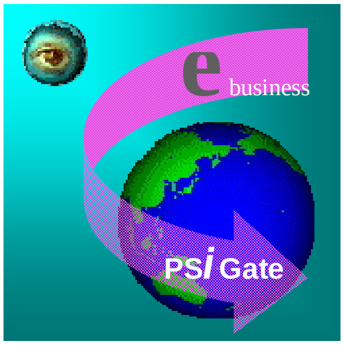
PSiGate 3-D Authentication (PSi3D)

Integration Guide

Version 2.06

Nov. 05, 2008



Index

Figures

Tables

1. About this manual

This manual is intended for the use of storefront's merchants who wish to use the service of PSiGate 3-D Authentication (PSi3D) system. The functionality of PSi3D is to verify cardholder account ownership during a purchase transaction in the remote environment.

2. Overview

2.1 3-D Secure™ Protocol

Payment authentication is the process of verifying cardholder account ownership during a purchase transaction in an online commerce environment.

Visa has developed the Three-Domain Secure (3-D Secure™) Protocol to improve transaction performance online and to accelerate the growth of electronic commerce (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 Credit cards and improving transaction performance.

The Three Domain Model divides payment systems as follows:

Issuer Domain	Systems and functions of issuer and its customers (cardholders)
Acquirer Domain	Systems and functions of the acquirer and its customers (merchants)
Interoperability Domain	Systems, functions, and messages that allow Issuer Domain systems and Acquirer Domain systems to interoperate worldwide

2.2 PSi3D

PSi3D acts as the role of Merchant Server Plug-in (MPI) that belongs to the part of Acquirer Domain. PSi3D creates and processes payment authentication messages, then sends the authentication results to merchant software. According to the authentication results, merchant software decides the further processing. PSi3D can add signification value in terms of increased sales, customer satisfaction, reduced fraud loses, and decreasing the operational costs associated with charge back processing resulting from cardholder repudiation of online purchase.

2.3 Support Version

The current PSi3D supports the following 3-D Secure Protocol.

- Version 1.0.1
- Version 1.0.2

3. Process flow

Figure 1 illustrates and Table 1 describes the steps in the purchase transaction flow.

