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 occurs 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 100,000 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>M/O/C</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_id</td>
<td>[0-9A-Za-z]</td>
<td>M</td>
<td>8</td>
<td>Shift4-assigned user ID</td>
</tr>
<tr>
<td>request_id</td>
<td>[0-9A-Za-z]</td>
<td>M</td>
<td>32</td>
<td>User-generated unique request ID</td>
</tr>
<tr>
<td>free_field</td>
<td>[0-9A-Za-z]</td>
<td>O</td>
<td>255</td>
<td>Free field for the user’s use</td>
</tr>
<tr>
<td>request_data</td>
<td>[0-9A-Za-z]</td>
<td>M</td>
<td></td>
<td>An array holding the request data. See <code>Request_data structure</code></td>
</tr>
</tbody>
</table>

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`.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>M/O/C</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>merchant_id</td>
<td>[0-9A-Za-z]</td>
<td>C</td>
<td>15</td>
<td>Registered merchant ID</td>
</tr>
</tbody>
</table>
AccountUpdater on Demand API Specifications

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>M/O/C</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sub_merchant_id</td>
<td>[0-9A-Za-z]</td>
<td>C</td>
<td>15</td>
<td>Registered sub merchant ID</td>
</tr>
<tr>
<td>pan_info</td>
<td>[0-9A-Za-z]</td>
<td>M</td>
<td></td>
<td>An array holding the PANs information. See <code>PAN_information structure - Request</code></td>
</tr>
</tbody>
</table>

**PAN_information structure - Request**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>M/O/C</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>original_card</td>
<td>[0-9]</td>
<td>M</td>
<td>19</td>
<td>Full card number</td>
</tr>
<tr>
<td>original_expiry_date</td>
<td>[0-9]</td>
<td>M</td>
<td>4</td>
<td>Card’s expiry date in YYMM format</td>
</tr>
</tbody>
</table>

**Request Examples**

1. **Clear (with no encryption)**

```json
{
    "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

