

Partner Integration Certification

Digital River

Table of Contents

[Overview 2](#_Toc78367152)

[Purpose 2](#_Toc78367153)

[Summary 2](#_Toc78367154)

[Requirements and Scope 2](#_Toc78367155)

[Front end ecommerce implementation 2](#_Toc78367156)

[Implementation Documentation (Requirements) 2](#_Toc78367157)

[Scope 3](#_Toc78367158)

[In scope for ecosystem partners 3](#_Toc78367159)

[In scope for Digital River 3](#_Toc78367160)

[Certification Approach 3](#_Toc78367161)

[Planning 3](#_Toc78367162)

[Milestone Entry Criteria 3](#_Toc78367163)

[Milestone Exit Criteria 3](#_Toc78367164)

[Commerce Partner Validation 4](#_Toc78367165)

[Milestone Entry Criteria 4](#_Toc78367166)

[Milestone Exit Criteria 4](#_Toc78367167)

[Digital River Security Certification 4](#_Toc78367168)

[Milestone Entry Criteria 6](#_Toc78367169)

[Milestone Exit Criteria 7](#_Toc78367170)

[Digital River Technical Validation 7](#_Toc78367171)

[Milestone Entry Criteria 7](#_Toc78367172)

[Milestone Exit Criteria 7](#_Toc78367173)

[Digital River Compliance Certification 7](#_Toc78367174)

[Milestone Entry Criteria 7](#_Toc78367175)

[Milestone Exit Criteria 8](#_Toc78367176)

[Issues and Prioritization 11](#_Toc78367177)

[Issue Triage Process 11](#_Toc78367178)

[Defect Severity Matrix 11](#_Toc78367179)

[Priority Matrix 12](#_Toc78367180)

# Overview

## Purpose

The purpose of this document is to provide a general overview of the Digital River certification process. This document is limited to defining the scope of the initial integration and does not cover client integrations into the ecosystem.

This document should be used in conjunction with the project requirements, test scenarios, and prescriptive test cases to determine the full coverage.

## Summary

Digital River requests ecosystem partners provide the following components as part of our certification process. The requirements can be summarized as:

1. An ecommerce front end created utilizing the partner ecosystem as evidence of functionality.
   1. This includes two sets of admin credentials used for configuration and customer service as well as at least one shopper account if Digital River is unable to create new shoppers.
2. Demonstration of functionality
3. Execution of minimal scenario set provided by Digital River
4. Order placement using all available payment methods against PTE environment
5. Access to Source Code wrapping SDK to enable ecommerce workflow
6. Sequence diagrams covering most common user scenarios

# Requirements and Scope

## Front end ecommerce implementation

The partner is responsible for building a store using their commerce ecosystem in conjunction with the ecommerce front end application for which it is built. Administrative access is also required for validation of the API key setup, SKU creation, and customer service functionality.

This ecommerce front end is required for use in validation of the successful integration between the partner commerce system and Digital River. Digital River will perform functional testing of the implementation and verify the flow to our systems. Validation will also include error handling and implementation efficiency (e.g. not making redundant calls).

## Implementation Documentation (Requirements)

Digital River and our ecosystem partner will document and review implantation details that can vary between ecosystems to be used by certification teams. These details include (but are not limited to):

* Payment methods
* Supported locales and payment methods
* Variants from standard implementation baseline

## Scope

### In scope for ecosystem partners

* Execution of all Digital River supplied scenarios with required documentation complete.
* Sequence diagrams delivered to Digital River

### In scope for Digital River

* Validation of data created by all scenarios executed by ecommerce partner
* Creation of minimal automation set mocking partner’s sequence flows
* Assessment of secure development of source code and strength of security controls implemented in applications (admin as well as commerce store)
* Validation of co

# Certification Approach

The certification process can be broken down into the major 3 areas:

1. Technical review – validation of the adherence to build standards, data schemes and technical best practices. Includes automation of sequence flows for use in pre-release validation on Digital River side.
2. Compliance and documentation review – validation of display and notice requirements as well as review of documentation provided by partner to facilitate ongoing support.
3. Security review – assessment of implementation security.

This section identifies the major certification milestones, any entry/exit criteria, and deliverables along with who is responsible for each.

## Planning

The ecosystem partner and Digital River will agree upon scope of implementation and timelines for certification.

