Web Services Guide

For Third Party Tokenisation Service Providers

Version: 1.1
25 April 2024

Publication number: TPWSG-1.1-4/25/2024

For the latest technical documentation, see the Documentation Portal.

Thredd 6th Floor, Victoria House, Bloomsbury Square, London, WC1B 4DA
Support Email: occ@thredd.com
Support Phone: +44 (0) 203 740 9682

Copyright

To the maximum extent permitted by law, Thredd Ltd shall not be liable to any person or organisation, in any manner whatsoever from the use, construction or interpretation of, or the reliance upon, all or any of the information or materials contained in this guide.

The information in these materials is subject to change without notice and Thredd Ltd. assumes no responsibility for any errors.

About this Guide

This guide is intended as a reference guide, to provide information on the available Thredd web services and fields in each web service, for third party tokenisation (digital wallet) service providers who offer services to Thredd customers and who need to use the Thredd web services API to integrate their service.

Target audience

This guide is aimed at third party developers who need to integrate their service to Thredd. You should know how to implement SOAP-based calls and handle the response.

Note: Third party service providers must request access to the APIs on a per customer basis.

What's changed?

If you want to find out what's changed since the previous release, see the Document History section.

How to use this Guide

Before you start:

- Make sure you can connect to the Thredd web service, by implementing a simple call, as explained in Using the API.

Implementing web service calls

- When implementing a web service request, you must at a minimum include the mandatory request fields and handle the fields that are mandatory in the response.
- Where a field requires you to submit a code value or returns a code value, the guide provides links to the relevant appendix for details. If in doubt as to which code to include in your request, you should use the default or recommended value.
- Do not change the default `xmlns` attributes (XML namespaces) in the SOAP request.
- Don't use spaces in xml tags.
- Please pay particular attention to XML tag name spelling and capitalisation. Different web services may sometimes adopt different case and naming conventions. If in doubt, always refer to the Thredd-provided SOAP WSDL. See Using the API.

Conventions used in this Guide

When reading the tables in this guide, note the following information is provided for each XML field:

Element	Description
Tag	The XML tag name. Please pay particular attention to the capitalisation and spelling. Where a tag name is used within text, this is formatted as in the following example: `<ActionCode>`

Type	The type of field value supported. Options include:
	N = number
	AN = alpha-numeric
	YYYY-MM-DD = date format: Year-Month-Date
	HHMMSS = time format: Hour-Minute-Second
	D = decimal
	B = boolean

Minimum / Maximum	The allowed minimum and maximum field length. If in doubt, refer to the WSDL or examples provided in the guide.

Element	Description
Length	
Request / Response	The status of the field in the request and response. Options are: Mandatory = must be included in the request and will be in the response Conditional = this field is mandatory under specified conditions. Refer to the description for details. Optional = can be included. May be in the response. Omit = you should omit this field. Will not be in the response

Other Documentation

Refer to the table below for a list of other relevant customer documents that should be used together with this guide.

Document	Description
Tokenisation Service Guide	Guide for Thredd customers, which provides details of the Thredd payment tokenisation (digital wallet) service, using MDES (Mastercard) or VDEP (Visa).
Web Service Guide	Guide for Thredd customers, which provides details of the available Thredd web services and how to use them.

Tip: For the latest technical documentation, see the Documentation Portal.

Overview

The Thredd web service API is based on SOAP Version 1.1.

SOAP (Simple Object Access Protocol) is a messaging protocol for exchanging structured information in the implementation of web services. It uses Extensible Markup Language (XML) for its message format and relies on application layer protocols such as HTTP for message negotiation and transmission. SOAP allows developers to invoke processes running on disparate operating systems (such as Windows, macOS, and Linux) to authenticate, authorise and communicate using XML.

The figure below describes how the web services API is used to integrate external systems to Thredd.

