Adobe Digital Publishing Security FAQ

Table of contents

DPS Security Overview

The intended audience for this document is IT and security professionals within companies that intend to use Adobe Digital Publishing Suite (DPS) to publish content and build apps on multiple platforms that allow end users to view that content. It is not intended to be a workflow document on how DPS works nor is it a tutorial on how to design, layout or publish content using DPS. It is intended to provide IT professionals with an understanding of the various DPS services, how they communicate inside and outside the DMZ, where customer data is stored, transformed and how it is distributed to mobile devices.

How secure is the Adobe Digital Publishing Suite? This question is asked in a variety of ways, from a variety of customers on an almost daily basis. It's a simple question with a wide array of possible answers. Adobe DPS is a complex product consisting of multiple clients and hosted services spanning multiple physical locations, built on top of a large complex technology stack. Security itself has different meanings across customer segments and potential uses for DPS. Rather than attempting to answer the question "How secure is DPS?," we've chosen to gather up many of the direct questions asked of DPS field engineers, product managers, and sales and answer them directly, letting each customer decide if DPS is secure enough for their use.

Network Service Topology:

The following network diagram describes the complete service topology for the Adobe Digital Publishing Suite (DPS).

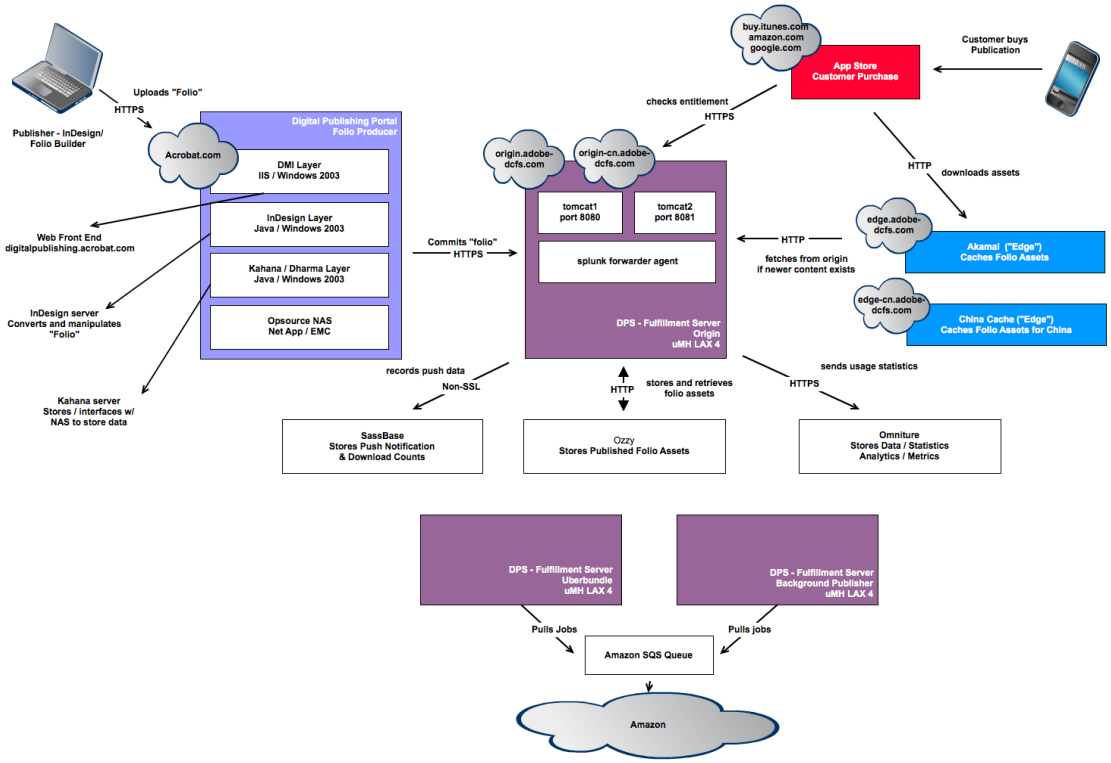

Figure 1: DPS Service Process diagram

Folio Producer Service Network Diagram:

The following diagram describes the network topology of the Folio Producer Service. It corresponds to the box labeled Digital Publishing Portal, Folio Producer in diagram number 1.

