SHIFT4™

API Specification

Account Updater on Demand

Version 1.3 | October 2025

Shift4 is the trading name of Credorax Bank Ltd., company registration no. C46342, and Source Limited, company registration no. C46916, having a registered address at 80 Strait Street, Valletta VLT 1436, Malta. Credorax Bank Ltd., is a credit institution established in Malta, authorized and regulated by the Malta Financial Services Authority, the UK Prudential Regulatory Authority and the Financial Conduct Authority. LEI code: 213800191YORJFDJF94.

Contents

Introduction 3
Intended Audience 3
Security/Authentication 3
Uniform Resource Locator (URL) Addresses 3
HTTP Specifications 3
Workflow 3
Account Updater on Demand APIs 6
Account Updates Request API 6
Result Retrieval API 13
Appendix A – Security and Authentication 20
AES-256 Encryption 20
SHA512 Signature 21
Appendix B – Error Response Codes 23
Appendix C – Account Updater Response Codes 24
Change History 25
Need Support? 26

Introduction

Shift4's Account Updater on Demand is a service designed to provide merchants with a fast, easy and exceptionally user-friendly method of querying any participating issuer or scheme, for account updates. This enables merchants who store their shoppers' card information to receive card data updates within 24 hours.

Intended Audience

This document is intended for software developers wishing to develop applications using Account Updater on Demand. It fully documents the REST application programming interface that enables developers to interact with the Shift4 application management platform. To use the information provided here, you should have a general understanding of the consuming web services and have an active Shift4 Account Updater on Demand service.

Security/Authentication

All HTTP requests must be sent over a secure TLS (Transport Layer Security) 1.2 channel. The service does not authenticate the TLS/SSL (Secure Sockets Layer) session using a client-based certificate, and thus does not employ a regular type of session authentication. Instead, the client is authenticated by its source IP, alongside a cipher sent in the request header. In addition to this authentication method and due to the fact that sensitive data is being transferred, some data fields must be sent AES-256 encrypted. Refer to *AES-256 Encryption* for further details.

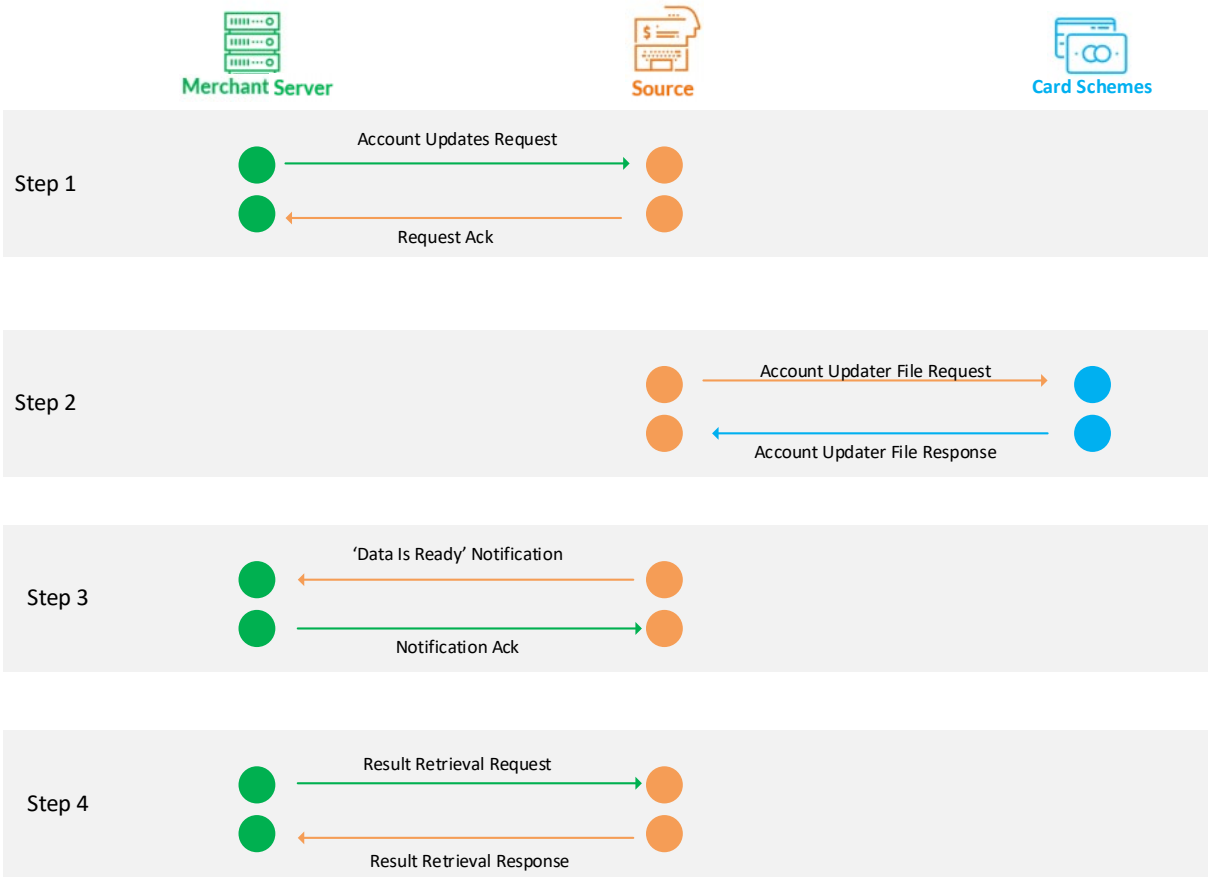
Uniform Resource Locator (URL) Addresses

