Contents
Introduction .................................................................................................................................................. 5
The Bluefin POI Management Application Overview ............................................................................... 7
  Merchant Setup ...................................................................................................................................... 7
  Merchant Users .................................................................................................................................... 7
  Locations .............................................................................................................................................. 7
  Shipments ............................................................................................................................................ 7
  Device management ............................................................................................................................... 7
  Device status changes ............................................................................................................................ 8
Audit tools .................................................................................................................................................. 8
Unit ordering request form ....................................................................................................................... 8
Contact / Support form ............................................................................................................................ 8
Your Device ............................................................................................................................................... 9
  Understanding device statuses ............................................................................................................... 9
    Deployed state .................................................................................................................................. 9
    Awaiting deployment state .................................................................................................................. 9
    Repair .............................................................................................................................................. 9
    Transit ............................................................................................................................................ 10
    Storage ........................................................................................................................................... 10
    Retired ........................................................................................................................................... 10
    Lost ................................................................................................................................................ 10
    Destroyed ....................................................................................................................................... 10
    Tampered ....................................................................................................................................... 10
    Refused ........................................................................................................................................ 10
Device ordering procedures ...................................................................................................................... 11
Device receiving procedures ..................................................................................................................... 11
Device storage procedures ....................................................................................................................... 17
  Secure storage options ......................................................................................................................... 17
  Secure storage access management ...................................................................................................... 17
  Secure storage logging .......................................................................................................................... 18
Device deployment procedures .................................................................................................................. 18
Authorizing devices ................................................................................................................................. 18
Introduction

The purpose of this document is to provide merchants with a clear understanding of the Bluefin P2PE solution. In order to gain the full benefits of scope reduction it’s important that the merchant understands their obligation to the P2PE process.

Specifically, this P2PE Implementation Manual (PIM) fulfills Bluefin’s responsibility to direct merchants in their effort to properly implement Bluefin’s Validated P2PE Solution in pursuance of completing the SAQ P2PE-HW which was developed to address requirements applicable to merchants who process cardholder data (CHD) only via hardware payment terminals included in a validated PCI SSC-listed PCI Point-to-Point Encryption (P2PE) Solution.

SAQ P2PE-HW merchants are defined as stated in the Payment Card Industry (PCI) Data Security Standard (DSS) Self-Assessment Questionnaire (SAQ) P2PE-HW Version 2.0, which is downloadable at http://www.pcisecuritystandards.org/ as the following:

SAQ P2PE-HW Merchants do not have access to clear-text cardholder data on any computer system and only enter account data via hardware payment terminals from a PCI SSC-approved P2PE solution. SAQ P2PE-merchants may be either brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants. For example, a mail/telephone-order merchant could be eligible for SAQ P2PE if they receive cardholder data on paper or over a telephone, and key it directly into a validated P2PE hardware device.

These merchants validate compliance by completing SAQ P2PE-HW and the associated Attestation of Compliance (AOC), confirming that:

- Your company does not store, process, or transmit any cardholder data on any system or electronic media (for example, on computers, portable disks, or audio recordings) outside of the hardware payment terminal used as part of a validated PCI P2PE solution.
- Your company has confirmed that the implemented PCI P2PE solution is listed on the PCI SSC’s List of Validated P2PE Solutions
- Your company does not store any cardholder data in electronic format, including no legacy storage of cardholder data from prior payment devices or systems, and
- Your company has implement all controls in this Bluefin Payment Systems P2PE Instruction Manual (PIM)

Additionally, you must maintain full compliance with the controls described in the current SAQ P2PE-HW at all times, and you recognize that if any changes are made to your P2PE environment, or if you accept cards in a method not covered by this P2PE solution, you must reassess your eligibility for the SAQ P2PE-HW and refer to your acquirer and/or payment brand for requirements for filing a new and perhaps different SAQ.
P2PE’s security foundation is built on two major components. The first is the secure encryption and decryption of data to ensure that data that is encrypted at the point of entry and remains encrypted until decrypted by Bluefin for processing. The second component is a strong chain of custody, and adherence to proper safety techniques and practices.

In this document you will learn about Bluefin’s management application that will assist in making the chain of custody documentation much easier, and will expedite complex and laborious tasks such as annual audits.

You will find step-by-step instructions that will walk you through the entire process from order delivery to the end-of-life (EOL) cycle for your P2PE solution.
The Bluefin POI Management Application Overview

The Bluefin POI (point-of-interaction) Management Application was designed to offer merchants an easy-to-use tool to help administer their own P2PE activities to help ensure compliance that will allow them to get the full benefits of PCI P2PE scope reduction. To access this website, the user will go to http://poimanager.payconex.net/. The major components of the application are listed below. As you go through the document, each of these components will be discussed in more detail.

**Merchant Setup**
Once a merchant is setup with Bluefin to use the P2PE program, a Bluefin representative will setup the merchant’s company profile in the application.

**Merchant Users**
The merchant will have the ability to designate key employees who will have access to the P2PE POI Management Application, and who will be permitted to conduct P2PE activities on behalf of the merchant. Shared username and passwords are expressly not allowed. Each unique user who will manage the POI devices should have their own unique account. Shared accounts are prohibited and it is the responsibility of the merchant to enforce by both security policy and internal management/audit. User accountability is a key component of the integrity of this solution. This feature of the security continuum answers the question of “who” interacts with or moves the POI.

**Locations**
Locations are an important part of the P2PE chain of custody process. Locations can be setup in the system either by a Bluefin employee, or by the merchant. Devices may only be transported and deployed from locations that are officially designated and approved by the merchant. This feature of the security continuum answers the question of “where” the POI is in its life-cycle. Each location will also have to have a central contact person listed. That central contact person will be the primary addresses for shipments.

**Shipments**
When a unit is shipped from Bluefin’s key injection facility (KIF)(operated by SpencerTech) the device will officially be designated as “In Transit.” Merchant representatives will be able to see the shipment and status details once logged in the system, and will be able to view shipment details such as the shipment tracking number. The shipment information will also include a manifest of devices for the shipment. This feature of the security continuum protects the POI during its change of location.

