Visa Europe Member Letter

VE 09/16
3 February 2016

Verified by Visa Changes

Audience: Issuers, Acquirers, Processors

Category: Operations, Risk/Fraud, Product

Subject: Visa is implementing three changes to Verified by Visa in line with industry technology changes.

Action required

Issuers and Acquirers must ensure their systems are able to implement the changes to Verified by Visa outlined below.

Change	Details	Effective date
Verified by Visa Digital Certificate Policy Updates	Visa will issue SHA-2 digital client and server certificates	Immediate
	Visa will stop issuing SHA-1 digital certificates.	8th April 2016
	No SHA-1 certificates will be accepted after this date	1st January 2017
Secure Connection and Encryption Policies Updated for Verified by Visa Transactions	Visa will no longer accept direct IP address connections for Verified by Visa transactions.	30th April 2016
	Visa will not allow RC4 cypher-encrypted connections to any Verified by Visa hardware	31st March 2016
	Visa will enable the use of TLS versions 1.1 and 1.2 encryption for all Verified by Visa hardware	30th June 2016
	Visa requires that secure connections to any Verified by Visa hardware use TLS Version 1.1 encryption or higher	30th June 2018
Discontinuation of Verified by Visa Card Range Messages	Visa will no longer accept Card Range Request (CRReq) and will not provide Card Range Response (CRRes) messages to the Directory Server	14th October 2016

Visa Europe
PO Box 39662
London W2 6WH
United Kingdom

www.visaeurope.com
Phone +44 (0) 20 7937 8111
Fax +44 (0) 20 7937 0877

Summary

This Member Letter announces three changes to Verified by Visa in line with recent Visa Inc updates:-

Verified by Visa Digital Certificate Policy Updates

Visa has updated its digital certificate policy to adopt stronger security for Verified by Visa transactions. Effective 1 January 2017, Internet service browsers will no longer accept digital certificates issued with Secure Hashing Algorithm-1 (SHA-1) encryption. To ensure Verified by Visa endpoints are ready, Visa has created a timeline of important dates. Acquirers wishing to apply for SHA-2 certificates may do so with immediate effect and Issuers are required to be able to process and sign SHA-2 certificates with effect from 8th April 2016.

Secure Connection and Encryption Policy Updates for Verified by Visa Transactions

To increase security for Verified by Visa transactions, Visa is updating its connection and encryption policies. The use of direct IP address connections will be discontinued for Verified by Visa transactions from 30th April 2016 and Transport Layer Security, Version 1.1 or higher will be required to connect to Verified by Visa hardware with effect from 30 June 2018.

Discontinuation of Verified by Visa Card Range Messages

Effective 14 October 2016, Visa will discontinue the use of Verified by Visa Card Range Messages to ensure uninterrupted authentication processing.

Background

As E-Commerce grows in volume and importance, and new competitors look for entry points to challenge the existing ways to pay, Visa needs to remain competitive and continue to offer a secure and reliable payment service. Verified by Visa 1.0 has been operating successfully for many years, and upgrades are now required to keep pace with changes in the technology and operating processes in the internet channel. This paper details three proposed changes required by VI.

Verified by Visa Digital Certificate Policy Update

Visa has updated its digital certificate policy to adopt stronger security for Verified by Visa transactions. Effective 1 January 2017, Internet service browsers will no longer accept digital certificates issued with Secure Hashing Algorithm-1 (SHA-1) encryption. To ensure Verified by Visa endpoints are ready, Visa has created a timeline of important dates.

Visa Europe
PO Box 39662
London W2 6WH
United Kingdom

www.visaeurope.com
Phone +44 (0) 20 7937 8111
Fax +44 (0) 20 7937 0877

Verified by Visa endpoints use three types of digital certificates: client, server and signing certificates. Client and server digital certificates are used by both merchant server plug-ins (MPIs) and access control servers (ACSes) to connect to the Visa Directory Server (DS) and the Authentication History Server (AHS). ACS endpoints use digital signing certificates to prove authenticity of the Payer Authentication Response (PARes) message.

For the past twenty years, SHA-1 has been one of the preferred hashing algorithms for online security. However, as vulnerabilities are identified, stronger methods of encryption have been introduced. The Certification Authority Browser Forum (CA / Browser Forum), in conjunction with the National Institute of Standards and Technology (NIST), has mandated the upgrade from SHA-1 to SHA-2 encryption through NIST Special Publication 800-131A, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths."

