Kount Central Implementation and Technical Documentation

Jan. 2015

Contents

Introduction

This document contains two sections. The first section is a high-level implementation guide designed for Payment Service Providers and Payment Gateways to provide general information regarding what preparations are necessary to implement the Kount Central solution. The second part, beginning on page 8, is a technical guide designed for IT staff who will specifically integrate Kount Central for use by Processors.

Introduction to Implementation Guide

Kount Central provides online payment processors such as Payment Service Providers and Payment Gateways, collectively referred to as Processors, with an easy and profitable way to provide enterprise-level fraud and risk protection for their customers (also known as e-commerce merchants). After a one-time, simple integration with Kount Central, Processors can offer their customers three levels of protection based on the needs of the customer.

1. **Kount Central Portfolio Manager:** Provides a "blanket" of protection for a Processor's customer base, Kount Central Portfolio offers fraud security services across the entire customer portfolio, reviewing all transactions handled by the Processor.
2. **Kount Central Fraud Manager:** Many of a Processor's customers are large enough to want fraud protection but do not require a complete fraud platform. Kount Central Fraud Manager enables the Processor to offer their customers the ability to configure straightforward fraud controls, allowing them to set the level of risk they are comfortable with.
3. **Kount Central Enterprise:** The largest and highest transaction volume merchants are critical to Enterprise-level businesses and need ultimate protection against payment fraud. Kount Central Enterprise can protect these top merchants with direct implementation to Kount Complete, the industry-leading fraud mitigation platform.

Kount Central RIS Implementation

The first step in implementing Kount Central is the one-time simple integration with the Kount Risk Inquiry Service (RIS). This integration is necessary to enable all three levels of Kount Central. The exact details of the RIS Integration will depend on which level or levels of protection the Processor wishes to utilize.

A brief overview of the RIS Modes specific to Kount Central is provided below. Detailed information about implementing RIS is provided in the **Risk Inquiry Service (RIS) Technical Specifications Guide**.

RIS Processing/Response

Kount Central introduces two new RIS Modes to support Kount Central Fraud Manager and to provide enhanced support for Kount Central Portfolio Manager.

Mode J

RIS Mode J evaluates only the customer specific fraud thresholds, filters and lists (Thresholds) that were configured in Kount Central Fraud Manager.

The RIS Response includes a list of any Thresholds that triggered, as well as the data that caused the threshold(s) to trigger.

Mode W

If Kount Central Fraud Manager is used in conjunction with Kount Central Portfolio Manager, RIS Mode W provides the ability to evaluate both the customer specific thresholds that were configured in Kount Central Fraud Manager, as well as the Processor's rules that were configured in Kount Central Portfolio Manager.

The RIS Response includes details about both the fraud rules as well as the thresholds that were triggered.

In certain circumstances, additional RIS Modes described in the **Risk Inquiry Service (RIS) Technical Specifications Guide** may be appropriate for use with Kount Central Portfolio Manager or Kount Central Enterprise. The Kount Merchant Services Team can provide detailed consultation about the different RIS Modes and their applicability to different use cases.

Device Data Collector Implementation

The **Device Data Collector** gathers information from an end-customer's device by redirecting the device browser momentarily to Kount then back to the merchant. This passive analysis obfuscates Kount's interaction with the end-customer and does not affect the end-customer's purchasing experience. Implementation of the Device Data Collector is strongly encouraged for use with Kount Central Enterprise and will improve the fraud detection capabilities for Kount Central Portfolio and Kount Central Fraud Manager.

If the Processor provides a hosted pay page (HPP) for use by merchants, the Device Data Collector should be implemented on the HPP. In addition, the Processor should encourage merchants who are not using a HPP to implement the Device Data Collector on their checkout pages.

Details about implementing the device data collector can be found in the **Data Collector** section of the **Risk Inquiry Service (RIS) Technical Specifications Guide**.

Kount Central Fraud Manager Implementation

Kount Central provides an API for use with Kount Central Fraud Manager (the Kount Central API). In order to offer Kount Central Fraud Manager functionality to its customers/merchants, the Processor must develop a customer-facing user interface for threshold configuration and must use the Kount Central API.

The Kount Central API supports the following actions:

- Enabling or Disabling Kount Central Fraud Manager for an individual customer.
- Configuring Thresholds for an individual customer.