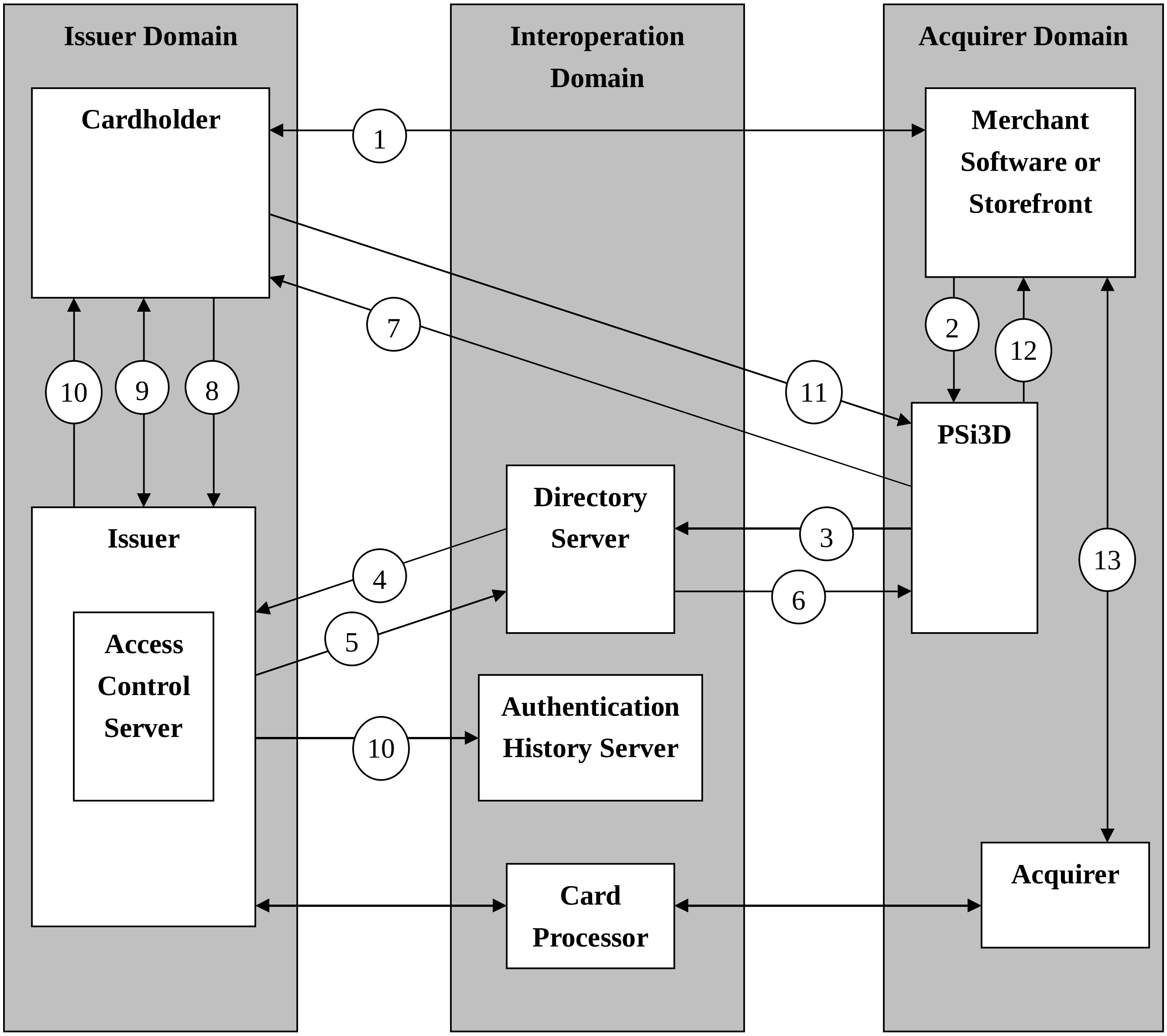


FIGURE 1: SAMPLE PURCHASE TRANSACTION

Step 1	Shopper browses at merchant site, add items to shopping cart, then check out.
Step 2	Merchant Software or Storefront sends authentication data (card information and purchase information) to PSi3D.
Step 3	PSi3D generates Verify Enrollment Request and sends to Directory Server.
Step 4	Directory Server queries appropriate Access Control Server (ACS) to determinate whether authentication is available
Step 5	ACS responds to Directory Server.
Step 6	Directory Server forwards ACS response PSi3D.
Step 7	PSi3D creates and sends Payer Authentication Request to ACS via shopper's browser.
Step 8	ACS receives Payer Authentication Request.
Step 9	ACS authenticates shopper by using processes applicable to the card information (password, PIN, etc.)
Step 10	ACS returns Payer Authentication Response to PSi3D and sends selected data to Authentication History Server.
Step 11	PSi3D receives and validates Payer Authentication Response.
Step 12	PSi3D sends Authentication Results to Merchant Software or Storefront.
Step 13	Merchant Software or Storefront processes authorization according to Authentication Results.

Table 1: Sample Purchase Transaction Steps' Description

4. PSi3D Url

This is the Url storefront should post authentication data to.

https://psi3d.psigate.com/psi3d/psipa

5. Authentication Data

The following table illustrates the format of authentication data posted from Merchant Software or Storefront to PSi3D. The sample code slip shows how to post authentication data to PSi3D via HTML form.

5.1 Data Fields

Filed name	Description	Max Length	Requirement	Note
PSi3D_Account	Merchant Account	20	Required	Provided by PSiGate
PSi3D_CardholderPAN	Account number; it must be the same PAN that will be used in the authorization request.	19	Required	The value may be: • Credit card number • A permanent account number that's only used online • Produced by the wallet as a proxy • Pulled from the merchant's local wallet • Or any other number that can be submitted for authorization
PSi3D_CardExpiryDate	Card expiration date	4	Required	YYMM
PSi3D_OID	Order ID	100	Optional	Should be unique for the merchant. Used for tracing transactions.

Table 2: Authentication Data

Filed name	Description	Max Length	Requirement	Note
PSi3D_Amount	The purchase amount.	12	Required	Up to 12- digit numeric amount in minor units of currency with all punctuation removed. Examples : If the purchase is for USD 123.45, the field will contain the value 12345. For currency codes and minor units, see ISO 4217.
PSi3D_Description	Order Description	125	Optional	
PSi3D_ReturnURL	The URL PSi3D will return to after finished the authentication	256	Required	
PSi3D_MD	Merchant data. Data used to identify the consumer session.	500	Optional	If using binary data, it must be base64 encoded. **If it is confidential data, it must be encrypted.**
PSi3D_RecurFlg	Recurring payment flag. Indicates the transaction is recurring payment (including installment) or not.	1	Required	1: Recurring payment 0: Non recurring payment

Table 2: Authentication Data, continued

Filed name	Description	Max Length	Requirement	Note
PSi3D_Frequency	Recurring frequency	3	Condition required	Required if PSi3D_ RecurFlg is 1. An integer indicating the minimum number of days between authorizations.
PSi3D_RecurExpiry	Recurring payment expiry date	8	Condition required	Required if PSi3D_ RecurFlg is 1. Format is YYYYMMDD. The date after which no further authorizations should be performed.
PSi3D_Installment	Installment payment data	3	Optional	An integer greater than one indicating the maximum number of permitted authorizations for installment payments.

