files that are used for diagnostic purposes. The tracing mechanism has been specifically implemented to ensure that no cardholder data is stored in a diagnostic trace file. In addition, detailed tracing of data traffic from serial devices can be temporarily enabled for debugging purposes; serial tracing can only be turned on or off by a user with administrative access to the U-Scan® system. U-Scan® systems are not left in this mode for production purposes, because enabling this level of tracing seriously degrades system performance. Fujitsu advises that Retailers should never activate serial tracing unless specifically requested by Fujitsu personnel to do so, that they should never leave this level of tracing enabled longer than is necessary to diagnose the problem, and that they should ensure it is turned off after the debugging process is concluded. Fujitsu advises that Retailers should not install or enable diagnostic tracing tools that would store cardholder data on a U-Scan® system.

PCI DSS requirement 10.2 mandates the use of automated audit trails, and PCI DSS requirement 10.3 specifies the following audit trail entries for all system components for each event: User identification, Type of event, Date and time, Success or failure indication, Origination of event, and Identity or name of affected data, system component, or resource. It is the

responsibility of the Retailer to implement processes to ensure that PCI DSS requirement 10 is satisfied. U-Scan® databases do not contain any cardholder or other sensitive data, so logging of U-Scan® database access and changes is not required. In addition to the application logging described above, U-Scan® systems support standard Windows event logging for application, system, and security events. A variety of Security Information Management products may be used in retail environments to centralize and manage event information; if the Retailer has deployed such a system in their environment they may choose to install it on their U-Scan® systems. Fujitsu does not recommend any specific product to be used for Security Information Management with a U-Scan® system. Fujitsu recommends that Retailers carefully evaluate the use of Security Information Management software in their environments before installing it on U-Scan® systems.

Network Environment

The following is a representation of a Retail network environment with U-Scan® deployed.



5.1 Secure Network Environment

U-Scan® systems are designed to operate in a retail POS environment on a secure internal network. U-Scan® systems are not web-facing, do not require access to the Internet, and should not be installed on an Internet-accessible network segment. All network traffic between U-Scan® systems and POS controllers should be over a secure network.

5.2 Remote Access

Remote access to U-Scan® systems is not required for normal operations; remote access is only required in order to gather diagnostic information or take remedial action in support of a U-Scan® system. Fujitsu recommends that remote access to U-Scan® systems be granted only

for the period required, disconnected when not in use, and be authenticated using a two-factor mechanism: username/password and an additional authentication item such as a token or certificate; technologies such as RADIUS or TACACS with tokens, or VPN with individual certificates are recommended. Non-console administrative access must be encrypted using technologies such as VPN or Windows Remote Desktop Protocol (RDP) with maximum strength encryption.

U-Scan® is normally installed with Funk Proxy host software to allow a remote user employing Proxy client software to perform remote diagnostic functions. Fujitsu recommends that this software be used in conjunction with the remote access controls discussed above, and that the default password for the Proxy host be changed to a strong password using the recommendations regarding passwords described above. Access to remote access user IDs and passwords should be restricted to those personnel who have a specific need to provide remote service to a U-Scan® system.

5.3 Wireless Network Considerations

U-Scan® can be implemented with an optional Mobile Attendant or iPad; this is a hand-held device that communicates with the U-Scan® systems via a wireless access point. U-Scan® systems are normally implemented using a wired network to communication with other U-Scan® units and POS controllers; wireless technology can be used to implement a U-Scan® system, in which case a wireless access point will be required. In all cases where a wireless access point is used in a U-Scan® implementation, the Retailer is responsible to ensure that the access point is implemented in a PCI DSS-compliant manner as indicated in requirements 1.3.8, 2.1.1, 4.1.1, 9.1.3, and 11.1.b which include the following requirements:

- Change the wireless vendor's defaults including, but not limited to, WEP keys, default SSID, passwords, SNMP community strings, and disabling of SSID broadcasts.
- Implement a perimeter firewall between any wireless networks and the payment card environment, configured to deny or control any traffic from the wireless environment.
- Use of Wi-Fi Protected Access (WPA) technology for encryption and authentication is supported by all current U-Scan systems and devices and should be used whenever the Retailers wireless access point is WPA-capable. If not WPA-capable then VPN or SSL at 128-bit should be employed. The Retailer should never rely exclusively on WEP to protect confidentiality and access to a wireless LAN. Retailers should use one of these methodologies in conjunction with WEP at 128-bit and rotate shared WEP keys quarterly and whenever there are personnel changes [PCI DSS 4.1.1].

6 Resources

- For information on the PCI DSS (Payment Card Industry Data Security Standard), see: https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm
- For information on the CISP (Cardholder Information Security Program) Best Practices program, see: http://usa.visa.com/merchants/risk_management/cisp.html
- For more information about Fujitsu Transaction Solutions Inc, see: http://www.fujitsu.com/us/services/retailing