Adobe® Identity Management Services Security Overview

Table of Contents

Adobe Security

At Adobe, we take the security of your digital experience seriously. Security practices are ingrained into our internal software development and operations processes and tools, and the Adobe Secure Product LifeCyle (SPLC) controls are implemented by our cross-functional teams to help prevent, detect, and respond to incidents in an expedient manner. Furthermore, our collaborative work with partners, leading researchers, security research institutions, and other industry organizations helps us keep up to date with the latest threats and vulnerabilities and we work to incorporate advanced security technologies and practices into the products and services we offer.

This white paper describes the defense-in-depth approach and security procedures implemented by Adobe to help bolster the security of your Adobe® Identity Management Services experience and your data.

Adobe Identity Management Services

Adobe Identity Management Services (IMS) sits between your enterprise end-users and your Adobe solution/s, handling all user authentication for any Adobe solution.

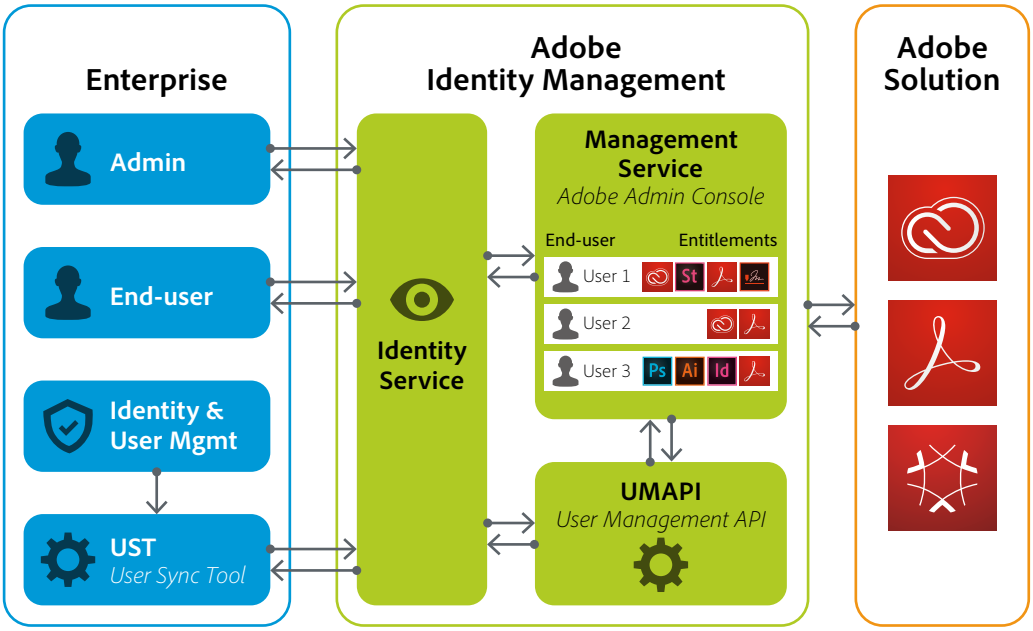


Figure 1: Adobe Identity Management Services

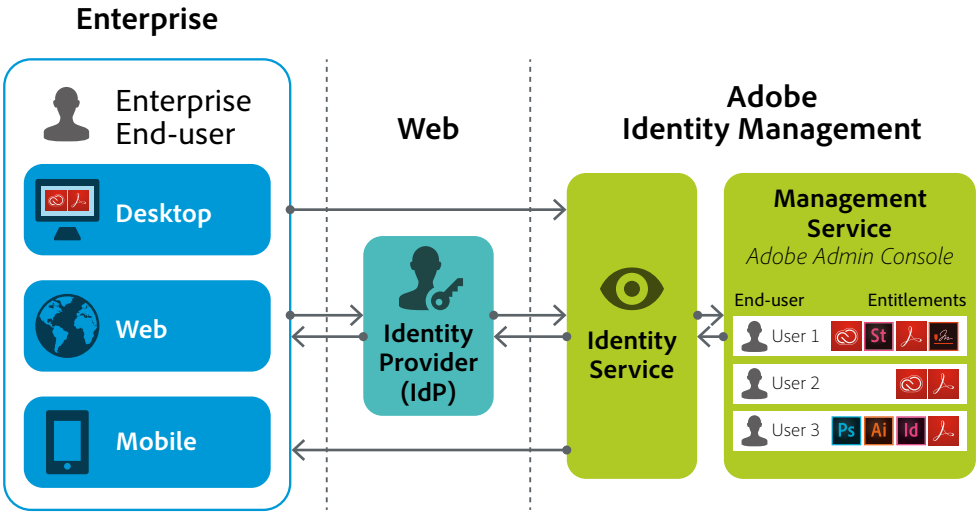
Adobe IMS consists of three components:

