Device Appendix I

PAX S500
Appendix I: PAX S500

This appendix is intended to be used in conjunction with the P2PE Version 2.0 Bluefin PIM Template document. Please make sure to review both documents in order to ensure proper compliance and usage for Bluefin’s P2PE product offering.

The number used in the different sections of this appendix document directly correlates to general usage points in the P2PE Version 2.0 Bluefin PIM Template document.

### 3.0 Remote Device Administration

The following guidance is intended to communicate PCI’s rules around merchants performing any actions while in the custody of the device that could invalidate the effectiveness of their P2PE solution.

For each of the two compliance points from PCI, the combination of the architecture of the PAX S500 devices and Bluefin’s P2PE Solution should prevent the merchant from accidently performing any of the PCI banned activities.

**Do not connect non-approved cardholder data capture devices.**

The P2PE solution is approved to include specific PCI-approved POI devices. Only those devices denoted in the Core PIM document in section 2.1 are allowed for cardholder data capture.

If a merchant’s PCI-approved POI device is connected to a data capture mechanism that is not PCI approved, (for example, if a PCI-approved SCR was connected to a keypad that was not PCI-approved):

- The use of such mechanisms to collect PCI payment-card data could mean that more PCI DSS requirements are now applicable for the merchant.

The PAX S500 is capable of supporting multiple PIN pads. However, the only PIN pad supported by Bluefin as part of its P2PE compliant program is the PAX SP20. Any other PIN pad devices, including PAX manufactured devices, and 3rd party devices, are not to be used in conjunction with Bluefin’s P2PE program.

**Do not change or attempt to change device configurations or settings.**

Changing or attempting to change device configurations or settings will invalidate the PCI-approved P2PE solution in its entirety. Examples include, but are not limited to:

- Attempting to enable any device interfaces or data-capture mechanisms that were disabled on the P2PE solution POI device
- Attempting to alter security configurations or authentication controls
- Physically opening the device
- Attempting to install applications onto the device
As per the PCI guidance, merchants are not allowed to add or update applications on the PAX P2PE devices. All new applications or application updates will exclusively be uploaded to the PAX BroadPOS system. Merchants may download approved applications and application updates from the BroadPOS system as they are made available.

Because of the controls over the BroadPOS system that are administered by Bluefin, merchants and end-users are not able to update or modify existing applications to disable encryption functionality and furthermore are not able to load altered or foreign applications that would disable encryption functionality.

The PAX BroadPOS terminal management system does not allow for any customization to settings in the payment application(s) that could disable encryption or other security features. Furthermore, full administrative access to the PAX BroadPOS terminal management system is limited to Bluefin Payment System personnel exclusively per P2PE guidance that can be found in Domain 1 of the P2PE standard. The PAX BroadPOS terminal management system does support unapproved remote application downloads to the merchant’s PAX S500 by the end-users; instead, only reviewed and approved applications provided by PAX and loaded into the PAX BroadPOS system can be uploaded to the distribution system for merchant download. For security purposes, all application loads to the PAX S500 exclusively come via BroadPOS, and those applications must be signed by PAX, and properly authenticated.

For more information on the security around application loading, please see the PAX S500 security policy, found at this link https://www.pcisecuritystandards.org/ptsdocs/PAX%204-40151%20Security%20Policy%2012114.pdf

3.1 Installation and Connection Instructions

Physical Connection Type Supported from the device:
Micro, RS232, RJ 45 Ethernet, RJ11 phone

Physical connection method to the host machine:
Devices should be directly plugged into the host computer / device for USB and RS232 connectors. Ethernet or modem connections should follow whatever the appropriate network usage guidance is for the merchant’s organization.

Physical connection method to the PAX S500 device:
All data connections and power connections come into the device via a detachable cable utilizing either an RJ45 or RJ11 or Micro USB connector.

Non-physical connection methods:
The PAX S500 devices do not support Bluetooth or WiFi connections.

Activation instructions:
This device requires no special actions to activate the device outside of the standard P2PE device activation practices covered in the PIM sections 3.1 and 4.2. Your point of sale software provider may require additional actions, but no actions are required by Bluefin.
**Additional instructions:**
For any additional instructions for the installation of the POI device, please reference any guidance from the hardware manufacturer. Additionally reference any guidance provided to you by the hardware or application software provider of your point of sale device.

Hardware mounting guidance can be obtained from the device manufacturer, PAX.

5.1 Instructions for physically inspecting POI devices and preventing skimming, including instructions and contact details for reporting any suspicious activity


**Visual Inspection**

**Top of device**
Housing inspection: Your device should fit together snugly. There should be no uneven gaps in the housing, or major scrapes or gouges that may indicate tool marks. Small blemishes are to be expected with the device over time, and concern should only be given to major physical damages in the housing where seals and seems in the device are. Other than the slat for swiping the card and a small slat on the bottom of the device, there should be no additional holes or slats found on the device.