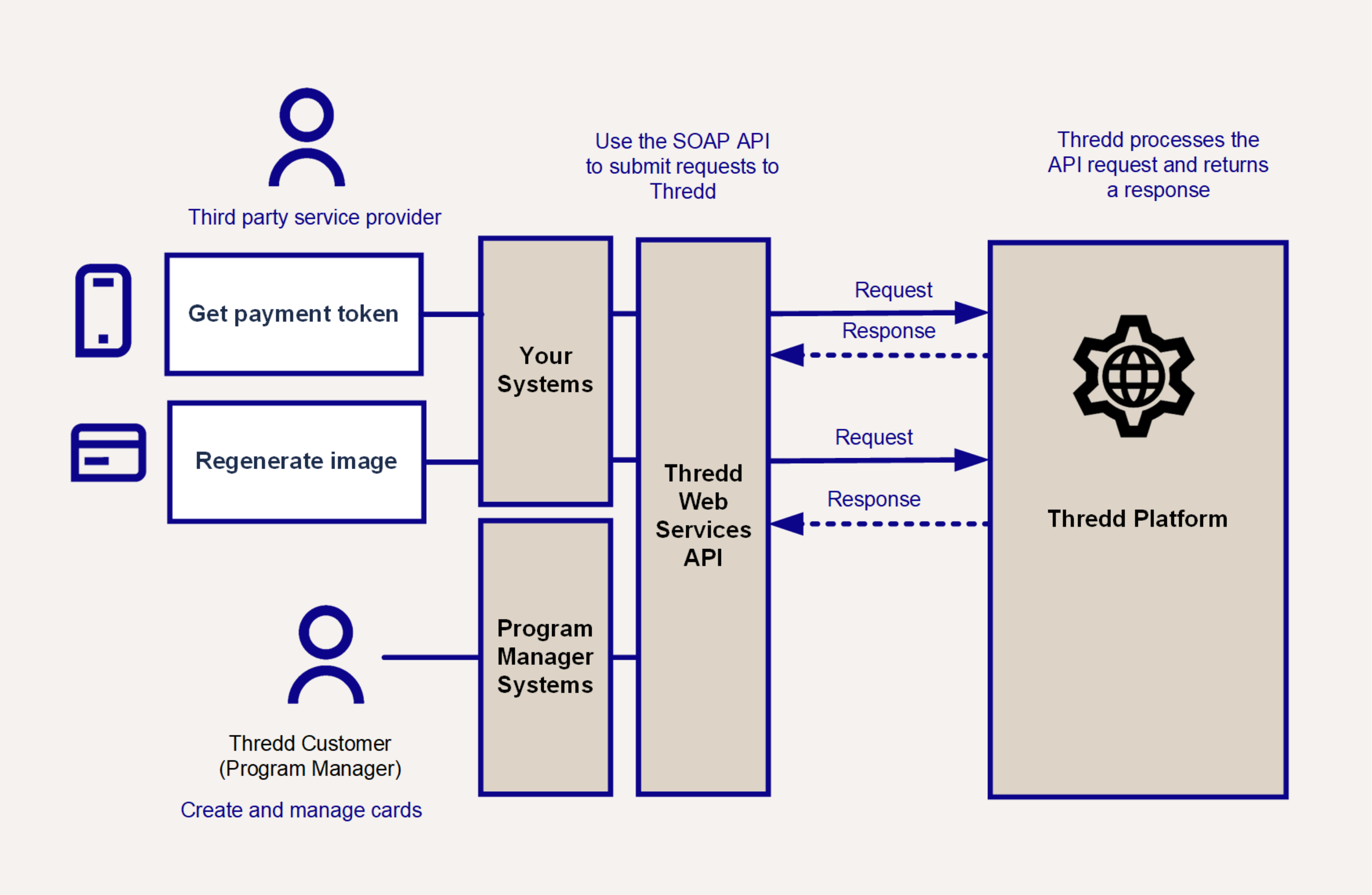

Third party service provider
Use the SOAP API to submit requests to Thredd
Thredd processes the API request and returns a response
Get payment token
Regenerate image
Your Systems
Program Manager Systems
Thredd Web Services API
Request
Response
Request
Response
Thredd Platform
Thredd Customer (Program Manager)
Create and manage cards

Figure 1: Figure: API Architecture Overview

Note: Third party integrators may require a different URL to access the SOAP Web Services. This will be confirmed during your project setup phase.

Using the API

This section provides tips on how to integrate to Thredd using the SOAP web services API.

Using the Web Services

View the WSDL

You can open the following URL in a browser to view the structure of the WSDL:

https://ws-uat.globalprocessing.net:13682/service.asmx?WSDL

If you are a third party integrator providing services such as tokenisation (digital wallet) or virtual card setup, you will require a dedicated URL. This will be confirmed during the project setup phase.

> **Tip:** We recommend you always refer to the WSDL for the correct XML tag name spelling and capitalisation, as different web services may sometimes adopt different case and naming conventions.

Install a SOAP Application

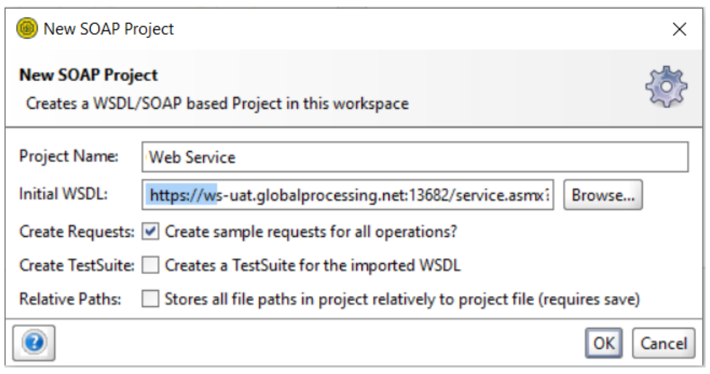
We recommend that you use an API tool that supports SOAP to test out the Thredd web services.

SOAPUI is an open-source application, which you can download and install on any computer, which enables you to submit test transactions to Thredd.

Load the SOAP WSDL

You can load the Thredd SOAP test WSDL into your SOAP tool. If you are using SOAPUI, then:

1. Select **File > New SOAP Project**.
2. Enter a project name and then, in the **Initial WSDL** field, paste the following URL: https://ws-uat.globalprocessing.net:13682/service.asmx?WSDL
3. Click **OK**.



New SOAP Project

New SOAP Project

Creates a WSDL/SOAP based Project in this workspace

Project Name: Web Service

Initial WSDL: https://ws-uat.globalprocessing.net:13682/service.asmx

Create Requests: ☑ Create sample requests for all operations?

Create TestSuite: □ Creates a TestSuite for the imported WSDL

Relative Paths: □ Stores all file paths in project relatively to project file (requires save)

Figure 2: Starting a new SOAP project and importing the WSDL

Introduction to the Web Services API

The table below lists the web services available to third party tokenisation service providers (ordered alphabetically).

API	Description
Ws_Payment_Token_Get	Gets the details for MDES (Mastercard Digital Enablement Service) Payment Token Cards.
Ws_Regenerate	Retrieves the card image configured in the Thredd platform for virtual and physical cards that have been converted which can then be displayed to the cardholder. If a customer wants to see the image some time after card creation you can regenerate the image. This web service can also be used to replace Lost or Stolen cards; the customer will be issued with a new PAN, CVV2 and Expiry Date.

