Update Bulletin

VeriShield

August 22, 2009

A recent announcement from RBS WorldPay regarding VeriShield is making the rounds, and several dealers have raised questions about how this system from Verifone compares and contrasts to Connected Payments and WinEPS.

The short answer is that VeriShield is not a payments application but an encryption system only, and its encryption limits you in several ways compared to WinEPS or Connected Payments and their built-in encryption.

VeriShield's encryption stops within the merchant's walls and must be converted to unprotected in-the-clear data before it is communicated to the processor. But Connected Payments provides encryption from card-swipe to the processor's data centers.

VeriShield can provide some additional protection for merchants using proprietary POS systems. However, any WinEPS or Connected Payments store already has data protection beyond what this solution is able to offer. Adding VeriShield would be redundant — and in fact it would force the merchant backwards.

The long answer:

VERISHIELD BASICS

What is VeriShield and what does it do? — VeriShield is an encryption system. It encrypts data from Verifone PIN pads which can be decrypted at a Verifone host or at a "decryption appliance" that can be purchased from Verifone. VeriShield is not an electronic payments system, POS payments engine or processing host — it is an encryption system only.

How does VeriShield operate in a retailer location? — VeriShield encryption is built into several recent Verifone PIN pad designs.

- When the shopper swipes the card on a VeriShield-equipped PIN pad, the data is immediately encrypted. The POS or payment engine cannot see the data as it goes through the POS terminal.
- When the encrypted data arrives at the in-store (or enterprise) payment application, that application must send the encrypted data to a Verifone host or local "decryption appliance" hardware for decryption.
- The decryption system then returns the unencrypted data back to the payment application, where it is then sent "in the clear" to the payment processor for authorization.
- The payment processor returns the authorization normally.

Verifone says that VeriShield provides "end-to-end" encryption, but you say the data has to come back from decryption in the clear, then go to the processor in the clear too. How is that considered "end-to-end"? — Verifone defines "end-to-end" as being ***inside*** the retailer's enterprise. Except for the data being in the clear coming back from the decryption appliance or

service, it is encrypted from the point at which it's swiped to the point at which the payment application communicates it to the payment processor.

So what's the big advantage of using VeriShield? — If the merchant has a POS system (e.g. IBM) that can't use WinEPS or Connected Payments, at least the merchant's data will be encrypted most of the time it's within the merchant's walls. That's a big step forward for stores with old or low-function payment systems.

VERISHIELD COMPARISONS WITH CONNECTED PAYMENTS AND WINEPS

Doesn't WinEPS or Connected Payments do this already? — Yes. WinEPS and Connected Payments both can encrypt the data at the PIN pad and send the encrypted data upstream.

How is WinEPS different than VeriShield then? — Comparing WinEPS first, this is a complete payments application, not just an encryption device. However, if we limit the discussion just to encryption capabilities, WinEPS also encrypts data at the PIN pad and keeps it encrypted until it is released to the processor, the same as with VeriShield. However, WinEPS also provides three key advantages:

1. Cost: WinEPS encryption is included with the product: there is no need to pay per-transaction fees for a decryption service or to purchase and maintain a custom Verifone decryption appliance. All the encryption capabilities are provided at no extra charge as part of WinEPS.
2. Flexibility: WinEPS encryption can operate on several Verifone (including MX, Everest Plus and Omni 490) and Hypercom PIN pads. According to Verifone, VeriShield is available only on the MX8000 series.
3. Speed: since WinEPS handles the encryption internally, there are no communications cycles required back and forth to an encryption/decryption device or remote service.

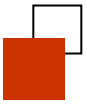
Does VeriShield have any disadvantages in comparison? Yes, there are two primary issues when you compare VeriShield to the encryption services already in WinEPS:

1. Security: since VeriShield data must go through a decryption cycle before the data is released to the processor, that means there will be another data communication required when the decrypted data is returned to the payment application "in the clear" from the remote VeriShield service or the "decryption appliance." These extra steps and the risks of in-the-clear card numbers don't exist with WinEPS or Connected Payments.
2. Lost features: since the data is encrypted by VeriShield, the POS payment application cannot use any features requiring knowledge of the card type. For example, this excludes credit→debit conversion, offline stand-in (store-and-forward) and auto-tender resolution. Cashiers must examine the card or otherwise identify the type of card or tender from the shopper prior to tender, instead of the payments system automatically kicking off the correct transaction type based on the card being swiped.[1]

Is VeriShield's encryption stronger or better somehow? — No, but you won't catch us criticizing it since the RBS announcement claims "AES-level" encryption, and both WinEPS and Connected Payments use 256-bit AES encryption, considered to be the strongest data protection algorithm in use today.

---

[1] WinEPS and Connected Payments now operate on the data in the POS terminal ***while that data is fully encrypted in 256-bit AES.*** OpenEPS does not need to decrypt the 256-bit AES from the PIN pad to perform all its functions in the POS. Since the Connected Payments data centers also operate on the data without decrypting it.



So why would a WinEPS user consider VeriShield? — VeriShield is not really appropriate for WinEPS users or merchants that could implement WinEPS since it breaks important functions in the payments system. VeriShield is designed to enhance systems that do not provide the security that WinEPS already offers, and is limited to merchants who have the latest Verifone PIN pads. If a merchant already uses WinEPS in the store connecting to the processor, VeriShield would only take the store "backwards" by eliminating features without providing anything of additional value.

How about Connected Payments — what does it offer compared to VeriShield? — Just with respect to encryption, Connected Payments now offers true "Post-to-Host" encryption from PIN pad to the payment processor, not just within the merchant's walls. Connected Payments data is encrypted at the PIN pad all way to — and through — the Connected Payments host; and now the communications between the Connected Payments host and the processors is also protected. For even more over-the-top security, Connected Payments communications are also simultaneously protected by communications certificates, SSL and tokens as well as encryption.

So besides Connected Payments' huge range of powerful applications, it also gives users an unmatched security solution that goes to deeper levels and travels the complete journey.

THE RBS WORLDPAY ANNOUNCEMENT

What is really being said in the RBS WorldPay announcement? — RBS is endorsing the VeriShield solution as a way for some merchants to reduce risks by encrypting data and communications.

What is RBS doing to support VeriShield? — According to the announcement, current activity is limited to endorsement and co-marketing. No technical, interface or integration work is being done by RBS at this time.

So how can an RBS WorldPay user get VeriShield? — Merchants using RBS WorldPay must purchase Verifone's decryption services or buy their own Verifone "decryption appliance." At some point in the future, RBS indicates that they may provide VeriShield's decryption services internally, depending upon the level of interest shown by RBS merchants.

In light of this announcement, will RBS still support Connected Payments? — RBS representatives were quick to say they don't regard VeriShield's encryption product to be a competitor to Connected Payments. They point out that VeriShield improves security for currently unprotected POS payment systems such as IBM, and that VeriShield cannot be used unless the customer has new Verifone MX terminals.

Would RBS consider a similar press release demonstrating support for Connected Payments? — Yes. RBS and StoreNext plan to make an announcement in the near future.

To Your Success,

Anthony van Seventer