- Production URL:
  - auondemand.credorax.net/rest/v1/update/pan
  - auondemand.credorax.net/rest/v1/results
- Integration URL:
  - auondemand-int.credorax.com/rest/v1/update/pan
  - auondemand-int.credorax.com/rest/v1/results

HTTP Specifications

- Protocol: HTTPS
- Method: Post
- Content-Type: application/json

Workflow



- The user sends an API call listing all the accounts he wishes to query (as detailed in *Account Updates Request API*).
- Shift4 sends a corresponding request file to the card schemes.
- Once a response is received back from a card scheme, Shift4 sends a "Data is Ready" notification to the user via the Shift4 notification engine. This normally occurrs up to 24 hours from the initial request. Each scheme's response triggers a notification. The user must acknowledge the "Data is Ready" notification.
  For more details about the Shift4 notification engine please refer to the *Data Open API Specifications* guide on the Shift4 Developer Portal.
- The user sends a Result Retrieval API call and Shift4 responds back with all the account update information (as detailed in Response API fields). The user can send this result retrieval API call either per each scheme or for both.

Notes:

- Once the user acknowledges the 'Data is Ready' notification, the result retrieval request is valid for 14 days. A request that arrives later than 14 days from user acknowledgment, will return an error code 20 - "Rejected. Querying for this process results has expired."

- If a user initiates an Account Updates API request before 15:00 UTC, the request is transmitted to the card schemes on the same day. If a user initiates an API request after 15:00 UTC, the request is transmitted to the card schemes on the following day.
- Each Account Updates request can contain up to 50,000 accounts.
- Each user can send up to 10 Account Updates requests and up to 10 Result Retrieval requests, per day.
- The indication that a card scheme's results are ready, is sent in the "Data is Ready" notification. The "Data is Ready" response is per card scheme. The user may choose to use the Result Retrieval API twice (once per each card scheme) or once (for both card schemes). For more details about the Shift4 notification engine please refer to Shift4's *Data Open API Specifications - Notification Engine* in Shift4 Developer Portal.

Account Updater on Demand APIs

This chapter describes the required parameters for all Account Updater APIs.

Note: In the following tables, **M** indicates a mandatory parameter, **O** indicates an optional parameter, and **C** indicates a parameter that is mandatory in certain cases.