Note: This is a small subset of the available Thredd web services API. For a full list of the API available to Thredd customers to manage their card program, refer to the Web Services Guide.

Card Regenerate Image

API: Ws_Regenerate

This web service retrieves the card details (PAN, CVV2,expiry date) configured on the Thredd platform which can then be displayed to the cardholder. If a cardholder wants to see the image some time after card creation you can regenerate the image by using this web service.

Record Description

Tag	Type	Minimum Length	Maximum Length	Description	Request	Response
<PublicToken>	AN	1	9	The card’s public token. Mandatory in request and response.	Mandatory	Mandatory
<RegenType>	N	1	1	Whether to regenerate the card. 0 = only return the CVV and do not regenerate; 1 = Regenerate the card only if it has a status of lost or stolen, else recreate the card image (note: legacy only, use Ws_Renew_Card. See Card Renew); 2 = Only create the card image, do not regenerate card.	Mandatory	Omit
<Sms_Required>	N	1	1	Whether an SMS is sent to the cardholder with the card's CVV. 1 = yes; 0 =No. The default is ‘0’. The SMS is configurable.	Mandatory	Omit
<Sms_Content >	N	1	1	Reserved for future use; set to 0.	Mandatory	Omit
<CVV>	AN	3	3	Card Verification Value, the 3-digit code printed on the back of the card.	Omit	Mandatory
<ActionCode>	AN	3	3	The action code for the response. See Action Codes.	Omit	Mandatory
<Image>	Base64 Binary			PGP-encrypted image of the card. Is only returned if a PGP key has been shared and configured.	Omit	Conditional
<ExternalRef>	AN	1	30	External reference code for the card. **Note**: Legacy field. Not used.	Optional	Omit
<TerminalID>	AN	1	15	Point of Sale (POS) or other terminal	Optional	Omit

Tag	Type	Minimum Length	Maximum Length	Description	Request	Response
				identifier, such as a hostname.		
< MailOrSMS>	AN	1	1	The cardholder's preferred contact method. 0 = SMS; 1 = email. 2 = SMS and email. Default value is ‘0’.	Optional	Omit
<CustAccount>	AN	1	25	Cardholder account number or reference number. You can use this reference to find the cards linked to a cardholder. Also displayed in Smart Client as *Customer Reference*.	Optional	Optional
<PAN>	N	16	19	Card Number displayed as masked. **Note**: For customers who are PCI DSS Compliant, the full PAN can be returned if required. This must be enabled at Program Manager level and will apply to all web services which return the PAN. Only returned for successful calls.	Omit	Conditional
<WSID>	N	1	19	Web service ID. Unique for every request.	Optional	Omit
<IssCode>	AN	1	4	Thredd Issuer (Program Manager) Code. Assigned by Thredd.	Optional	Omit
<FeeWaiver>	N	1	1	Indicates whether to waive any web service fee set up on the system: 0 = No, 1=Yes. Default is 0.	Optional	Omit

Request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:hyp="http://www.globalprocessing.ae/HyperionWeb">
   <soapenv:Header>
      <hyp:AuthSoapHeader>
         <hyp:strUserName>******</hyp:strUserName>
         <hyp:strPassword>******</hyp:strPassword>
      </hyp:AuthSoapHeader>
   </soapenv:Header>
   <soapenv:Body>
      <hyp:Ws_Regenerate>
         <hyp:PublicToken>123456789</hyp:PublicToken>
         <hyp:RegenType>1</hyp:RegenType>
         <hyp:Sms_Required>0</hyp:Sms_Required>
         <hyp:Sms_Content>0</hyp:Sms_Content>
         <hyp:ExternalRef>ABCD001</hyp:ExternalRef>
         <hyp:TerminalID>POS-TEST</hyp:TerminalID>
         <hyp:MailOrSMS>0</hyp:MailOrSMS>
         <hyp:WSID>2021123456789678</hyp:WSID>
         <hyp:IssCode>CLIENT</hyp:IssCode>
      </hyp:Ws_Regenerate>
   </soapenv:Body>
</soapenv:Envelope>
```

Response

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
   <soap:Body>
      <Ws_RegenerateResponse xmlns="http://www.globalprocessing.ae/HyperionWeb">
         <Ws_RegenerateResult>
            <PublicToken>123456789</PublicToken>
            <ActionCode>000</ActionCode>
            <CVV>123</CVV>
            <PAN>123456******4321</PAN>
         </Ws_RegenerateResult>
      </Ws_RegenerateResponse>
   </soap:Body>
</soap:Envelope>
```

Payment Token Get

API: Ws_Payment_Token_Get

This web service gets the details for both Mastercard Digital Enablement Service (MDES) payment token cards and Visa Token Service (VTS) cards.

Your request must provide one of the following card details: PAN, PublicToken, DPAN or Payment_Token_ID. If the MDES or VTS card is not specified, the call returns all linked MDES or VTS cards.

