Adobe Experience Manager Mobile On-demand Services, Security Overview

Table of Contents

Adobe Security

At Adobe, we take the security of your digital experience seriously. From our rigorous integration of security practices into our internal software development process and tools to our cross-functional incident response teams, we strive to be proactive and nimble. What's more, our collaborative work with partners, researchers, and other industry organizations helps us understand the latest security best practices as well as continually incorporate security techniques into the products and services we offer.

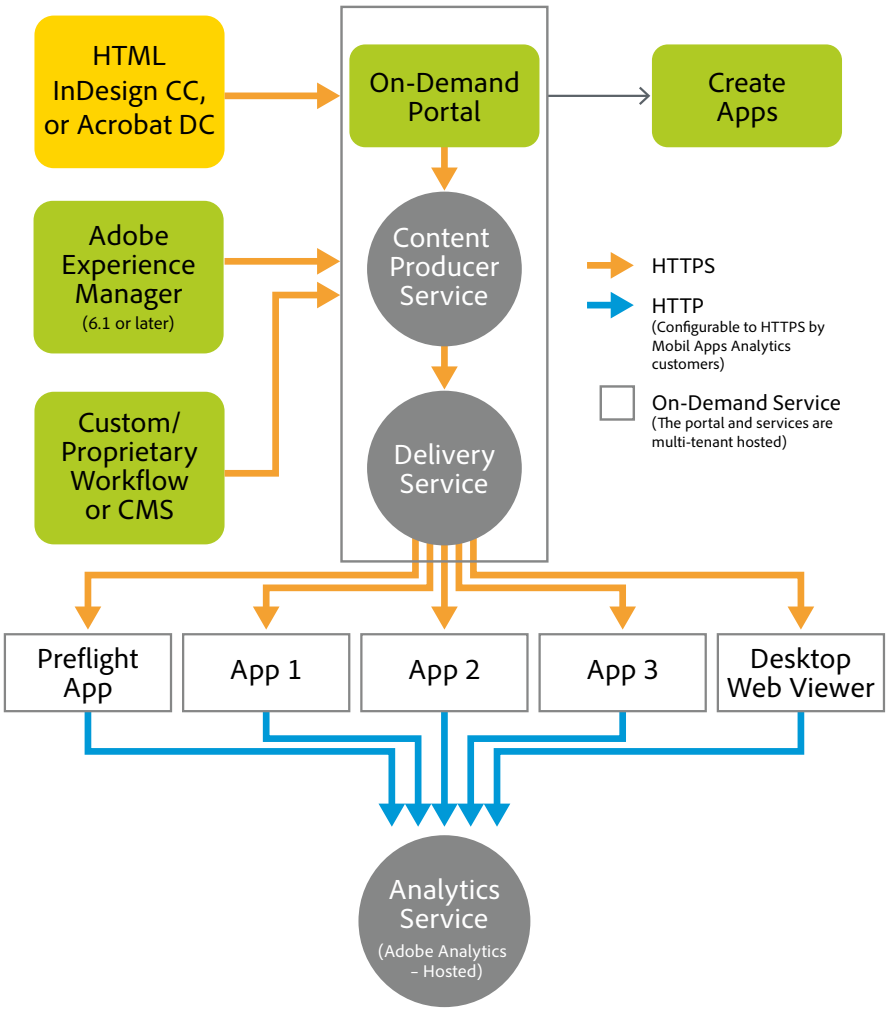
Adobe Experience Manager Mobile combines On-demand Services with On-premise Software or Managed Services. The purpose of this document is to aid customers in understanding Experience Manager Mobile On-demand Services security. The target audience is IT security architects involved in examining vendors and applications for corporate approval.

About Experience Manager Mobile

Experience Manager Mobile is a platform that enables corporations, organizations and higher educational institutions to design, build, market, and measure apps on mobile devices. Experience Manager Mobile integrates with Adobe Creative Cloud software (including InDesign CC and later), Adobe Document Cloud (Acrobat DC), Adobe Experience Manager Assets/Sites and Adobe Marketing Cloud. Experience Manager Mobile enables efficient creation of mobile apps for a variety of enterprise use cases including brand affinity, sales enablement, and marketing communications.

