Visa Secure – User Interface Guide for 3-D Secure 1.0.2

Version 1.0

Visa Confidential

Important Information on Confidentiality and Copyright

Contents

Tables

Figures

Introduction

The *Visa Secure User Interface Requirements for 3-D Secure 1.0.2, Version 1.0* contains the following information:

- Issuer ACS Requirements
- Merchant Requirements

Audience for the Visa Secure User Interface Requirements for 3DS 1.0.2

This global Guide is intended for merchants and acquirers who are implementation, or making infrastructure changes to an existing Visa Secure implementation.

References

3-D Secure 1.0.2

- Specification
  - *3-D Secure Protocol Specification—Core Functions*
- Technical Requirements
  - *3-D Secure Functional Requirements—Merchant Plug-in*

Industry Standards

- *Payment Card Industry Data Security Standard (PCI DSS)*

Visa

- Brand Standards
  - Visa Secure symbol, artwork, reproduction, and application guidelines can be accessed through Visa Online or at www.productbrandstandards.com
- Visa Secure Guides
  - Visa Secure Program Guide
  - Visa Secure Issuer Implementation Guide for 3DS 1.0.2
  - Visa Secure Merchant/Acquirer Implementation Guide for 3DS 1.0.2

Contact Information

- Visa Secure—For questions about Visa Secure, contact your Visa regional support team:
  - Americas (U.S., Canada, Latin America, and Caribbean (LAC)): vbvsupport@visa.com
  - Asia Pacific (AP) and Central Europe, Middle East, and Africa (CEMEA): vbveast@visa.com
  - European Region: customersupport@visa.com
- Visa Rules—For information on Visa rules, contact: visarulesinquiries@visa.com

1 Issuer User Interface (UI) Requirements

The Issuer ACS must comply with Visa Secure user interface (UI) requirements including:

- General UI Requirements
- Risk-Based Authentication and Attempted Authentication Processing Page
- Dynamic Password Entry Page
- Static Password Entry Page
- Browser Alert for Cardholder Clicking on Exit or X Button

1.1 General UI Requirements

General user interface requirements apply to all Visa Secure implementations:

- There must be no competitive branding on Visa Secure user interface pages including but not limited to MasterCard SecureCode, American Express' SafeKey, and JCB's J/Secure.
- The background of any user interface page must be white.
- There must be no external links or advertising, no links to other sites, and no advertising or other communications messages.
- The user interface page is presented as an inline page. The page content must be set to display 390 pixels high by 400 pixels wide, without scrolling.
  - The ACS must not attempt to re-size or re-position the Visa Secure window.
- Issuers that support a password (either static or dynamic):
  - For the Password Entry Page, the issuer logo is mandatory and must appear in the upper-right corner. The Visa Mark is optional. If present, it must appear in the upper right corner.
  - Logos of other issuer services are not permitted. Third-party logos must not be displayed.

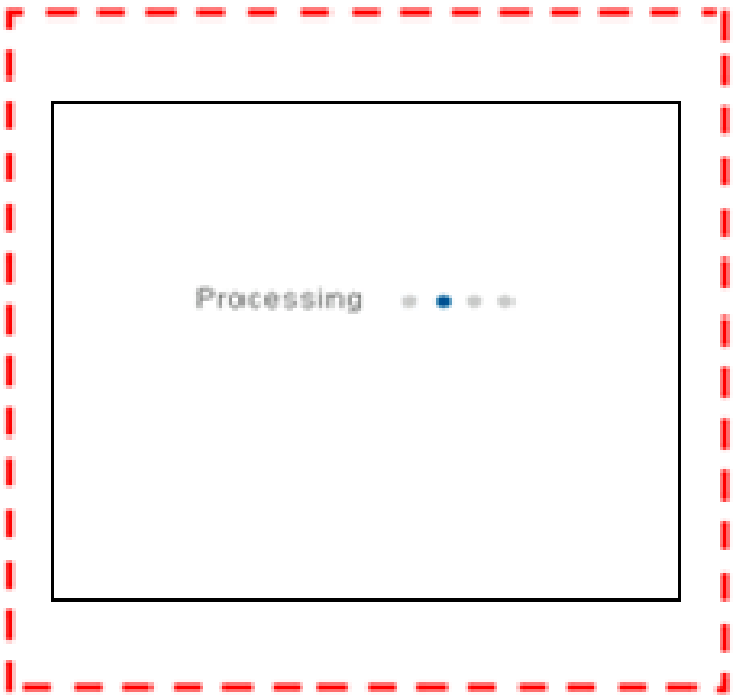
1.2 Risk-based Authentication and Attempted Authentication Processing Page