Record Description

Tag	Type	Minimum Length	Maximum Length	Description	Request	Response
<WSID>	N	1	19	Web service ID. Unique for every request.	Mandatory	Mandatory
<IssCode>	AN	1	4	Thredd Issuer (Program Manager) Code. Assigned by Thredd. If only <IssCode> is present in the request then this method returns the pending fee details of all cards belong to the given program manager.	Mandatory	Mandatory
<TxnCode>	AN	1	2	The Transaction Code. See Transaction Codes. Default value is 9.	Mandatory	Mandatory
<PAN>	N	16	19	Card Number. Unique card identifier.	Conditional	Omit
<PublicToken>	N	9	9	Thredd 9-digit public token of the card.	Conditional	Omit
<DPAN>	AN	16	19	Digital PAN value for the card.	Conditional	Omit
<Payment_Token_ID>	N	1	20	Payment token identifier for the MDES or VTS Card.	Conditional	Omit
<LocDate>	YYYY-MM-DD	10	10	The local current date in *year-month-date* format.	Mandatory	Mandatory
<LocTime>	HHMMSS	6	6	The local current time, in *hour-minute-second* format.	Mandatory	Mandatory
<ActionCode>	AN	3	3	The action code for the response. See Action Codes.	Omit	Mandatory

Payment Token Get Res Info

Tag	Type	Minimum Length	Maximum Length	Description	Request	Response
<Creator>	AN	1	10	Name of the system or process that created the token (e.g., MC-MDES and VISA-T).	Omit	Mandatory
<Creator_PAN_Ref>	AN	1	48	The token creator's unique reference to the linked card.	Omit	Mandatory
<Creator_Token_Ref>	AN	1	48	The token creator's unique reference for this payment token. (Mastercard Token Unique Reference (TUR) and Visa Token reference ID.)	Omit	Mandatory
<PANT>	N	16	19	PAN for the card linked to the MDES or VTS card.	Omit	Mandatory
<Payment_Token >	N	16	19	Payment token Device PAN for the MDES or VTS card.	Omit	Mandatory
<Payment_Token_ExpDate >	Date	10	10	Expiry date of the payment token.	Omit	Mandatory
<Payment_Token_ID>	N	1	20	Payment token identifier for the MDES or VTS card.	Omit	Mandatory
<Payment_Token_Type >	AN	1	2	Payment token type. See Payment Token Types.	Omit	Mandatory
<Wallet_ID>	AN	1	10	Name of the wallet provider this payment token uses (e.g., APPLE, ANDROID, SAMSON).	Omit	Mandatory
<Thredd_Status>	N	2	2	The Thredd status of the payment token for transacting. See Status Codes.	Omit	Mandatory
<Tokenised_Datetime>	DateTime	19	19	Date and time when tokenised, in the format: *yyyy-mm-ddhhmmss*.	Omit	Mandatory
<Tokenised_Status>	AN	1	1	Tokenised status of this payment token: U = unknown; 0 = not tokenised; 1=tokenised.	Omit	Mandatory
<Txn_Status>	AN	1	1	Status of the payment token as received from the payment token	Omit	Mandatory

Tag	Type	Minimum Length	Maximum Length	Description	Request	Response
				creator (normally Visa or Mastercard). After tokenisation, this is not changed by Thredd. A = Active D = Deleted (once in this status, it is normally never changed) I = Inactive N = Not Tokenised P = Pending S = Suspended U = Unknown X = Deactivated		
<Txn_Status_ Actor>	AN	1	10	Indicates which system last changed the transaction status.	Omit	Mandatory
<Txn_Status_ Change_ Datetime>	DateTime	16	16	Date and time that the transaction status was last changed. In the format: *yyyy-mm-ddhhmmss*.	Omit	Mandatory
<Accepted_ Terms_Date_ GMT>	DateTime	16	16	Date (in GMT) that terms and conditions were accepted by the cardholder (as received from the network).	Omit	Mandatory
<Accepted_ Terms_Version>	AN	1	32	Version of the terms and conditions which were accepted by the cardholder (as received from the network).	Omit	Mandatory
<Auth_Datetime>	DateTime	16	16	Date and time when the tokenisation request was last responded to.	Omit	Mandatory
<Auth_Decision>	AN	1	1	Final tokenisation decision: U = unknown 0 = approve digitisation request A = approve digitisation request (with additional authentication).	Omit	Mandatory
<Auth_RSPSRC>	AN	10	10	Name of the system or process that approved the tokenisation (e.g., MC-MDES and ISSUER).	Omit	Mandatory
<Auth_Status>	AN	1	1	Status of the authorisation to digitise this payment token:	Omit	Mandatory

Tag	Type	Minimum Length	Maximum Length	Description	Request	Response
				U = unknown 0 = approve digitisation request A = approve digitisation request (with additional authentication) 1 = decline digitisation request **Note**: this is not the same as a transaction authorisation.		
<Digitisation_Ref>	AN	1	64	Unique reference (per payment_token_issuer_id) which all digitisation messages use, to link them together.	Omit	Mandatory
<Wallet_Account_Score>	N	1	1	Risk score for the account, received from the wallet provider during digitisation: 1 = highest risk; 2 = higher risk 3 = neutral; 4 = lower risk; 5 = least risk	Omit	Mandatory
<Wallet_Device_Score>	N	1	1	Risk score for the device received from the wallet provider during digitisation: 1 = highest risk; 2 = higher risk 3 = neutral; 4 = lower risk; 5 = least risk	Omit	Mandatory
<Wallet_Reasons>	AN	1	24	Wallet service provider tokenization recommendation reason codes. See Wallet Tokenisation Reason Codes.	Omit	Mandatory
<Activation_Code>	AN	1	40	Activation code to be sent directly to the cardholder to activate this payment token.	Omit	Mandatory
<Activation_Code_Expdate	DateTime	16	16	Date and time when the activation code expires, in GMT (UTC). In the format: *yyyy-mm-ddhhmmss.*	Omit	Mandatory

<Activation_Method>	N	1	1	Which activation method was used:
				0 = none;
				1 = SMS to mobile phone;
					Omit	Mandatory