### Milestone Entry Criteria

* Agreed upon implementation documentation (requirements)
* Schedule with major milestones

### Milestone Exit Criteria

* Digital River to provide system integrator with high level scenarios and prescriptive test cases for execution by partner

## Commerce Partner Validation

The ecosystem partner is responsible for providing evidence that all implementation requirements are met by implementing a site on the ecommerce front end using the delivered build standards. They are also responsible for testing the implementation and providing Digital River with the results of the test case execution and a walk-through of the admin setup and store. This validation will be completed against Digital River’s PTE Environment.

### Milestone Entry Criteria

* Store created with ecommerce front end and integrated with Digital River’s PTE environment.
* Digital River scenarios to be executed by ecosystem partner provided

### Milestone Exit Criteria

* All planned scenarios to be executed by ecosystem partner are complete with no priority 1 defects.
* Any open Priority 2 or 3 defects reviewed with Digital River and agreed upon for deferral.
* Open issues must have estimated timelines for resolution or exemption approval.
* Demo of ecommerce store and admin for Digital River.
* Results of Digital River prescriptive test cases delivered.

## Digital River Security Certification

Below is a breakdown of the validation areas required for the Security Certification. The ecosystem partner is required to pass the following questions to maintain security certification:

##### Authorization

* Is the placement of authentication and authorization check correct?
* Is there execution stopped/ terminated after for invalid request? i.e. when authentication/authorization check fails?
* Are the checks correct implemented? Is there any backdoor parameter?
* Is the check applied on all the required files and folder within web root directory?
* Are security checks placed before processing inputs?
* Is there execution stopped/ terminated after for invalid request? I.e. when authentication/authorization check fails?
* In case of container-managed authentication –
* Is the authentication based on wed methods only?
* Does the authentication get applied on all resources?
* Is the authentication based on web methods only?
* Is password Complexity Check enforced on the password?
* Is password disclosed to user/written to a file/logs/console?
* Does application design call for server authentication (anti-spoofing measure)?
* Does application support password expiration?

##### Business Logic and Design

* Are there unused configurations related to business logic?
* If request parameters are used to identify business logic methods, is there a proper mapping of user privileges and methods/actions allowed to them?
* Check if unexposed instance variables are present in form objects that get bound to user inputs. If present, check if they have default values.
* Check if unexposed instance variables present in form objects that get bound to user inputs. If present, check if they have default values.
* Check if unexposed instance variables are present in form objects that get bound to user inputs.
* Check if unexposed instance variable present in form objects that get bound to user inputs. If present, check if they have default values.
* Are the checks correct implemented? Is there any backdoor parameter?
* Is the check applied on all the required files and folder within web root directory?
* Is there any default configuration like Access – ALL?
* Does the configuration get applied to all files and users?
* Does the centralized validation get applied to all requests and all the inputs?
* Does the centralized validation check block all the special characters?
* Are there any special kind of requests skipped from validation?
* Does the design maintain any exclusion list for parameters or features from being validated?
* Is there any known flaw(s) in API’s/Technology used? For eg: DWR
* Does the design framework provide any inbuilt security control?
* Like <%:%> in ASP.NET MVC?
* Is the application taking advantage of these controls?
* Are privileges reduced whenever possible?
* Is the program designed to fail gracefully?
* Are all of the entry points and trust boundaries identified by the design and are in risk analysis?

##### Cryptography

* Is password stored in an encrypted format?
* Are database credentials stored in an encrypted format?
* Is the data sent on encrypted channel? Does the application use HTTP Client for making external connections?
* Is all PII and sensitive information being sent over the network encrypted for?
* Are there any special kind of requests skipped from validation?
* Keys are not held in code.

##### Data Management

* Data is validated on server side
* HTTP headers are validated for each request
* Is all XML input data validated against an agreed schema?
* Is output that contains untrusted data supplied input have the correct type of encoding URL?
* Has the correct encoding been applied to all data being output by the application?

##### Design

* Check if they have default values
* Check if they get initialized before form binding

##### General

* Are there backdoor/unexposed business logic classes?
* Are external libraries, tools, plugins used by the application functions the most recent version of these protocols, parched and process in place to keep them updated?
* Classes that contain security secrets (like passwords) are only accessible through protected API’s
* Plain text secrets are not stored in memory for extended periods of time.
* Array bounds are checked.
* All sensitive information used by application has been identified.

##### Input Validation

* Input data is constrained and validated for type, length, format, and range.
* Are all the untrusted inputs validated?

##### Logging and Auditing

* Are logs logging personal information, passwords, or other sensitive information?
* Do audit logs log connection attempts (both successful and failures)?
* Is there a process(s) in place to read audit logs for unintended/malicious behaviors?