Account Updates Request API

Uniform Resource Locator (URL) Addresses

- Production URL:
  - auondemand.credorax.net/rest/v1/update/pan
- Integration URL"
  - auondemand-int.credorax.com/rest/v1/update/pan

API header

The user must include a signature in a bearer token, in the header authentication. The signature should be the SHA512 hash of all the request values and the user's unique authentication key, as described in *SHA512* .

API body fields

The following table describes the fields of the request body:

Name	Type	M/O/C	Length	Description
user_id	[0-9A-Za-z]	M	8	Shift4-assigned user ID
request_id	[0-9A-Za-z]	M	32	User-generated unique request ID
free_field	[0-9A-Za-z]	O	255	Free field for the user's use
request_data	[0-9A-Za-z]	M		An array holding the request data. See *Request_data structure*.

Request_data structure

The request_data array lists the actual accounts and the related merchants in the following format. Because this field holds sensitive data, it must be sent AES-256 encrypted, as detailed in Appendix A – Security and Authentication.

Name	Type	M/O/C	Length	Description
merchant_id	[0-9A-Za-z]	C	15	Registered merchant ID

Name	Type	M/O/C	Length	Description
sub_merchant_id	[0-9A-Za-z]	C	15	Registered sub merchant ID
pan_info	[0-9A-Za-z]	M		An array holding the PANs information. See *PAN_information structure - Request*

PAN_information structure - Request

Name	Type	M/O/C	Length	Description
original_card	[0-9]	M	19	Full card number
original_expiry_date	[0-9]	M	4	Card's expiry date in YYMM format

Request Examples

1. *Clear (with no encryption)*

```
{
  "user_id": "user123",
  "request_id": "1234",
  "free_field": "something",
  "request_data": [
    {
      "merchant_id": "merchant123",
      "pan_info": [
        {
          "original_card": "1234123443214321",
          "original_expiry_date": "2002"
        },
        {
          "original_card": "1234123443214322",
          "original_expiry_date": "2002"
        }
      ]
    },
    {
      "merchant_id": "merchant1234",
      "pan_info": [
        {
          "original_card": "1234123443214323",
```

```
          "original_expiry_date": "2002"
        }
      ]
    }
  ]
```


2. *Encrypted*


```
{
  "user_id": "user123",
  "request_id": "1234",
  "free_field": "something",
  "request_data":
"CEqm/AnzrxyMK2MtjBODe77nOg5Yd3t2jWgyu4nbvSyU76+ZVPlW5WEtueGcG1CfOQscs
E4yq+ztv9WOsyyDuCoBmBiWka9CD3Nv2s9DuOXPkRrpFsI38weRxcRu+1Iqo7ZWzmYbI2y
ZC7L82r6lz2QJB7qOZRc/t4Ob+COA8VXAjS+S+Hoti6jkT5Etedee1bmljUbfGOExBQK+Q
Y5ts6pNJoh5WLhLeFkZax+E7nguxVqPRuJaweHdkpxRtfjL2ZfLNvAzGR/R/kWFRPJPEFV
7ECcP98mJ4y9Y7iDxM5Ts74txnlm4l8uV6v+cRRyZc727mAXTkECol0g4Lpdx3cZbn9FfA
QK1HOmpbWAENvgb7QkPEF8dQoNxcn0uGHZIWHQCobLuwgKg4c5Eo2icFqkp6mIb/Gaw59P
sOlOofEChjxd2VntSBHGbmQKNakp+3G7DmikeUTP6+eCBOhIwH1D+jndrt5X+p+54VpOhb
zlVcdhOQTHjswlOyEO+iNtIoC5gOdyneh6mvLK1puZksNCuV3wffz67kf07w8VAP+MGfNV
h3B3fYYjHD/eOEvfkEUPMAhwnYFoIH6oYtjTnxR6X1wtSSIQBWDOE0d2t8bxWpy8o5DoIR
sEjhju9cfWXAShAQRrF3ilsSxP4HFd28A=="
}
```


Response API fields

The following table describes the notification fields:

Name	Type	M/O/C	Length	Description
request_method	[A-Za-z]	M	4	Possible values: **API** **File**
general_response	[A-Za-z]	M	16	General response. Possible values: **Approved:** all records are approved, and the request will be transmitted to the scheme **Rejected:** the entire request was rejected
error_code	[0-9]	O	2	Returned only if general_response=**rejected** **Refer to *Appendix B* for the full list of errors**
error_description	[0-9A-Za-z]	O	128	Returned only if general_response=rejected **Refer to *Appendix B* for the full list of errors**

Name	Type	M/O/C	Length	Description
request_timestamp	[0-9A-Za-z]	M	32	Timestamp when the request was submitted. The AU process cutoff should be aligned according to this value.
process_id	[0-9A-Za-z]	M	32	Unique ID per request, assigned by Shift4, in UUID4 format
request_id	[0-9A-Za-z]	M	32	Request echo
free_field	[0-9A-Za-z]	O	256	Request echo
PAN_count	[0-9]	M	8	Number of PANs submitted in the request Returned only if: error_code=08 or general_response=approved
rejected_PAN_count	[0-9]	O	8	The number of invalid PANs submitted in the request Returned only if error_code=08
unregistered_merchants_count	[0-9]	O	8	The number of unregistered merchants submitted in the request Returned only if error_code=03
request_data		O		The invalid PANs, returned if error_code=08 The list of unregistered merchants, returned if error_code=03 Note: This field is always sent AES-256 encrypted

Response Examples

1. *Approved response*

```
{
  "request_method": "API",
  "general_response": "Approved",
  "request_timestamp": "sometime",
  "process_id": "process1",
  "request_id": "1234",
  "free_field": "something"
  "PAN_count": "10"
}
```

2. *Rejected response*


```
{
  "request_method": "API",
  "general_response": "Rejected",
  "error_code": "05",
  "error_description": "Number of records exceeds the max limit.",
  "request_timestamp": "sometime",
  "process_id": "process1",
  "request_id": "1234",
  "free_field": "something"
}
```


3. *Rejected response due to invalid PAN (clear)*


```
{
  "request_method": "API",
  "general_response": "Rejected",
  "error_code": "08",
  "error_description": "One or more account data (PAN level) is
invalid.",
  "request_timestamp": "sometime",
  "process_id": "process1",
  "request_id": "1234",
  "free_field": "something",
  "PAN_count": "10",
  "rejected_PAN_count": "1",
  "request_data": [
    {
      "merchant_id": "merchant123",
      "pan_info": [
        {
          "original_card": "AB1234",
          "original_expiry_date": "0120",
          "record_error_code": "101"
          "response_code_description": "Invalid PAN data."
        }
      ]
    }
```

```
  ]
}
```

4. *Rejected response due to unregistered merchant (clear)*

```
{
  "request_method": "API",
  "general_response": "Rejected",
  "error_code": "03",
  "error_description": "One or more merchants is not register to this
service.",
  "request_timestamp": "sometime",
  "process_id": "process1",
  "request_id": "1234",
  "free_field": "something",
  "unregistered_merchants_count" : "2",
  "request_data": [
    {
      "merchant_id": "merchant123"
    },
    {
      "merchant_id": "merchant124"
    }
  ]
}
```

5. *Rejected response (encrypted)*

```
{
  "request_method": "API",
  "general_response": "Rejected",
  "error_code": "03",
  "error_description": "One or more merchants is not register to this
service.",
  "request_timestamp": "sometime",
  "process_id": "process1",
  "request_id": "1234",
  "free_field": "something",
  "unregistered_merchants_count" : "2",
```

```
  "request_data":
"ERLsbOgaESaU2OqL4jL3DwJSUAT1aOK3TRe6fW2wnRr2wOuiKwOwCNil7rsXIcXyWTrUM
nq5Whw1OdJG/EsbLi/LwchUyleVt1i4bHjUwzSnKtIM/N/kCpnFK5hgW16YQF8v6JHyzFH
phgZLLTpKphO2RbL7R/iscZQHTiEHT8Gt6ANEvS8YkYn6wOnCMYWxJLUBM9Or9OGjrIAhq
rMFkqbldJY1yiq4dAhcpHQNset/XN2Q=="

}
```

Note: In every case where the request_data field is sent in the response, it is sent AES-256 encrypted.