```json
{
  "user_id": "user123",
  "request_id": "1234",
  "free_field": "something",
  "request_data": "CEqm/AnzrxyMK2MtjB0De77n0g5Yd3t2jwgyuy4nbvSyu76+ZVP1w5WetueGcGlcfQqcsE4yq+ztv9w0syyDucoBmBiwka9CD3nVz59Dr0XPKRrpfS13weRxcRu++IYqo7ZzwzyBiy2yzC7I82r612QJB70Q/R/c4t0b+C0A09VXaaj+s+s+Hot16jT5etede1bmljubFG0ExBQK+QY5ts6PNoh5WHLhEfkZax+E7nguxVqPRUJaweHdKpxRtfjLZ9fLNVAZGR/R/kwFRPJPEFV7ECcp98mJ4y9y7idXm5TS74txn1m418uv6v+cRRyZc727mAXTkEco10g4Lpxd3cZbn9fAqK1H0mpBWAENvgb7QKFPE80q0Nxc00uGHZIWHQcob1wVgkg9c5Eo2iCfQkpm6Ib/Gaw59PsolooFeChjxd2Vnt5BHGbmqK Napk+3G7DmikeUTP6+eCB0hIwH1D+jntrt5x+p+54vpoohb z1Vcdh0QTHjsw10yEO+1Ng1oGdymehe6mVLK1puZksNCuV3wffz67kfo7w8VAP+MGFVnh3B3fyYJhD/e0EvfkeUDEMAhwNYF0tIH6oyTjtNnxR6X1wtsSIQBwDOE0d2t8bxwpy8o5DoIRsEjhju9cfWXAShAQpRf31sSxp4HFDz8A=="
}
```

Response API fields

The following table describes the notification fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>M/O/C</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>request_method</td>
<td>[A-Za-z]</td>
<td>M</td>
<td>4</td>
<td>Possible values: API, File</td>
</tr>
<tr>
<td>error_code</td>
<td>[0-9]</td>
<td>O</td>
<td>2</td>
<td>Returned only if general_response=rejected</td>
</tr>
<tr>
<td>error_description</td>
<td>[0-9A-Za-z]</td>
<td>O</td>
<td>128</td>
<td>Returned only if general_response=rejected</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>M/O/C</td>
<td>Length</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------</td>
<td>-------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>request_timestamp</td>
<td>[0-9A-Za-z]</td>
<td>M</td>
<td>32</td>
<td>Timestamp when the request was submitted. The AU process cutoff should be aligned according to this value.</td>
</tr>
<tr>
<td>process_id</td>
<td>[0-9A-Za-z]</td>
<td>M</td>
<td>32</td>
<td>Unique ID per request, assigned by Shift4, in UUID4 format</td>
</tr>
<tr>
<td>request_id</td>
<td>[0-9A-Za-z]</td>
<td>M</td>
<td>32</td>
<td>Request echo</td>
</tr>
<tr>
<td>free_field</td>
<td>[0-9A-Za-z]</td>
<td>O</td>
<td>256</td>
<td>Request echo</td>
</tr>
<tr>
<td>PAN_count</td>
<td>[0-9]</td>
<td>M</td>
<td>8</td>
<td>Number of PANs submitted in the request</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Returned only if:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>error_code=08</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>general_response=approved</td>
</tr>
<tr>
<td>rejected_PAN_count</td>
<td>[0-9]</td>
<td>O</td>
<td>8</td>
<td>The number of invalid PANs submitted in the request</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Returned only if error_code=08</td>
</tr>
<tr>
<td>unregistered_merchants_count</td>
<td>[0-9]</td>
<td>O</td>
<td>8</td>
<td>The number of unregistered merchants submitted in the request</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Returned only if error_code=03</td>
</tr>
<tr>
<td>request_data</td>
<td></td>
<td>O</td>
<td></td>
<td>The invalid PANs, returned if error_code=08</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>The list of unregistered merchants, returned if error_code=03</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Note: This field is always sent AES-256 encrypted</td>
</tr>
</tbody>
</table>

**Response Examples**

1. **Approved response**

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

```json
{
    "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)

```json
{
    "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"
                }
            ]
        }
    ]
}
```
4. **Rejected response due to unregistered merchant (clear)**

```json
{
    "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)**

```json
{
    "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": "ERLsb0gaESaU20qL4jL3DwJ3SUAT1a0K3TRe6fw2wnRr2w0RiKw0wcNi17rsXlCyWTrUM nq5whw10dJG/EsblLWykhNQ7vsnKtIM/N/kCp5hsw16YQF8v6jHyxqFH phgZLLTPkh02RbL7R/iscZQHTieEHT8Gt6ANEtv58kyn6whOnCMYwxJLUBM90r90GjrIAhq rMFkqbdJY1yi4dAhcpHQNset/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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>M/O/C</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_id</td>
<td>[0-9A-Za-z]</td>
<td>M</td>
<td>8</td>
<td>Shift4-assigned user ID</td>
</tr>
<tr>
<td>process_id</td>
<td>[0-9A-Za-z]</td>
<td>M</td>
<td>32</td>
<td>The Unique ID per request, assigned by Shift4, in UUID4 format, returned in the response to the initial request</td>
</tr>
<tr>
<td>brand</td>
<td>[0-9A-Za-z]</td>
<td>M</td>
<td>12</td>
<td>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</td>
</tr>
</tbody>
</table>

