XS 3.3.2 US Update Software Release Notes

Affected products
RL2000 (8” Display), RT2000 (10.4” Display), RL5000, FT5000

March 18, 2016
Version 1.0
INTRODUCTION

PLATFORMS AFFECTED

<table>
<thead>
<tr>
<th>HARDWARE SUPPORT</th>
<th>SOFTWARE REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

DESCRIPTION OF CHANGES

<table>
<thead>
<tr>
<th>T9 EPP SUPPORT</th>
<th>EMV BALANCE INQUIRY TRANSACTION CODE FOR MASTERCARD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4</td>
</tr>
<tr>
<td>CARD READER/EPP STATUS MONITORING INFORMATION</td>
<td>5</td>
</tr>
<tr>
<td>DIALUP MODEM SETTINGS</td>
<td>6</td>
</tr>
<tr>
<td>HOST CONFIGURED MAXIMUM WITHDRAWAL AMOUNT</td>
<td>6</td>
</tr>
<tr>
<td>VIRTUAL KEYBOARD</td>
<td>6</td>
</tr>
<tr>
<td>EMV KERNEL</td>
<td>7</td>
</tr>
<tr>
<td>CHANGES FROM 1.0.0</td>
<td>7</td>
</tr>
<tr>
<td>SUPPORT OF US APPLICATION IDS (AIDS)</td>
<td>7</td>
</tr>
<tr>
<td>AUTOMATICALLY SELECT US EMV APPLICATIONS</td>
<td>7</td>
</tr>
<tr>
<td>MAGISTRIP CARD READ BEHAVIOR</td>
<td>7</td>
</tr>
<tr>
<td>SSL SHA-2 CERTIFICATES</td>
<td>7</td>
</tr>
</tbody>
</table>

REVISION HISTORY

8
Introduction

This document describes new functionality for the 3.3.2 US software release for RL2000 (8” Display), RL5000, RT2000 (10.4” Display), and FT5000 ATMs. The differences described are from version 3.2.0 SP1.

Platforms Affected

This release is for the following families:
- RL2000 8” Display, RL5000, RT2000 10.4” Display, FT5000

Hardware Support

The following is a list of hardware supported by this software:
- **Main Board:** X2 CE5
- **Display:** 10.4” VGA (RL/RT/FT), 8” VGA (RL2000)
- **Card Reader:** MagTek 215 Dip Reader, Sankyo ICM330 Dip Reader
- **EPP:** T1, T5, T7, T9
- **Dispenser:** SDD, MiniMech, NMD50, NMD100, TDM1xx, TDM2xx
- **Security Module:** SN-01.01.001, SM-01.01.001, ST-01.01.000 (TDM w/ASM)
- **Printer:** Seiko 80mm/60mm USB Printer
- **Modem:** Triton USB Modem, TDL Gateway Modem, MultiTech USB Modem

Software Requirements

The following load files are included with this release:
- xu34xce3.3.2.tfv – US Update load file (can be installed on any previous X2 CE5 software)
Description of Changes

**T9 EPP Support**

This software release adds support of the T9 PCI 3.0 EPP. The behavior of the T9 EPP is mostly identical to the T5 EPP except for the following:

- Per PCI 3.0 requirements, the T9 EPP contains a removal detection switch that is signaled if the EPP is ever removed from the ATM. In order to re-activate the EPP for use in an ATM after removal, go to Management > Diagnostics > Keypad > Activate EPP. Contact Triton Technical Support to retrieve the correct activation code to re-activate the EPP. There is a charge for this service.

- Left and right halves of 3DES keys must be different. This prohibits the practice of assigning the same value to both the left and right halves to render it a 1DES key. This is a requirement for both PIN and MAC keys.

- No two 3DES keys may have the same value. For example, the PIN master key and the MAC master key must have different values to each other.