**Device management**
At any given time a merchant will be able to see any POI unit that is assigned to their company, and see the status of the device.
**Device status changes**
The merchant will be able to administer the status of the device and use the device management screens to administer device states and assist in chain of custody activities.

**Audit tools**
Merchants will be able to take a snapshot of all their device statuses at the time of their annual internal audit which is required by the SAQ P2PE-HW. Additionally, merchants will be able to identify any unplanned excess or shortages of units and promptly notify Bluefin of said occurrences. In order to keep in compliance with P2PE regulations merchants will also be able to attest to the receipt and usage of the P2PE Instruction Manual (PIM).

**Unit ordering request form**
Merchant representatives will be able to request new units from Bluefin using this request form.

**Contact / Support form**
Merchant representatives will be able to request support from Bluefin using this request form.
Your Device

Your Bluefin P2PE payment solution utilizes two ID TECH SRED PTS 3.0 devices, the SecuRED™ and the SREDKey™. Throughout this document the device will either be identified by its product name (SecuRED or SREDKey), or by the general industry term as a Point of Interaction (POI) device.

Understanding device statuses

**Deployed state**
This device has been approved by the merchant to be in active use. Once a merchant marks a device as being deployed, it will be added to the list of approved devices that will be able to submit credit card data. Devices are identified and tracked by serial number. This number is printed on the tamper-evident bags, shipment boxes, and by output from the device itself. It is non-configurable and is part of the device integrity through its life-cycle. Any changes in serial number should prompt your systems as to a potential breach of security.

**Awaiting deployment state**
This state only applies to devices that have been issued by Bluefin, but are not yet in the hands of the merchant.

**Repair**
This state should be selected if a device needs to be removed from service for repair. Selection of this state will disable the device’s ability to submit cardholder data. Additionally selection of
this state will notify a Bluefin employee who will coordinate with the requesting merchant representative to have the device shipped to the proper facility for repair.

Transit
This state is used anytime that a device is in transit between locations. This state is not selectable by the merchant, but instead is designation that a device is involved in a shipment activity.

Storage
This state is used when a device is in possession of a merchant, but is not deployed. This state disables the device from being usable for submitting cardholder data to the Bluefin P2PE solution. Bluefin accepts/rejects transmission from a POI based on its status.

Retired
This state is used when a device will no longer be used by a merchant. If a merchant opts out of the P2PE program all of their units will automatically be switched to the retired state. If a merchant wishes to have fewer P2PE devices under their control, they may also select the retired state for said device. Retired devices are unable to submit cardholder data to the Bluefin P2PE solution.

Lost
This state is used when a merchant is unable to identify the location of their POI device. Lost devices are unable to submit cardholder data to the Bluefin P2PE solution. Additionally, this state will trigger an alert to a Bluefin employee who will assist the merchant in determining the best next-steps to resolve the issues associated with a lost POI device.

destroyed
In the event that a unit is destroyed or rendered inoperable due to physical harm to the POI device, this state should be selected. Destroyed devices are unable to submit cardholder data to the Bluefin P2PE solution. Additionally this state will trigger an alert to a Bluefin employee who will assist the merchant in determining the best next-steps to resolve the issues associated with a destroyed device.

Tampered
In the event that a merchant believes that a P2PE POI device has been tampered with, selecting this state will immediately remove the device’s ability to submit cardholder data to the Bluefin P2PE solution. Additionally, this state will trigger an alert to a Bluefin employee who will assist the merchant in determining the best next-steps to resolve the issues associated with a tampered device.

Refused
A merchant may choose to refuse a shipment. In such a case the merchant would inform Bluefin of their decision through the POI management application to return the units in an
unopened condition. Incidents that would fall under this scenario would be when units are accidently ordered, or unit is lost by the carrier and turns up later.

Device ordering procedures

If additional units are needed you can place an order by contacting Bluefin at p2pesupport@bluefin.com or by phone at 800-675-6573. A Bluefin account representative will work with you to coordinate a shipment. Please note that unit orders can only be placed by merchant employees who are listed in the POI management application. If you are not listed in the application please coordinate with a senior member of your team who is listed as a company representative in the system in order to make your unit request.

Device receiving procedures

**Reviewing the status of your pending shipment**

Once a merchant receives confirmation that the order for their units has been submitted, within a few business days (once the order is prepared for shipment) the merchant will be able to log into the Bluefin POI Management System and review the status of their pending shipment. The merchant should review the serial numbers of the devices contained in the shipment and confirm the carrier and tracking number for the shipment, the destination location information, as well as the merchant representative whom the order is targeted for.

**Review and inventory of your shipment**

When the responsible party at the merchant location takes possession of the shipment of POI devices they must log the confirmation of the receipt of those devices into Bluefin’s POI Management System.

Immediately, upon receipt the merchant should inspect the shipment box for major damage such as tears or holes, and must visually inspect that the packaging has not been re-taped or resealed.

The merchant representative should also visually inspect the contents of the shipment box which should contain the expected number of cardboard boxes which contain an outer sticker that indicates the serial number of each POI device.
Inside each of the cardboard boxes (as depicted above) the POI device should be contained within two packaging elements.

The outer element is a tamper-evident bag. This bag will be sealed with serialized sticker / tape. This sticker is a tamper-evident sticker.

If the sticker / tape has not been tampered with it should look like the photo below. Minor evidence of potential tampering with the sticker (rumpling or minor stretching) may occur while the box is in transit.

If the sticker/tape has been removed or tampered with, the sticker may look like the image below.
If you see a sticker on the tamper-evident bag near this level of evidence you should consider the device as having been tampered with. Notice that the tamper sticker is in two parts, and the word “void” can clearly be seen.

Inside the tamper-evident bag is a plastic bubble wrap bag. This (reddish-clear) bag is used to ensure that the POI device is not damaged while being shipped. There are no tamper evident features of the plastic bubble wrap. That material exists to simply keep the product from breaking during shipment.