Result Retrieval API

Uniform Resource Locator (URL) Addresses

- Production URL:
  - auondemand.credorax.net/rest/v1/results
- Integration URL:
  - auondemand-int.credorax.com/rest/v1/results

API header

The user must include a signature in a bearer token, in the header authentication. The signature should be the SHA512 hash of all the request values and the user's unique authentication key, as described in *SHA512* .

API body fields

The following table describes the fields of the result retrieval body:

Name	Type	M/O/C	Length	Description
user_id	[0-9A-Za-z]	M	8	Shift4-assigned user ID
process_id	[0-9A-Za-z]	M	32	The Unique ID per request, assigned by Shift4, in UUID4 format, returned in the response to the initial request
brand	[0-9A-Za-z]	M	12	The card schemes whose account updates you wish to receive. If you specify multiple values for this field, use a comma-separated format. Possible values: • Visa • MC • Unknown

Note:

- The “brand” parameter value should be in keeping with the information received in the “Data is Ready” notifications.
- Each result can be retrieved just once, whether you use a specific card brand name or multiple values.
  If the results for both brands have already been queried, the response will

hold the error:
"**14**" – "**Rejected. The "Account Updater" data for <brand> has been retrieved**"

- If an account that was included in the Account Updates request is, to the best of our knowledge, neither a Visa nor a Mastercard account, Shift4 marks the account with Brand="Unknown". You can retrieve those accounts by sending a Result Retrieval Request with "Unknown" in the "brand" field.
- The response will include the maximum available information.
- If there are no available results for any of the "brand" parameter values, the response will hold the error: **"18" - "Rejected. The "Account Updater" data isn't available yet."**

Result Retrieval Example

```
{
  "user_id": "user123",
  "process_id": "process123"
  "brand": "Visa,MC"
}
```

Response API fields

The following table describes the account update information sent in response to the result retrieval call:

Name	Type	M/O/C	Length	Description
request_method	[A-Za-z]	M	4	File or API
general_response	[A-Za-z]	M	16	General response. Possible values: **Approved:** The result retrieval request is valid, results are detailed in the following parameters. **Rejected: The result retrieval request is not valid, the error is detailed in the following parameters.**
timestamp	[0-9A-Za-z]	O	32	The timestamp when the request was submitted

Name	Type	M/O/C	Length	Description
error_code	[0-9]	O	2	The error code of the result retrieval request, returned if general_response=Rejected. **Refer to** *Appendix B* **for the full list** of errors
error_description	[0-9A-Za-z]	O	128	The error description of the result retrieval request, returned if general_response=Rejected. **Refer to** *Appendix B* **for the full list** of errors
request _id	[0-9A-Za-z]	O	32	The user request ID of the original request, returned if general_response=Approved
free_field	[0-9A-Za-z]	O	256	The original request echo, returned if general_response=Approved
process_id	[0-9A-Za-z]	O	32	The Shift4 process ID of the original request, returned if general_response=Approved.
PAN_count	[0-9]	O	8	The number of PANs in the response, returned if general_response=Approved.
response_data		O		An array holding the response data, returned if general_response=Approved. See *Response_data structure*

Response_data structure

The response_data array lists the actual accounts and the related merchants in the following format. Because this field holds sensitive data, it is always sent AES-256 encrypted, as detailed in Appendix A.

Name	Type	M/O/C	Length	Description
merchant_id	[0-9A-Za-z]	C	15	Registered merchant ID
sub_merchant_id	[0-9A-Za-z]	C	15	Registered sub merchant ID
pan_info	[0-9A-Za-z]	M		An array holding the received PANs information. See *PAN_information structure - Response*

PAN_information structure - Response

Name	Type	M/O/C	Length	Description
brand_type	[0-9A-Za-z]	M	9	Possible values: • Visa • Mastercard
original_card	[0-9]	M	19	Full card number
original_expiry_date	[0-9]	M	4	Card's expiry date in YYMM format
au_response_code	[0-9A-Za-z]	M	2	Account Updater response code. **Refer to *Appendix C* for the full list**
au_response_code_description	[0-9A-Za-z]	M	256	Account Updater response message. **Refer to *Appendix C* for the full list**
new_card	[0-9]	O	19	New card number, returned in case of a new card number.
new_expiry_date	[0-9]	O	4	New card expiration date, returned in case of a new expiration date.