Tag	Type	Minimum Length	Maximum Length	Description	Request	Response

				2 = email;
				3 = cardholder called an automated call centre;
				4 = cardholder called a human call centre;
				5 = website;
				6 = mobile application;
				7 = voice phone call		

<Device_ID>	AN	1	48	Unique ID of the secure element in the device.	Omit	Mandatory
<Device_IP>	AN	1	15	IP address (full or last part only) of the device at time of binding / digitisation.	Omit	Mandatory
<Device_Lang2>	AN	1	2	Device language code as ISO 639-1 (2 letter lowercase) code.	Omit	Mandatory
<Device_Latitude>	N	1	3	Device latitude in degrees at time of digitisation request: -90 (south pole) to +90 (north pole). +ve=North, -ve=South (from equator). Example: +63.2 = North 63.2 degrees, -82.6 = South 82.6 degrees.	Omit	Mandatory
<Device_Longitude>	N	1	3	Device longitude in degrees at time of digitisation request: -180 to +180; +ve = East, -ve = West (of Greenwich). Example: 176.2 = East 176.2 degrees, -98.5 = West 98.5 degrees.	Omit	Mandatory
<Device_Name>	AN	1	20	Name the cardholder assigned to the device in the wallet.	Omit	Mandatory
<Device_Tel_Num>	AN	1	15	Device telephone number (full or last part only).	Omit	Mandatory
<Device_Type>	AN	1	1	The type of device used at the terminal. See Device Types.	Omit	Mandatory
<FirstName>	AN	1	40	Cardholder's first name as provided by the wallet provider during digitisation. May not be provided, or just the initial letter.	Omit	Mandatory

Tag	Type	Minimum Length	Maximum Length	Description	Request	Response
<LastName>	AN	1	40	Cardholder's last name as provided by wallet provider during digitisation. May not be provided, or just the initial letter.	Omit	Mandatory
<Wallet_ Account_Hash>	AN	1	64	Wallet provider hash of account details (optional)or PBKDF2 hash of the cardholder’s account ID with the wallet provider.	Omit	Mandatory

Request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:hyp="http://www.globalprocessing.ae/HyperionWeb">
   <soapenv:Header>
      <hyp:AuthSoapHeader>
         <hyp:strUserName>******</hyp:strUserName>
         <hyp:strPassword>******</hyp:strPassword>
      </hyp:AuthSoapHeader>
   </soapenv:Header>
   <soapenv:Body>
      <hyp:Ws_Payment_Token_Get>
         <hyp:WSID>202112345678967890</hyp:WSID>
         <hyp:IssCode>PMT</hyp:IssCode>
         <hyp:TxnCode>2</hyp:TxnCode>
         <hyp:PAN></hyp:PAN>
         <hyp:PublicToken>123456789</hyp:PublicToken>
         <hyp:DPAN>0987654321012</hyp:DPAN>
         <hyp:Payment_Token_ID></hyp:Payment_Token_ID>
         <hyp:LocDate>2017-01-01</hyp:LocDate>
         <hyp:LocTime>123456</hyp:LocTime>
      </hyp:Ws_Payment_Token_Get>
   </soapenv:Body>
</soapenv:Envelope>
```

Response

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
   <soap:Body>
      <Ws_Payment_Token_GetResponse xmlns="http://www.globalprocessing.ae/HyperionWeb">
         <Ws_Payment_Token_GetResult>
            <WSID>202112345678967890</WSID>
            <IssCode>PMT</IssCode>
            <TxnCode>2</TxnCode>
            <PublicToken>123456789</PublicToken>
            <PaymentTokenGetResInfo>
               <PaymentTokenGetResInfo>
                  <Creator>PMT</Creator>
                  <Creator_PAN_Ref/>
                  <Creator_Token_Ref/>
                  <PANT>1234567890123456</PANT>
                  <Payment_Token>*****1234</Payment_Token>
                  <Payment_Token_ExpDate/>
                  <Payment_Token_ID>2</Payment_Token_ID>
                  <Payment_Token_Type>C</Payment_Token_Type>
                  <Wallet_ID>APPLE</Wallet_ID>
                  <GPS_Status>00</GPS_Status>
                  <Tokenised_Datetime/>
                  <Tokenised_Status>1</Tokenised_Status>
                  <Txn_Status>X</Txn_Status>
                  <Txn_Status_Actor></Txn_Status_Actor>
                  <Txn_Status_Change_Datetime/>
                  <Accepted_Terms_Date_GMT/>
                  <Accepted_Terms_Version/>
                  <Auth_Datetime/>
                  <Auth_Decision/>
                  <Auth_RSPSRC/>
                  <Auth_Status>1</Auth_Status>
                  <Digitisation_Ref>11111111111111</Digitisation_Ref>
                  <Wallet_Account_Score/>
                  <Wallet_Device_Score/>
                  <Wallet_Reasons/>
                  <Activation_Code/>
                  <Activation_Code_Expdate/>
                  <Activation_Method/>
                  <Device_ID/>
                  <Device_IP/>
                  <Device_Lang2/>
                  <Device_Latitude/>
                  <Device_Longitude/>
                  <Device_Name/>
                  <Device_Tel_Num/>
                  <Device_Type>M</Device_Type>
                  <FirstName/>
                  <LastName/>
                  <Wallet_Account_Hash/>
               </PaymentTokenGetResInfo>
            </PaymentTokenGetResInfo>
            <LocDate>2017-01-01</LocDate>
            <LocTime>123456</LocTime>
            <SysDate>2017-11-17</SysDate>
            <ActionCode>000</ActionCode>
         </Ws_Payment_Token_GetResult>
      </Ws_Payment_Token_GetResponse>
   </soap:Body>
</soap:Envelope>
```

Appendices Overview

This section contains a list of appendices with further reference information. See the table below.