Note that T9 EPP device status report from Management > Diagnostics > Keypad > Device Status will indicate if the EPP has previously been removed since the last activation:

Remove detector activated: TRUE

The following are new error codes added to support the T9 EPP:

<table>
<thead>
<tr>
<th>Error code</th>
<th>Description</th>
<th>Cause</th>
<th>Recommended action</th>
</tr>
</thead>
<tbody>
<tr>
<td>625</td>
<td>SPED – Not Activated</td>
<td>The EPP has not yet been activated for use</td>
<td>Activate EPP in Diagnostics &gt; Keypad &gt; Activate EPP</td>
</tr>
<tr>
<td>626</td>
<td>SPED – Not Authorized</td>
<td>The EPP has been removed from the ATM.</td>
<td>Call Triton Tech Support for activation code and instructions.</td>
</tr>
</tbody>
</table>

**EMV Balance Inquiry Transaction Code for MasterCard**

Per MasterCard rules, the EMV Balance Inquiry Transaction Code sent in tag 9C in the transaction request should be “30”. All other card types will use a value of “31” for this tag.
Card Reader/EPP Status Monitoring Information

This software release adds the ability to send card reader and EPP information in status monitoring data sent to the ATM host processor. Status monitoring is set in Management > Terminal Configuration > General Parameters > ATM Monitoring. When selecting option 9, the status monitoring settings will scroll through the following values (default is disabled):

- **Disabled**
- **Status Monitoring** (No changes from previous software)
- **Advanced Status Monitoring** (Adds card reader and EPP information – contact Triton for information on the format of this data)
**Dialup Modem Settings**

The settings in *Management > Diagnostics > Modem > Device Status* for the host will show the following, this may be different from some previous software versions:

- **Byte Size:** 7
- **Parity:** Even
- **Stop Bits:** 1

**Host Configured Maximum Withdrawal Amount**

This software release allows the host to set a maximum withdrawal amount of up to 4 numeric digits ($9999). Previously this configuration was limited to 3 numeric digits. See TDL specification for details on setting this amount using the ‘w’ Miscellaneous FID through the host processor interface.

**Virtual Keyboard**

As already supported in ARGO software, this software release includes a new option for the on-screen virtual keyboard that is used for alpha entry in Management Functions to use a “cell phone” style entry method, referred to as “Phone Entry” in the lower right corner of the display. The ATM will default to the current alpha entry method, referred to as “Triton Entry”. The ATM will always use the last entry method selected for all management users.

For RL/FT/RT/Traverse, the only addition is the ability to change the entry method by using the bottom right screen key:

For “Phone Entry” the following menu will be displayed:
Note: When using the virtual keypad in Diagnostics > Modem/Ethernet > Configure Modem or Triton Connect Settings, the virtual keypad must be brought up before entering this menu.

**EMV Kernel**
This software release contains a new version of the EMV kernel. The version listed in Management > Terminal Configuration > More Options > EMV Configuration > Terminal EMV Configuration will be 1.0.1.0. This kernel has been tested according to EMVCo Type Approval Terminal Level 2 Test Cases document version 4.3d November, 2014.

**Changes from 1.0.0**
The following changes have been made from EMV Kernel version 1.0.0:
- Support new test cases Interoper 29 02, 29 03 and MTIP 31 USM 01 01
- Application label incorrect when issuer code table index supported
- General memory leak fixes

**Support of US Application IDs (AIDs)**
This load file adds the following application ID to the available list of EMV applications:
- Visa US: A0000000980840
- Maestro US: A0000000042203
- Discover: A0000001523010
- Discover US: A0000001524010
- JCB US: A0000000065
- DNA US: A000000620

All of these applications are enabled by default.

**Automatically Select US EMV Applications**
This update adds the capability for the ATM to automatically select US applications over other applications with the same IIN on a chip card. The US AIDs are designated as priority applications in this software update.

**Magstripe Card Read Behavior**
This software version changes the method in which magstripe cards are read with EMV enabled at the ATM:
- If a magstripe only (non-chip) card is removed before the system finishes attempting to read the chip, the ATM will continue to process the card as magstripe.
- If a chip card is removed before the system finishes attempting to read the chip, the ATM will instruct the customer to re-insert the card and leave it in the reader until instructed.

**SSL SHA-2 Certificates**
Starting in 2017, PCI is requiring host processors to use SHA-2 for all SSL communications over TCP/IP instead of using SHA-1. Certificate Authorities are now creating certificates that
conform to this standard. In order to use one of these certificates for a host processor (or Triton Connect), the ATM software must be updated so the newer certificates can be accepted.

This software update also includes support for the following SHA-2 root certificates:
- GoDaddy
- Thawte
- Verisign
- TrustWave
- RapidSSL/GeoTrust
- TrendMicro
- Entrust

**Revision History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 18, 2016</td>
<td>1.0</td>
<td>Initial version</td>
</tr>
</tbody>
</table>