



# VeriShield Protect Frequently Asked Questions

*What is VeriShield Protect and how does it work?*

## **How does VeriShield Protect work?**

VeriShield Protect uses a revolutionary patented format preserving encryption technology to encrypt the card data, account number and discretionary data, before it enters the retailer's or processor's payment system and keeps it secure until it leaves. This requires the VeriShield Protect application to be installed into the payment terminal (encrypts the card information), and also requires a *Decryption Appliance* (DA) to be installed at the host processor or retailer's switch to decrypt the card number for subsequent processing.

## **Can SSL be used to encrypt the card data instead?**

SSL only encrypts the transaction between the payment terminal and the POS terminal, assuming SSL is supported on the POS terminal. Once at the POS terminal the SSL packet is decoded and processed. Even if SSL is then used to send the transaction upstream to the host processor, the data would be in the clear within the POS system. This method does protect against someone gathering data on the payment terminal to POS terminal connection, but is not as complete, nor as secure a solution as is VeriShield Protect. VeriShield Protect protects data in transit and at rest. SSL only protects data in transit.

*Does VeriShield Protect work with my existing PIN pads and terminals?*

## **Will this solution work on my existing MX800 Series terminals?**

Yes, but the existing MX800 series terminals must be upgraded with the VeriShield Protect service. This requires licensing software and an additional encryption key to be injected into the payment terminal at a secure facility.

## **Will this solution work on my existing V<sup>x</sup> Solutions terminals?**

Yes, but the existing V<sup>x</sup> Solutions terminals must be upgraded with the VeriShield Protect service. This requires licensing software and an additional encryption key to be injected into the payment terminal at a secure facility. In addition, it may be required to upgrade the payment application depending upon the capabilities built into the application. There are no hardware modifications necessary.



**Will VeriShield Protect work on other terminals like the Omni 7000, the Everest or the PINpad 1000SE?**

No, these terminals do not have the multi-purpose encryption engine required to support VeriShield Protect.

**If the terminal is PCI PED compliant, why do I need VeriShield Protect?**

PCI PED compliance ensures the payment hardware and cardholder's private data is secure. VeriShield Protect helps further secure cardholder information by encrypting all customer-specific data that might enter the retailer's or processor's payment system. The current PCI DSS standards do not currently require this information to be encrypted **inside** of the retailer's payment environment, which represents an area of significant vulnerability and has become a recent focus of data criminals. In many integrated environments, this information is also sent in the clear between the payment terminal and the POS terminal.

**If the terminal is EMV compliant, why do I need VeriShield Protect?**

EMV is an authentication standard rather than a data security standard. This fact is important because both Visa and Mastercard have officially released PCI-DSS compliance mandates for merchants to be achieved by the end of 2010.

**What are these dates?**

Visa set **September 30, 2010, as the deadline for acquirers to validate their Level 1 merchants comply with the Payment Card Industry Data Security Standard**, which additionally requires that firewalls be installed and physical access to cardholder is restricted among other measures. Acquirers face fines and mandates to take corrective action for failing to meet the deadline. Visa Europe, as an autonomous licensee of Visa Inc., sets its own deadlines.

Mastercard states that all Level 1 merchants that have engaged an internal auditor before 15 June 2009 must validate compliance with the PCI DSS via an annual onsite assessment conducted by a PCI SSC certified QSA by 31 December 2010. To fulfill this requirement by the 31 December 2010 deadline, MasterCard strongly encourages that all Level 1 merchants engage a PCI SSC certified QSA immediately.

**Once I upgrade to VeriShield Protect, is there any way to ensure my payment terminals only work in the VeriShield Protect mode?**

VeriShield Protect includes access to an exclusive back-end application referred to as VeriShield Secure Device Management Service (VSDMS). VSDMS provides a real-time status and alert system to monitor compliance of each and every transaction as it occurs. The data generated by this system is also very useful in demonstrating internal security controls are in place; important components needed for regulatory compliance.



*Does VeriShield Protect work with my existing POS system?*

**Will changes have to be made to POS systems that handle card data in order to take advantage of VeriShield Protect?**

VeriShield Protect is based on patented encryption technology referred to as “*VeriShield Hidden Encryption (or VHE)*”, a type of format preserving encryption. This exclusive VeriFone solution is compatible with most existing application infrastructure and should not require you to make POS application changes. This is possible because once the card information has been encrypted, patented VHE algorithms convert the data string back into the format that the POS application expects, allowing the transaction to be processed normally.

**Does VeriShield Protect encrypt both dial and IP-based transactions?**

Yes.

**Does VeriFone offer VeriShield Protect as a managed solution?**

Yes. VeriShield Protect is available on VeriFone’s managed gateway, where the decryption appliance can be hosted.

**Will changes have to be made to my enterprise applications that handle card data in order to take advantage of VeriShield Protect?**

No, unless your enterprise application also includes a transaction switch. Please consult your VeriFone account professional to qualify any enterprise application.