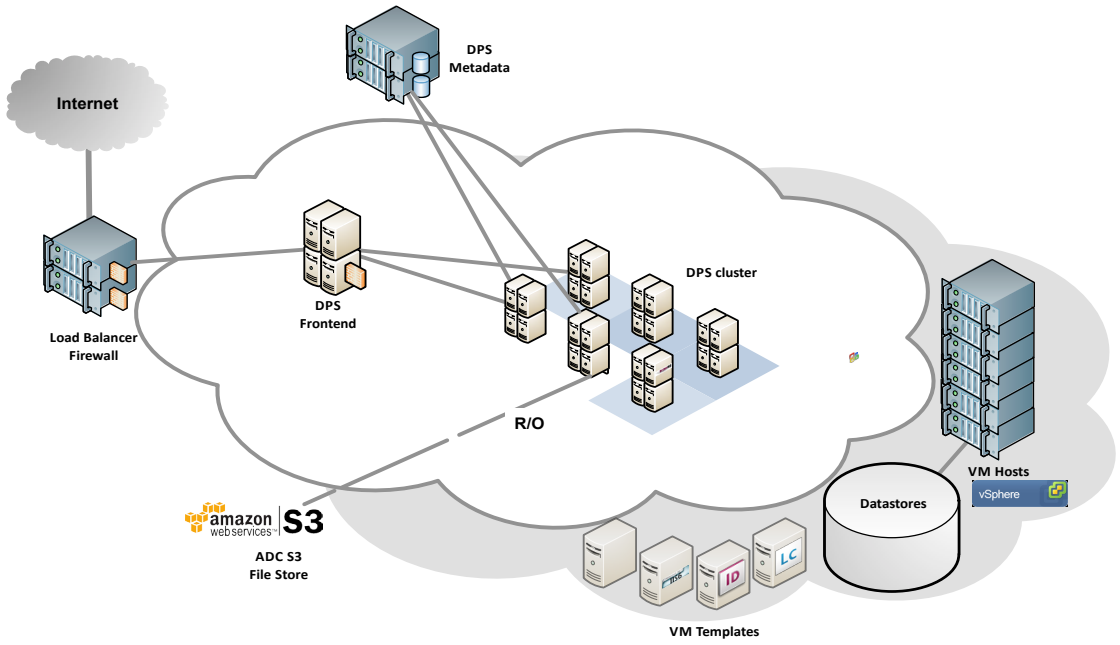

Figure 2–Folio Producer Network Diagram

Fulfillment Server Network Diagram:

The following document describes the network topology of the Distribution Service. It corresponds to box labeled DPS – Fulfillment Server in diagram 1.