The Issuer ACS presents a simple processing page to the cardholder when the Issuer ACS receives a Payer Authentication Request (PAReq) message from a merchant and the ACS supports risk-based authentication or an Attempts Server is providing an attempts response.

1.2.1 Example

The following figure provides an example of a risk-based authentication or an attempted authentication processing page. The Issuer ACS provides the content in the red box; it will be framed by an inline page formatted by the merchant with content such as the URL, merchant logo, etc.

Figure 1–1: Risk-based Authentication and Attempted Authentication Processing Page



1.2.2 Requirements

- Browser Window. The ACS must support the Processing Page as illustrated in Figure E-1.
- At a minimum, the screen must display "Processing...." centered on the page.
  - It may also contain an indicator to provide a visual cue to customers that the purchase process is continuing in the background (so they know the system is working and not frozen). It is

important that this indicator have some kind of simple movement such as dots or arrows moving from left to right.

- Issuer may optionally place their logo and/or Visa Mark graphic elements on this page.
- No informational or promotional text or external links are permitted.
- The cardholder must not be required to click a button to continue.
- The ACS must not request the cardholder's email address.
- The timer on the page must be set to zero.

1.3 Dynamic Password Entry Page

This section outlines the user interface requirements for the dynamic password entry page and applies to issuers supporting a dynamic password authentication method (such as one-time passcode).

1.3.1 Example

The following figure provides an example of a dynamic password entry page. The Issuer ACS provides the content in the pink box while the rest of the page elements are provided by the merchant.

Figure 1–2: Dynamic Password Entry Page

1.3.2 Requirements

The requirements for the dynamic password entry page are outlined in the following table.

Table 1–1: Dynamic Password Entry Page Requirements

#	Element	Requirement
1.	Browser Window Requirements	The ACS **must** support the following: A 20-pixel margin exists within the designated 390 pixels high by 400 pixels wide, displayed as an inline page. All elements must appear within this area, as shown in Figure E-2 and Figure E-3. The text must display as 12-pixel aliased Arial Regular HTML text in Web-safe gray (R: 102, G: 102, B: 102) or black. These are the text requirements except for the dynamic password resend mechanism and the "forgot your password" prompt. See items 10 and 11 in this table. No page served by an ACS should **exceed 32 KB** of data. This size limit is inclusive of all text, graphics, source code, scripts (local or remote), etc. The primary purpose of this size limit is to minimize the amount of time required to download a page to the cardholder's browser.
2.	Issuer Name/Logo	The issuer name or logo must be displayed. See Figure 1-2. The issuer's name or logo should align with the top right margin, as shown in Figure 1-2. The maximum size of the issuer's identity graphic is 140 pixels wide by 47 pixels high. Only the logo of the issuer name is allowed; logos of other issuer services are not allowed. Third-party names or logos are not permitted.
3.	Visa Mark	The Visa Mark is optional. If present, it must be inserted in the upper left corner of the page, in a space that is 81 pixels wide by 51 pixels high. This mark is to be displayed as shown, aligned top right to the margin.
4.	Page Headline	**Dynamic Password:** The page **must** display the headline *Added Protection* above the text *Please submit your dynamic password*. **Note:** "Dynamic password" can be replaced with the language used by the issuer to communicate this password to the cardholder. Examples include "dynamic password" or "one-time password".

