Visa Risk Guidance

Dynamic Cardholder Verification Method Best Practices

Purpose of this Document

This document provides guidance for issuers that plan to develop or use a third-party dynamic Cardholder Verification Method (CVM) service to authenticate their cardholders. Dynamic CVMs, such as One-Time Passcodes (OTP), are becoming more prevalent for on-line banking and e-commerce transactions as financial institutions aim to strengthen their customer authentication capabilities. Visa developed the following dynamic CVM best practices for issuers to consider and assess the security features of these solutions.

Background

Issuers utilize a number of factors to authenticate and authorize financial transactions including payments. A well designed payment authentication system will balance risk mitigation with cardholder experience to minimize friction during a transaction. Advanced solutions designed to specifically provide robust authentication while minimizing risk are now available within the payments industry. These solutions typically rely on network and cloud based innovations to provide issuers with a risk based approach in making authentication and authorization decisions.

Visa recommends the use of risk-based authentication and authorization solutions, like Visa's Consumer Authentication Service (VCAS),[1] that allow issuers to request a CVM only for high-risk card not present transactions. Visa further recommends that issuers consider authentication solutions that facilitate the use of dynamic CVMs, like OTPs, to limit the exposure of sensitive static cardholder information, such as CVV2, PIN and personal information gathered via security questions.

Historically, payment transactions have relied primarily on static data elements such as CVV / CVV2 to authenticate the card and signature / PIN to authenticate the cardholder. Today we are increasingly migrating to dynamic authentication mechanisms through solutions such as EMV chip cryptograms for card authentication and OTPs for cardholder authentication. Globally, Visa will continue to support a range of CVMs including signature, PIN and no-signature for low-value, low-risk transactions in addition to emerging solutions such as dynamic OTPs and biometric factors like voice or fingerprint. In the longer term, Visa expects that network and cloud based innovations will further limit the need for issuers to require a static or dynamic CVM for the vast majority of payment transactions.

Dynamic CVM Security Goals

Visa has developed best practices for the development and deployment of dynamic cardholder verification methods to:

1. Promote the secure design and implementation of dynamic CVM solutions using a risk-based approach that incorporates a CVM at the appropriate time for the acceptance channel.

2. Limit exposure of sensitive static payment information that can be compromised and used to commit fraud.
3. Provide guidance to help issuers integrate effective dynamic CVM solutions regardless of the third-party solution provider.

[1] For more information on E-commerce authentication solutions go to www.visa.com

Following are best practices for the development and deployment of dynamic cardholder verification methods:

	Best Practice
	1. **Ensure a risk-based layered approach is used when invoking a dynamic CVM.** Since consumer challenges add friction to a transaction, issuers should invoke the use of dynamic CVMs for high-risk / high-value Card Not Present (CNP) transactions and selectively incorporate dynamic CVMs that are appropriate for the level of risk.
	2. **When using One Time Passcodes (OTP) implement controls for their secure distribution or use a secure application deployed on the consumer's device.** Use of mobile phones for the distribution of OTP via SMS or email can introduce risks and should include controls to monitor this distribution method. Care should be taken to ensure that mobile network operators' processes will not lead to account takeover or related fraud. If network availability adversely impacts the distribution of OTPs, clients may wish to consider the use of a secure application for OTP generation. If using mobile app generated OTPs, the app should perform careful checks to determine if the phone operating environment is intact and secure (e.g., the phone has not been "rooted" and is malware free). Even with such methods, it should be recognized that on-phone OTP generation is likely more susceptible to fraud than server-based OTP as the phone can be more vulnerable to attack.
	3. **If entities implement a physical 'hard' token for OTP generation, the following should be considered:** The issuance and use of individual 'hard' tokens can be expensive to implement, reissue and track. This can also result in clients managing multiple individual tokens for each banking relationship. Hence, entities should consider the use of multi-use tokens to minimize end user inconvenience by limiting the number of tokens users are required to manage. To ensure OTP generating tokens are protected from misuse, they should be protected by some form of authentication to diminish their usefulness to a fraudster.
	4. **Ensure OTPs are valid for only a limited period of time.** To limit the exposure of OTPs being intercepted and used fraudulently, OTPs should only be valid for a limited period of time.
	5. **When evaluating dynamic CVM solutions, consider the use of Payment Card Industry (PCI) PIN Transaction Security (PTS) Approved Hardware Security Modules (HSM) and the use of industry approved algorithms in vendor solutions.**

Best Practice

A. Use of PCI PTS Approved HSMs ensures that a host-based CVM solution uses secure cryptographic hardware for key management.

B. Cryptographic algorithms for the storage / protection or distribution of OTPs should use ANSI X9 or ISO approved algorithms with appropriate key lengths between issuers and service providers. www.ansi.org www.iso.ch

C. PCI PTS Approved HSMs are compliant random number generators and can be used for secure generation of unpredictable OTPs.

D. Issuers should validate that service providers use key management practices aligned with the PCI PIN Security Requirements.

E. Service providers should comply with the PCI Data Security Standard (PCI DSS), which provides robust payment card data security processes.

For PCI Standards and Listing of Approved HSMs go to: www.pcisecuritystandards.org

6. **Evaluate the potential to leverage dynamic consumer authentication solutions deployed for on-line banking for CNP payment transactions.**

Visa encourages issuers to review the strategies used in online banking authentication, such as a risk-based approach, when designing CNP authentication solutions. Additionally, it is a best practice to not send a challenge to a device that is being authenticated. (e.g. if the consumer is transacting from a new mobile device and is therefore being challenged with an OTP, do not send an SMS OTP to that device.)

7. **Leverage consumer device information as part of a risk-based approach to invoking dynamic CVMs.**

Technologies like device fingerprinting, unique device IDs etc. exist today that uniquely identifies a consumer device. These are already widely used by online marketing and advertising companies to uniquely identify their customers. Banks are also using these same technologies to enable a high degree of trust with their clients for on-line banking applications. Consider using similar solutions in the design of a risk-based dynamic authentication approach for payment transactions leading to a more positive cardholder experience.

Best Practices Feedback

Visa has developed these best practices to support the use of the dynamic CVMs. As such, Visa welcomes any feedback on these best practices. To provide feedback or comments on these best practices, send an e-mail to cisp@visa.com with "Dynamic CVM" in the subject line.