Key Components of Experience Manager Mobile

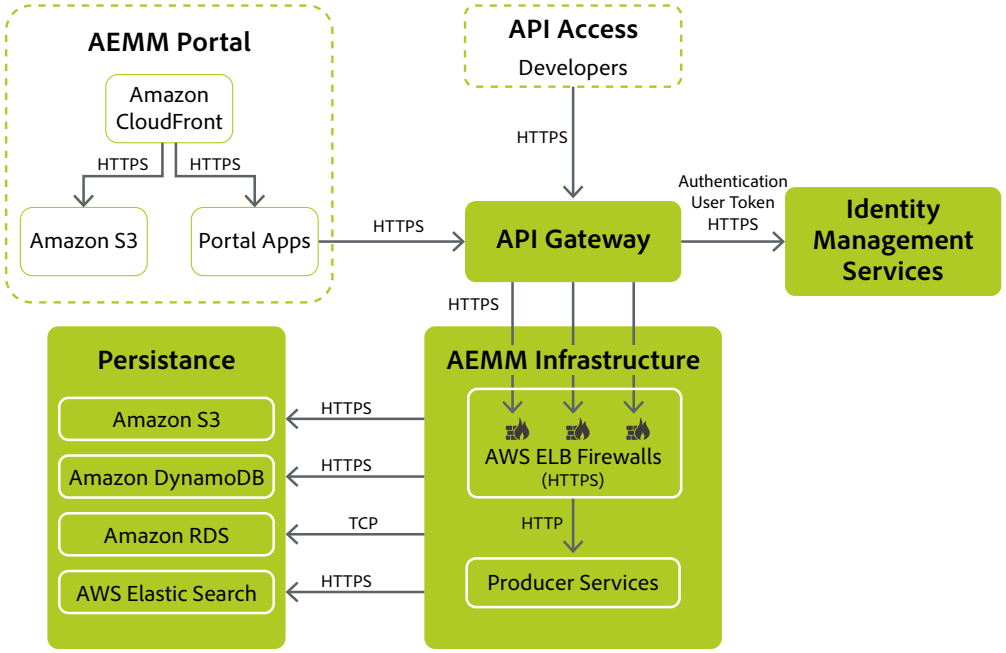
Experience Manager Mobile provides an end-to-end platform for building, managing and monitoring applications. Content can be created in the On-premise Software or Managed Services component of Experience Manager Mobile, Adobe Experience Manager Assets/Sites, Adobe InDesign CC or later, Adobe Document Cloud or a variety of HTML authoring tools including third-party content management systems (CMS) and custom workflows.



Adobe Experience Manager Mobile Components

Adobe Experience Manager: Experience Manager Mobile includes access to Adobe's CMS, which can be deployed either on your own servers via the On-premise Software option, or via the Adobe Managed Services option. Note that you can use Experience Manager Mobile On-demand Services without installing or using the On-premise Software or Managed Services component. In that scenario, you would only be using the multi-tenant hosted On-demand Service (the On-demand Portal, Content Producer Service, Apps, Delivery Service and Analytics Service).

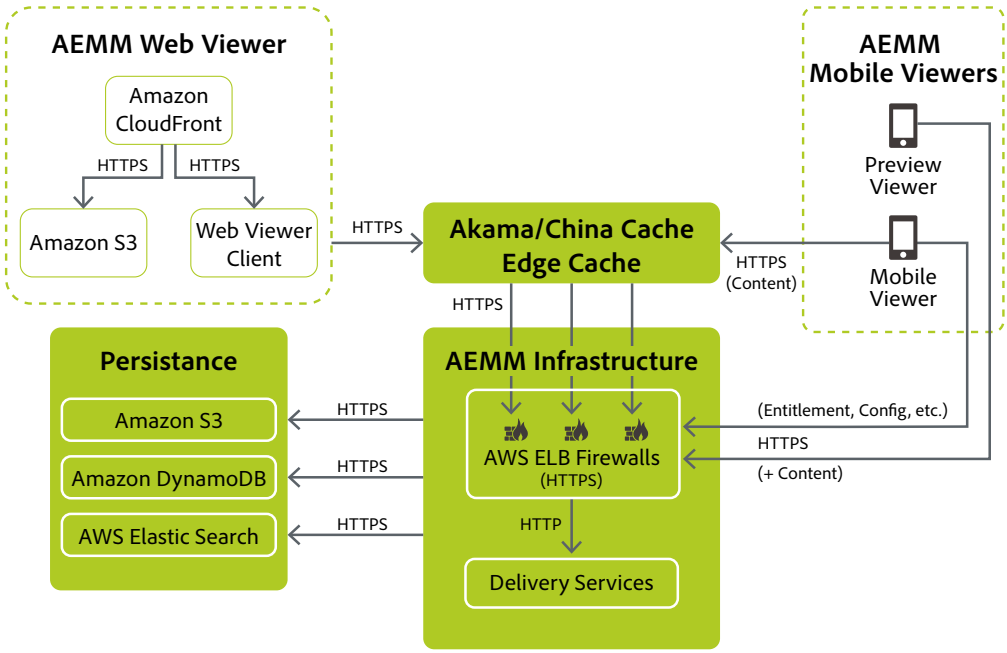
Content Producer Service: In the On-demand Portal, you can manage and publish content through the Content Producer Service. After you upload your HTML content, or content from InDesign, Acrobat, Adobe Experience Manager Sites/Assets, or another CMS or workflow, you can assemble and re-order content, add metadata, and publish content to your apps in the form of a .article file. The Content Producer Service hosts the .article files which support a range of file formats, including PDF, JPEG, and HTML5.



Adobe Experience Manager Mobile Content Producer Service Network Diagram

Apps: The On-demand Service Apps feature creates a native mobile app for iOS, Android, or Windows, and lets you upload your icons and assets to build a branded application for distribution through leading app marketplaces or for private publication within your organization.

Delivery Service: The Delivery Service hosts digital content in .article file format and distributes this content to tablet and smartphone devices, as well as to desktop web browsers. The Delivery Service stores content in a non-encrypted state. When a content consumer downloads content, the content is cached on edge servers owned by a content delivery network (currently Akamai and ChinaCache (for supporting delivering in People's Republic of China, planned for mid-2016) and stored in the same format as in the Delivery Service. The mobile app connects to the Delivery Service over a HTTPS connection ensuring that content is encrypted during download to mobile devices.