#	Element	Requirement
5.	Partial Card Number	The last four digits of the card number must be displayed as a confirmation of the payment card account for which the authentication will apply. The display name for this field must be 'Card Number'.
6.	Authentication Transaction Date	The transaction date in the Payer Authentication Request (PAReq) message. The display name for this field must be 'Date'.
7.	Merchant Name	The merchant name as included in the PAReq message. The display name for this field must be 'Merchant'.
8.	Purchase Amount and Currency Type	The currency type is the currency designated in the merchant's PAReq message. If a cardholder shops at an international merchant location, the purchase amount in the PAReq message will be in the transaction currency displayed when the cardholder selected *Buy* at the merchant site. The display name for this field must be 'Amount'.
9.	Password Entry Field	The field for entry of the password: • **Dynamic**—The display name of this field should match the language the issuer is using to communicate this password to the cardholder. Examples include "Dynamic Password" or "One-Time Password".
10.	Dynamic Password Resend Mechanism	This is only applicable to issuers supporting dynamic password. The ACS must provide a mechanism to allow the cardholder to have the dynamic password resent to him/her. The *Request New Dynamic Password* prompt must be displayed in 10-pixel text under the password entry field. **Note:** "Request New Dynamic Password" may be replaced with the language the issuer is using to communicate the dynamic password to the cardholder. For example, it could be replaced with "Request New One-Time Password". The cardholder may access this dynamic password resend mechanism at any time from the Dynamic Password Entry Page.

#	Element	Requirement
11.	"Forgot Your Password" Password Recovery Mechanism	This is only applicable to issuers supporting static password. The ACS must use a password recovery mechanism to assist cardholders who may have forgotten their password. The *Forgot your Password?* prompt must be displayed in 10-pixel text under the password entry field. Two approaches are allowed: • A hint statement, or hint and response, created by the issuer • Identity verification questions The cardholder may access this password recovery process at any time from the Standard Password Entry Page. The ACS must not permit the Password Hint to contain the cardholder's password. The password recovery process may contain instructional text and issuer contact information, along with the Password Hint, secret questions, or identity verification questions.
12.	Personal Message	A short text message unique to the cardholder, designed to reassure the cardholder that they are connected with the issuer's site when entering their password. **Note:** The ACS must support a Personal Message. For static password, the ACS must not permit the Personal Message to contain the cardholder's static password or static password hint. The display name for this field must be 'Personal Message'. The Personal Message is a text string of up to 30 characters.
13.	Submit Button	A form element that should align with the center of the bottom margin. When clicked in conjunction with the submission of a password, it allows the ACS to validate the password. If the password is validated, the ACS responds to the merchant with a positive authentication response.
14.	Help Button	A static gif, accompanied by Help text that links to a Help page with instructional text. Also provides information (typically a customer service email address or call center number) to contact the issuer in the event of difficulties. The Help text must be supported at the ACS and must not link to any external site, including the issuer's site.

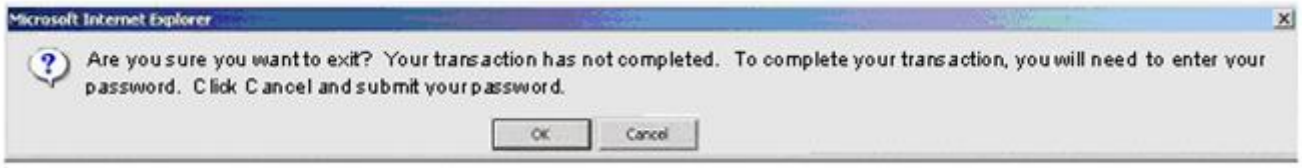
#	Element	Requirement
15.	Exit Link (Cancel may be used in place of Exit)	The cardholder must be provided with a means of not proceeding with the password entry. However, if the cardholder selects 'Exit', the issuer must present a browser alert. See Figure E–4 for an example. If the cardholder clicks OK, the ACS must return a failed PARes to the participating merchant to prevent fraudulent users from avoiding authentication. This alert should appear to advise the cardholder that continuing with the cancellation terminates the purchase with the participating merchant.
16.	Exit Browser Alert	If the cardholder clicks on the upper right-hand X to close the inline page, or if the cardholder clicks on the browser Back button, a browser alert must be displayed to inform the cardholder that the transaction will terminate. See Figure E–5 for an example.