Response Examples

1. *Rejected response*


```
{
  "request_method" : "API",
  "general_response": "Rejected",
  "error_code": "05",
  "error_description": "Rejected. Number of records exceeds the max limit."
}
```


2. *Approved Response (Clear)*


```
{
  "request_method": "API",
  "genral_response": "Approved",
  "timestamp": "sometime",
  "request_id": "request1",
  "free_field": "something",
  "process_id": "process1",
  "PAN_count": "3",
  "response_data": [
    {
      "merchant_id": "merchant1",
      "pan_info": [
        {
          "brand_type": "Visa",
          "original_card": "4434567890120345",
          "original_expiry_date": "0823",
          "au_response_code": "A",
          "au_response_code_description": "New account number and/or new expiration date.",
          "new_card": "4434567890120346",
          "new_expiry_date": "0926"
        },
        {
          "brand_type": "Mastercard",
          "original_card": "5534567890987654",
          "original_expiry_date": "0823",
          "au_response_code": "B",
```

```
          "au_response_code_description": "New expiration date, same
account number.",
          "new_card": "",
          "new_expiry_date": "0824"
        }
      ]
    },
    {
      "merchant_id": "merchant2",
      "pan_info": [
        {
          "brand_type": "Visa",
          "original_card": "4534567890987654",
          "original_expiry_date": "0823",
          "au_response_code": "E",
          "au_response_code_description": "No updates were found but
the account is valid.",
          "new_card": "",
          "new_expiry_date": ""
        }
      ]
    }
  ]
```


3. *Approved Response (encrypted)*


```
{
  "request_method": "API",
  "genral_response": "Approved",
  "timestamp": "sometime",
  "request_id": "request1",
  "free_field": "something",
  "process_id": "process1",
  "PAN_count": "3",
```

```
  "response_data":
"ERLsbOgaESaU2OqL4jL3DwJSUAT1aOK3TRe6fW2wnRr2wOuiKwOwCNil7rsXIcXyWTrUM
nq5Whw1OdJG/EsbLi/LwchUyleVt1i4bHjUwzSnKtIM/N/kCpnFK5hgW16YQF8v6JHyzFH
phgZLLTpKphO2RbL7R/iscZQHTiEHT8Gt6ANEvS8YkY6yi8OVevOoTsUBSAQgvMdXq3AFI
Dt2a2zyiIqEqVYACimh6JCpaK7IAD3QjrJ/UOW8HCZsl4KuJS4gB/MvTqxccSFj27DOsFH
JtDN2xI61SNveXfaslsaAAAbmalbsnbyjngP9yiObpvwHSsRTghOhmAS2tgqCwSQu7sDwE
8uCJHOSwlip8/9SdOjUlQs8FpDa4M9L7lt2gzqeEyv+03QPFItNnTd7vcxvxcbk90BVwTS
ILRM53KrU6bd+XKnG1uBBL8lAwSNka/8G6MAJmIK375S+Achs7sdq9mXdzpL0GhkFiRmhA
t5K1MZCkgDlLZQHA6hjWQN/S8lsd1TPdwSd9DcgYK/byZQPgesc7E0PwcPYVuNjOPygssS
Ba7DrBacHFyRZrc7BGR+1eHkUo+wXe3EfK9gyrkXrIOwh718J+Tw1cDIk7CaukGjj3hiDn
6wOnCMYWxJLnb,mfLKFLFKvdbdbUBM90r9OGjrIAhqrMFkqbldJY1yiq4dAhcpHQNset/X
N2Q=="

}
```