Adobe Experience Manager Mobile Delivery Service Network Diagram

Analytics Service: The included Adobe Analytics Essentials for Mobile service enables you to view key application usage metrics, such as installs, crashes, device type, app versions, and readership/engagement metrics. If you have full Adobe Analytics, you can also access more detailed drill-down reports, which can be custom-tailored for your unique business requirements.

On-Demand Portal Project Settings: The On-demand Portal project settings allow administrators to manage configurations and settings for all Experience Manager Mobile On-demand Services projects within their organization. Through a collection of web forms, administrators can define granular user roles & permissions, enable, disable, and configure settings as well as provide details necessary to link with your Adobe Analytics account, if appropriate. For more information about user accounts (Adobe ID's, roles & permissions), see the Account Administration help pages and the "Adobe Experience Manager Mobile Authentication (Adobe ID)" section later in this document.

If You Are Using Adobe Experience Manager Mobile for Content Management

After creating content in an HTML template using the drag-and-drop interface in the On-premise Software or Managed Services component of Experience Manager Mobile or Adobe Experience Manager Assets/Sites, you sync this over an encrypted HTTP connection (HTTPS). Experience Manager Mobile On-demand Services will create articles and collections of articles based on the content and the templates provided and push these for distribution in mobile apps. For more information about the security practices of the On premise Software or Managed Services component of Experience Manager Mobile or Adobe Experience Manager Assets/Site security, please see the documentation for your version of Adobe Experience Manager as well as the Adobe Experience Manager Security Overview white paper.

If You Are Using a Third-Party CMS or Custom Workflow

If you are creating and managing content from a third-party CMS, or if you are using a custom workflow that leverages the Experience Manager Mobile On-demand Services Content Producer Service APIs, your content is synced to Experience Manager Mobile over an encrypted HTTP connection (HTTPS). Experience Manager Mobile On-demand Services will create articles and collections of articles based on this synced content and push these for distribution in mobile apps. Please refer to security documentation for your third-party system for information specific to that system.

If You Are Creating Content with Adobe InDesign CC, Acrobat DC, or an HTML Tool

After creating content using Adobe InDesign CC or later, Acrobat DC, or your favorite HTML authoring tool on your desktop, you transform this content into a .article file, which contains the images, fonts, and the manifest associated with your content in addition to the content itself. You can then upload the article to Experience Manager Mobile On-Demand Services using an encrypted HTTP connection (HTTPS). You can then manage and publish the .article file for distribution to your content consumers.

Experience Manager Mobile Content Flow

To better understand Experience Manager Mobile and product security practices, let's discuss the flow of content from development to distribution.

Step 1: As mentioned above, you use the On-premise Software or Managed Services component of Experience Manager Mobile, Adobe Experience Manager Assets/Sites, your preferred HTML authoring tool, third-party CMS, or custom workflow, Adobe InDesign or Adobe Acrobat to create content. This content file contains the content, images, fonts, and the manifest associated with your content.

If you are using InDesign or your own HTML authoring tools, you load the content through the Content Producer Service. If you are creating content using the On-premise Software or Managed Services component of Experience Manager Mobile or Adobe Experience Manager Assets/Sites, you simply press the 'upload'' button to sync your HTML templates & screen content with Content Producer Service to move to the next step in the workflow.

Step 2: After uploading your content, authorized users (managed by project settings in the On-demand Portal) can then view and test the content on a mobile device using the Experience Manager Mobile Preflight App or a branded preview version of your app built by you in the Experience Manager Mobile Apps tool.

Step 3: When you are ready to publish your content, clicking 'publish' in the Content Producer Service sends the content to the Delivery Service over an HTTPS connection via a content delivery network.

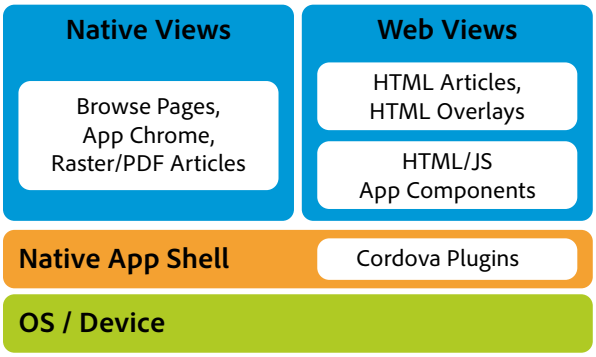
Step 4: If you want to create a custom-branded application to host your content, you can use the Apps tool in the Experience Manager Mobile On-demand Portal. End users can then download the latest content through this app. Experience Manager Mobile creates custom apps for iOS, Android and Windows, and can also deliver your branded app experience to desktop web browsers.

Step 5: If you want to make your content sharable via social networks, such as Facebook and Twitter, you can enable this within the On-demand Portal Project Settings. When enabled, your users can share an article or a portion thereof via a link. That content can also be accessible via the Desktop Web Viewer in a similar format to the mobile device.

Step 6: If you want to delete content, you can do so at any time during the term of your contract. If you cancel your Experience Manager Mobile subscription, published content is unavailable to apps upon contract termination, but content will remain on Experience Manager Mobile servers for at least 30 days after the cancellation date. After 30 days, Adobe reserves the right to remove content from its servers on an as-needed basis. Upon formal request, Adobe will irrevocably remove deleted content from your active or terminated account.