Table 2: Authentication Data, continued

5.2 Test Account Information

PSiGate's testing environment supports a shared test account that you are welcome to use while developing and testing your interface.

To process a transaction through the test account,

- set the PSi3D_Account value to "1000016"
- set the CardholderPAN to "401200103714111"

To review your VBV transactions, https://psi3d.psigate.com/psi3dv/merlogin.htm
To review your MasterCard SecureCode transactions, https://psi3d.psigate.com/psi3dm/merlogin.htm
The Login information of either website follows:

CID: 1000016
Password: psitesting

5.3 Sample Code

The sample code describes how to post authentication data to PSi3D via HTML form.

```
<FORM name=”PSi3DForm” action=”https://psi3d.psigate.com/psi3d/psipa”
    method=”POST”>
    <TABLE>
        <TR><TD> Merchant Account: </TD>
           <TD><INPUT type=”text” name=”PSi3D_Account” value=”1000016”>
             </TD>
        </TR>
        <TR><TD> CardholderPAN: </TD>
           <TD><INPUT type=”text”
                name=”PSi3D_CardholderPAN”
                value=”401200103714111”>
             </TD>
        </TR>
        <TR><TD> CardExpiryDate: </TD>
           <TD><INPUT type=”text”
                name=”PSi3D_CardExpiryDate”
                value=”1308”>
             </TD>
        </TR>
        <TR><TD> Amount: </TD>
           <TD><INPUT type=”text”
                name=”PSi3D_Amount”
                value=”543254”>
             </TD>
        </TR>
        <TR><TD> ReturnURL: </TD>
           <TD><INPUT type=”text”
                name=”PSi3D_ReturnURL”
                value=”https://merchant.com/ResultPage.asp”>
             </TD>
        </TR>
        <TR><TD> Merchant Data: </TD>
           <TD><INPUT type=”text”
                name=”PSi3D_MD”
                value=”SessionId=49320759453”>
             </TD>
        </TR>
        <TR><TD> Recurring Payment: </TD>
           <TD><INPUT type=”text”
                name=”PSi3D_RecurFlg”
                value=”0”>
             </TD>
        </TR>
    </TABLE>
    <INPUT type=”submit” name=”submit” value=”Authentication”>
</FORM>
```

6 Authentication Results

PSi3D will post the following fields to Merchant Software or Storefront via shopper's browser. Merchant must catch the fields in **bold** and include them in the subsequent authorization request submitted to the acquirer if authentication is successful or a proof of authentication attempt (PSi3D_Ret_ResultCode = "0" or PSi3D_Ret_ResultCode = "3").

6.1 Return fields

The following table shows the format of return fields.

Filed name	**Description**	**Max Length**	**Note**
PSi3D_Ret_MerchantID	Merchant identifier	24	
PSi3D_Ret_OID	Order ID	100	Returns the same value as PSi3D_OID if provided from merchant.
PSi3D_Ret_Amount	The purchase amount	20	Returns the same value as PSi3D_Amount
PSi3D_Ret_Currency	The purchase currency	3	Currency Code
PSi3D_Ret_MD	Merchant data. Data used to identify the consumer session.	500	Returns the same value as PSi3D_MD if provided from merchant.
PSi3D_Ret_ResultCode	Indicates the result of the authentication.	1	See Table 4 for details.
PSi3D_Ret_XID	Transaction Identifier	28	Exactly 28 characters. **This field must be sent to the acquirer during authorization.**
PSi3D_Ret_CAVV	Cardholder Authentication Verification Value	28	Exactly 28 characters. **This field must be sent to the acquirer during authorization.**
PSi3D_Ret_ECI	Electronic Commerce Indicator	2	2 decimal digits. **This field must be sent to the acquirer during authorization.**