**Confirming receipt of your shipment**

The merchant will then be required to confirm their shipment order in the system by selecting the serial number of the POI and navigating to the receipt of shipment screen. Once on this screen the merchant representative will be required to attest to the receipt of each POI device. Proper attestation requires confirming the serial number of the device (found on a sticker on the cardboard packaging of the device box) and then opening the cardboard box and verifying the serial number from the tamper-evident bag. Please note that the tamper-evident bag SHOULD NOT BE OPENED UNTIL THE DEVICE IS IN THE FIELD LOCATION WHERE IT WILL BE DEPLOYED. This is important to preserve the tracking and chain of custody. Additionally, the merchant should keep the cardboard box that the device was shipped in as it will be the primary way in which a merchant can identify the serial number of the device without having to remove the device from the tamper-evident bag.

**Handling of devices that are Waiting Deployment**

If the merchant does not want the P2PE device to be immediately deployed, steps should be taken to physically secure the devices until their deployment. Devices should be kept in their cardboard box and should ABSOLUTELY not be removed from their
tamper-evident bag. Devices that are to be left unsupervised should be stored in a location with the most limited access possible. Suitable options include a locked desk, cabinet, closet, safe or other similar secured and enclosed space. Only approved merchant representatives should have access to the devices during this transition period.

**Handling of devices that are Waiting for Storage**

Devices that are intended for storage, but are awaiting transition to storage should follow the same protocols as handling devices awaiting deployment (see above).

**Handling of devices that are Waiting for Transit**

Devices that are intended for another location and are awaiting transit to another location should follow the same protocols as handling devices awaiting deployment (see above).

**Handling of devices that are immediately Stored**

Devices that are immediately stored should first be marked as accepted in the shipment receipt page. Upon attesting to receipt of the devices, the merchant representative should immediately place the devices in storage following the detailed storage instruction contained in this document.

**Handling of devices that are immediately Deployed**

Devices that are immediately placed into use should first be marked as accepted in the shipment receipt page within the POI Management Application. Upon attesting to receipt of the devices, the merchant representative should immediately place the devices in their deployment environment following the detailed deployment instruction contained in this document.

**FAQ about shipment receiving problems**

The following FAQ covers both inbound shipments from Bluefin and its partner Spencer Technologies, as well as internal shipments where the merchant is shipping a device from one approved company location to another approved company location.

All devices that are received by the merchant should come from existing shipments found within the Bluefin POI Management Application. If any shipments come from a source other than the originating location in the application, the merchant should identify those packages as being potentially malicious. The merchant should use the contact form in the Bluefin POI Management Application website to contact a Bluefin representative who can work with the
merchant to determine if the shipment was simply accidently shipped to the merchant without following proper shipment protocols or if the shipment is indeed malicious from a non-Bluefin source.

**Device is lost by carrier.**
**Device is never recovered.**

The merchant should go to the device list page and mark the unit as lost. The merchant will then need to coordinate a request for a unit to replace the lost unit.

**Device is lost by carrier.**
**Device is recovered by carrier in less than 10 business days from estimated delivery.**

Merchant and Bluefin employees are not required to take any action. They may wait for carrier to complete shipment.

**Device is lost by carrier.**
**Device is recovered by carrier, but after 10 business day from estimated delivery. External and tamper-evident packaging are intact.**

Merchant may use the Bluefin contact form to tell the Bluefin P2PE coordinator that their unit has arrived unopened.

The merchant should follow the standard device receipt process.

**Device is sent to the wrong location by carrier, or human error.**
**Device is returned to proper destination, external packaging intact. Tamper-evident packaging also intact.**

Merchant may use the Bluefin contact form to tell the Bluefin P2PE coordinator that their unit has arrived unopened.

The merchant should follow the standard device receipt process.

**Device is sent to the wrong location by carrier, or human error.**
**Device is returned to proper destination, external packaging damaged or opened. Tamper-evident packaging is intact.**

If tamper-evident packaging is unopened, it is a non-event.
Device is sent to the wrong location by carrier, or human error. 
Device is returned to proper destination, external packaging damaged or opened. Tamper-evident packaging is not intact.

Merchant verifies that the package is received. Once the device(s) is logged, it should be marked as a tampered device.

Device is received by merchant, but not signed for by designated addressee. 
Device is logged by designated addressee, and confirmation of tamper-evident is intact.

If tamper-evident packaging is unopened, it is a non-event, and no special action needs to be taken.

Device is received by merchant, but not signed for by designated addressee. 
Device is logged by designated addressee, and reports breakage of tamper-evident package.

As long as the receipt of the device is logged by a merchant representative who has an account in the Bluefin Mobile Payment application it is perfectly acceptable that another merchant employee takes initial receipt of the devices from the carrier.

Device is received by merchant, confirmed by carrier. 
Device is lost by merchant, and is recovered within 10 business days. 
External packaging is intact. Tamper-evident packaging is also intact.

Merchant and Bluefin employees are not required to take any unique responsive action. Devices should be marked as received immediately upon being found.

Device is received by merchant, confirmed by carrier. 
Device is lost by merchant, and is recovered within 10 business days. 
External packaging is not intact, tamper-evident packaging is intact.

This is a non-event if the tamper-evident packaging is still intact. Merchant and Bluefin employees are not required to take any unique responsive action. Devices should be marked as received immediately upon being found.
Device is received by merchant, confirmed by carrier.
Device is lost by merchant, and is recovered within 10 business days.
External packaging is not intact; tamper-evident packaging is also not intact.

Merchant verifies that the package is received. Once the device(s) is logged, it should be marked as a tampered device.

Device is received by merchant, but has illegible serial number information on the product packaging outside of the tamper-evident packaging.

If tamper-evident packaging is intact, and the device is in its deployment location, merchant staff member may fill out receipt of chain of custody based on serial number from device after it is removed from tamper-evident packaging.

If tamper-evident packaging is intact, and the device is its deployment and or storage location, merchant may open tamper-evident packaging, and retrieve the serial number from the device. Merchant may then reseal the package, affix a clear transparent piece of packing tape to the device and sign it with their signature. Signature must span both sides of the packaging being taped back together, and be large enough that any cut or tear to open the bag would cut or tear the signature.

Device storage procedures

Secure storage options
Devices that are placed into secure storage should still be in the original tamper-evident serialized bag. However, if the unit has already been deployed and or is no longer in the original tamper-evident serialized bag, the unit should place in a new tamper-evident serialized bag. Tamper-evident serialized bag materials can be requested from Bluefin using the contact form.