Appendix A – Security and Authentication

AES-256 Encryption

Almost every API message within this service holds sensitive data, such as a credit card number. In order to secure the process, each sensitive API parameter must be sent encrypted in the requests, and is sent encrypted in the responses. The encryption is based on:

- Secret Key – the user's authentication key.
- Algorithm type - AES/CBC/PKCS5Padding
- Key size – 256 bits
- No initialization vector

Encryption Example

Here is an example of how the encryption is calculated using the following original request:

```
{
  "user_id": "user123",
  "request_id": "1234",
  "free_field": "something",
  "request_data": [
    {
      "merchant_id": "merchant123",
      "pan_info": [
        {
          "original_card": "1234123443214321",
          "original_expiry_date": "2002"
        },
        {
          "original_card": "1234123443214322",
          "original_expiry_date": "2002"
        }
      ]
    },
    {
      "merchant_id": "merchant1234",
      "pan_info": [
        {
          "original_card": "1234123443214323",
```

```
          "original_expiry_date": "2002"
        }
      ]
    }
  ]
}
```

With the authentication key being: “secretkey1234567891234567891234 5”.

The result of applying AES-256 to the request data is:

```
{
  "user_id": "user123",
  "request_id": "1234",
  "free_field": "something",
  "request_data":
"CEqm/AnzrxyMK2MtjBODe77nOg5Yd3t2jWgyu4nbvSyU76+ZVPlW5WEtueGcG1CfOQscs
E4yq+ztv9WOsyyDuCoBmBiWka9CD3Nv2s9DuOXPkRrpFsI38weRxcRu+1Iqo7ZWzmYbI2y
ZC7L82r6lz2QJB7qOZRc/t4Ob+COA8VXAjS+S+Hoti6jkT5Etedee1bmljUbfGOExBQK+Q
Y5ts6pNJoh5WLhLeFkZax+E7nguxVqPRuJaweHdkpxRtfjL2ZfLNvAzGR/R/kWFRPJPEFV
7ECcP98mJ4y9Y7iDxM5Ts74txnlm4l8uV6v+cRRyZc727mAXTkECol0g4Lpdx3cZbn9FfA
QK1HOmpbWAENvgb7QkPEF8dQoNxcnOuGHZIWHQCobLuwgKg4c5Eo2icFqkp6mIb/Gaw59P
sOlOofEChjxd2VntSBHGbmQKNakp+3G7DmikeUTP6+eCBOhIwH1D+jndrt5X+p+54VpOhb
zlVcdhOQTHjswlOyEO+iNtIoC5gOdyneh6mvLK1puZksNCuV3wffz67kf07w8VAP+MGfNV
h3B3fYYjHD/eOEvfkEUPMAhwnYFoIH6oYtjTnxR6X1wtSSIQBWDOE0d2t8bxWpy8o5DoIR
sEjhju9cfWXAShAQRrF3ilsSxP4HFd28A=="
}
```

SHA512 Signature

Every message is associated with a package signature sent as an Authentication header in order to ensure the authenticity of data transfer. This package signature, in turn, contains the SHA512 hash of all the JSON body and the user's unique authentication key, which will be received once onboarding to the Account Updater on Demand service is finished.

Calculating the Signature

1. Apply the HMAC-SHA512 hashing algorithm to the JSON body of the request and the user’s authentication key.
2. Append the result of step 1 to the request’s authentication header.