Timeline for Verified by Visa Digital Certificate Policy Update

Date	Certificate Policy Update	Who Will Be Affected
8 October 2015	Visa will begin issuing SHA-2 digital client and server certificates	Verified by Visa MPI and ACS endpoints
8 April 2016	Visa will no longer issue any SHA-1 digital certificates	Verified by Visa ACS Endpoints Verified by Visa MPI and ACS endpoints
1 January 2017	CA / Browser Forum deadline: No SHA-1 certificates will be accepted after this date	Verified by Visa MPI and ACS endpoints

Acquirers wishing to apply for SHA-2 certificates may do so with immediate effect and Issuers are required to be able to process and sign SHA-2 certificates with effect from 8th April 2016. From April 8 onwards VI will only issue SHA-2 certificates.

There will be no change to the process by which certificates are requested and issued and replacement certificates will be charged as a Production Change at €125 per certificate as set out in Section 8.15.2 of the Visa Europe Fee guide.

Visa Europe
PO Box 39662
London W2 6WH
United Kingdom

www.visaeurope.com
Phone +44 (0) 20 7937 8111
Fax +44 (0) 20 7937 0877

Secure Connection and Encryption Policies Updates for Verified by Visa Transactions

To increase security for Verified by Visa transactions, Visa is updating its connection and encryption policies.

Effective 30 April 2016, Visa will no longer accept direct IP address connections for Verified by Visa transactions. All Verified by Visa endpoints, merchant server plug-ins (MPIs) and access control servers (ACSs) that connect to the Visa Directory Server (DS) and the Authentication History Server (AHS) using direct IP addresses must update to fully qualified domain names (FQDN) that use a domain name system (DNS) lookup.

Verified by Visa MPIs and ACSs connect to the Visa DS and the AHS using multiple versions of Transport Layer Security (TLS) and Rivest Ciphers (RC) encryption, which has been an industry standard to secure Internet connections since 1999. To ensure the most robust security currently available, effective 31 March 2016, Visa will not allow RC4 cypher-encrypted connections to any Verified by Visa hardware. Effective 30 June 2016, Visa will enable the use of TLS versions 1.1 and 1.2 encryption for all Verified by Visa hardware and effective 30 June 2018, Visa will require that secure connections to any Verified by Visa hardware use TLS, Version 1.1 encryption or higher.

To protect the integrity and security of the payments system, Visa reserves the right to disable any connections that use legacy encryption methods.

Key dates:

- Use of direct IP address connections discontinued for Verified by Visa transactions (30 April 2016)
- Transport Layer Security, Version 1.1 or higher required to connect to Verified by Visa hardware (30 June 2016)

Discontinuation of Verified by Visa Card Range Messages

Visa will discontinue the use of Verified by Visa Card Range Messages to ensure uninterrupted authentication processing.

Effective 14 October 2016, Visa will no longer accept Card Range Request (CRReq) and will not provide Card Range Response (CRRes) messages sent to the Visa Directory Server (DS). Providers of merchant server plug-ins (MPIs) will need to make updates to eliminate the use of these messages.

Currently, a small number of MPIs use CRReq and CRRes messages to request a list of participating issuer card ranges from the Visa DS, which are internally cached to perform an issuer participation check locally before sending a Verification Enrolment (VE) message. Only 0.06% of all authentication messages globally are card range messages. The synchronization of card ranges between the Visa DS and the

MPI's local cache can be difficult for MPI to manage, and any missing ranges would prevent a transaction from being processed. Today, network infrastructure and Internet speed have improved considerably and these messages are no longer needed.

Merchant's MPI providers will need to discontinue the use of Card Range messages (CRReq / CRRes) by October 2016. Instead they must send VE messages for every transaction they wish to authenticate. VE messages will perform an issuer participation check within the Visa DS. There is no impact for Issuers.

For more information

If you have any queries about this Member Letter, please contact Visa Europe Customer Support on your country-specific number, or email customersupport@visa.com.

Mark Antipof
Chief Officer, Sales and Marketing

Visa Europe
PO Box 39662
London W2 6WH
United Kingdom

www.visaeurope.com
Phone +44 (0) 20 7937 8111
Fax +44 (0) 20 7937 0877