Front of device
The EMV slot is located on the lower front end of the device. Please inspect it to make sure that no foreign devices are attached or inserted, and ensure that the area if free of any obvious tamper marks such as tool marks.
Seal inspection: The bottom of the S500 contains the data connection ports. No additional openings or holes into the device other than those pictured should be present on the device.

Left side of device
The left side of the device features a micro USB connection port. The USB port is not used in the Bluefin P2PE solution.
Connection inspection: The S500 supports numerous data connection and networking options.

**LINE + PHONE**: Supports RJ11 phone line connection into the device via the LINE, and then an additional connection via the PHONE port that allows an existing phone to still be connected.

**LAN**: Supports network connection via RJ45 connector.

**PIN PAD**: Supports connection via XXXXXX connector to optional PIN pad.

**RS232**: Supports connection via RJ11 to a RS232 serial adapter.

---

**Connection from the S500**

Connection Inspection:

The S500 can be plugged into phone lines via RJ11 male adapters, networks via RJ45 male adapters, and serial ports via RS232 female adapters.

*RJ11 with RS232 adapter show for reference.
**Weight Verification**

Weight verification: In the event that the merchant would like to verify the weight of their device as a method of tamper investigation, the following weight information is provided. Please keep in mind that the listed device weight does not include attachment cables, or accessories. The device should weigh approximately 455 grams according to factory specifications. To improve accuracy in documentation, it is suggested that when the unit arrives and is first deployed, the weight of the device should be recorded and compared against the factory specification. The device should be weighed on a postal scale or similar device, with both the POI unit and cord resting fully on the scale. Over time the device weight may fluctuate slightly, but any noticeable weight increase could be an indicator that the device has been tampered with, and that the device may contain additional malicious hardware in it.

---

**Application Interface**

The PAX S500 can be loaded with one of four different applications. Two of the applications are intended to be used to run the device in “stand-alone” mode, meaning that a merchant can run the device and process payments without being connected to a point of sale or host device.

The PAX S500 can also be loaded with two versions of the application for “semi-integrated” mode, meaning that a merchant must attach the device to a point of sale system or host device in order to get the S500 to perform transaction activities.

---

The PAX S500 with stand-alone application

Includes application versions:
- Bluefin-HC-Retail-S500
- Bluefin-Bluefin-HC-Restaurant-S500

The PAX S500 with both versions of the stand-alone application does not support inputs or outputs with a POS or other host machine in the merchant environment. All application commands are done via the onboard application in the device utilizing the physical keys of the device and the devices’ LCD screen.

---

The PAX S500 with semi-integrated application

Includes application versions:
- Bluefin-HC-Retail-S500-Integration
- Bluefin-HC-Restaurant-S500-Integration

Both versions of the PAX S500 support inputs and outputs with point of sale systems or other host devices in the merchant environment.

Guidance for taking the output of the PAX S500 and formatting it for use with Bluefin’s PayConex gateway interface can be obtained by emailing integrations@bluefin.com. Guidance for usage and
formatting of third party gateways or services that utilize Bluefin’s Decryptx product can be provided by the third party service provider. Merchants unsure of their third party provider can contact a Bluefin representative via the contact information provide in the main PIM document in section 1.2. An overview of supported transactions can be found in this document.

In order to keep P2PE compliance, all cardholder data (PAN) must be exclusively entered into the device via existing supported card holder data methods. These methods include keyed entry, swipe entry, and access via the EMV slot. All other methods of transferring card holder data (PAN) into the device are prohibited and unsupported.
PAX S300/500 Semi-Integrated Application Supported Transactions

Summary
For P2PE solutions using a semi-integrated application build on either the PAX S500 or S300, please use the following guide to help identify the supported transactions that can be sent to the device. The document below outlines the supported inputs and outputs supported by the application.

For additional application integration guidance, please reference the Bluefin PAX integration guide.

ECR/POS Inputs
The following request parameters are available via the PAX S300 & S500 devices running the Bluefin Retail Restaurant semi-integrated application:

- **Tender Type** – Credit, Debit, EBT
- **Trans Type** – Sale, Auth, Return, Inquiry, Void Sale, Void Auth
- **Amount** – US dollars and cents in format “00.00”
- **Cashback Amt** – US dollars and cents in format “00.00”
- **Clerk ID** – not used
- **Zip** – 9 digit numeric
- **Tip Amt** – not used, US dollars and cents in format “00.00”
- **Tax Amt** – not used, US dollars and cents in format “00.00”
- **Street** – not used, alphanumeric
- **Surcharge Amt** – not used, US dollars and cents in format “00.00”
- **PO Num** – not used, numeric
- **OrigRefNum** – not used, numeric
- **InvNum** – not used, numeric
- **ECRRefNum** – set to “1”, numeric
- **AuthCode** – not used, numeric