**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

```json
{
  "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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>M/O/C</th>
<th>Length</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>request_method</td>
<td>[A-Za-z]</td>
<td>M</td>
<td>4</td>
<td>File or API</td>
</tr>
<tr>
<td>general_response</td>
<td>[A-Za-z]</td>
<td>M</td>
<td>16</td>
<td>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.</td>
</tr>
<tr>
<td>timestamp</td>
<td>[0-9A-Za-z]</td>
<td>O</td>
<td>32</td>
<td>The timestamp when the request was submitted</td>
</tr>
<tr>
<td>error_code</td>
<td>[0-9]</td>
<td>O</td>
<td>2</td>
<td>The error code of the result retrieval request, returned if general_response=Rejected. Refer to Appendix B for the full list of errors</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>M/O/C</td>
<td>Length</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------</td>
<td>-------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>error_description</td>
<td>[0-9A-Za-z]</td>
<td>O</td>
<td>128</td>
<td>The error description of the result retrieval request, returned if general_response=Rejected. Refer to Appendix B for the full list of errors</td>
</tr>
<tr>
<td>request_id</td>
<td>[0-9A-Za-z]</td>
<td>O</td>
<td>32</td>
<td>The user request ID of the original request, returned if general_response=Approved</td>
</tr>
<tr>
<td>free_field</td>
<td>[0-9A-Za-z]</td>
<td>O</td>
<td>256</td>
<td>The original request echo, returned if general_response=Approved</td>
</tr>
<tr>
<td>process_id</td>
<td>[0-9A-Za-z]</td>
<td>O</td>
<td>32</td>
<td>The Shift4 process ID of the original request, returned if general_response=Approved.</td>
</tr>
<tr>
<td>PAN_count</td>
<td>[0-9]</td>
<td>O</td>
<td>8</td>
<td>The number of PANs in the response, returned if general_response=Approved.</td>
</tr>
<tr>
<td>response_data</td>
<td></td>
<td>O</td>
<td></td>
<td>An array holding the response data, returned if general_response=Approved. See Response_data structure</td>
</tr>
</tbody>
</table>

**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.

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

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

1. Rejected response

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

2. Approved Response (Clear)

```json
{
   "request_method": "API",
   "general_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."
               },
               {
                   "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",
"general_response": "Approved",
"timestamp": "sometime",
"request_id": "request1",
"free_field": "something",
"process_id": "process1",
"PAN_count": "3"
"response_data":
"ERLsb0gaESau20ql4jL3DwJSUAT1a0K3TRe6fw2wnRr2wOuiKw0Cni17rsXICxyWTrU
mq5hw10dJG/EsblI/LwchUy1evt1i4bHjUwzSnKtIM/N/kCpnFK5hgW16yQF8v6jHyzF
phgZLLtpKph0ZrBl7R/isCZQHtiEHT8tG6A3vS8YKv6Yi8OvEv0oTsU8SAQgvMdXq3AFA
Dt2aZzy1IQeqVYACimh6Jcpak71AD3qjr3/U0w8HCZs14kuJS4g8/MVtqxxcSFj27D0sF
H3tDN2xI6iSNveXfas1saAAAAbmalbsnbyjngP9yi0bpvvH5sRTgOhmAs2tgqCwSQu7sDwE
8uCJH0swl8p/95d0ujuQS8Fpda4M9L71t2gzqeEyv+03QpFItNnTt7vCvxxbcbk9OBVwTS
ILRM53Kru6bd+XKnGlU8BL8LAmSNka/8G6MAjmIK375S+Achs7sdq9mXdpL0GhkFDtmhA
b5k1MZcKgD1LZQA6hjWqN/S81sd1TPdwSd9DcyK/YbyZQpYs3c7EOPwcPYVunJ0Pygss
Ba7DrBacHFyRZr7c7BGR+1eHkuw+wXe3EfK9gyrkXrI0wh718J+Tw1cDik7CauKGjJ3hiDn
6w0nCMYwxJLnb,mfKFLFVdbdbUBM90t9O6jriAhqrMFkqbldJY1yi4dAhcpHQNset/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:

```json
{
    "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"
            }
        ]
    }
}
```
"original_expiry_date": "2002"
}
]
}
]
}

With the authentication key being: "secretkey12345678912345678912345".