Appendix	Description
Action Codes	Action codes returned by Thredd in response to a request.
Transaction Codes	Transaction codes used in a web service response.
Status Codes	Codes that represent the status of a card.
Transaction Types	Codes that represent the transaction type.
Transaction Status	Codes that represent the transaction status.
Payment Token Types	Payment token types.

Action Codes

The following action codes may be returned in the <ActionCode> tag of a web service response.

Code	Description	How is it used?
118	No card record, deny	Used to indicate the PAN/Pubtoken/CustAccount/AccountID in the request has no associated card record in the database.
210	Invalid DPAN	Used to indicate that the supplied tokenised PAN is invalid.
211	Invalid Payment Token Id	Used to indicate that the supplied Payment Token id is invalid.
212	Card and Payment Token details do not match	Used to indicate that the supplied Card details and Payment Token do not relate.
214	No associated Payment Token for the card details supplied	There is no associated Payment Token for the card details supplied.
406	Invalid IssCode	IssCode does not match the credentials supplied.
409	Invalid PAN, PAN must be composed of digits	Used when PAN is not a valid number composed of digits.
410	Invalid PublicToken, PublicToken must be composed of digits	Used when PublicToken is not a valid number composed of digits.
440	Archived card, deny	If the request relates to an archived card record, the request is denied. (Applies to the following web services: Create_Card, Create_Wallet, Regenerate, Regenerate_Wallet and ws_Renew.)
609	Invalid FeeWaiver	Indicates FeeWaiver is invalid.
613	Invalid WSID specified in the request	Indicates supplied WSID is invalid.
651	Invalid Sms_Required	Indicates the parameter value was invalid.
652	Invalid Sms_Content	Indicates the parameter value was invalid.
708	Invalid Card Design, its a MutliFX product	Indicates the parameter value was missing or an invalid value.
788	Invalid MailOrSMS	Indicates the parameter value was invalid.
800	WSID is missing in the request.	Parameter was not supplied but is required.
801	IssCode is missing.	Parameter was not supplied but is required.
802	TxnCode is missing	Parameter was not supplied but is required.
804	LocDate is missing	Parameter was not supplied but is required.
805	LocTime is missing	Parameter was not supplied but is required.

Code	Description	How is it used?
810	PAN, PublicToken or CardDesign is missing in the request.	Parameter was not supplied but is required.
876	RegenType/Replace is empty or invalid.	Parameter was not supplied but is required, or is an invalid value
878	Invalid character in Card Name.	Non - european characters are not allowed in Card Name
904	Format error, deny	Generic format error condition eg used by Account Enquiry to indicate invalid format in 'txnfilter' value received in request or when the security details do not match with the selected authMethod
997	Soap username is null or empty	SOAP authentication
998	Soap password is null or empty	SOAP authentication
999	Security error - SOAP authentication failed. Deny	Indicates the SOAP authentication user name or password is incorrect.

Transaction Codes

The following transaction codes are used in the `<TxnCode>` tag of a web service response.

Code	Description
0	Card Activation
1	Card Load
2	Status Change
3	Balance Enquiry
4	Customer Enquiry
5	Card Statement
6	Load Verification
7	Balance Transfer
8	Card Unload
9	Card Enquiry
10	Activate / Load
11	Card Unload / Status Change
12	Transaction Void
13	Cardholder Update
14	Cardholder Details Enquiry
15	Load Demand
16	Balance Adjustment
17	Extend Expiry
18	Manage PIN
19	External Approve
20	Card Reload

Status Codes

Refer to the table below for status codes that can be used within the <NewStatCode> tag to set the status of a card using the Card Change Status (Ws_Status_Change) web service, and the Card Unload and Change Status (Ws_UnLoad_StatusChange). These statuses are set as **Can be changed** in the table below. Other statuses can be returned in a response to a card status request.

Note: The action code 654 is returned if an attempt is made to change the status of a card with an irreversible status.

Note: The action code 825 is returned if an attempt is made to change the status of a card to a non-editable status.

Status Code	Description	Scheme effect for a payment token	Can be changed
00	All Good. Indicates that the card is good for use, but does not indicate whether it is active. **Tip**: A card must have its <IsLive> flag changed to 1 to be considered active. You cannot activate a card by changing its status to 00. To activate a card, use Ws_Activate.	Activate / Re-activate	Yes
01	Refer to card issuer. **Note:** Do not use status 01. This is for Thredd use only.	Call Issuer	No
02	Card not yet activated	Suspend	No
03	Invalid merchant	Suspend	No
04	Capture Card	Deactivate / Delete	Yes
05	Do not honour	Suspend	Yes
06	Unspecified Error	Suspend	No
08	Honour with identification	Activate	No
10	Partial Approval	Activate	No
12	Invalid Transaction	Suspend	No
13	Invalid Amount	Suspend	No
14	Invalid card number (no such number)	Suspend	No
15	No such issuer	Suspend	No
17	Customer cancellation	Suspend	No
1A	Strong Cardholder Authentication (SCA) required	Suspend	No
30	Format error	Suspend	No
31	Issuer sign-off	Suspend	No
32	Completed partially	Suspend	No