1.4 Browser Alerts for Cardholder Clicking on Exit or X Button

1.4.1 Example 1

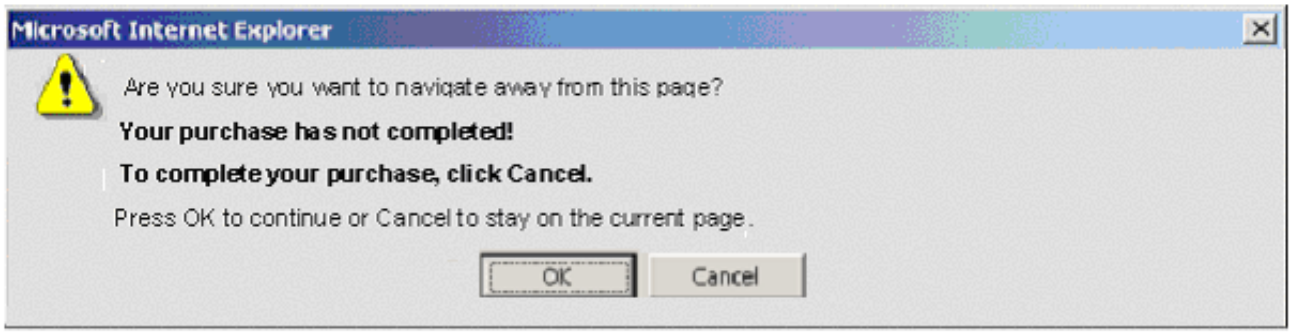
The text "password" in the following alert can be replaced with the language the issuer is using to communicate the password to the cardholder. Other examples include dynamic password or one-time password.

Figure 1–3: Example of Browser Alert for Cardholder Clicking the Exit Button



1.4.2 Example 2

Figure 1–4: Example of Browser Alert for Cardholder Clicking the X Button



2 Merchant User Interface (UI) Requirements

The merchant website must comply with Visa Secure user interface (UI) requirements. This section outlines the user interface requirements and best practices for the following:

- Checkout Page
- Authentication Page
- Refresh/Back Button Alert
- Authentication Failure Page

