# Safe-T for SMB Security Bundle Reduced SAQ

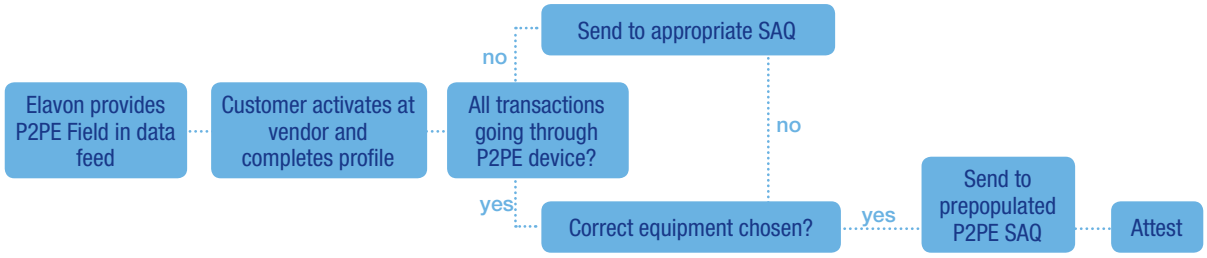
## Built to reduce risk & PCI scope

Customers must meet the following criteria to qualify for the reduced SAQ through our PCI Compliance Manager program:

- Use appropriate equipment that supports encryption. Required Equipment:

| | | | |
|---|---|---|---|
| Ingenico iCT 220 | Ingenico iWL 250 | Ingenico iPP 320 | Verifone Vx680 |
| Ingenico iCT 250 | Ingenico iPP 220 | Verifone Vx520 | Verifone Vx820 |

- Have the appropriate VAS checked within the Eclipse System – either Safe-T Silver or Safe-T Gold
- Pay the fees for encryption
- Have 100% of the transactions for that MID be processed through the device that encrypts the transactions. If other equipment/processes are used customer must complete standard SAQ (B-IP, C, C-VT or D)
- Is the customer using the supplied Security Policy Template in the portal? If so, we are pre-populating some answers. If not, additional questions may be asked about that document per PCI SSC guidelines.




**Trustwave Validation Path:** Trustwave uses a "wizard" approach that asks simpler questions, which completes the SAQ questions behind the scenes. There is no way to quantify the exact number of questions the customer will answer when going through the process; however, it equates to a maximum of 31 SAQ questions.

**Sysnet Validation Path:** PCI Compliance Manager Portal will ask Profile questions and SAQ Questions:

- Do you have a current valid (within the last 12 months) PCI DSS Self-Assessment Questionnaire (SAQ) or Attestation of Compliance (AoC)?
- Please select the method(s) that best describes how you accept payment cards? (Please select all that apply) Face to Face and/or E-commerce /Internet and/or MO/TO
- Choose point of Sale Device (Terminal, POS, etc.) Terminal
- Are all credit card transactions processed by your organization processed using encryption and tokenization?
- Compatible Point to Point Encryption Devices: Please select all of your POS Terminals and Pin Entry or Swipe Devices (Choose Device)
- Do your paper (printed, imprint or hand written) vouchers or receipts include full payment card numbers?
- Do you permit anyone in your organization to send or receive full card numbers via email or instant messaging?
- Does your company otherwise store, transmit or receive cardholder data electronically in any other way (for example, via CD-ROM, USB drive, e-mail, an internal network or the Internet) for any other purposes?
- Do you believe that your organization has been subjected to a card data security compromise in the past 12 months?
- Do you have a relationship with more than one acquirer?
- The Payment Card Industry Data Security Standard (PCI DSS) requires that you have an Information Security Policy in place in your organization that covers all relevant areas of the Standard. We can provide you with a policy template if you do not currently have one. (Choose one of three options.)

Elavon

| Modified SAQ | |
|---|---|
| 3.1(a) | Is data storage amount and retention time limited to that required for legal, regulatory, and business requirements? |
| 3.1(b) | Are there defined processes in place for securely deleting cardholder data when no longer needed for legal, regulatory, or business reasons? |
| 3.1(c) | Are there specific retention requirements for cardholder data? For example, cardholder data needs to be held for X period for Y business reasons. |
| 3.1(d) | Is there a quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements? |
| 3.1(e) | Does all stored cardholder data meet the requirements defined in the data-retention policy? |
| 3.2.2 | For all paper storage, the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored after authorization? |
| 9.9.1(a) | Does the list of devices include the following?<br>• Make and model of device • Location of device (for example, the address of the site or facility where the device is located)<br>• Device serial number or other method of unique identification |
| 9.9.1(b) | Is the list accurate and up to date? |
| 9.9.1(c) | Is the list of devices updated when devices are added, relocated, decommissioned, etc.? |
| 9.9.2(a) | Are device surfaces periodically inspected to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device) as follows? Note: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings. |
| 9.9.2(b) | Are personnel aware of procedures for inspecting devices? |
| 9.9.3(a) | Do training materials for personnel at point-of-sale locations include the following?<br>• Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.<br>• Do not install, replace, or return devices without verification.<br>• Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).<br>• Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer). |
| 9.9.3(b) | Have personnel at point-of-sale locations received training, and are they aware of procedures to detect and report attempted tampering or replacement of devices? |
| 12.1.1 | Is the security policy reviewed at least annually and updated when the environment changes? |
| 12.6(a) | Is a formal security awareness program in place to make all personnel aware of the importance of cardholder data security? |
| 12.10.1(a) | Has an incident response plan been created to be implemented in the event of system breach? |