See the **Kount Central Technical Documentation** on page 8 for specific information regarding the Kount Central API.

Kount Central API Authorization and Authentication

Authorization and Authentication is managed by the Kount Central API which uses an API Key solution based on OAuth2.0 This dramatically simplifies the way Processors interact with the API. Details are contained in the **Kount Central Technical Documenation** on page 8.

An API Key will be provided by Kount Merchant Services. The API Key is required for all Kount Central API requests.

Processor/Customer Configuration

In order for a Processor's customer to utilize Kount Central Fraud Manager, the customer must first be added to Kount Central. Adding, removing, and changing a customer can be performed by the Kount Central API.

Processor/Customer Threshold Configuration

Once a Processor's customer has been added to Kount Central, the Kount Central API can be used to obtain the current Threshold configuration and to make changes.

Introduction to Technical Documentation: Kount Central and RIS

Kount Central Fraud Manager provides a set of straightforward fraud controls (Thresholds) that a Processor can provide to their customers, and an API (the Kount Central API) that the processor can use to configure the Thresholds. It is the responsibility of the Processor to create a user interface that is a front-end to the Kount Central API and that their customers can use to configure their specific Thresholds.

Kount Central Portfolio Manager and Kount Central Enterprise provide access to the Agent Web Console (AWC). The AWC is a sophisticated user interface that enables a Processor in the case of Portfolio Manager, or a Processor's largest customers in the case of Enterprise, to manage all facets of their fraud protection program, including configuring fraud rules, reviewing suspect transactions, and reporting on transaction history.

The Kount Risk Inquiry Service (RIS) is a real-time web service that determines the fraud risk of a transaction and evaluates the fraud rules configured in the AWC and/or the Thresholds configured via the Kount Central API. Once the evaluation has been completed, RIS returns a response indicating if the transaction should be approved, declined, or held for further review.

This document provides an overview of the implementation of RIS and the Kount Central API specific to Kount Central Fraud Manager.

Refer to the **Risk Inquiry Service (RIS) Technical Specifications Guide** for in-depth information on integrating RIS.

Refer to the online Kount Central API documentation at `https://api.kount.net/kc/index.html` for in-depth information on integrating the Kount Central API.

Contact your Kount Merchant Services representative for more information and consultation regarding implementation of Kount Central Portfolio Manager or Kount Central Enterprise.

RIS Mode J

Mode J is a simplified RIS call. It only performs Kount Central Fraud Manager threshold evaluation for the specified customer, and does not include Kount Central Portfolio Manager Rule evaluation or calculation of a Kount Score. Mode J transactions are not available in the AWC, search, or data mart. This gives Mode J the advantage of increased performance.

Many thresholds require data that is optional to Mode J only be evaluated if the necessary input is provided. For example, address distance thresholds require an address.

Mode J has the same input requirements as Mode Q with the addition of CUSTOMER_ID.

Each Kount Central Fraud Manager threshold has a built-in decision: “review” or “decline”. The overall decision for the transaction is determined by the highest priority threshold that was triggered. For example, if four review thresholds are triggered, and one decline threshold is triggered, the overall decision is “decline”.

Example mode J response:

```
VERS=0600
MODE=J
TRAN=3X830K3DKD06
MERC=100100
KC_CUSTOMER_ID=1
KC_TRIGGERED_COUNT=2
KC_WARNING_COUNT=0
KC_DECISION=D
KC_EVENT_1_CODE=emailVelocityReview
KC_EVENT_1_EXPRESSION=3 > 2
KC_EVENT_1_DECISION=R
KC_EVENT_2_CODE=orderTotalDecline
KC_EVENT_2_EXPRESSION=4999 > 1
KC_EVENT_2_DECISION=D
```

RIS Mode W

Mode W is basically a Mode Q with Mode J response appended to the end. Thresholds are evaluated in addition to Kount Central Portfolio Manager rules. Mode W transactions are available in the AWC, search, and data mart. Mode W has the same input requirements as mode Q, with the addition of CUSTOMER_ID.

In a Mode W, the threshold decision/response is appended to the Mode Q decision/response. It is the responsibility of the Processor to evaluate both decisions in a Mode W and take appropriate action.