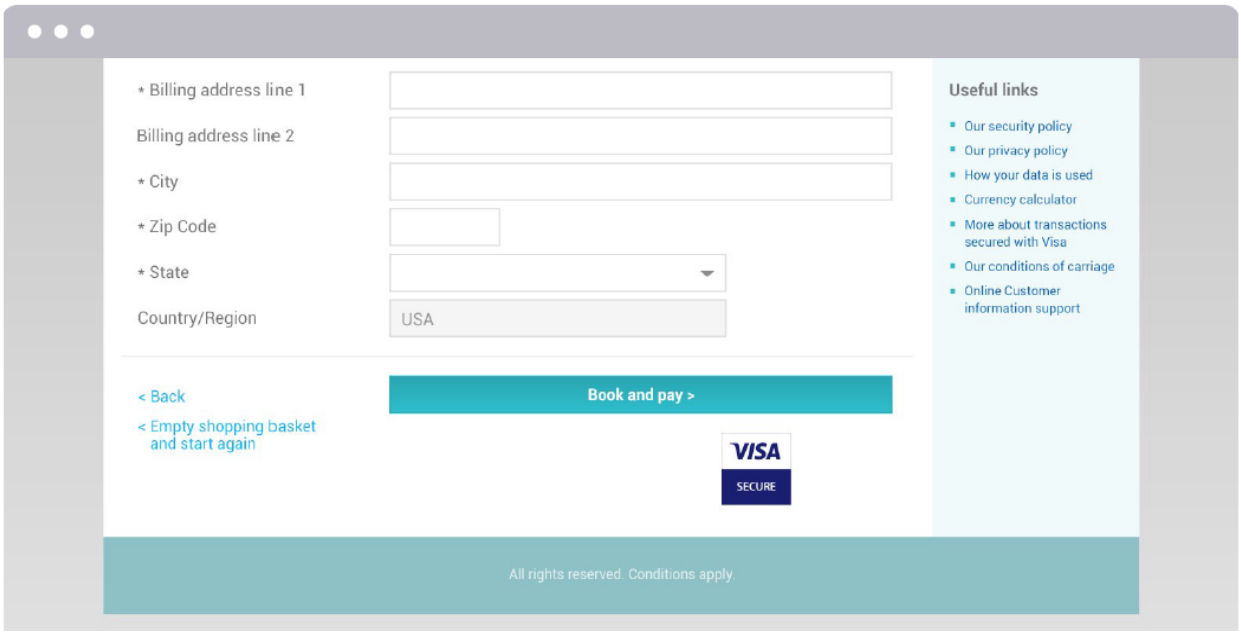
2.1 Checkout Page

It is recommended that merchants include the Visa Secure merchant symbol on the checkout page. The presence of the symbol helps build cardholder awareness that Visa Secure is part of the merchant's overall checkout process reassuring the cardholder that if a cardholder entry/challenge page is displayed to the cardholder, it is legitimate and not associated with phishing.

The Visa Product Brand Standards website at http://www.productbrandstandards.com provides information on the use of the Visa Secure symbol. See References in the Introduction for more information.

The following provides an example of a merchant checkout page containing the Visa Secure merchant symbol.

Figure 2–1: Merchant Checkout Page with Visa Secure Badge



2.2 Authentication Page

Once the cardholder completes the merchant checkout page and clicks on the "submit" or "buy" button, an authentication page will be displayed to the cardholder[1]. The merchant sets up the authentication page and the Issuer ACS populates it with the authentication information based on the authentication method that the issuer supports.

For example, the authentication page could be a simple processing page for risk-based authentication (see Figure 4-2: Authentication Page with Top Frame, Risk-Based Example) or it could request the cardholder to provide a dynamic password (Figure 4-3: Authentication Page with Side Frame, Password Example). The specific contents of the authentication page are transparent to the merchant; the merchant only needs to ensure that the set up for the authentication page meets Visa requirements.

The following provides the requirements and best practices for the authentication page:

- Inline Page—The authentication page must use an inline page. The use of a pop-up page is not permitted. In addition, for U.S. merchants and all new implementations, the inline page must be framed.

[1] Assuming the issuer participates in Visa Secure and the card is eligible for authentication.

- No Promotional Messages—The merchant must not display promotional messages to cardholders. It is important that cardholders have confidence in the authentication session with their card issuer.
- Size—The frame opened for the Issuer ACS to present the Visa Secure window must be large enough to present the entire 390 pixel width by 400 pixel length authentication page, without scrolling, over a standard range of browser resolutions. To implement a framed inline page, merchants may place a frame at the top of the page and/or on the side of the page, as illustrated in the following figures.
- Text—It is recommended that the merchant provide the following text at the top of the page:
  - Processing, please wait. Do not click the refresh or back button or this transaction may be interrupted.
- Status Indicator—Visa also recommends that merchants include a "processing" indicator next to the inline text to provide a visual cue to customers that the purchase process is continuing in the background (so they know the system is working and not frozen). It is important that the status indicator have some kind of simple movement such as dots or arrows moving from left to right.

Figure 2–2: Authentication Page with Top Frame (Risk-based Example)