Table 3: Return fields

Filed name	**Description**	**Max Length**	**Note**
PSi3D_Ret_TXStatus	Transaction Status	1	Indicates whether a transaction qualifies as an authenticated transaction. Y: Authentication Successful Customer was successfully authenticated. N: Authentication Failed Customer failed authentication. Transaction denied. U: Authentication Could Not Be Performed. Authentication could not be completed, due to technical or other problems. A: Attempts Processing Performed. Authentication could not be completed, but a proof of authentication attempt (CAVV) was generated.
PSi3D_Ret_ErrCode	Error Code	5	See Table 5, 6, 7 for details.
PSi3D_Ret_ErrMsg	Error Description	256	See Table 5, 6, 7 for details.
PSi3D_Ret_ErrDetail	Error Detail	256	May identify the specific data element(s) (comma-delimited list) that caused PSi3D_Ret_ErrCode or a description of system failure. See Table 5, 6, 7 for details.
PSi3D_Ret_VendorCode	Vendor Code	256	Vendor specific error code or explanatory text to be used for trouble shooting.

Table 3: Return fields, continued

6.2 Result Code Causes and Responses

The Result Code is returned from the field of PSi3D_Ret_ResultCode. Merchants should do further processing according to the following table. The column of CCE should be used if the acquirer is using Clear Commerce Engine, otherwise Merchants should refer to the column of Non-CCE.

PSi3D Result Code	Description	Merchant Action (Non-CCE)	Merchant Action (CCE)
0	Cardholder Enrolled Authentication Successful.	Submit authorization request with PSi3D_Ret_XID , PSi3D_Ret_CAVV, and PSi3D_Ret_ECI to acquirer.	Set PayerSecurityLevel to 2, set PayerAurhenticationCode to the returned PSi3D_Ret_CAVV, and set PayerTXnId to the returned PSi3D_Ret_XID.
1	Cardholder authentication failed.	The merchant should disallow the purchase. Merchants are not permitted to submit transactions where the cardholder failed payment authentication. Prompt for a new card.	Do not submit the transaction to the CCE. It will be rejected. Prompt for a new card.
2	Authentication could not be performed.	Try PSi3D again or process a normal authorization request.	Try PSi3D again or set PayerSecurityLevel to 4.
3	Proof of authentication attempt was generated. Authentication was not available, but functionality was available (through the Issuer, Visa, or a third party) to generate a proof of authentication attempt.	For Visa, submit authorization request with PSi3D_Ret_XID , PSi3D_Ret_CAVV, and PSi3D_Ret_ECI to acquirer. **For MasterCard or MaestroCard, please contact to your payment service provider to decide which fields should be sent with your authorization request.**	Set PayerSecurityLevel to 6, set PayerAuthenticationCode to the returned PSi3D_Ret_CAVV, and set PayerTXnId to the returned PSi3D_Ret_XID.

Table 4: Result Code

7 Error Messages

7.1 Errors from PSi3D

PSi3D generates the following errors:

Error Code	Error Description	Error Detail
P01	Acquire BIN required.	PSi3D_AcqBIN
P02	Acquire BIN too long.	PSi3D_AcqBIN
P03	Unable to add ErrMsg for VEReq to DB.	A description of the failure
P04	Unable to add ErrMsg for retried VEReq to DB.	A description of the failure
P05	Unable to add merchant data to DB.	A description of the failure
P06	Unable to add PAReq to DB.	A description of the failure
P07	Unable to add retried VEReq to DB.	A description of the failure
P08	Unable to add retried VERes to DB.	A description of the failure
P09	Unable to add retried VERes syntax ErrMsg to DB.	A description of the failure
P10	Unable to add VEReq to DB.	A description of the failure
P11	Unable to add VERes to DB.	A description of the failure
P12	Unable to add VERes syntax ErrMsg to DB.	A description of the failure
P13	Cardholder PAN not in one of card ranges.	PSi3D_CardholderPAN
P14	Cardholder PAN required.	PSi3D_CardholderPAN
P15	Cardholder PAN too long.	PSi3D_CardholderPAN
P16	Unable to deflate PAReq.	A description of the failure
P17	PSi3D (or PSi3DRes) initiation error.	A description of the failure
P18	Invalid amount.	PSi3D_Amount
P19	Invalid card expiry date.	PSi3D_CardExpiryDate
P20	Merchant data too long.	PSi3D_MD
P21	Merchant ID required.	PSi3D_MerchantID
P22	Merchant ID too long.	PSi3D_MerchantID
P23	Merchant not registered.	PSi3D_MerchantID,PSi3D_AcqBIN
P24	Merchant return URL required.	PSi3D_ReturnURL
P25	Merchant return URL too long.	PSi3D_ReturnURL
P26	No supported protocol.	protocol
P27	Order ID too long.	PSi3D_OID
P28	Posting ErrMsg for retried VERes failed.	A description of the failure
P29	Posting ErrMsg for VERes failed.	A description of the failure
P30	Posting VEReq failed.	A description of the failure
P31	Unable to query merchant configuration information.	A description of the failure
P32	Reposting VEReq failed.	A description of the failure
P33	Unable to send PAReq.	A description of the failure
P34	Unable to send return data to merchant.	A description of the failure