JSON Data Structures

The Kount Central API leverages the JSON (JavaScript Object Notations) data-interchange format for all input and response data. JSON is an efficient format for both machine and human readability, and allows for extremely robust and flexible data exchange. See json.org for more details and information on JSON.

Within this document, JSON will be represented using the following formatting to facilitate easy identification:

```
{“merchantId”:999999, “customerId”: “Customer 1”}
```

API Keys

The Kount Central API uses OAuth2.0 for authentication, using the current JWT (JSON Web Token) specification for key structure. Keys are used not only to authenticate, but to identify the customer and their permissions.

http://tools.ietf.org/html/draft-ietf-oauth-json-web-token-25

There are two types of keys that can access the Kount Central API.

Gateway Key

Gateway keys are obtained from Kount Merchant Services. A gateway key controls access for Processors. Processors have the ability to manage their customers, as well as customer-centric operations such as threshold configuration. A gateway key does not expire, and can be revoked at any time. Kount cannot recover forgotten keys, but can regenerate a new key, revoking all previous keys for that Processors.

Gateway Customer Keys

Customer keys give access to customer related functionality such as threshold configuration. Customer keys are generated through the API using a gateway key. Customer keys auto-expire after one hour, making them similar to a session id. Generating additional customer keys will not revoke previous keys.

API Endpoint Management

For the most up-to-date information about API endpoint usages and relevant data types, refer to

https://api.kount.net/kc/index.html

API Endpoint Permissions

Processor Only Endpoints

- getCustomer
- addCustomer
- updateCustomer

Processor/Customer Endpoints

- generateCustomerKey
- updateThresholds
- getThresholds

See **Appendix B** under **RIS Optional Keys** in the **Risk Inquiry Service (RIS) Technical Specifications Guide** for more information about these RIS Keys.

Kount Central Thresholds

The following Thresholds are currently supported in Kount Central Fraud Manager and can be configured via the Kount Central API.

The Thresholds are categorized based on RIS Modes, Authorization Request Data, and Device Data Collector. The categories are:

- Basic Thresholds
- Pre-Authorization Thresholds
- Data Collector Thresholds

Within each category, the Thresholds are further organized based on their specific function.

NOTE: All Thresholds support Mode W but only a subset of them support Mode J.

Basic Thresholds

These Thresholds can be evaluated with any Kount Central RIS Mode and require only standard RIS Input data.

Billing Address Deliverable Filters

Review or Decline the transaction if the Billing Address provided by the customer is not deliverable.

Codes:

- billingAddressDeliverableDecline
- billingAddressDeliverableReview

Billing and Shipping Address Match Filters

Review or Decline the transaction if the Billing and Shipping Address provided by the customer are not an exact match.

Codes:

- billShipAddressNotMatchDecline

- billShipAddressNotMatchReview

Billing to Shipping Distance Thresholds

Review or Decline the transaction if the Billing to Shipping Distance (in Kilometers) exceeds the specified value.

Codes:

- billingToShippingAddressDecline
- billingToShippingAddressReview

Device IP Country Lists

Review or Decline the transaction if the Device IP Country matches any of the selected values.

Codes:

- blacklistIPCountryDecline
- blacklistIPCountryReview

Network Type Lists

Review or Decline the transaction if the Network Type matches any of the selected values.

Codes:

- blacklistNetworkTypeDecline
- blacklistNetworkTypeReview

Payment Country Lists

Review or Decline the transaction if the BIN Country matches any of the selected values.

Codes:

- blacklistPaymentCountryDecline

- blacklistPaymentCountryReview

Comment: BIN Country is only available when Credit Cards are used for the transaction.

Shipping Address Country Lists

Review or Decline the transaction if the Shipping Address Country matches any of the selected values.

Codes:

- blacklistShippingCountryDecline
- blacklistShippingCountryReview

Credit Card Velocity Thresholds

Review or Decline the transaction if the number of transactions with the same Credit Card in the last hour exceeds the specified value.

Codes:

- cardPtokVelocityDecline
- cardPtokVelocityReview

Device IP Velocity Thresholds

Review or Decline the transaction if the number of transactions with the same Device IP in the last hour exceeds the specified value.

Codes:

- deviceIPVelocityDecline
- deviceIPVelocityReview

Device IP to Billing Distance Thresholds

Review or Decline the transaction if the Device IP to Billing Distance (in Kilometers) exceeds the specified value.