App Extensibility in Experience Manager Mobile

Apps produced by Experience Manager Mobile can be extended through use of JavaScript, delivered as "screens", that accesses a set of plugins provided as part of the application shell. These plugins are configured to access certain device capabilities on the underlying mobile device running the app. Use of the plugin by a specific screen is configured through the IsTrustedContent setting available as a setting on an individual screen. By default, IsTrustedContent is set to 'false'. This default value prevents screens from accessing the underlying device. Users that want to extend their Experience Manager Mobile apps to access local file storage, device capabilities like GPS and Camera need to set the value to 'true'.



Experience Manager Mobile App Extensibility Architecture

Entitlements & Restricted Collections in Experience Manager Mobile

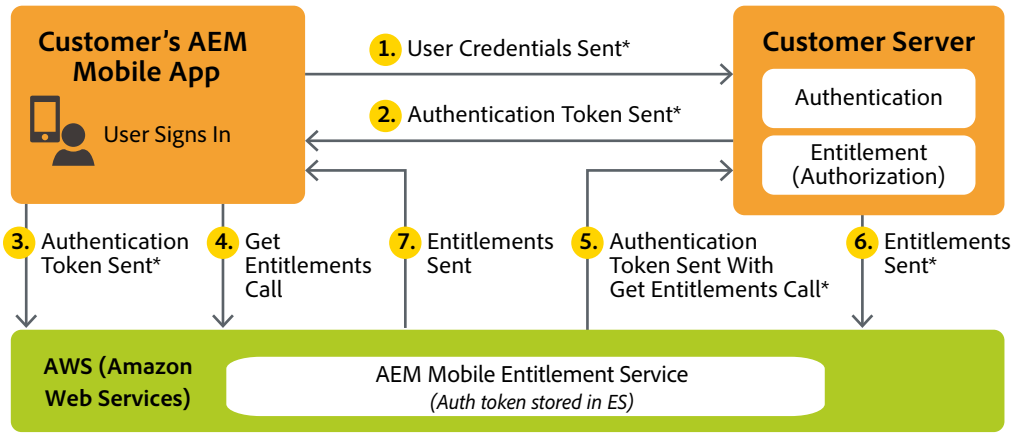
Within an Experience Manager Mobile native app and web viewer, access to content items can be controlled via entitlements. Each screen can have its own setting that determines if it is freely accessible or requires that the user is entitled to it. Even without entitlement, the mere existence of the item is not hidden in navigation screens. This allows publishers of magazine-type apps to entice users to purchase content via an app store.

To hide the existence of content based on user entitlements or roles (as you may wish to do for a typical enterprise app) Restricted Collections can be used. For example, if you are a pharmaceutical company, you may wish to show physicians certain content, while salespeople can only view a subset of that content or entirely different content.

In order to enable Restricted Collections, you must configure your own server that determines which users are authorized to view which content. Your service acts as a policy manager to directly entitle your users, and helps you to restrict confidential or sensitive content based on user credentials or roles. Restricted Collection references are not visible on app navigation screens unless the user is authenticated and entitled to the content. For more information on Restricted Collections, see the help article Set Up Restricted Collections.

Direct Entitlement

Direct entitlement is a method for you to determine which content your users have access to. Direct entitlement can be used to offer different content to different users signed-in to an Experience Manager Mobile app (a user sign-in screen is built-in to Experience Manager Mobile apps that use it). Setting up direct entitlement requires a third-party service or your own server. This service implements the Adobe Experience Manager Mobile Direct Entitlement API.



Calls between the app and the Entitlement Service always use HTTPS.

* The customer is in control of whether the URL is HTTP or HTTPS. The customer specifies the URL to call for Authentication when they define their Entitlement Service. It is strongly recommended that the customer specifies an HTTPS URL. If HTTPS is specified, calls between AEM Mobile and the customer's servers will use HTTPS.

Direct Entitlement Service Calls

When using direct entitlement, the user's credentials (user name and password) are sent from the Experience Manager Mobile app to the customer's servers and the customer's servers send an auth token back to the app. That auth token is then sent to the Experience Manager Mobile Entitlement Service hosted on Amazon AWS servers. For native apps, credentials are not sent to the Entitlement Service/AWS — only the auth token. When using the web viewer, credentials are passed through the entitlement service (via HTTPS), but not stored by the service.

That auth token is then used when the Experience Manager Mobile Entitlement Service checks if a user is entitled to download a particular content item. A 'get entitlements' call to the customer's direct entitlement service is made to check list of content items that the user wants to access. The call between the app and the customer's servers to send the user's credentials is based on the URL provided when the customer sets up & defines their entitlement service. It is recommended that customers specify an HTTPS URL and, if so, the call is made using HTTPS. Calls between the viewer and the Adobe Entitlement Services on AWS to send the auth token are always made using HTTPS.

For more information, see the Set Up Direct Entitlement article in Experience Manager Mobile help.