The area / storage space should have the following attributes.

The units should be under some type of lock and key mechanism to ensure that access is strictly controlled.

Units can be placed in an unsecure location such as an unlocked filing cabinet, cabinet drawer or other semi-public space provided that the units are in a locked device such as a safe, lock box, locked storage tub, or similar construct.

Secure storage access management
When a device is placed into secure storage, access to the devices should be strictly controlled. Only authorized employees should be able to access the area / storage space where the devices are being kept.
Secure storage logging
During the time that the devices are in storage, a log should be kept of who has gained access to the area / storage space and who may have had the opportunity to come in contact with the device.

The log should include the employee’s name, the business reason for being in the area / storage space, the date, the time they entered the area, and the time they left the area. These logs should be maintained by the merchant for no less than one year.

Device deployment procedures

Authorizing devices

The first step in deploying a device is logging into the Bluefin POI Management Application and selecting your specific POI unit that you would like to activate. Click on DEVICES, and then select the device you would like to activate. Click on the EDIT button.

Next change the status of the device by clicking DEPLOY in the buttons at the top right of the page. Then click the large green SUBMIT button in the bottom left.

By changing the status you are authorizing the Bluefin P2PE solution to move your device to the approved device list, so once your unit is plugged in you will automatically be able to run P2PE transactions with that device without any device modifications or complicated device activation procedures. After you have run your first transaction across the device the state of the device will be show as ACTIVE.

Inspecting devices before deployment

Each device should be inspected before deployment. Upon removing from the tamper-evident packaging the merchant should inspect the device for any physical damage.

The device should be weighed to verify it is within the factory specs for weight.

The device connectors and or cables should be inspected for modifications or damage.

The serial number on the device should be verified.

The device should be free of stickers other than the stickers listed in the device description.

Please see the detailed inspection instructions further in the document on inspections that should be done when deploying a device to a retail or call center environment. Also please note the instructions on inspections you should do if the device will be placed into storage.
**Initial transaction**

Please note that the device must be updated in the Bluefin POI Management Application as being “deployed” prior to the device actually being deployed. If this action has not occurred, the device will not be able to process a transaction with the Bluefin P2PE solution.

Merchants at their own discretion may choose to run a test transaction for their first transaction with the device. Merchants could make a purchase through their POS system, and upon successful processing of the card verify that both the device and the merchants POS system are setup properly. Merchants at their own discretion could then perform a refund on the transaction if they so desired.

**Physical deployment best practices**

Please note that modification to the device such as attachment of adhesives, cable locks, or other add on hardware while not banned by the P2PE specifications can have negative impacts when conducting tamper evidence inspections. Merchants should not permanently attach anything to the main unit of their POI device.

Merchants can explore using cable lock systems, or even cable staples / fasteners to ensure that the device is not easily pulled free. The use of systems like this does not modify the device or in any way impede visual inspection. Keep in mind that the devices will need to be periodically weighed, so any fasters should be removable.

Devices should be placed in a low access yet high visibility area. For example in a retail environment the unit should be placed on the counter where it can be observed, but not so close to the customers where the customer could gain easy access to manipulate the device without supervision. For a call center type environment the device should be placed on a desk where it’s not obstructed by desktop clutter, and should not be placed in such a manner where people other than the individual responsible for the device can get convenient access to the POI device.

Devices should be plugged directly into the primary computer, point of sale device, or mobile device, which will be running the payment application. Devices should never be run through the USB hubs, cable extenders, daisy chained with other USB connections, or attached to any other device other than the primary device.

Merchants should take steps to ensure a level of protection with their devices when left unattended for long periods of time. Methods could include, but are not limited to securing corded devices via their cords, locking up the POI separately in the evenings, or ensuring the devices remain under video monitoring.

**Device handling when used with a mobile solution**
Special care should be taken in the deployment of mobile POI devices. Whenever possible, do not let the mobile POI out of your hand, and do perform the swiping yourself to reduce the instance of POI tampering or theft. If you must allow the cardholder to directly interact with the POI, never let the device out of your sight or presence and remain with the cardholder at all times during the interaction. Once you have the POI back in your hands, visually inspect that the POI swiper is still present and attached firmly. Also, inspect that the POI swiper is the same device that was on the unit when handed to the cardholder to prevent device substitution.

Mobile POI devices will not accommodate any sort of physical fasteners since they are not corded devices. Because of this care should be taken in the deployment environment with the POI units. Merchants should consider having a lockable area where the unit could be stored for a short period of time, or merchant should ensure that the unit will be in view of a camera system to ensure that unauthorized access of the device is captured.

**Practices to avoid**

Merchants must ensure that the following activities do not occur with their POI devices. If the following activities are performed on a POI device, the merchant runs the risk of losing their P2PE scope reduction qualification.

- Do not physically open the device. Doing so can result in the encryption keys in the device being destroyed, and the device being rendered inoperable.
- Do not attempt to install any applications, or data on the device.
- Do not attempt to alter any security configurations or authentication controls
- Do not attempt to interface with the device with the intent of modify any device interfaces, or data capture mechanisms.
Understanding the automated device protection services

The Bluefin P2PE solution features several automated safeguards to help ensure the safety and security of our merchant’s credit card date. When these automated protective services are engaged, it can lead to temporary or permanent deactivation of your device. These actions are done to protect your organization from the liability that could occur with the loss of card holder data. There are two automated protection scenarios are listed below.

Card holder data protection

Credit card numbers are often referred to as the primary account number or PAN. Bluefin’s P2PE solution is designed to protect again PAN data ever being improperly displayed. P2PE is built on the principle that PAN data is encrypted in the POI device prior to the data entering the merchant’s computer or device. In the event that a device is ever tampered with a common tactic that is seen is that the POI device is modified to transmit PAN data in the clear. The Bluefin POI management application is able to detect if there is every any unencrypted PAN data, and if there is, it immediately deactivate the POI device so that is no longer able to run transactions. This even also causes an alert to a Bluefin account manager who will contact the impacted merchant to arrange for the remove of the device.