Codes:

- deviceToBillingAddressDecline
- deviceToBillingAddressReview

Device IP to Shipping Distance Thresholds

Review or Decline the transaction if the Device IP to Shipping Distance (in Kilometers) exceeds the specified value.

Codes:

- deviceToShippingAddressDecline
- deviceToShippingAddressReview

Email Velocity Thresholds

Review or Decline the transaction if thenumber of transactions with the same Billing Email Address in the last 24 hours exceeds the specified value.

Codes:

- emailVelocityDecline
- emailVelocityReview

MasterCard EMS Score Thresholds

Review or Decline the transaction if the EMS Score is greater than the specified value.

Codes:

- masterCardEmsDecline
- masterCardEmsReview

Order Total Amount Thresholds

Review or Decline the transaction if the Order Total Amount (in fractional base currency, i.e. pennies) exceeds the specified value.

Codes:

- orderTotalDecline
- orderTotalReview

Shipping Address Deliverable Filters

Review or Decline the transaction if the Shipping Address provided by the customer is not deliverable.

Codes:

- shippingAddressDeliverableDecline
- shippingAddressDeliverableReview

Suspect IP Address Filters

Review or Decline the transaction if the Device IP address is found on a global list known to be associated with fraud.

Codes:

- suspectIPDecline
- suspectIPReview

Transaction Velocity Thresholds

Review or Decline the transaction if the number of transactions in the last 24 hours exceeds the specified value.

Codes:

- transactionVelocityDecline
- transactionVelocityReview

Universal Chargeback Card Filters

Review or Decline the transaction if the Card is found in the universal chargeback list.

Codes:

- universalChargebackCardDecline
- universalChargebackCardReview

Pre-Authorization Thresholds

These Thresholds can be evaluated with any Kount Central RIS Mode but require data obtained from a Payment Authorization request. Device Data Collector is neither required nor optional.

AVS Street Response List Thresholds

Review or decline the transaction if the AVS Street Authorization Response matches any of the values selected.

Codes:

- blacklistAvsStreetResponseDecline
- blacklistAvsStreetResponseReview
- blacklistAvsZipResponseDecline
- blacklistAvsZipResponseReview

CVV Response Thresholds

Review or Decline the transaction if the CVV Authorization Response matches any of the specified values.

Codes:

- blacklistCvvResponseDecline
- blacklistCvvResponseReview

Data Collector Thresholds

These Thresholds can only be evaluated with Kount Central RIS Mode W and require the Device Data Collector be present on the payment page.

Device Fingerprint Velocity Thresholds

Review or decline the transaction if the number of transactions with the same device fingerprint in the last hour exceeds a specified value.

Codes:

- deviceFingerprintVelocityDecline

- deviceFingerprintVelocityReview

Comments: The Device Data Collector is required for these Thresholds to be evaluated.

Fraud Risk Filters

Review or Decline the transaction if the fraud risk is High.

Codes:

- highRiskDecline
- highRiskReview

Review the transaction if the Fraud Risk is Medium.

Codes:

- mediumRiskReview

Comments: The Device Data Collector is considered optional for these filters but is considered more accurate when it is present.

Phone Billing Filters

Review or Decline the transaction if the billing phone number has no directory match.

Codes:

- invalidBillingPhoneDecline
- invalidBillingPhoneReview

Glossary of Terms

- **AWC (Agent Web Console)** - front-end interface to Kount Complete, used in Kount Central Enterprise and Kount Central Portfolio Manager.
- **Customer** - E-commerce merchant using Kount Central services through a Processor. Customers will use Kount Central Fraud Manager through a Processor's implementation of the Kount Central API.
- **Endpoint** - An entry point to Kount Central API functionality.
- **Gateway** - See **Processor**.
- **Key** - API Key used to authenticate against an Endpoint.
- **Processor** - Primary customer of Kount Central and consumer of the Kount Central API. Provides E-commerce services to Customers.
- **Response** - A reply from an endpoint.
- **Risk Inquiry Service (RIS)** - Real-time web service that evaluates the risk of a transaction.
- **Threshold** - A pre-defined, configurable rule that triggers on transaction data. The core of the Kount Central Fraud Manager product.
- **Token** - See **Key**.


Kount®