Status Code	Description	Scheme effect for a payment token	Can be changed
33	Expired card (Capture). Made non-editable for removing the status from Smart Client.	Deactivate / Delete	No
36	Restricted card (Capture). Made non-editable for removing the status from Smart Client.	Deactivate / Delete	No
37	Card acceptor call acquirer security (Capture). Made non-editable for removing the status from Smart Client.	Deactivate / Delete	No
38	Allowable PIN tries exceeded (Capture)	Deactivated	No
41	Lost card Do not use if temporarily blocking a tokenised digital PAN (DPAN). We recommend you use status code G1 instead.	Suspend	Yes
43	Stolen card This status is irreversible.	Deactivate / Delete	Yes
46	Closed Account	Deactivate / Delete	Yes
51	Insufficient funds	Suspend	No
54	Expired card Do not use status 54.	Suspend	Yes
55	Incorrect PIN	Suspend	No
57	Transaction not permitted to cardholder	Suspend	Yes
58	Transaction not permitted to terminal	Suspend	No
59	Suspected Fraud	Suspend	Yes
61	Exceeds withdrawal amount limit	Suspend	No
62	Restricted card	Suspend	Yes
63	Security violation	Suspend	Yes
64	Original amount incorrect	Suspend	No
65	Exceeds withdrawal frequency limit	Suspend	No
66	Card acceptor call acquirer's security department	Suspend	No
67	Card to be picked up at ATM	Deactivate / Delete	No

Status Code	Description	Scheme effect for a payment token	Can be changed
68	Response received too late	Suspend	No
69	Invalid or missing data to verify card, cardholder or other.	Suspend	No
70	Cardholder to contact issuer	Suspend	Yes
71	PIN not changed	Suspend	No
75	Allowable number of PIN tries exceeded	Suspend	Yes
76	Invalid <To> Account in Field 3	Suspend	No
77	Invalid <From> Account in Field 3	Suspend	No
78	Card not activated yet	Suspend	No
79	Unacceptable PIN - Transaction declined Retry	Suspend	No
80	Network error	Suspend	No
81	Foreign network failure	Suspend	No
82	Timeout at IEM	Suspend	No
83	Card destroyed This status is irreversible.	Deactivate / Delete	Yes
85	Approved (special)	Activate	No
86	PIN validation not possible	Suspend	No
87	Purchase Amount Only, No Cash Back Allowed	Suspend	No
88	Cryptographic failure	Suspend	No
89	Unacceptable PIN	Suspend	No
90	Invalid ARQC/CVV1/CVV2/CVV3/iCVV	Suspend	No
91	Issuer or switch is inoperative	Suspend	No
92	Unable to route	Suspend	No
93	Violation of Law	Suspend	No
94	Duplicate transmission	Suspend	No
95	Reconcile error	Suspend	No

Status Code	Description	Scheme effect for a payment token	Can be changed
96	System malfunction	Suspend	No
98	Refund given to customer	Suspend	Yes
99	Card voided	Deactivate / Delete	Yes
C0	Requires SCA, Card	Suspend	No
C1	Requires SCA, non-card	Suspend	No
G1	A short-term block which temporarily blocks card usage for all card transactions (excluding Credits and Refunds) for a short period.	Suspend	Yes
G2	Short-term full block (all transactions are blocked).	Suspend	Yes
G3	Long-term block (excluding Credits and Refunds).	Suspend	Yes
G4	Long-term full block (all transactions are blocked).	Suspend	Yes
G5	Thredd Protect Short-term Debit Block	Suspend	Yes
G6	Thredd Protect Short-term Full Block	Suspend	Yes
G7	Thredd Protect Long-term Debit Block	Suspend	Yes
G8	Thredd Protect Long-term Full Block	Suspend	Yes
G9	IVR Lost/Stolen Block (like 41 Lost)	Deactivate / Delete	No
N0	Force STIP	Suspend	No
N7	Decline for CVV2 failure	Suspend	No
P5	PIN Change/Unblock request declined	Suspend	No
P6	Unsafe PIN	Suspend	No

Notes

- All statuses, apart from 43 and 83, are reversible.
- Do not use status 01 (refer to Card Issuer or 54 (expired card) as these are for Thredd use only.
- Changing the status to 99 (card voided) or 98 (refund to customer) automatically generates a card balance adjustment down to 0.00.
- You should use the following status codes for blocks:
  - Temporary Block: G1 or G2.

    Use when you want merchants to try again. Visa guidelines instruct merchants to attempt up to 15 retries over 30 days. A card block will block all non-credit, Balance enquiry and tokenisation (digital wallet) transactions. Refunds and Credits will be permitted.
  - Permanent Block: G3 or G4. Use when you don’t want merchants to try again. Visa expect that the card should not return to the '00 Approve' state at all, or at least not within 30 days.

Transaction Status

Refer to the table below for a list of transaction status values for the `<StatusCode>` field.

Type	Description
A	Accepted
C	Cleared
I	Declined
R	Removed
S	Settled
V	Reversed

Payment Token Types

Refer to the table below for a list of transaction types.

Type	Description
C	Contactless Device PAN
CF	Card on File PAN
CL	Cloud-base payments PAN
P	Real PAN (i.e. a normal ISO form factor card)
SE	Secure Element PAN
U	Unknown
V	Virtual PAN (i.e. virtual card)
BW	Browser-accessible wallet

General FAQs

This section provides answers to frequently asked questions.

Transactions

What is the primary key or identifier for a transaction?

ItemId is the primary key or identifier for a transaction.

Tokenisation Services

Where can I find out more about the Thredd Tokenisation (Digital Wallet) service?

For detailed information on setting up and integrating the Thredd Tokenisation (Digital Wallet) service, see the Tokenisation Service Guide.

How can I send an activation code to the cardholder's phone number?

If you want to use the SMS activation code service to send an Activation Code Notification (ACN) to the cardholder, you must include the mobile phone number of the cardholder when creating the card: first use the Card Create web service to create the card and then use the Card Activate web service to activate the card via SMS.