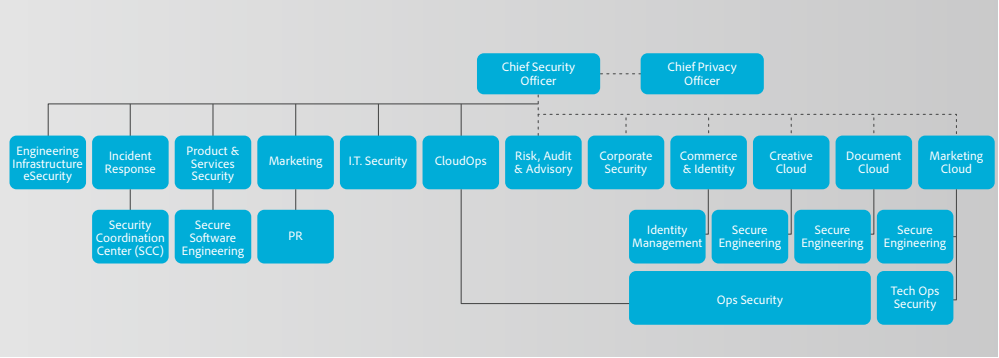
Experience Manager Mobile Storage and Storage Options

Content uploaded to the Content Producer Service is stored in the cloud on Amazon S3 (Amazon Simple Storage Service), a data storage infrastructure for storing and retrieving any amount of data. The On-demand Services portion of Experience Manager Mobile is a multi-tenant hosted solution built on top of Amazon Web Services (AWS). As an Experience Manager Mobile customer, you retain control and ownership of your data at all times. Please see Adobe's Terms of Use and Privacy Policy for more information. The Content Producer Service links all stored content to a master account and virtually separates content in storage using that account. The content is not stored in a format that can be accessed by any other Adobe service other than the Content Producer Service. Upon publishing content, it is stored in a format and location accessible to the Delivery Service. All connections from the app and the web viewer to the Delivery Service are over HTTPS so content is encrypted during transfer. Individual assets are URI accessible over HTTPS and not encrypted at rest on the Delivery Service.

The Adobe Security Organization

As part of our commitment to the security of our products and services, Adobe coordinates all security efforts under the Chief Security Officer (CSO). The office of the CSO coordinates all product and service security initiatives and the implementation of the Adobe Secure Product Lifecycle (SPLC).

The CSO also manages the Adobe Secure Software Engineering Team (ASSET), a dedicated, central team of security specialists who serve as consultants to key Adobe product and operations teams, including Adobe Experience Manager Mobile. ASSET researchers work with individual Adobe product and operations teams to strive to achieve the right level of security for products and services and advise these teams on security practices for clear and repeatable processes for development, deployment, operations, and incident response.



Adobe Security Organization

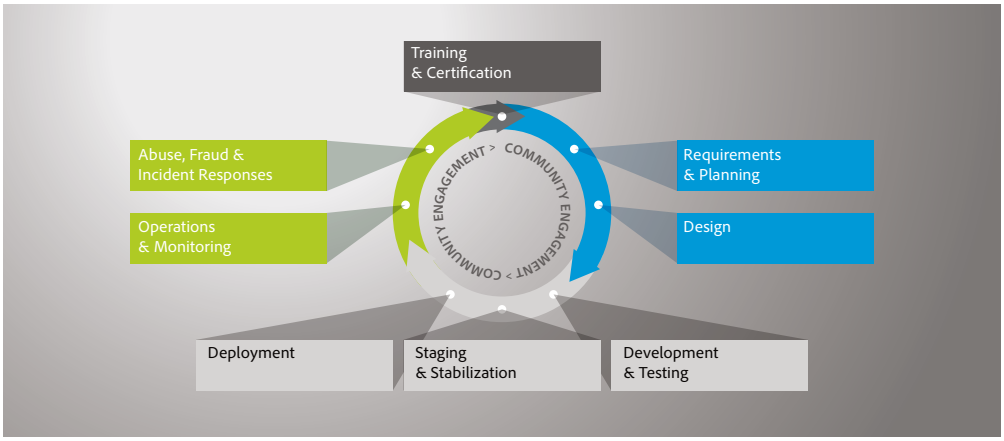
Adobe Secure Product Development

As with other key Adobe product and service organizations, the Experience Manager Mobile organization employs the Adobe Software Product Lifecycle process. A rigorous set of several hundred specific security activities spanning software development practices, processes, and tools, the Adobe SPLC is integrated into multiple stages of the product lifecycle, from design and development to quality assurance, testing, and deployment. ASSET security researchers provide specific SPLC guidance for each key product or service based on an assessment of potential security issues. Complemented by continuous community engagement, the Adobe SPLC evolves to stay current as changes occur in technology, security practices, and the threat landscape.

Adobe Secure Product Lifecycle

The Adobe SPLC controls include, depending on the specific Experience Manager Mobile component, some or all of the following recommended best practices, processes, and tools:

- Security training and certification for product teams
- Product health, risk, and threat landscape analysis
- Secure coding guidelines, rules, and analysis
- Service roadmaps, security tools, and testing methods that guide the Adobe Experience Manager Mobile security team to help address the Open Web Application Security Project (OWASP) Top 10 most critical web application security flaws and CWE/SANS Top 25 most dangerous software errors
- Security architecture review and penetration testing
- Source code reviews to help eliminate known flaws that could lead to vulnerabilities
- User-generated content validation
- Static and dynamic code analysis
- Application and network scanning
- Full readiness review, response plans, and release of developer education materials



Adobe Secure Product Lifecycle (SPLC)

Adobe Security Training

Adobe Software Security Certification Program

As part of the Adobe SPLC, Adobe conducts ongoing security training within development teams to enhance security knowledge throughout the company and improve the overall security of our products and services. Employees participating in the Adobe Software Security Certification Program attain different certification levels by completing security projects.