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

```json
{
    "user_id": "user123",
    "request_id": "1234",
    "free_field": "something",
    "request_data":
        "CEqm/AnzrzyMK2Mtjb00De77m0g5Yd3t2jwgyu4nbvSyU76+zVPlW5EtueGCGLcfOQscesE4yq+zttv9w0syDuCo8Mbiwka9CD3nv2s9Du0XPKRpfSi38weRxcRu+1Iqo7ZwzmyBiZyZc7L82r6lZ2QJB7q0Zrc/t4OoB/cOA8VXAJa5+S+Hoti6jktT5etedeelbmjubFG0EXBQK+QY5ts6pNJo5WlHeFkZax+E7nguxVQPRuJawehDkpxRtfjLZfLNvAzGR/R/kWFRP3PEPV7EccP98m34y971dXR5TS74txn1m418uv6v+cRRy2C7Z27mAxtkECo10g4Lpxd3c2bn9FfAQK1HOmpbWAEvngb7QkPEF8dQ0Xnc0UgH2IWQcobiUwkgkg4c5Eo2iCQkq6mIb/Gaw59Pso10fEchxd2VnxbHhGbmQKn+kp+3G7DmikeUTP6+eCBoh1wHId+jndrt5X+p+s54vopohzlVcdhUQTHjsw10yeo+iNtioC5g0yneh6mVLK1puZksNCuV3wffz67kf07w8VAP+MGfNVh3B3fYyjHd/eOEvfKkEPWMAhwnYFoIH6oytjTnxR61lwtS5QBWDOE0d2t8Bxwpy8o5DoIRsEjhju9cfWXASHAQRF3f1sSxP4HFd28A=="
}
```

**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:

```json
{
    "user_id": "user123",
    "request_id": "1234",
```
"free_field": "something",
"request_data":
"CEqm/AnzrxMK2MttjB0De77n0g5Yd3t2jwgyu4nbvSyu76+ZVP1w5WEtueGcGlcfQqcsE4yq+zT9W0sysyDuCoBmBiWka9C3D3v2s9du0XPKrRpFsI38weRxcRu+1Iiqo7WzrmYb12yZC7L82r6lz2QJB7q0Z7c/t4o8+COA8VXaJ5+S+Hoti6jkt5Etedee1bmljubFG0ExBQK+QY5ts6P3h5W5hLefKzax+E7nguxVqPRuJaweHdkpxRtfjLZ2FlnVaZGR/R/kwFrpJPE;rF
7ECC98m34y97iDyn5Ts74txn1m418uv6v+cRRyZc727maxTKeCo10g4Lpxd3czbn9FfA
QK1H0mpbWAENvgb7QkPEF8dQQNxcn0uGhZIWhQCObluwkg9c45Ec02icFqkp6MiB/Gaw59P
so10ooFeChjd2Vnt5BHGBmQKNa+k+3G7DmiuETPP6+eCB0hIwH1D+jndr5x+p+54VpOhb
zlVcdh0QTjhsL0yEO+iNToC5gOdyneh6mVLK1puZksNCuV3wffz67kf07Vw8VAP+MGfNV
h3B3fYY3HD/eOEvfkEUPMAHwnyFoIH6oYtjTnxR6X1wtSISIQ8wDvOE0d2t8bxwpy8o5DoIR
sEjhju9cfWXAShAQQrF3ilsSxP4HFd28A=="
}

With the authentication key being: “secretkey12345678912345678912345”.

The result of applying HMAC-SHA512 to the request body and key is:
83c814b6297ca06386cfff9d70b282090b7e542dc41b6e9c2e847a38091680272134a6c976ab8d7f0d1
485f30c3b6ac0d19fec62a271c8f39ac5f30bf94e0b08
# Appendix B – Error Response Codes

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

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

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Subject/Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2</td>
<td>November 2023</td>
<td>Rebrand as Shift4</td>
</tr>
</tbody>
</table>
| 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