Data irregularity

Data irregularity can sometimes be an indicator that tampering may have occurred. Bluefin’s POI management application is constantly surveying the data output from the POI units to make sure that the formatting and structure of the data is within expectations. In the event that data falls outside of expectation, an email alert is sent to a Bluefin employee who will manually review the output of the POI device in question. Should that device be deemed problematic, a Bluefin employee will then mark the device as tampered and remove it from being able to run transactions. If such a decision is made a Bluefin employee will immediately contact the merchant and coordinate a replacement for the POI unit.
Annual Audit

Each year, prior to the annual anniversary of the merchant becoming enrolled in the Bluefin P2PE solution, the merchant will be required to complete a self-audit of all the units associated with the merchants account. The audit will consist of two activities. The first is an accurate inventory of all devices associated with a merchant. The second is an annual attestation that the content of Bluefin’s P2PE Instruction Manual (PIM) have been reviewed and followed throughout the year.

Device inventory

The merchant will need to go into the annual audit screen, and attest to the devices listed. If any of the devices are listed in the wrong location or with the wrong state, the merchant will need to update the state of the device.

Once all devices have been attested to, and all appropriate actions have been taken to assure the greatest level of accuracy in the attestation, the merchant can mark that inventory audit as being complete and that audit will then be stored in the system and serve as a document of record for inventory audit.

Confirmation of P2PE Instruction Manual Adherence

For the annual attestation of adherence to the PIM the merchant will be able to view the PDF of the current PIM associated with their account, and then click to confirm that they are familiar with the contents of the PIM and that they have followed the procedures that are contained in it.

Handling audit discrepancies

Additional units – In the event that a merchant has more units than listed in the audit inventory screen the merchant will be able to log the serial number of the extra devices in their audit. Merchants who have additional units beyond the units assigned to them maybe have a the threat of a malicious device. These devices should be removed from service immediately. Coordination should be done with Bluefin to assure that the devices were not a simple undocumented over allocation to the merchant. If after research the issue a chain of custody for the devices cannot be established, the units should be treated as tampered unit.

Missing units – In the event that a merchant is unable to produce a unit at the time of the audit deadline, the units should be marked as lost.
**Status changes** – If a device has inaccurate information for its current device state, the merchant may update the state in the same manner that state updates are normally done.

**Location changes** - If a device has inaccurate information for its current device location, the merchant may update the location in the same manner that state updates are normally done.

**Substituted devices** – If the merchant has the correct number of units, but certain serial numbers do not match the anticipated serial numbers the device(s) in question should be treated as possible malicious device. These devices should be removed from service immediately. Coordination should be done with Bluefin to assure that the devices were not a simple undocumented over allocation to the merchant. If after research the issue a chain of custody for the devices cannot be established, the units should be treated as tampered unit.
Security Practices

Security practices for device Inspection for non-deployed devices kept in storage

Devices that are in storage should be inspected once a quarter. Devices designated for storage should be left in their individual boxes. The outside of the box should contain a product description sticker that also includes the serial number of the device. Please note that it is unlikely that the serial number of the device can be read through the tamper-evident serialized bag, and the device should not be removed from the bag until deployment.

To perform a quarterly inspection the merchant should follow these steps.

1. Merchants should log into the Bluefin POI Management Application and verify the serial number that should be on the serialized bag.
2. Merchants should also verify the serial number of the device.
3. Devices in storage should be checked to verify that both serial numbers match the serial numbers on record for the devices.
4. Opening the unit box, and damage to the box itself is acceptable.
5. The tamper-evident serialized bags should be free of visual indicators of tears, punctures, cuts, and stretch marks. The tamper-evident adhesive should have no major signs of having been opened / removed / modified.
Security practices for device inspection for deployed devices in a retail or customer service environments

Devices deployed in retail or customer service environment should be inspected every 90 days. The merchant should keep their own logs that detail the inspection date, and the individual responsible for the inspection. These logs are for the merchant’s own record keeping to help in troubleshooting whether or not a device has been tampered with.

Inspection Procedures for ID TECH SecuRED™:

1. Visual Device Confirmation: Your merchant account has been setup to use the ID TECH SecuRED device. Your device should look like the device below. If your device does not resemble the device below you may have a device substitution.

Fig 2. SecuRED POI device profile photo
2. **Connection Inspection**: The cable leading from the device should have no additional cables grafted to it. There should be a single cable that terminates into a standard male USB connector. Please see the photo below for reference. If any additional devices are connected to the USB connector in between the POI device and the computer / device being used for data entry you may have a malicious device.

**Fig 3. SecuRED USB connector photo**

![SecuRED USB connector photo](image)

**Fig 4. SecuRED USB connector attached to SecuRED device photo**

![SecuRED USB connector attached to SecuRED device photo](image)
3. 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.

Fig 5. SecuRED POI front of unit device photo.
Fig6. SecuRED POI close up view of the front of the device.
Fig 7. SecuRED POI close up view of the back of the device.
4. Seal inspection: The bottom of the SREDKey is the major point of entry into the device. Please note the placement of the two stickers on the device. Sticker #1 covers a screw hole at the bottom of the device near the rear (the proximity of the cord connector indicates the rear portion of the device.) Sticker #2 runs the width of the device and covers a slit at the bottom of the device. If any of these stickers appears to have been previously removed your device may have been tampered with. Additionally the screws found in the base of the device are all matte black Phillips head screws. Any screws with a different head or material cover may be an indicator of a tampered device. There should be no additional stickers on the device. Additional stickers should be removed, and the area under the sticker inspected for damage. Please see the photo below.

5. Fig 8. SecuRED POI device bottom of unit photo

6. Weight verification: The device should weight approximately 123 grams (4.4 ounces) according to factory specifications. When the unit arrives and is first deployed the weight of the device should be recorded and compared against the factory specification. 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 hardware in it.
Inspection Procedures for ID TECH SREDKey™:

1. Visual Device Confirmation: Your merchant account has been setup to use the ID TECH SREDKey device. Your device should look like the device below. If your device does not resemble the device below you may have a device substitution.

