SD HELOC Advance Developer Guide

# Overview

This document is intended to guide BK and customer technical resources with configuring and developing integration code to handle receipt of notifications sent to the customer, when a borrower requests an advance against their HELOC loan or deletes a previously requested advance.

# Event Gateway Setup

The EG team should be engaged to help setup the customer to receive events via the BK Event Gateway. Servicing Digital uses a generic message format that encapsulates the JWE (encrypted JWT) payload within the overall Event Gateway message. EG provides options for XML and JSON message formats.

# Encryption Keys

Servicing customers will provide their public key to BKFS, preferably using a JWKS web site and the key identifier, as part of the implementation process. The configuration of the key is handled thru the setup of the HEADVNOTIC feature to reference one of the JWKS\*\* features. The JWKS00-JWKS05 features are

available to use for one or more integrations with the servicer’s web site. Black Knight provides the Servicing Digital Signing key from a public JWKS web site that can be used by the customer for verification of the JWS that is embedded within the JWE.

**Note:** Coordination must be established between the customer and BK to ensure each party notifies each other of when new keys are going to be published. An overlap period would be required so that the new and old keys are still valid during key “rollover.”

## API Specification

The API specification documents the JSON message format sent by the Servicing Digital system to the servicers event notification end point. Note that the servers and path are place holders that should be replaced with the actual URL for the customers web service that will receive the notification POST. Please contact your support team from Black Knight for the specification.

# Message Details

The message sent by BK includes data that is in plain text with non-sensitive data such as the loan number, as well as an embedded JWE that contains the full details for the advance.

SD will send a message with one of two message topics, when a borrower adds or deletes a draw request using Servicing Digital:

* ELOC/DrawAdded
* ELOC/DrawDeleted

SD sets the “Source” of the message to *ServicingDigital* to differentiate SD messages from MSP sourced events:

<egnp:ObjSrcNm name="System">*ServicingDigital*</egnp:ObjSrcNm>

SD will set the encoded JWE as the value of the SDMessage\_v1 element:

<sd:SDMessage\_v10 formatType="JWE">**{Encoded JWE}** </sd:SDMessage\_v10>

# HEADVNOTIC Feature Configuration

The HEADNOTIC feature is used to enable and configure the ability to receive notifications from the Event Gateway whenever a borrower makes an advance request or cancels an advance request. This feature has two properties that must be configured:

* **JWKS Feature Reference** - By default this property is set to JWKS00. The value may only be set to one of 5 encryption related features:  JWKS00 – JWKS05.  This property determines what feature is used to specify the public key used to encrypt the message payload data.
* **Assertion Type** – This property controls the format of the assertion / message payload. For test systems it is acceptable to set this property to JWT to make it simpler to debug, but for production this **must be** configured to create a JWE (encrypted JWT.)

# JWKS (Encryption) Feature Configuration

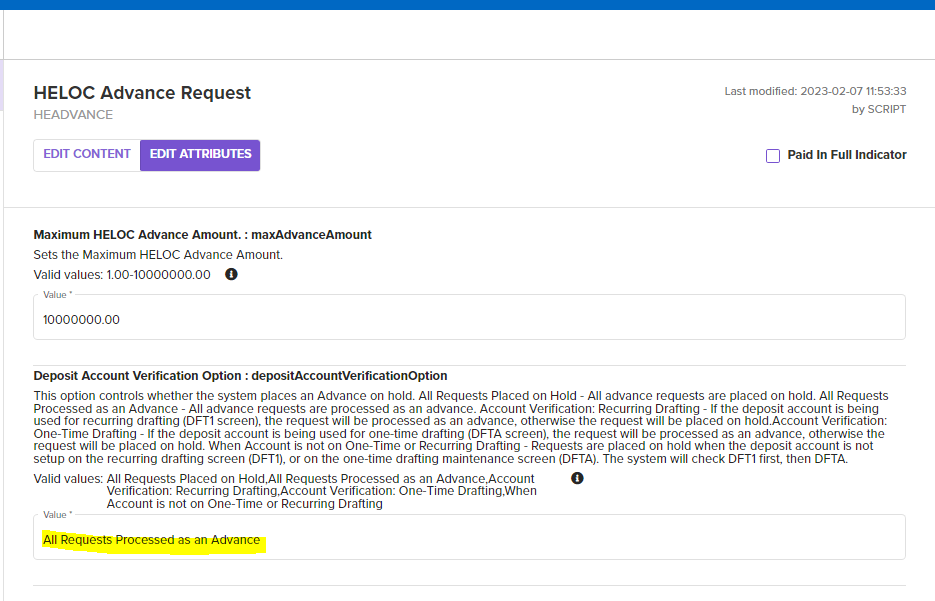
There are 5 available features that can be setup to provide the public key certificate that is used to encrypt the JWE (encrypted JWT.) The certificate can be provided either “hard coded” as a PEM String or via a JWKS web site that is used to download the public key certificate. It is the client’s responsibility to update this information, or work with client support to update this information, if it changes for a new certificate:

* **JWKS Encryption Certificate** – A PEM certificate to use when encrypting the payload.
* **JWKS Encryption Key Identifier** – The key identifier to use when downloading the certificate from the JWKS web site provided by the customer.
* **JWKS Encryption URL** – The URL of a web site that provides the public key used for encryption, in JWKS format.

Graphical user interface, text, application, email

Description automatically generated

# HEADVANCE Feature Configuration



The HEADVANCE feature must be enabled for the HELOC Advance functionality to be enabled in servicing digital. There are currently 2 properties that can be configured, the Deposit Account Verification Option, affects whether the system posts an Advance or places an Advance Funds Hold.

# Example Message



# Sample Java Decryption Code

This is a simple example that shows the basic steps to decode a JWE using the Java Nimbus library. It creates a public and private key then uses the public. It requires maven to build and run the example:

mvn compile exec:java -Dexec.mainClass="App"



The information contained in or supplied with this document (the “Information”) is the property of Black Knight Technologies, LLC, or one of its affiliates or subsidiaries (collectively, “Black Knight”) and contains the confidential, proprietary, and/or trade secret information of Black Knight. The Information cannot be used, modified, extracted, copied, or distributed without the prior written consent of Black Knight. With or without Black Knight’s prior written consent, Black Knight will not be liable for the disclosure or use of the Information. The intended recipient shall not use any part of the Information contained in, or supplied with this document, in any way to the competitive disadvantage of Black Knight, and will take all steps designed to assure its compliance with this provision. Nothing herein shall be construed, nor is Black Knight providing, any legal or compliance advice.

If this document contains proposal language, this proposal is neither an offer nor intended by Black Knight, upon acceptance by the intended recipient, or otherwise, to create a binding agreement with Black Knight. Such an agreement shall be reflected only by a definitive contract executed by both parties.

If this document contains feature or functionality specifications (the “Specifications”), Black Knight does not guarantee the accuracy of the Specifications for any product, service, or functionality identified. The Specifications contained in this document may not be complete or up to date, and Black Knight is not responsible for notifying the recipient of changes in the Specifications.

TM SM ® Trademark(s) of Black Knight IP Holding Company, LLC, or an affiliate.

© 2023 Black Knight Servicing Technologies, LLC. All Rights Reserved.