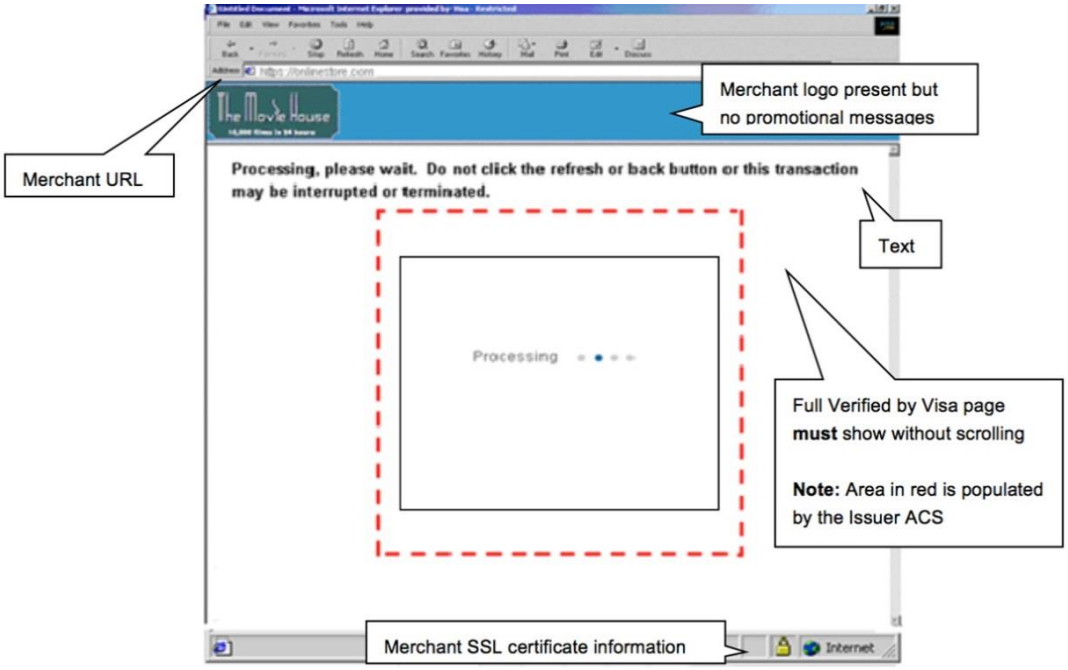
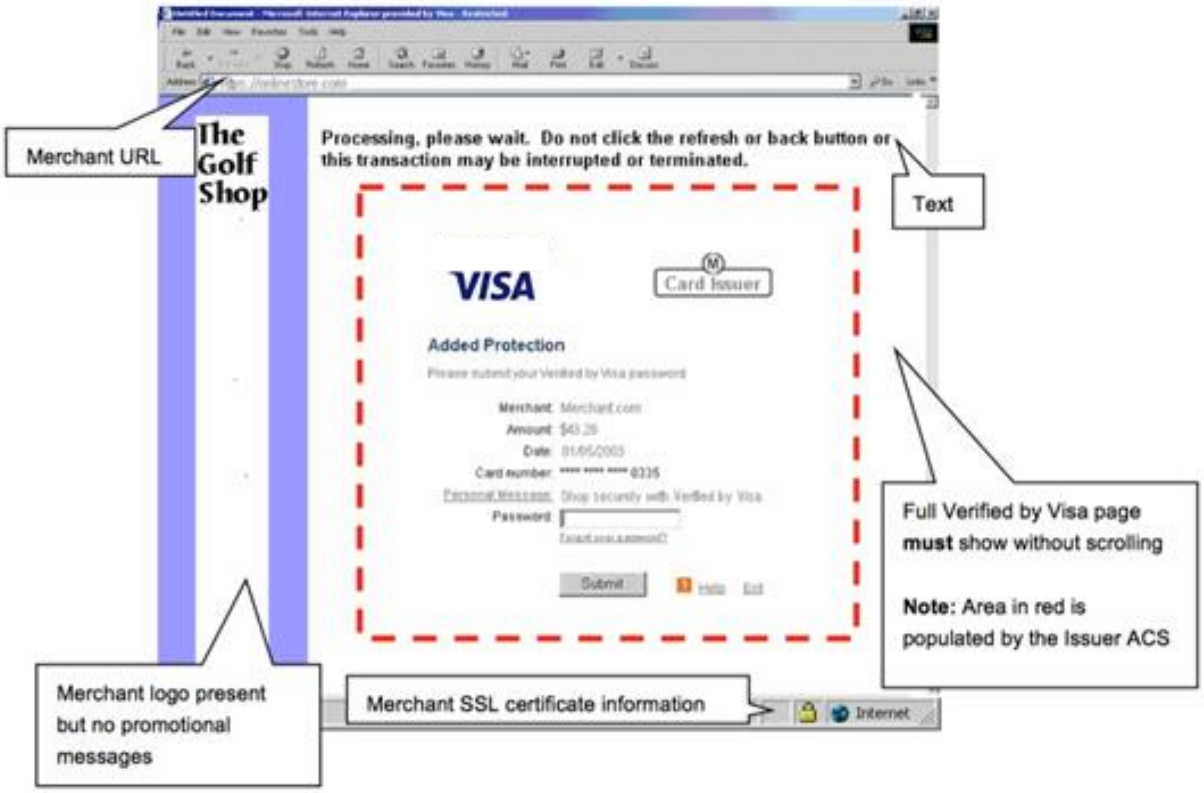