Signature Calculation Example

Here is an example of how the signature is calculated using the following original request:

```
{
  "user_id": "user123",
  "request_id": "1234",
```

```
  "free_field": "something",
  "request_data":
"CEqm/AnzrxyMK2MtjBODe77nOg5Yd3t2jWgyu4nbvSyU76+ZVPlW5WEtueGcG1CfOQscs
E4yq+ztv9WOsyyDuCoBmBiWka9CD3Nv2s9DuOXPkRrpFsI38weRxcRu+1Iqo7ZWzmYbI2y
ZC7L82r6lz2QJB7qOZRc/t4Ob+COA8VXAjS+S+Hoti6jkT5Etedee1bmljUbfGOExBQK+Q
Y5ts6pNJoh5WLhLeFkZax+E7nguxVqPRuJaweHdkpxRtfjL2ZfLNvAzGR/R/kWFRPJPEFV
7ECcP98mJ4y9Y7iDxM5Ts74txnlm4l8uV6v+cRRyZc727mAXTkECol0g4Lpdx3cZbn9FfA
QK1HOmpbWAENvgb7QkPEF8dQoNxcn0uGHZIWHQCobLuwgKg4c5Eo2icFqkp6mIb/Gaw59P
sOlOofEChjxd2VntSBHGbmQKNakp+3G7DmikeUTP6+eCB0hIwH1D+jndrt5X+p+54VpOhb
zlVcdhOQTHjswlOyEO+iNtIoC5gOdyneh6mvLK1puZksNCuV3wffz67kf07w8VAP+MGfNV
h3B3fYYjHD/eOEvfkEUPMAhwnYFoIH6oYtjTnxR6X1wtSSIQBWDOE0d2t8bxWpy8o5DoIR
sEjhju9cfWXAShAQRrF3ilsSxP4HFd28A=="
}
```


With the authentication key being: “secretkey1234567891234567891234 5”.

The result of applying HMAC-SHA512 to the request body and key is:

83c814b6297ca06386cfff9d70b282090b7e542dc41b6e9c2e847a38091680272134a6c976ab8d7ffd1
485f30c3b6ac0d19fec62a271c8f39ac5f30bf94e0b08

Appendix B – Error Response Codes

This appendix describes the possible response error codes and their descriptions.

Code	Description
01	Rejected. Invalid authentication.
02	Rejected. Invalid permission.
03	Rejected. One or more merchants is not registered to this service.
04	Rejected. Request structure is wrong.
05	Rejected. Number of records exceeds the max limit.
06	Rejected. Number of requests exceeded the max daily limit.
07	Rejected. Request ID parameter is not unique.
08	Rejected. One or more account data (PAN level) is invalid.
12	Rejected. Querying for this process results is not allowed for this user.
13	Rejected. Mandatory field “process_id” is missing.
14	Rejected. The "Account Updater" data for <brand> has been retrieved
15	Rejected. Invalid format.
16	Rejected. invalid request structure.
18	Rejected. The "Account Updater" data isn't available yet.
19	Rejected. Initial request was rejected.
20	Rejected. Querying for this process results has expired.
21	Rejected. Failed due to unexpected technical issue.
22	Rejected. Request timed out.
101	Invalid PAN data.
102	Invalid expiry date.

Appendix C – Account Updater Response Codes

This appendix describes the possible response codes received in result retrieval responses. A response code is returned for each account in the response, based on the information received from the schemes.

Code	Description
A	New account number and/or new expiration date.
B	New expiration date, same account number.
C	Account is marked as closed.
D	Contact cardholder for updated information.
E	No updates were found but the account is valid.
F	No match for the data provided. Participating BIN/ issuer.
H	No match for the data provided. Non-participating BIN/issuer.
I	Error – Non-numeric Account Number.
J	Error – Invalid Expiration Date format.
K	Error – Merchant isn't registered to the service.
L	Error – Sub merchant isn't registered to the service.
O	Cardholder opted out from service.
1	Error – Account number does not start with 2, 3, 4, 5 or 6.
2	Error – Account number contains non-numeric characters or is not the proper length.

Change History

Version	Subject/Date	Description
1.3	October 2025	Change in the amount of the account updater on demand requests
1.2	November 2023	Rebrand as Shift4
1.1 rev 1	September 2020	Changes in the “brand” field Addition of Error Response Code 14
1.1	June 2020	Added card scheme response details
1	October 2019	Revised text
0.1	August 2019	Preliminary release

Need Support?

Contact our 24/7 Client Relations Center for any additional information or technical issue:

US: +1.617.715.1977

UK: +44.20.3608.1288

EU: +356.2778.0876

Email: support.europe@shift4.com