##### Session Management

* Does the design handle Session Managements securely?
* No Session Management parameters are passed in URLS
* Session Management checks:
* Cookies expire in a reasonable short time
* Cookies are encrypted
* Data is validated
* ID is complex
* Storage is secure

##### User Management and Authentication

* User and role-based privileges are documented
* Authentication cookies are not persisted
* Authentication cookies are encrypted
* Authentication credentials are not passed by HTTP GET
* Authorization check are granular (page and directory level)
* Authorization based on clearly defined roles
* Authorization works properly and cannot be circumvented by parameter manipulation
* Authorization cannot be bypassed by cookie manipulation

##### Web Services

* Web service has documentation protocol is disable if the application does not need dynamic
* Web service endpoints address in Web Services Description Language (WSDL) is check for validity
* Web service protocols that are unnecessary are disable (HTTP GET and HTTP POST)

### Milestone Entry Criteria

* All known open issues communicated

### Milestone Exit Criteria

* All security questions answered
* No open security issues requiring remediation

## Digital River Technical Validation

Digital River will evaluate the technical implementation by reviewing the logged requests and responses from prescriptive scenarios completed by our ecommerce Partner to ensure they follow the standards outlined at <https://docs.digitalriver.com/digital-river-api/>

and <https://www.digitalriver.com/docs/digital-river-api-reference/> . In addition, Digital River will do time-boxed testing (1 week) of the UI. During this milestone Digital River will focus validation on the following items:

* Log validation
  + Adherence to agreed-upon implementation (requirements) .
* Adherence to build standards, data schemas, and best practices
  + Verify there are no extraneous or unnecessary calls e.g. identical requests or not sending deltas of SKUs
  + Verify there is no hard-coded data
* UI validation
  + Negative scenarios and error handling
  + Administrative areas for managing keys

Digital River will also automate API flows based off the partner identified sequences.

### Milestone Entry Criteria

* Any open issues from partner testing reviewed
* URL and login information for Administration and storefront
* All prescriptive scenarios executed by partner and required documentation provided to Digital River

### Milestone Exit Criteria

* No open Digital River identified technical certification issues requiring remediation
* Automated regression flows implemented

## Digital River Compliance Certification

During the compliance certification Digital River will review the storefront to ensure all compliance requirements and best practices have been applied. They will also review all implementation details to ensure sufficient detail has been provided to enable the ongoing support of the integration between Digital River and the partner ecommerce ecosystem.

### Milestone Entry Criteria

* Demonstration of administration screens and shopper site
* Any open issues from partner testing reviewed
* Link and accounts provided to Digital River to access administrative screens and shopper site

### Milestone Exit Criteria

* All required compliance components validated
* No open compliance issues requiring remediation
* Any best practices not met reviewed and agreed upon by stakeholders
* All integration documentation reviewed by stakeholders

##### Entities and Disclosures

* Digital River entity disclosures
  + Reseller disclosure identifying correct Digital River selling entity on call checkout pages and transaction notices
* Digital River terms of sale and privacy policy
  + Footer
    - Link to Digital River’s Privacy and Policy Terms of sales on all checkout pages and transaction notices
  + Order Review Page (final page prior to consumer payment submitted)
    - Checkbox requiring consumer acceptance
    - Cannot complete order without acceptance of terms
      * Terms of Sale (displayed as link)
      * Privacy Policy (displayed as link)
        + Active Acceptance

EU and ROW shoppers must accept Digital River’s reseller disclosure and Privacy Policy

* Regional Disclosures (based on region)
  + Legal Notice
  + Cancellation Right
  + Cookie Policy
  + Banner notice of the use of cookies
* Required Locations
  + Checkout pages
    - Cart
    - billing/shipping address
    - payment
    - order review pages
  + Transaction Notices (Customer email notifications)
    - Successful cancellation of all or part of order (physical products)
    - failed cancellation of all or part of order (physical products)
    - order confirmation
    - shipment confirmation
    - physical goods return instructions emails
    - refund confirmation
    - delayed shipment right to cancel notifications

##### Tax Management

* Final tax calculations
  + Digital River is responsible for final tax calculations. All relevant attributes must be included in checkout
    - shipFrom
      * US: state, postal code, country
      * CA: province, country
      * EU: country
    - shipTo
      * US: state, postal code, country
      * CA: province, country
      * EU: country
    - SKU taxCode
  + Tax Display
    - Based on region

* SKU setups
  + SKU creation for Digital River requires several values including but not limited to
    - id (sku)
    - eccn
    - country of origin
    - name
    - taxcode
    - additional field depending on type of product and payment method
  + Display of regulatory fees (physical goods only)
  + ECCN (Export Control Classification Number)
  + hsCode must be added to the SKU if using Digital River landed cost estimator
    - * If using landed cost estimator hsCode is required