- **ExtData** – 56k varchar field. This field should be used to pass properly formatted XML data to Bluefin custom_data in adherence with Bluefin’s API. Please refer to the Bluefin API for data formats/values for the API parameters listed below. The acceptable Bluefin Data parameters are to be passed within an opening and closing <PAX> tag.
<table>
<thead>
<tr>
<th>group</th>
<th>transaction_description</th>
<th>custom_id</th>
<th>cashier</th>
<th>first_name</th>
<th>last_name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>street_address1</td>
<td>street_address2</td>
<td>city</td>
<td>state</td>
<td>zip</td>
</tr>
<tr>
<td></td>
<td>country</td>
<td>phone</td>
<td>email</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>transaction_id</td>
<td>allow_partial</td>
<td>ip_address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>level2_tax</td>
<td>level2_zip</td>
<td>level2_order_id</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>level2_merchant_reference</td>
<td>send_customer_receipt</td>
<td>send_merchant_receipt</td>
<td>restaurant_server_id</td>
<td>restaurant_gratuity</td>
</tr>
<tr>
<td></td>
<td>disable_avs</td>
<td>disabled_cvv</td>
<td>disable_fraudfirewall</td>
<td>payment_type</td>
<td>installment_number</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>install_count</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>success_url</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>decline_url</td>
</tr>
</tbody>
</table>

Sample XML Pass through data from PAX’s ExtData to Bluefin’s custom_data field:

```xml
<PAX>
  <group/>
  <transaction_description>This is a test</transaction_description>
  <custom_id>123456</custom_id>
  <custom_data>Custom Data Goes Here</custom_data>
</PAX>
```
<cashier>JOK</cashier>

<first_name>Test</first_name>

<last_name>PAXstuff</last_name>

<street_address1>123 Test Street</street_address1>

<street_address2>APT 2</street_address2>

<city>Tulsa</city>

<state>OK</state>

<zip>12345</zip>

<country>US</country>

<phone>555-555-5555</phone>

<email>test@test.com</email>

<transaction_id></transaction_id>

<allow_partial>0</allow_partial>

<ip_address>12.34.56.78</ip_address>

<level2_tax>0.00</level2_tax>

<level2_zip>12345</level2_zip>

<level2_order_id>1111</level2_order_id>

<level2_merchant_reference>Level2 Stuff</level2_merchant_reference>

<send_customer_receipt>0</send_customer_receipt>

<send_merchant_receipt>0</send_merchant_receipt>

<restaurant_server_id>333</restaurant_server_id>

<restaurant_gratuity>0.00</restaurant_gratuity>

<disable_avs>0</disable_avs>

<disabled_cvv>0</disabled_cvv>

<disable_fraudfirewall>0</disable_fraudfirewall>
<payment_type></payment_type>

<installment_number>1</installment_number>

<installment_count>10</installment_count>

<success_url>http://www.google.com</success_url>

<decline_url>http://www.yahoo.com</decline_url>

<zip>12345</zip>

<custom_data>asdlkfjslkdjalskdjalskdjal</custom_data>

</PAX>

Notes

1. On both devices, a max buffer size of 2076 bytes is enforced. In the device ExtData request, any XML data in excess of 2076 bytes will cause a MAXIMUM SIZE EXCEED error returned back to the ECR/POS.

2. In the ExtData, Additional Information Subgroup, the request of Orig PAN and Orig Expiry Date are NOT ALLOWED and will return an error to the ECR/POS.

Device Outputs

The following are the response parameters from the PAX S500 & S300 semi-integrated applications:

- Result Code
- Result Txt
- AuthCode
- Approved Amt
- AvsResponse
- BogusAccountNum
- CardType
- CvResponse
- Host Code
- Host Response
- Message
RefNum

Remaining Balance

Extra Balance

Requested Amt

Timestamp

ExtData -- The ExtData response yields additional data elements in XML format. They are as follows:

```xml
<PLCardPresent>0</PLCardPresent>
<PLEntryMode>1</PLEntryMode>
<PLNameOnCard>TEST/BLUEFIN</PLNameOnCard>
<AmountDue>0</AmountDue>
<TipAmount>0</TipAmount>
<CashBackAmount>0</CashBackAmount>
<MerchantFee>0</MerchantFee>
<TaxAmount>0</TaxAmount>
<ExpDate>1222</ExpDate>
<ECRRefNum>1</ECRRefNum>
<BatchNum>1</BatchNum>
<CARDBIN>370000</CARDBIN>
```

Upon receipt of the request, and prior to the response, Bluefin posts the following data elements to its PayConex system:

- Transaction ID
- Issue Date/Time
- Terminal Type
- Payment Type
- Transaction Type
- Amount
- Auth Message
- Auth Code
AVS Result
Payment Issuer
Card Number
Card Expiration Date
Billing Address Name
Billing Address Street
Billing Address City
Billing Address State
Billing Address Zip
Billing Address Country
Customer Phone
Customer Email
Company
Cashier
Remote IP Address
Remote Host Name
Batch ID
Batch Date
Trace Number
Group
Custom ID

Description
Custom Data