Figure 2–3: Authentication Page with Side Frame (Passcode Example)



2.3 Refresh/Back Button Alert

When a customer is uncertain of the procedure or whether he/she is doing things correctly, a common impulse is to click on the Back or Refresh button. In the event that this occurs, it is recommended that the merchant display an alert to the cardholder. The alert communicates to the cardholder that taking this action will disrupt an important process and the purchase transaction will not be completed. The alert sends a clear message to the cardholder that things are progressing as they should be.

Figure 2–4: Refresh/Back Button Alert

2.4 Authentication Failure Page

When authentication fails (i.e., the merchant receives a Payer Authentication Response message with a value of N), the merchant can assess the risk of the transaction using information and tools outside of Visa Secure to determine whether to accept the risk of the transaction and proceed with authorization or terminate the transaction:

- Proceed with Authorization—If the merchant decides to proceed with authorization, the merchant uses an ECI 07 (non-authenticated e-commerce transaction) and sends the authorization message to the issuer where the issuer can approve or decline the transaction. If approved and the transaction proves to be fraudulent, the merchant assumes liability.
- Terminate Transaction—If the merchant decides not to proceed with authorization, the suggested wording for the failed authentication message to the cardholder is:
  - Authentication Failed: Your financial institution has indicated that it could not authenticate this transaction via Visa Secure. You may complete the purchase by clicking here to select another form of payment.

It is recommended that merchants provide an easy, simple recovery mechanism to cardholders that fail Visa Secure authentication. On the page where the merchant provides the "Authentication Failed" message, the recovery mechanism may either provide an immediate opportunity for the cardholder to enter a new payment card number, including a different Visa card number, and click to Try Again or provide a button that, when clicked, presents a new page that allows the cardholder to easily reinitiate the purchase.

A.1 Glossary

Term	Definition
0-9	
3-D Secure (3DS)	The Three Domain Secure (3-D Secure™ or 3DS) protocol has been developed to improve transaction performance online and to accelerate the growth of e-commerce. The objective is to benefit all participants by providing issuers with the ability to authenticate cardholders during an online purchase, thus reducing the likelihood of fraudulent usage of payment cards and improving transaction performance. Visa owns 3DS 1.0.2 and licenses it to other payment providers. EMVCo owns 3DS 2.0. Visa's offering of 3DS is called Visa Secure.
3-D Secure Specification	A software protocol that enables secure processing of transactions over the Internet and other networks.
A	
Access Control Server (ACS)	A server hardware/software component that supports Visa Secure authentication and other functions. The ACS is operated by the issuer, ACS provider, or the issuer's processor. In response to Visa Directory Server inquiries, the ACS verifies that the individual card account number is eligible for authentication, receives authentication requests from merchants, authenticates the cardholder during online purchases, and provides digitally-signed authentication response messages (containing the authentication results and other Visa Secure data) to the merchant and to the Authentication History Server.
Acquirer	A member that signs a merchant or payment facilitator or disburses currency to a cardholder in a cash disbursement, and directly or indirectly enters the resulting transaction receipt into interchange.
Attempts Response	A message from a Visa Secure issuer in response to an authentication request, indicating that the issuer or cardholder is not participating in Visa Secure.
Authentication Data	All transaction-related data associated with a Visa Secure authentication request.