The program has four levels, each designated by a colored 'belt': white, green, brown, and black. The white and green levels are achieved by completing computer-based training. The higher brown and black belt levels require completion of months- or year-long hands-on security projects.

Employees attaining brown and black belts become security champions and experts within their product teams. Adobe updates training on a regular basis to reflect new threats and mitigations, as well as new controls and software languages.

Various teams within the Experience Manager Mobile organization participate in additional security training and workshops to increase awareness of how security affects their specific roles within the organization and the company as a whole.

Adobe Common Controls Framework

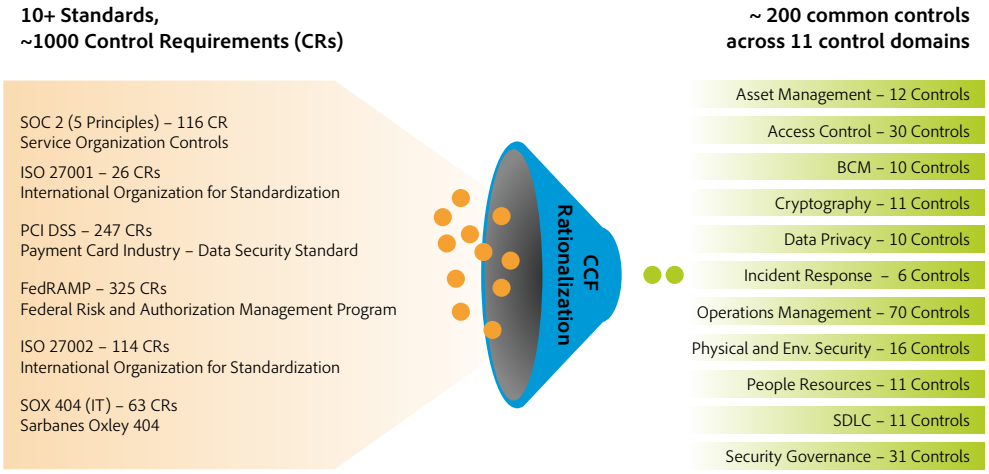
To protect from the software layer down, Adobe uses the Adobe Secure Product Lifecycle, which is described in the following section. To protect from the physical layer up, Adobe implements a foundational framework of security processes and controls to protect the company's infrastructure, applications, and services and help Adobe comply with a number of industry accepted best practices, standards, and certifications.

In creating the Adobe Common Controls Framework (CCF), Adobe analyzed the criteria for the most common security certifications and found a number of overlaps. After analyzing more than 1000 requirements from relevant cloud security frameworks and standards, Adobe rationalized these down to approximately 200 Adobe-specific controls. The CCF control owners know exactly what is required to address the expectations of Adobe stakeholders and customers when it comes to implementing controls.

Amazon Web Services (AWS) also maintains its own compliance and assertions with an ISO27001, SOC2, and other industry Security Frameworks.

All Adobe services are governed by a comprehensive set of documented security processes and have been subject to numerous security audits to maintain and improve quality.

Adobe is in the process of developing, implementing, and refining the security processes and controls for operations in order to comply with the requirements for SOC 2 Trust Services Principles and the ISO 27001 security standard. Please visit the Adobe Security resources portal to view a list of security white papers including the Adobe Security and Privacy Certifications white paper for more information on compliance Adobe's overall compliance strategy.



Adobe Experience Manager Mobile Hosting

Components of Experience Manager Mobile On-demand Services are hosted on Amazon Web Services (AWS), including Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Simple Storage Service (Amazon S3), in the United States. Amazon EC2 is a web service that provides resizable compute capacity in the cloud, making web-scale computing easier. Amazon S3 is a highly redundant data storage infrastructure for storing and retrieving any amount of data, at any time, from anywhere.

The AWS platform provides services in accordance with industry-standard practices and undergoes regular industry-recognized certifications and audits. You can find more detailed information about AWS and Amazon's security controls on the AWS security site.

Operational Responsibilities of AWS and Adobe

AWS operates, manages, and controls the components from the hypervisor virtualization layer down to the physical security of the facilities in which Experience Manager Mobile On-demand Services components operate. In turn, Adobe assumes responsibility and management of the guest operating system (including updates and security patches) and application software, as well as the configuration of the AWS-provided security group firewall.

AWS also operates the cloud infrastructure used by Adobe to provision a variety of basic computing resources, including processing and storage. The AWS infrastructure includes facilities, network, and hardware, as well as operational software (e.g., host OS, virtualization software, etc.) that supports the provisioning and use of these resources. Amazon designs and manages AWS according to industry- standard practices as well as a variety of security compliance standards.

Secure Management

Adobe uses Secure Shell (SSH) and Transport Layer Security (TLS) for management connections to manage the AWS infrastructure.

About Amazon Web Services (AWS)

Geographic Location of Customer Data on AWS Network

The following information is from the AWS: Overview of Security Processes White paper. For more detailed information about AWS security, please consult the AWS white paper.

Adobe stores all Experience Manager Mobile On-demand Services customer data in Amazon Web Services' US East Region. For customers within the United States, Adobe stores analytic data in San Jose, California or Dallas, Texas facilities. For customers outside the U.S., Adobe stores analytic data in the London, U.K. facility of Amazon Web Services.