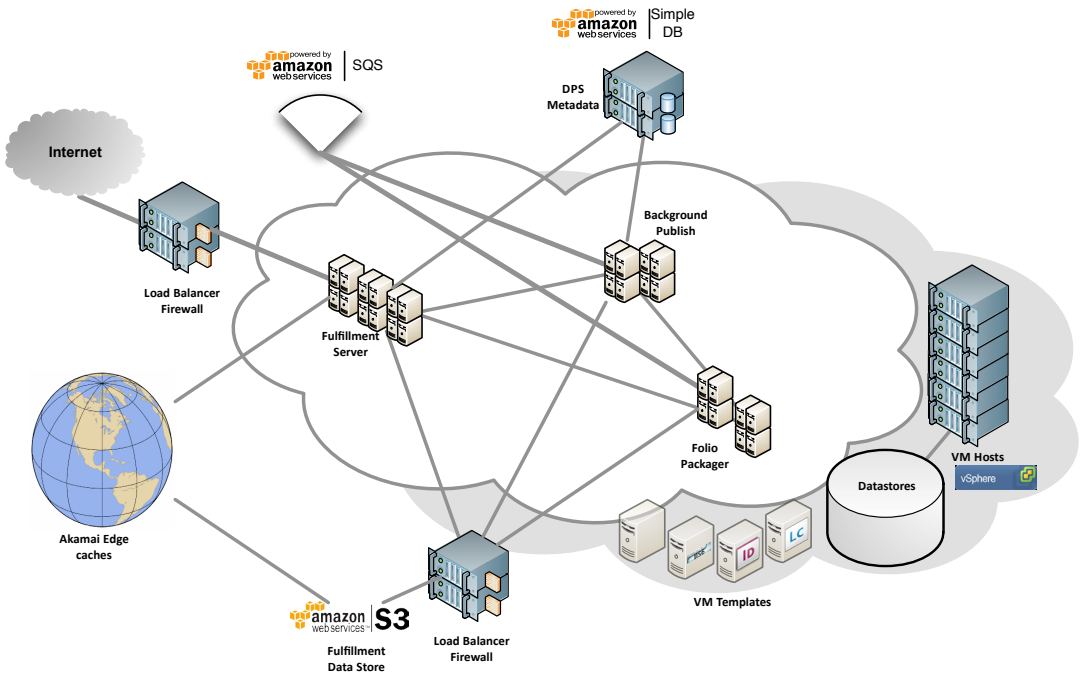

Figure 3 – Fulfillment Server

FAQ

How is my content secured during the creation process?

During the content creation process DPS provides multiple methods to ensure content is secure. When using the folio builder panel all content creation activities are performed over a secure HTTPS connection between the panel and the folio producer service. This is also true for any users that create content using an editorial workflow system built on top of the folio producer APIs. The repository where content is stored is keyed to a specific Adobe ID and all storage is virtually separated by that key. Users also have the option to create offline folios that exist only on their local hard drives until uploaded to the folio producer service.

Is my content secured at rest?

Content is not encrypted while at rest on the folio producer service. It is also not stored in a state that is accessible to any services other than the FP API, folio builder panel or folio producer or distribution service. The Folio Producer Service is based on Acrobat.com. Users cannot browse to the uploaded folio and perform any functions outside of the DPS ecosystem. Browse access has been disabled from the Acrobat.com organizer.

Is it secured during transfer?

During the content creation (upload) step all content transfers are performed over secure HTTPS connections. When content is published it is moved from the Folio Producer Service to the Distribution service. When content is downloaded from the distribution service the connection path between the mobile device and the distribution service is performed over regular HTTP.

Is it secured after publishing?

Published folios on the distribution service can be accessed via HTTP Rest APIs. Folios published privately require login to the distribution service in order to retrieve a token used to access the private folio.

How is the system designed?

Please refer to the previous network diagrams that show the service infrastructure and topology of DPS. All network connections are marked with HTTP or HTTPS connections to outline the security of the network connection.

What do you do with confidential data?

There is no differentiation in DPS of confidential vs non confidential user created content. Customers should not highly confidential data in a folio.

What security testing is done by Adobe Systems?

Adobe performs a security scan of the DPS system prior to every release. This scan looks for non secure network setup across firewalls, load balancers and server hardware. Adobe has highly trained operations staff who are trusted with creating a secure network topology and infrastructure not only for DPS but also for other Adobe hosted products and services including Photoshop.com, Adobe Creative Cloud and Adobe Marketing Cloud.

Adobe also periodically contracts out to have 3rd party security companies run a complete set of penetration testing activities on the external and internal systems. This penetration testing involves Adobe engineers and consists of software scans as well as a visual inspection of the code and the pre hardened operating systems and technology stack.

Can I get copies of those reports?

Copies of the pre-release security scan are available on request. Please contact your sales support staff to request a copy.

What security testing can customers do?

Customers are permitted to run their own external security scan of the DPS externally facing infrastructure. No customers are allowed to perform penetration or load testing on externally facing DPS systems. Customers that attempt to perform this sort of testing are in violation of the DPS terms of use and are subject to contract termination or service suspension.

Do you run any Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS)?

Yes, both our Folio Producer Service and our Distribution Service are actively monitored by IDS and IPS systems.

Where is my data located?

DPS is physically located in multiple locations depending on the service. Hardware is currently located in Los Angeles, San Jose, London and New Jersey as well as a variety of Amazon data centers located in the US East region.

Can I audit your data centers?

Adobe hardware is co-located in data centers with other companies. In order to protect all companies, access is strictly limited to approved vendors and operation staff. DPS is also physically located in a variety of Amazon data enters in the US East region. Access to those data centers is limited by Amazon's terms of use.

Is my data segregated?

Data is virtually segregated by account across all DPS services. We consider data integrity to be vital across the DPS solution and have taken all considerations to make sure that there is no data bleed between users across folio creation and production as well as across all data gathered for analytics.