Term	Definition
Authentication Request	A request for cardholder authentication from a Visa Secure merchant.
Authentication Response	A response from a Visa Secure issuer, or Visa on behalf of an issuer, in response to an authentication request. Authentication responses include: • Attempt Responses • Authentication Confirmations • Authentication Denials • Unable-to-Authenticate Responses
Authorization	A process where an issuer, a VisaNet processor, or stand-in processing approves a transaction. This includes offline authorization.
C	
Cardholder	An individual who is issued and authorized to use either or both a: • Card • Virtual Account
Cardholder Authentication	The process used to ensure that the transaction is being initiated by the rightful owner of the Visa account.
D	
Directory Server	See Visa Directory Server.
Dynamic Password	See One-Time Passcode.
E	
Electronic Commerce Indicator (ECI)	A value used in an e-commerce transaction to indicate the transaction's level of authentication and security.
I	
Issuer	A member that enters into a contractual relationship with a cardholder for the issuance of one or more card products.
Issuer Domain	The systems and functions of issuers and cardholders in 3-D Secure. See also Merchant/Acquirer Domain and Interoperability Domain.

Term	Definition
M	
Merchant	An entity that accepts a Visa Card for the sale of goods or services and submits the resulting transaction to an acquirer for interchange, directly or via a payment facilitator. A merchant may be a single merchant outlet or represent multiple merchant outlets.
Merchant Server Plug-In	A module integrated into merchant store-front applications used to process Visa Secure authentication transactions. It provides an interface to the merchant commerce server.
O	
One-Time Passcode	A passcode that the issuer provides to the cardholder (usually via text or email) which can be used on one transaction to verify the identity of the cardholder.
P	
Payer Authentication Request (PAReq)	A message sent from the MPI to the Issuer ACS through the Visa Directory Server to initiate cardholder authentication. See "Authentication Request."
Payer Authentication Response (PARes)	The Issuer ACS response to the Payer Authentication Request (PARes). See "Authentication Response."
Personal Assurance Message	A message selected by the cardholder during the static password activation process that is displayed during the authentication process to indicate that the password request is from a valid source. The personal message is between 1 and 30 characters and must not contain text that is included in the password.
Proof of Attempted Authentication	See Attempts Functionality.
R	
Risk-Based Authentication	Risk-based authentication is a Visa Secure authentication approach. It may include analyzing historical data about the cardholder and merchant as well as taking into consideration the specifics of the transaction such as the amount or location. The risk profile is used to determine if authentication is successful, failed, or if step-up authentication (such as a one-time passcode) is required. See Step-up Authentication for additional information.

Term	Definition
S	
Step-Up Authentication	When the issuer supports risk-based authentication and the results of authentication indicate that further authentication is required, the issuer can optionally request additional authentication from the cardholder such as via a one-time passcode. This additional authentication method is referred to as step-up authentication.
T	
Technology Provider	An entity that provides technical services in support of the Visa Secure program.
Three-Domain Secure	See 3-D Secure.
V	
Visa Secure	Visa's implementation of the 3-D Secure Protocol.
Visa Secure Badge	A mark used in conjunction with Visa Secure. One of the Visa-owned marks.
Visa Secure Signing Certificate	The certificate used to digitally sign authentication responses sent from the ACS to a Visa Secure merchant. Upon receipt, the merchant verifies the digital signature to ensure that the response was sent from an authorized ACS.
Verify Enrollment Request (VEReq)	A message sent from the MPI to the Issuer ACS via the Visa Directory Server to verify that the issuer participates in Visa Secure and the card is eligible for authentication.
Verify Enrollment Response (VERes)	A message sent from the Issuer ACS (or Visa Directory Server on its behalf) in response to a Verify Enrollment Request.
Visa Directory Server	A server hardware/software component that is operated by Visa, whose primary function is to route authentication requests from merchants to specific Access Control Servers and to return the results of authentication.
VisaNet	The systems and services, including the V.I.P. System, Visa Europe Authorization Service, and BASE II, through which Visa delivers online financial processing, authorization, clearing, and settlement services to members, as applicable.