* + - All SKUs must be setup with an ECCN as well as tax code to comply with US Export Control Laws
* Regulatory fees (physical products only)
  + Based on region
    - US/Canada/Mexico
      * Disclosed to consumer prior to final submission of order
    - EU
      * Price of goods and/or services, inclusive of tax and regulatory fees, displayed throughout the checkout pages. 'Prices includes VAT' must display next to the price.
* Global tax ID Management
  + Outside US, VAT/Tax Identification captured
    - Display of VAT or disclosure if not possible to calculate
  + US Tax Certificates/Tax Management
    - If B2B or tax exempt sales are expected in the United Sates. Digital River requires clients to include Digital River Global Tax management feature capabilities.
      * Set customer type to business or individual
      * Support upload of US tax certificate
        + companyName
        + taxAuthority
        + startDate
        + endDate
        + fileID
* Import duties + tax (hsCode)
  + hsCode must be added to the SKU if using Digital River landed cost estimator
  + If using landed cost estimator hsCode is required

##### Risk Management

* Block and hold transactions
  + Messaging for Fraud Block and Fraud Hold handlded by implementation partners/connectors
* Fraud decisions
  + DigitalRiver.js code must be included on checkout pages
    - entity required
    - locale optional
  + IP address of the shopper must be included in all create checkout calls
* Refunds, returns, chargebacks/disputes
  + State/webhook responses must be handled
  + Must ensure the commerce application is informed about changes to order status in the case of chargebacks/disputes

##### Legal Compliance

* Consumer protection
  + Shopper facing requirements
    - Short description of goods or service
      * If applicable
        + Technical requirements or limitations
        + Limited term of use
    - Call to Action Button
      * Clear that purchase being made, Complete Your Purchase or Buy Now
    - Customer support
      * Help pages with FAQs and contact information for Customer Service
    - Fulfillment
      * Request/notice must be submitted no later than 7 days after payment authorization to ensure the transaction does not fail for settlement
* Trade compliance
  + Supported ship from/ship to (trading patterns)

# Issues and Prioritization

## Issue Triage Process

Regular project meetings will be held to discuss open issues to ensure they are being addressed by either the commerce partner or Digital River. During these meetings Digital River will walk through all open issues documented in Jira.

The triage process will include representatives from Project Management, Product, Engineering, Partner Enablement, and Security as needed.

## Defect Severity Matrix

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Level** | | **Definition** | | **Example** | |
| **Severity 1 – Critical** | | These bugs cause a crash, hang, serious data corruption/loss, or pose a critical security risk.  Defect does not have a feasible workaround. Customer greatly impacted.   This is a commerce stopping defect without a workaround. | | * Unrecoverable crashes, hangs * Causes serious data corruption or loss * Fatal assertion failures * A non-fatal assertion that does not cause exception/hang after clicking [Ignore] is NOT a Severity 1 bug * High risk security issues * Unrecoverable errors * Extremely severe functionality problems that make it impossible to use a device | |
| **Severity 2 – Major** | | This is a serious defect that causes a frequently used feature to operate contrary to the spec. This is a defect affecting application flow with an existing workaround. | | * Non-fatal assertion failures * Major functionality issues * Memory leaks leading to device lockup * Security bugs without significant vulnerability * Frequent deadlocks * Occasional crash, recoverable on restart * Government regulatory/legal issues | |
| **Severity 3 – Average** | | This would be a defect or design change request to meet a mandatory requirement. This is a defect that impairs system usability, but all main functions are available. | | * Minor functionality issues * Major UI issues * Mandatory requirements * Feature required to enable important new functionality needed by customer(s) | |
| **Severity 4 – Minor** | | This is primarily a cosmetic problem or other small distractions that ought to be corrected.  This is a cosmetic defect that does not affect any of the application main functions. | | * Issues that don’t noticeably affect customer experience * Trivial bugs * Spelling/Localization errors * Very low customer impact * Poorly worded phrases | |

## Priority Matrix

|  |  |  |
| --- | --- | --- |
| **Level** | **Definition** | **Example** |
| **Priority 1 – High** | Issue must be fixed for next phase of testing or launch | All launch blockers and critical functionality. |
| **Priority 2  - Medium** | Highly desirable but not progress blocking | Issues which need to be addressed but due to time constraints may be delayed to a later phase of validation. |
| **Priority 3 - Low** | Nice to have but not currently scheduled | Fix if time and resources allow. |