How do I send a confirmation SMS to the cardholder upon successful token activation in Apple Pay?

Thredd can configure your product so that your end customers receive an SMS notification after successfully activating their Apple Pay token. You must ensure that you provide the cardholder's mobile number when creating the card.

Note: Thredd will receive a Tokenization Complete Notification (TCN) from Apple Pay if the activation is successful. We do not receive notifications for unsuccesful activations.

How can I retrieve the DPAN?

You can use the ws_Payment_Token_Get web service to get the DPAN for a card. See Payment Token Get.

The DPAN is returned in the <Payment_Token > field as a masked value.

Do Thredd customers need to be PCI compliant to support MDES/VDEP?

To support MDES/VDEP integration on Android Pay or Apple Pay, customers must either be PCI DSS Compliant or be using a third party wallet provider for their virtual card. Both Apple and Google mandate Push Provisioning, which requires handling the full PAN.

Thredd customers do not need to be PCI compliant for wallets that do not mandate Push Provisioning.

- **OUTOFBAND** – Thredd sends the authentication request to your systems, using the endpoint set up for your Programme. Your systems must handle the authentication.

Note: OUTOFBAND is currently not available.

Document History

Refer to the table for details of changes to this guide..

Version	Date	Description	Author
1.1	25/04/2024	Updates to content to align with taxonomy updates on our Documentation Portal.	WS
	10/08/2023	Removal of Ws_Check web service and update to glossary and action codes to only show what is relevant to third party web services.	JB
	07/06/2023	Updated Operations email address to be occ@thredd.com	MW
	30/11/2022	Updated the Copyright Statement.	MW
1.0	04/01/2021	First version of the guide.	WS

Contact Us

Please contact us if you have queries relating to this document. Our contact details are provided below.

Thredd Ltd.

Support Email: occ@thredd.com

Support Phone: +44 (0) 203 740 9682

Our Head Office

6th Floor,
Victoria House,
Bloomsbury Square,
London,
WC1B 4DA

Telephone: +44 (0)330 088 8761

Technical Publications

If you want to contact our technical publications team directly, for queries or feedback related to this guide, you can email us at: docs@thredd.com.

1 Glossary

A

Apata

Apata provide an Access Control Server (ACS) that enables support for the 3D Secure cardholder authentication scheme. See: https://apata.com/

B

BIN

A Bank Identification Number, or BIN, refers to the initial sequence of 4 to 6 numbers on a credit card and used to identify the card’s issuing bank or other financial institution. The BIN is the lynch pin that ties an issuer to its cards and transactions.

C

Card Service Code

3 digit code on the magnetic strip of a card which indicates where it is valid for use.

Card Verification Value

The Card Verification Value (CVV) on a credit card or debit card is a 3 digit number on VISA, MasterCard and Discover branded credit and debit cards. Cardholder's are typically required to enter the CVV during any online or cardholder not present transactions. CVV numbers are also known as CSC numbers (Card Security Code), as well as CVV2 numbers, which are the same as CVV numbers, except that they have been generated by a 2nd generation process that makes them harder to guess.

CVC2

The Card Verification Value (CVV) on a credit card or debit card is a 3 digit number on VISA, MasterCard and Discover branded credit and debit cards. Cardholder's are typically required to enter the CVV during any online or cardholder not present transactions. CVV numbers are also known as CSC numbers (Card Security Code), as well as CVV2 numbers, which are the same as CVV numbers, except that they have been generated by a 2nd generation process that makes them harder to guess.

D

DPAN

Device PAN. The PAN value set up on the cardholder’s device. This is not visible to the cardholder, but is the PAN used for the transactions as far as the merchant is concerned.

I

Issuer Code

Thredd Issuer (Program Manager) code, assigned by Thredd. Each Program Manager is assigned their own unique issuer code on the system.

M

MDES

The MasterCard Digital Enablement Service (MDES) helps transform any connected device into a commerce device to make and receive payments. The MDES platform is used in iPhone 6, iPhone 6 Plus and Apple Watch to enable secure payments to take place for contactless and in-app payments.

N

Non-reloadable card

Card which is loaded with funds at the time of card creation, but cannot be reloaded after this.

P

PAN

A payment card number (PAN), primary account number, or simply a card number, is the card identifier found on payment cards, such as credit cards and debit cards, as well as stored-value cards, gift cards and other similar cards.

PRODUCT_REF

The predefined reference code associated with the card, which is included in the XML file sent to the card manufacturer. This field is called the <ProductRef> on ws_create_card and the <DesignRef> on ws_customer_enquiry and ws_customer_enquiry_v2

Program

Logical grouping of your products set up in Smart Client. This is setup with whatever the customer (issuer or program manager) wants. Can be viewed in reports or via the web services API and may also be sent to the card manufacturer.

Program Manager

A Program Manager is a Thredd client who manages their own card service program.

S

SFTP

Secure File Transfer Protocol. File Transfer Protocol FTP) is a popular unencrypted method of transferring files between two remote systems. SFTP (SSH File Transfer Protocol, or Secure File Transfer Protocol) is a separate protocol packaged with SSH that works in a similar way but over a secure connection.

Single use card

Card which can only be used for a single transaction.

V

VPN

Virtual Private Network. A secure, encrypted remote connection over the public internet to the private Thredd network, designed to safeguard the security and integrity of the network. Users are set up to access defined Thredd services via their VPN connection.

W

WSDL

Web Service Definition Language (WSDL) is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. WSDL files are central to testing SOAP-based services. SoapUI uses WSDL files to generate test requests, assertions and mock services.