Data replication for Amazon S3, DynamoDB and RDS data objects occurs within the regional cluster where the data is stored and is not replicated to data center clusters in other regions.

Isolation of Customer Data/Segregation of Customers

AWS uses strong tenant isolation security and control capabilities. As a virtualized, multi-tenant environment, AWS implements security management processes and other security controls designed to isolate each customer, such as Experience Manager Mobile, from other AWS customers. Adobe uses the AWS Identity and Access Management (IAM) to further restrict access to compute and storage instances.

Secure Network Architecture

AWS employs network devices, including firewall and other boundary devices, to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services. ACLs, or traffic flow policies, exist on each managed interface to manage and enforce the flow of traffic.

Amazon Information Security approves all ACL policies and automatically pushes them to each managed interface using AWS's ACL-Manage tool, helping to ensure these managed interfaces enforce the most up-to-date ACLs.

Network Monitoring and Protection

AWS uses a variety of automated monitoring systems to provide a high level of service performance and availability. Monitoring tools help detect unusual or unauthorized activities and conditions at ingress and egress communication points.

The AWS network provides significant protection against traditional network security issues:

- Distributed Denial Of Service (DDoS) Attacks
- Man in the Middle (MITM) Attacks
- IP Spoofing
- Port Scanning
- Packet sniffing by other tenants

You can find more information about Network Monitoring and Protection in the AWS: Overview of Security Processes white paper on the Amazon website.

Intrusion Detection

Adobe actively monitors all of the Adobe Experience Manager Mobile On-demand Services components using industry- standard intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).

Logging

Adobe conducts server-side logging of Experience Manager Mobile On-demand Services customer activity to diagnose service outages, specific customer problems, and reported bugs. The logs only store Adobe IDs to help diagnose specific customer issues and do not contain username/password combinations. Only authorized Adobe technical support personnel, key engineers, and select developers can access the logs to diagnose specific issues that may arise.

Service Monitoring

AWS monitors electrical, mechanical, and life support systems and equipment to help with the immediate identification of service issues. In order to maintain the continued operability of equipment, AWS performs ongoing preventative maintenance.

Data Storage and Backup

Adobe stores all Experience Manager Mobile On-demand Services data in Amazon S3, which provides a storage infrastructure with high durability. To help provide durability, Amazon S3 PUT and COPY operations synchronously store customer data across multiple facilities and redundantly store objects on multiple devices across multiple facilities in an Amazon S3 region. In addition, Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data. For more detailed information about AWS security, please consult the AWS: Overview of Security Processes white paper.

Change Management

AWS authorizes, logs, tests, approves, and documents routine, emergency, and configuration changes to existing AWS infrastructure in accordance with industry norms for similar systems. Amazon schedules updates to AWS to minimize any customer impact. AWS communicates with Adobe, either via email, or through the AWS Service Health Dashboard when service use is likely to be adversely affected.

Patch Management

AWS maintains responsibility for patching systems that support the delivery of AWS services, such as the hypervisor and networking services. Adobe is responsible for patching its guest operating systems (OS), software, and applications running in AWS. When patches are required, Adobe supplies a new, pre- hardened instance of the OS and application rather than an actual patch.

Adobe Experience Manager Mobile Authentication (Adobe ID)

After receiving an invitation to join the team from their administrator, users must create an Adobe ID, which is used each time they access Experience Manager Mobile On-demand Services. Adobe ID leverages the SHA 256 hash algorithm in combination with password salts and a large number of hash iterations. Adobe continually monitors Adobe ID accounts for unusual or anomalous account activity and evaluates this information to help quickly mitigate threats to the security of your Adobe ID account.

Certificate and Key Storage

Experience Manager Mobile Apps tool requests users to provide their digital certificates and provisioning profiles in order to sign their apps. All certificates reside locally on the signing machine and do not transfer to Adobe (or AWS) during 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 who choose to use the Adobe push notification service for iOS must upload their push certificates to an Adobe server. Adobe follows Apple's guidance on third-party management of push certificates.

Adobe Risk & Vulnerability Management

Security Testing

Adobe engages with approved third-party security companies to perform penetration testing to help us discover potential security vulnerabilities and improve the overall security of Adobe products and services. Upon receipt of our vendor's report, Adobe documents discovered vulnerabilities, evaluates severity and priority, and then creates an appropriate mitigation strategy or remediation plan.

Adobe performs a security scan of Experience Manager Mobile On-demand Services prior to every release. Conducted by highly trained operations staff trusted with creating a secure network topology and infrastructure not only for Experience Manager Mobile but also for all Adobe hosted products and services, this security scan looks for insecure network setup issues across firewalls, load balancers, and server hardware. Copies of the security scan are available under NDA upon request.

Customers may run their own external security scan of the externally facing infrastructure for Experience Manager Mobile On-demand Services by contacting Adobe Tech Support. However, they may NOT perform penetration or load testing on externally facing Experience Manager Mobile On-demand Services systems. Customers attempting to do so are in violation of the Experience Manager Mobile terms of use and Adobe reserves the right to terminate the contact or suspend service.

Incident Response and Notification

As new vulnerabilities and threats evolve, Adobe strives to respond and mitigate newly discovered threats. In addition to subscribing to industry-wide vulnerability announcement lists, including US-CERT, Bugtraq, and SANS, Adobe also subscribes to the latest security alert lists issued by major security vendors.