Table 5: Errors From PSi3D

Error Code	Error Description	Error Detail
P35	Unable to update Current Version to DB.	A description of the failure
P36	VERes syntax error.	The specific data element(s) (comma-delimited list) with invalid format or a description of system failure.
P37	VERes syntax error for retried VEReq.	The specific data element(s) (comma-delimited list) with invalid format or a description of system failure.
P38	Unable to query merchant data from DB.	A description of the failure
P39	Unable to inflate PaRes.	A description of the failure
P40	Unable to add PARes syntax ErrMsg to DB.	A description of the failure
P41	Posting ErrMsg for PARes failed.	A description of the failure
P42	PARes syntax error.	The specific data element(s) (comma-delimited list) with invalid format or a description of system failure.
P43	PARes signature validation error.	A description of the failure
P45	Unable to add CRReq to DB.	A description of the failure
P46	Unable to add CRRes syntax ErrMsg to DB.	A description of the failure
P47	Posting ErrMsg for CRRes failed.	A description of the failure
P48	CRRes syntax error.	The specific data element(s) (comma-delimited list) with invalid format or a description of system failure.
P49	Unable to add CRRes to DB.	A description of the failure
P50	Unable to clear Card Range Cache.	A description of the failure
P51	Unable to refresh Card Range Cache.	A description of the failure
P52	Unable to add return data to DB.	A description of the failure
P53	Cardholder authentication failed.	The specific data element(s) (comma-delimited list) that caused authentication failure or a description of system failure.
P54	Unable to add PARes to DB.	A description of the failure
P55	Posting CRReq failed.	A description of the failure

Table 5: Errors From PSi3D, continued

Error Code	Error Description	Error Detail
P56	Unable to retrieve ACS URL.	A description of the failure
P57	Accessing CardRange table error.	A description of the failure
P58	Invalid MD.	Invalid PARes Form from ACS or unknown person
P59	TranIDs object is null.	PSi3D service may not be started.
P60	ACS is unable to authenticate.	
P61	Cardholder Not Participating.	PSi3D_CardholderPAN
P62	Invalid recurring payment flag.	PSi3D_RecurFlg
P63	Invalid recurring frequency.	PSi3D_Frequency
P64	Invalid recurring payment expiry date.	PSi3D_RecurExpiry
P65	Invalid installment payment data.	PSi3D_Installment
P98	Transient system failure.	A description of the failure
P99	Permanent system failure.	A description of the failure

Table 5: Errors From PSi3D, continued

7.2 Errors for Invalid Request Code

This table described the errors for Invalid Request Code from Directory Server or ACS.

Error Code	Error Description	Error Detail
I50	Acquirer not participating in 3-D Secure.	
I51	Merchant not participating in 3-D Secure.	
I52	Password required, but no password was supplied.	
I53	Supplied password is not valid.	
I54	ISO code not valid.	Name of invalid element(s); if more than one element is detected, this is a comma-delimited list.
I55	Transaction data not valid.	Name of invalid element(s); if more than one element is detected, this is a comma-delimited list.
I56	VEReq or PAReq was incorrectly routed.	Name of element(s) that caused the ACS to decide that VEReq or PAReq was incorrectly routed.
I57	Serial Number can not be located.	
I58	Issued only by the Directory Server.	“Access denied, invalid endpoint.”
I98	Transient system failure.	A description of the failure
I99	Permanent system failure.	A description of the failure

Table 6: Errors for Invalid Request Code

7.3 Errors for Error Handling

These errors are for Error Handling between components in 3-D Secure generated by Directory Server or ACS.

Error Code	Error Description	Error Detail
E1	Root element invalid.	The invalid root element.
E2	Message element not a defined messages.	The invalid message element.
E3	Required element missing.	Name of required element that was omitted.
E4	Critical element not recognized.	Name of critical element that was not recognized.
E5	Format of one or more elements is invalid according to the specification.	Name of invalid element(s); if more than one invalid element is detected, this is a comma-delimited list.
E6	Protocol version too old.	The oldest version supported.
E98	Transient system failure.	A description of the failure.
E99	Permanent system failure.	A description of the failure.

Table 7: Errors for Error Handling