Fig 2. SREDKey POI device profile photo
2. Connection Inspection: The cable leading from the device should have no additional cables grafted to it. There should be a single cable that terminates into a standard male USB connector. Please see the photo below for reference. If any additional devices are connected to the USB connector in between the POI device and the computer / device being used for data entry you may have a malicious device.

Fig 3. SREDKey USB connector photo

Fig 4. SREDKey USB connector attached to SREDKey device photo
3. Housing inspection: Your device should fit together snuggly. 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.

Fig 5. SREDKey POI side of unit device photo.
Fig6. SecuRED POI close up view of the front of the device.
Fig 7. SREDKey POI close up view of the back of the device.
4. Seal inspection: The bottom of the POI is the major point of entry into the device. Please note the placement of the two stickers on the device. Sticker #1 covers a screw hole at the bottom of the device near the rear (the proximity of the cord connector indicates the rear portion of the device.) Sticker #2 covers a recessed area at the bottom of the device. If any of these stickers appears to have been previously removed your device may have been tampered with. Additionally the screws found in the base of the device are all matte black Phillips head screws. Any screws with a different head or material cover may be an indicator of a tampered device. There should be no additional stickers on the device. Additional stickers should be removed, and the area under the sticker inspected for damage. Please see the photo below.

Fig 8. SREDKey POI device bottom of unit photo
5. Weight verification: The device should weight approximately 264 grams (9.3 ounces) according to factory specifications. When the unit arrives and is first deployed the weight of the device should be recorded and compared against the factory specification. 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 hardware in it.
Security practices for device inspection for deployed devices in a remote or unattended locations

Merchants may choose to deploy POI devices in conjunction with remote or unattended locations. In these scenarios the merchant should take steps to ensure that devices are inspected as frequently as possible, and that tamper tracking techniques such as cameras are used to track the status and interaction people have with the device.

Security practices in the event that a device has been tampered with

In the event that the merchant strongly believes that their device has been tampered with the following steps should be followed.

1. A merchant representative should log into the Bluefin POI Management Application, locate the impacted device by its serial number, and change the device status to “tampered.” Please note, that by performing this action the device will be moved to the “banned” list of POI units and will be unable to capture and send credit card data.
2. Merchants should then physically unplug the device, and remove it from the area in which the device was used immediately.

The device should be placed in a tamper-evident serialized bag, or if that is not available the device should be wrapped in a clear Ziploc style bag. The top of the Ziploc bag should be rolled several times to prevent it from easily being unrolled and then secured with packing tape. That packing tape should then be signed with a sharpie marker with the name of the merchant representative who removed the device as well as dated.

The device should then be stored in a locked area (filing cabinet, secure storage room, etc...) until shipping instructions are provided by Bluefin.

3. Devices will be returned to the custody of Bluefin or its representatives where they will be subjected to inspection, and if warranted additional forensics will be conducted and or the unit will be destroyed. Specific shipping instructions will be provided by a Bluefin account representative at the time of the incident.
4. Merchants will need to coordinate with their Bluefin representative to secure a replacement unit.

Security practices for shipping devices between locations

Merchants are responsible for ensuring that when devices in their custody are in transit that proper chain of custody controls are put in place. For the purposes of this document transit is defined as when a merchant ships a device from one physical location to another physical
location through the means of a trusted courier. P2PE policies require that shipments be considered transit, and as such should be tracked.

Approved merchant representatives can access the Bluefin POI management application website and can create a new shipment if a device needs to be move from one approved merchant location to another. The merchant will need to make sure that both the origin location and the destination location are preexisting locations in the system prior to setting up the shipment.

When the shipment screen has been accessed the merchant will be able to see the devices that are at the current location, and select from those devices for the shipment. Once the units are assigned to the shipment, the merchant can pick the destination from previously created destination. Once this process has been completed the merchant can then go in and update the shipment information with the shipment details (carrier name, and tracking number) and then complete the shipment process.

Devices should be in a tamper-evident bag, either in the original serialized bag the device was shipped in from Bluefin, or in a tamper-evident bag selected by the merchant.

Upon receipt merchants should follow the standard receipt process used for the initial receipt of the devices.

Security practices for transporting devices between merchant locations

Devices in the custody of approved merchant representatives may be moved from location to location while under the direct supervision of an approved merchant representative if the device is sealed in tamper-evident serialized packaging.

Security practices when granting third party access to devices

Bluefin will never send a Bluefin employee or subcontractor employee to a merchant’s location to inspect / repair / remove devices without first contacting the merchant representatives listed in the POI Management Application for that specific location where the device is located.

If a merchant receives a communication from someone claiming to be a Bluefin employee and the merchant has doubts as to the validity of that representative the merchant can contact Bluefin’s main customer service line at 800-675-6573 and ask to be connected to a member of the tech support team. The team member should be able to confirm the validity of the representative who requested access to the merchant and their POI devices.

If the representative cannot be confirmed, then access to the merchant’s facility and POI devices should be denied by the merchant.
If the merchant is sure that the representative is a confirmed representative of Bluefin the merchant can make preparations for the representative to visit their facility. During the course of the visit the representative should be accompanied throughout their travel in the building.

The merchant should keep a log of any onsite visits by a Bluefin representative or one of its contracting representatives. The log should contain the name of the representative who visits, their contact phone number, contact email address, their company name, the date of their visit, the time they arrived and the time they departed. These logs should be saved for a period of up to one year.
Firmware Updates

Factory firmware updates

The ID Tech SecuRED and SREDKey devices are only updatable via administrative controls at Bluefin vendor facilities. In the event that a firmware upgrade is required the device will need to be shipped to the vendor location.

For such shipping events the encryption key will need to be removed from the device. In order to remove the key the merchant will have to trigger a tampering activity with the device. The best way to do this with either ID Tech POI device is to loosen the sticker covering a screw on the bottom of the unit. The merchant will need to use a precision screwdriver and turn the screw until the point it becomes nearly loose from the device. The merchant will then need to tighten the screw to ensure the screw does not become lost. After completing this action, the unit will enter tamper mode, which will reset the device to factory settings and remove the encryption key. Removal of the key will render the device inoperable.