**Since the critical customer information is encrypted, a *Decryption Appliance* is required. Can this decryption occur at my switch?**

Yes, decryption can occur at the retailers switch. However, for best protection, it is recommended that the decryption process occur at the host processor.

VeriFone can provide a *Decryption Appliance* for the retailer that runs on their respective switch if desired.

**Can I still perform debit encouragement at the point of sale with VeriShield Protect?**

Yes. The VeriShield Protect algorithm does not encrypt the ISO prefix (typically the first six digits of the card) since it is needed by the POS to properly route transactions. With these digits still in their original format (unencrypted), the debit prompting feature is unaffected and therefore still supported.

**Will VeriShield Protect work with gift cards and private label credit cards?**

VeriShield Protect can work with most card types.



**What if a specialty card such as a gift or loyalty card needs to remain in the clear? How does the VeriShield Protect solution deal with this?**

The VeriShield Protect solution has been designed with flexibility in mind to meet the current and future demands of the payment marketplace. The solution utilizes an exception BIN table so that the merchant can specify a particular BIN range or series of BIN ranges remain in the clear and not be encrypted.

*What do I need to get started?*

**What are the major components required to implement VeriShield Protect?**

VeriShield Protect consists of both hardware and software at both ends of the transaction path:

- At the point of sale, the countertop device or PIN pad needs to have the VeriShield Protect operating system module loaded as well as the VeriShield Protect secure encryption key. The key loading must be completed at a secure key injection facility.
- A Decryption Appliance must reside at the retailer's switch, host processor or VeriFone's managed gateway.

**How do I upgrade my existing devices with the VeriShield Protect service?**

For the Vx Solutions and MX 800 Series products already deployed in the field, they will need to be returned to a secure facility for the upgrade process, including VeriShield Protect key injection and application load. If your devices have been pre-loaded with VeriShield Protect keys, then the upgrade process can be done without sending the devices back to VeriFone.

*What is unique about the VeriShield Protect encryption process?*

**Can the VeriShield Protect encryption key be injected at my store?**

No. Due to PCI security rules, secure key injection will have to be preformed in a secure, PCI-approved facility. Upgrading to the new software module should be done at the same time as Key injection to minimize interruption of service.

**Can the VeriShield Protect encryption algorithm be the same encryption key used for debit?**

No. The VISA PIN Security Program rules require that encryption keys must be single function. The current debit key can only be used for debit PIN encryption.

**Can I have the VeriShield Protect application and the secure key injected when I install the terminals even though I am not ready to encrypt the transactions because the host product is not installed?**

Yes. The VeriShield Protect application can be loaded and the secure key injected during deployment. Once installed, the VeriShield Protect service



resides in a dormant state until it is activated. When the host is ready to begin decrypting transactions, VeriShield Protect can be activated.

**What card data is encrypted?**

The VeriShield Hidden Encryption (VHE) solution encrypts magnetic card Track 2 data on each and every transaction. VHE encrypts PAN and track equivalent data on each EMV transaction.

**Is there any distinguishable difference between VHE encrypted and non-encrypted data?**

There is no distinguishable difference between clear text data and the VHE generated encrypted data, meaning it will pass all standard checks at the POS level such as MOD 10 or LRC.

*Do I have to change any of my internal processes when I implement VeriShield Protect?*

**Can I still print the truncated PAN (last four digits of the card) on receipts?**

Yes. By not encrypting the last 4 digits of the Personal Account Number, this information is available to be printed on POS receipts, so there is no change in the POS applications to support receipt printing.

**If card holder data is encrypted using VeriShield Protect, how can I perform chargebacks when necessary?**

Retailers can still perform chargebacks by finding transaction information using other methods. Instead of searching for transactions based on the card number, retailers can also use the transaction amount, store/lane number, and transaction date to find the transaction in question. The unencrypted BIN range and last four digits of the card number can also be used to search for and match transactions. Additional methods of retrieving transactions may exist depending on your payment system and Processor. Note that the card companies do not require the entire PAN to be stored to handle charge backs. However, some acquirer's systems may still require this information.

*When is VeriShield Protect Available?*

**Is VeriShield Protect available now?**

Yes. VeriShield Protect is available for immediate implementation for retailers and processors.



### **How long does it take to implement VeriShield Protect?**

VeriShield Protect can be implemented in 60 to 90 days. The gating item is likely to be the time to modify either the retailer's switch or the acquirer's host system to integrate with the decryption appliance. Implementation can be immediate with VeriFone's managed gateway solution.

### *Where can I get more information on VeriShield Protect?*

Visit [www.verifone.com/definitivesecurity](http://www.verifone.com/definitivesecurity), contact your VeriFone account representative, or send an email to [verishield@verifone.com](mailto:verishield@verifone.com), for additional information on VeriShield Protect.

Copyright © 2009 VeriFone and Semtek Innovative Solutions Corporation. All rights reserved. No portion of this document may be reproduced or distributed in any form or by any means without the prior written permission of said companies. All trademarks are the property of their respective owners