When a significant vulnerability is announced, the Adobe PSIRT (Product Security Incident Response Team) communicates the vulnerability to the appropriate teams within the Experience Manager Mobile organization to coordinate the mitigation effort.

For incidents, vulnerabilities, and threats that impact the AWS Data Center, the Amazon Incident Management team employs industry-standard diagnostic procedures to drive resolution during business- impacting events. Staff operators provide 24x7x365 coverage to detect incidents, manage the impact and resolution, and inform Adobe and other AWS customers.

For Experience Manager Mobile, we also centralize incident response, decision-making, and external monitoring in our Security Coordination Center (SCC), providing cross-functional consistency and fast resolution of issues.

When an incident occurs, the SCC works with the Experience Manager Mobile incident response and development teams to help identify, mitigate, and resolve the issue using the following proven process:

- Assess the status of the vulnerability
- Mitigate risk in production services
- Quarantine, investigate, and destroy compromised nodes (cloud-based services only)
- Develop a fix for the vulnerability
- Deploy the fix to contain the problem
- Monitor activity and confirm resolution

Forensic Analysis

For incident investigations, Adobe uses industry-standard tools and methodologies. The company adheres to a forensic analysis process that includes complete image capture or memory dump of an impacted machine(s), evidence safe-holding, and chain-of-custody recording. Adobe may engage with law enforcement or third-party forensic companies when it determines it is necessary.

AWS Data Center Physical and Environmental Controls

AWS physical and environmental controls are specifically outlined in a SOC 1, Type 2 report. The following section outlines some of the security measures and controls in place at AWS data centers around the world. For more detailed information about AWS security, please consult the AWS: Overview of Security Processes white paper or the Amazon security website.

Physical Facility Security

AWS data centers utilize industry standard architectural and engineering approaches. AWS data centers are housed in nondescript facilities and Amazon controls physical access both at the perimeter and at building ingress points using professional security staff, video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

Fire Suppression

AWS installs automatic fire detection and suppression equipment in all AWS data centers. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Controlled Environment

AWS employs a climate control system to maintain a constant operating temperature for servers and other hardware, preventing overheating and reducing the possibility of service outages. AWS data centers maintain atmospheric conditions at optimal levels. AWS personnel and systems monitor and control both temperature and humidity at appropriate levels.

Backup Power

AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

Video Surveillance

Professional security staff strictly controls physical access both at the perimeter and at building ingress points for AWS Data Centers using video surveillance, intrusion detection systems, and other electronic means.

Disaster Recovery

AWS data centers include a high level of availability and tolerate system or hardware failures with minimal impact. Built in clusters in various global regions, all data centers remain online 24/7/365 to serve customers; no data center is "cold." In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites. You can find more information about AWS disaster recovery protocols on the Amazon Security website.

Adobe Corporate Locations

Adobe maintains offices around the world and implements the following processes and procedures company-wide to protect the company against security threats:

Physical Security

Every Adobe corporate office location employs on-site guards to protect the premises 24x7. Adobe employees carry a key card ID badge for building access. Visitors enter through the front entrance, sign in and out with the receptionist, display a temporary Visitor ID badge, and are accompanied by an employee at all times. Adobe keeps all server equipment, development machines, phone systems, file and mail servers, and other sensitive systems locked at all times in environment-controlled server rooms accessible only by appropriate, authorized staff members.

Virus Protection

Adobe scans all content submitted to the Content Producer Service for viruses before storing it on Adobe systems.

Adobe Employees

Employee Access to Customer Data

Adobe maintains segmented development and production environments for Experience Manager Mobile On-demand Services, using technical controls to limit network and application-level access to live production systems. Employees have specific authorizations to access development and production systems.

Background Checks

Adobe obtains background check reports for employment purposes. The specific nature and scope of the report that Adobe typically seeks includes inquiries regarding educational background; work history; court records, including criminal conviction records; and references obtained from professional and personal associates, each as permitted by applicable law. These background check requirements apply to regular U.S. new hire employees, including those who will be administering systems or have access to customer information. New U.S. temporary agency workers are subject to background check requirements through the applicable temporary agency, in compliance with Adobe's background screen guidelines. Outside the U.S., Adobe conducts background checks on certain new employees in accordance with Adobe's background check policy and applicable local laws.

Employee Termination

When an employee leaves Adobe, the employee's manager submits an exiting worker form.

Once approved, Adobe People Resources initiates an email workflow to inform relevant stakeholders to take specific actions leading up to the employee's last day. In the event that Adobe terminates an employee, Adobe People Resources sends a similar email notification to relevant stakeholders, including the specific date and time of the employment termination.

Adobe Corporate Security then schedules the following actions to help ensure that, upon conclusion of the employee's final day of employment, he or she can longer access to Adobe confidential files or offices:

- Email Access Removal
- Remote VPN Access Removal
- Office and Datacenter Badge Invalidation
- Network Access Termination

Upon request, managers may ask building security to escort the terminated employee from the Adobe office or building.

Customer Data Confidentiality

Adobe treats customer data as confidential. Adobe does not use or share the information collected on behalf of a customer except as may be allowed in a contract with that customer and as set forth in the Adobe Terms of Use and the Adobe Privacy Policy.

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of your Experience Manager Mobile On-demand Services data. At Adobe, we take the security of your digital experience seriously.

Please visit Adobe's security information site for more information about security efforts across our products and services.

Adobe

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