Before doing this action, merchants should be sure that they have coordinated this activity with their Bluefin account manager in order to ensure that replacement units can be shipped to the merchant to help ensure that the merchant experiences no transaction processing downtime.

The merchant will then need to log into the Bluefin POI Management Application, and mark the status of the device as repair. Please note that performing this action will remove the device from the list of approved devices that are permitted to send transaction details to Bluefin’s P2PE solution.

The merchant will then need to follow the return unit instructions found in this document.

Returning retired units

If a unit is set to be retired because it is being replaced, no longer needed or the merchant is leaving the Bluefin P2PE program, the following steps should be taken.

1. Remove the unit from service
2. Update the device status in the Bluefin POI Management Application and mark the unit as retired. This status change will disable the device from being used as part of the Bluefin P2PE solution.
3. Coordinate with your Bluefin account representative to get the necessary packaging materials to return the unit.
4. In order to remove the key the merchant will have to trigger a tampering activity with the device. The best way to do this with an ID TECH SecuRED device is to loosen the sticker covering a screw on the bottom of the unit. (see photo below) The merchant will need to use a precision screwdriver and turn the screw until the point it becomes nearly loose from the device. The merchant will then need to tighten the screw to ensure the screw does not become lost. After
completing this action, the unit will enter tamper mode, which will reset the device to factory settings and remove the encryption key. Removal of the key will render the device inoperable.

5. Using the tamper-evident material sent from Bluefin, secure the device and ship it to

   Spencer Technologies
   102 Otis St.
   Northborough, MA 01532

Your Bluefin account manager will provide a RMA number for you to use with your shipment as well.

6. In the Bluefin POI Management Application, select the create shipment function, and then select the unit to be shipped. Select the location where the unit will need to be shipped. All units will need to be sent to the SpencerTech Key Injection facility. Complete the shipment form with the shipment detail including the tracking number.

7. The only acceptable mail carriers who may be used for shipments are FedEx and UPS.

8. Devices should be placed in the tamper-evident packaging provided by Bluefin, and the device should be packed so that it won't be damaged in transit. Merchants should use packing paper, air packs, Styrofoam, or bubble wrap to secure the device within the packaging.

Returning tampered units

First make sure that the security practices for a tampered unit have been followed. After that follow these steps for shipping preparation.

1. Remove the unit from service immediately.

2. Update the device status in the Bluefin POI Management Application and mark the unit as tampered. This status change will disable the device from being used as part of the Bluefin P2PE solution.

3. Coordinate with your Bluefin account representative to get the necessary packaging materials to return the unit.

4. In order to remove the key the merchant will have to trigger a tampering activity with the device. The best way to do this with an ID Tech SecuRED device is to loosen the sticker covering a screw on the bottom of the unit. (see photo below) The merchant will need to use a precision screwdriver and turn the screw until the point it becomes nearly loose from the device. The merchant will then need to tighten the screw to ensure the screw does not become lost. After completing this action, the unit will enter tamper mode, which will reset the device to factory settings and remove the encryption key. Removal of the key will render the device inoperable.

5. If available use the tamper-evident material sent from Bluefin, or if instructed by your Bluefin account representative follow the steps for device securement listed in security practices for a tampered unit and then ship it to:
Your Bluefin account manager will provide a RMA number for you to use with your shipment as well. In the Bluefin POI Management Application, select the create shipment function, and then select the unit to be shipped. Select the location where the unit will need to be shipped. All units will need to be sent to the SpencerTech Key Injection facility. Complete the shipment form with the shipment detail including the tracking number.

6. The only acceptable mail carriers who may be used for shipments are FedEx and UPS.
7. Devices should be placed in the tamper-evident packaging provided by Bluefin, and the device should be packed so that it won’t be damaged in transit. Merchants should use packing paper, air packs, Styrofoam, or bubble wrap to secure the device within the packaging.

Returning damaged units

If a unit is damaged, and the damage renders the unit inoperable the following steps should be taken.

1. Remove the unit from service
2. Update the device status in the Bluefin POI Management Application and mark the unit as damaged. This status change will disable the device from being used as part of the Bluefin P2PE solution.
3. Coordinate with your Bluefin account representative to get the necessary packaging materials to return the unit.
4. In order to remove the key the merchant will have to trigger a tampering activity with the device. The best way to do this with an ID Tech SecuRED device is to loosen the sticker covering a screw on the bottom of the unit. (see photo below) The merchant will need to use a precision screwdriver and turn the screw until the point it becomes nearly loose from the device. The merchant will then need to tighten the screw to ensure the screw does not become lost. After completing this action, the unit will enter tamper mode, which will reset the device to factory settings and remove the encryption key. Removal of the key will render the device inoperable.
5. Using the tamper-evident material sent from Bluefin, secure the device and ship it to:

   Spencer Technologies
   102 Otis St.
   Northborouh, MA 01532

   Your Bluefin account manager will provide a RMA number for you to use with your shipment as well. In the Bluefin POI Management Application, select the create shipment function, and then select the unit to be shipped. Select the location where the unit will need to be
shipped. All units will need to be sent to the Spencer Technologies Key Injection facility. Complete the shipment form with the shipment detail including the tracking number.

6. The only acceptable mail carriers who may be used for shipments are FedEx and UPS.

7. Devices should be placed in the tamper-evident packaging provided by Bluefin, and the device should be packed so that it won’t be damaged in transit. Merchants should use packing paper, air packs, Styrofoam, or bubble wrap to secure the device within the packaging.

**Returning units for repair**

If a unit is damaged, and if the Bluefin account manager and the merchant believe the device is repairable, the following steps should be taken.