What sort of information is stored in your logs?

Our server side logging contains as much information as possible to diagnose service outages, specific customer problems and reported bugs. The logs do not contain username / password combinations but do contain Adobe id's to help diagnose specific customer problems around production problems.

Who has access to logging information?

Logging information is limited to specific individuals charged with diagnosing direct customer issues.

Who in Adobe has access to my data?

Access to customer data is limited to a small amount of technical support personnel and key engineers. Adobe personnel will not modify customer data nor attempt any operation that causes the modification of data unless given explicit instructions by the customer after their identity has been verified according to Adobe Customer support policies and procedures.

How are those employees vetted?

Adobe performs deep background checks on every employee as well as a system of audits to ensure that customer support logs all interaction with customer data.

What is the process for notifying a customer of any security issues or non authorized access to customer data?

Adobe has multiple paths to notify customers of any security issues. Technical support has multiple contacts for each and every DPS customer and will reach out directly in case of non authorized access to customer data. Any medium to large issue will result in direct customer contact as well as an email sent to all subscribed DPS customers, notifications on the user forums and DPS status page and additional methods. General status updates are provided on the DPS status page–*http://status.adobedps.com/*

How is my data backed up/stored/transported?

DPS data is not backed up in the traditional sense of a magnetic backup that is stored in a secure location and restored as needed. Folios under creation are versioned on a redundant storage system. This system is constantly monitored for issues and corrections made as needed. Published folios on the distribution service are also stored on a redundant storage system. Early in 2013, folio storage will migrate to Amazon's S3 system and all redundancy will be transparent across multiple data centers in a single region (US East).

What is your disaster recovery plan?

In case of a major disaster that takes out an entire Amazon region, Adobe has the ability to set up complete environments quickly. In this scenario, customers would be expected to recreate folios from the original source content on the new environment.

What happens to my data when my contract with Adobe expires?

Customers can delete their published folios at any time prior to the expiration of a contract. After the contract expires, published content will remain on the DPS servers for at least 90 days. After the 90 day window, Adobe reserves the right to remove content from the distribution service on an as needed basis.

What secure data (certificates, keys, credentials) do you store on Adobe infrastructure?

The App builder service (where a user is asked for certificates and provisioning profiles in order to sign a customer app), leaves all certificates local on the signing machine. No certificates are transferred to Adobe as part of this process.

In order to complete the subscription verification process we do require that customers register their app store shared key for each app they build that offers in app purchase of subscriptions. This is a private key and Adobe conforms to Apple guidance on how this key is transported, stored and used as part of the subscription verification process using the iOS SDK.

Users that chose to use the Adobe push notification service for iOS are required to upload their push certificates to an Adobe server. Adobe follows Apple guidance on 3rd party managing of push certificates.

Can a customer store data on their own systems?

No. Adobe requires that all folio content be stored on our hosted service.

We require all data stored locally inside our own firewall, can we use DPS?

There is one limited way for customers that require all data remain inside their firewall to use DPS. Customers can create an offline folio (stored locally), use this offline folio to create a single edition app (1 folio embedded in the app), sign this app with an enterprise certificate and make this app available for download inside the corporate firewall. This is a very limiting scenario as it requires customers to rebuild their app for any changes in content.

Explain the various DPS accounts

Currently DPS offers the following types of accounts.

DPS Enterprise
DPS Professional
DPS Creative Cloud
DPS Free

Enterprise or professional accounts can be assigned none to all of the following roles.

Master account – used to administer other accounts in the same company
Application account – create content, publish, create app, links analytics
App builder – can log into app builder service to create apps

DPS creative cloud accounts can only build single edition apps, DPS Free accounts can be used to create content but can not publish to the distribution service.

Do you require secure passwords?

No, the only requirement for an Adobe ID password is that it contains at least 6 characters.

How are forgotten passwords retrieved?

http://helpx.adobe.com/x-productkb/policy-pricing/account-password-sign-faq.html#main-pars_header_1

How can we report security issues to Adobe Systems?

Security related issues can be brought to our attention by calling Adobe technical support.

For more information

Digital Publishing Suite: *http://www.adobe.com/products/digital-publishing-suite-family.html*
DPS Developer Center: *http://www.adobe.com/devnet/digitalpublishingsuite.html*

Adobe
Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com