1. Remove the unit from service
2. Update the device status in the Bluefin POI Management Application and mark the unit as damaged. This status change will disable the device from being used as part of the Bluefin P2PE solution.
3. Coordinate with your Bluefin account representative to get the necessary packaging materials to return the unit.
4. In order to remove the key the merchant will have to trigger a tampering activity with the device. The best way to do this with an ID Tech SREDKey device is to loosen the sticker covering a screw on the bottom of the unit. (see photo below) The merchant will need to use a precision screwdriver and turn the screw until the point it becomes nearly loose from the device. The merchant will then need to tighten the screw to ensure the screw does not become lost. After completing this action, the unit will enter tamper mode, which will reset the device to factory settings and remove the encryption key. Removal of the key will render the device inoperable.
5. Before doing this action, merchants should be sure that they have coordinated this activity with their Bluefin account manager in order to ensure that replacement units can be shipped to the merchant to help ensure that the merchant experiences no transaction processing downtime.
6. Using the tamper-evident material sent from Bluefin, secure the device, and ship it to

   Spencer Technologies
   102 Otis St.
   Northborough, MA 01532

   Your Bluefin account manager will provide a RMA number for you to use with your shipment as well.
7. In the Bluefin POI Management Application, select the create shipment function, and then select the unit to be shipped. Select the location where the unit will need to be shipped. All
units will need to be sent to the Spencer Technologies Key Injection facility. Complete the shipment form with the shipment detail including the tracking number.

8. The only acceptable mail carriers who may be used for shipments are FedEx and UPS.

9. Devices should be placed in the tamper-evident packaging provided by Bluefin, and the device should be packed so that it won’t be damaged in transit. Merchants should use packing paper, air packs, Styrofoam, or bubble wrap to secure the device within the packaging.
Opting out of P2PE

The process for opting out

After the initial term of any legally binding agreement between the merchant and Bluefin has expired, and that agreement has not been renewed for one or more additional terms, the merchant may opt out of Bluefin’s P2PE program. It is recommended, but not required that merchants provide their Bluefin account representative with notice of their intent to discontinue their usage of the P2PE solution 30 days prior to the intended date of discontinuing use of the P2PE solution.

The reason for this is so that Bluefin can provide alternate secure methods for the merchant to process card present or MOTO transactions. If a merchant will be continuing to process these types of transactions with Bluefin, then 30 days would provide adequate time to furnish the merchant with new end-to-end encryption hardware.

When the merchant is completely ready to be removed from the P2PE solution, a merchant representative will need to review the opt-out language hosted on Bluefin’s P2PE POI Management Application website. The content and language will be similar to the example provided below. *Once the merchant representative has acknowledged reading and accepting the opt-out terms, the application will immediately mark all P2PE POI units in the custody of the merchant as “retired.” Retired units will be unable to process credit card transactions.* Because this acknowledgment will deactivate the units, it’s important that the merchant already have the new end-to-end encrypted units from Bluefin on site and deployed prior to canceling their P2PE solution.

All opt-out requests must be submitted through the Bluefin POI Management Application interface to ensure documentation of the opt-out process is properly captured for PCI compliance reasons.

Opt-out terms

1. P2PE provides the most secure PCI approved method for the capture and transmission of credit card data. By encrypting the card data at the point of entry, prior to entering the merchant’s computer / device the data remains secure and undecipherable until being captured and decoded by Bluefin’s servers.

   By formally requesting to opt-out of the P2PE program, the merchant acknowledges that the security provided by Bluefin’s P2PE solution will no longer be available to them, and as such the merchant puts themselves at risk that card data could be captured in their environment.

2. It is the merchant’s responsibility to pursue alternative means by which to provide secure card data capture in lieu of using Bluefin’s P2PE solution. The merchant should pursue other PCI DSS (Data Security Standard) compatible strategies such as exploring the use of other encrypted
devices that provide end-to-end encryption functionality. Bluefin does provide end-to-end encryption services and products which can help provide a secure card data capture solution, although these solutions do not provide the same level of PCI DSS scope reduction as P2PE.

By formally requesting to opt-out of the P2PE program, the merchant acknowledges that they will be responsibility to pursue alternate methods for secure card data capture and transmission. Merchants should review their own PCI assessment resources or seek the aide of PCI Qualified Security Assessor (QSA) if unsure of a suitable alternate solution to replace P2PE with another suitable PCI DSS compliant solution.

3. Bluefin’s P2PE solution provides its merchant with a certified P2PE solution that provides drastic PCI DSS scope reduction for merchants actively using the solution.

By formally requesting to opt-out of the P2PE program, the merchant acknowledges that they will be responsibility to reassess their eligibility for PCI DSS scope reduction, and re-evaluate the proper assessment status that they will now need to comply with after removing Bluefin’s P2PE solution from its environment.

Merchants should review their own PCI assessment resources or seek the aide of PCI QSA if unsure of the PCI DSS audit impact.

4. By opting out of Bluefin’s P2PE solution it is the responsibility of the merchant to inform their Acquirer of their status change. Status changes may impact the services and pricing extended by their acquirer.

By formally requesting to opt-out of the P2PE program, the merchant acknowledges that they will be responsible to notify their acquirer directly. In the event that Bluefin has informed the acquirer of the status change, it is still the obligation of the merchant to directly inform their acquirer in addition to any notifications that the merchant believes that Bluefin may have already communicated.

5. By opting out of Bluefin’s P2PE solution it is the responsibility of the merchant to inform the card brands they work with of their status change and the subsequent impact that will have on the merchants PCI DSS status. Status changes may impact the services and pricing extended by their card brands.

By formally requesting to opt-out of the P2PE program, the merchant acknowledges that they will be responsibility to notify their card brands directly. In the event that Bluefin has informed the card brands of the status change, it is still the obligation of the merchant to directly inform the card brands they work with in addition to any notifications that the merchant believes that Bluefin may have already communicated.
Handling instruction for devices after leaving the P2PE solution

All POI devices handled by Bluefin include an encryption key specific to Bluefin. This encryption key is only valid when used in conjunction with the Bluefin P2PE Validate Solution. Merchants not actively using the Bluefin P2PE Solution will not be able to process transactions using their devices.

When a merchant leaves the program, their devices are eligible to receive their security deposit back. P2PE devices may also be traded one for one for a non-P2PE end-to-end encryption device. Additionally, units may also be resold to Bluefin if there was no security deposit collected, or if the merchant chooses to not trade in for a non-P2PE device.

In the event that a unit is marked for either return or trade, Bluefin will provide product packaging (RMA – Return Merchandise Authorization) for the return of the device(s). Merchants however will be responsible for the shipping costs.

Bluefin requests, however, that any unit not returned or traded back to Bluefin be physically destroyed.