- **Adobe Identity Service:** Handles authentication and validation of the end-user, including federation and runtime Single-Sign-On (SSO);
- **Adobe Admin Console:** Provides a central location for managing Adobe entitlements across your entire organization. It handles user management, cloud service and desktop license entitlement, federation configuration, and data loss prevention security features.
- **Adobe User Management API (UMAPI):** Manages enterprise users and entitlements in the Adobe Admin Console at the API level.

In addition, Adobe IMS includes the Adobe **User Sync Tool (UST)**, a set of Python scripts that you install on a server inside your network. The UST moves user and group information via the UMAPI from your organization's enterprise directory system (such as Microsoft Active Directory or other LDAP system) to your organization's directory in the Adobe Admin Console.

Named User Licensing

In 2012 Adobe moved from a serialized license model to a subscription-based **Named User Licensing** model, in which every user of Adobe desktop software would be identified by a unique identifier. The license code is no longer embedded in the desktop software for perpetual use. Rather, it is a part of a subscription model where the desktop applications periodically reach out to the Adobe servers to validate that the application is entitled to the end-user. These entitlements and unique identifiers are managed by the Adobe Identity Management Services platform which allows those end users to authenticate to their deployed desktop software and to Adobe cloud services.



In the diagram above, you can see the interaction of the end-user with the Adobe Identity Management system through Named User Licensing. The end-user has the Adobe applications installed locally on their desktop (as has been the case for the past 35 years), or their mobile devices.

When an end-user attempts to activate or launch their software, use one of the mobile applications, or access one of the cloud services, that endpoint reaches out to the Adobe IMS. It talks to the Adobe Identity service which, depending on the Named User Identity Type, either allows the end-user to log in directly, or it passes control to the customer's Identity Provider (IdP), which performs a Federated Single Sign On authentication. On successful authentication, end-user's entitlements are verified and their requested action is completed.

The named end-user is now allowed to use the software or services to which they are entitled.

User Identity Types

Adobe User Licensing supports three identity types:

Adobe ID is for Adobe-hosted, user-managed accounts. These accounts are designed for individuals and are created, owned, and controlled by the individual users. Adobe IDs are governed by the General Terms of Use which states that the individual retains all ownership and rights to their content. Adobe ID accounts only have access to enterprise resources if an IT administrator enables access through the Admin Console.

Enterprise ID is an Adobe-hosted, enterprise-managed option for accounts that are created and controlled by IT administrators from the enterprise organization. The organization owns and manages the user accounts and all associated assets. User accounts are managed through the Adobe Admin Console and/or the UMAPI.

Federated ID is an enterprise-managed account where all identity profiles are provided via Single Sign-On identity management systems and are created, owned, and controlled by the enterprise IT organization. Adobe will integrate with most any SAML 2.0 compliant identity provider (IdP). User accounts are authenticated through the identity provider and authorized via the Adobe Admin Console.

Most enterprise organizations use Enterprise or Federated IDs for their employees, contractors, and freelancers, provided their email is within the companies' claimed domains. Adobe IDs may be used if the end-user email is not within a company domain.

User Identity Management

You can manage user identities in your enterprise either manually, or automatically.

Manual user management

- **Individually** via the Adobe Admin Console where an administrator can add, delete or change users one at a time within the interface
- **In bulk** where an administrator can upload a CSV spreadsheet of users into the Admin Console

Automated user management

- With the **UMAPI** to programmatically add, update or remove users using code that you develop
- With the **User Sync Tool (UST)** to sync specific users from your enterprise directory and then add/remove the users to the appropriate license pools in the Adobe Admin Console using code that Adobe has developed. Adobe Help & Support pages provide more details about the UMAPI and the User Sync tool.

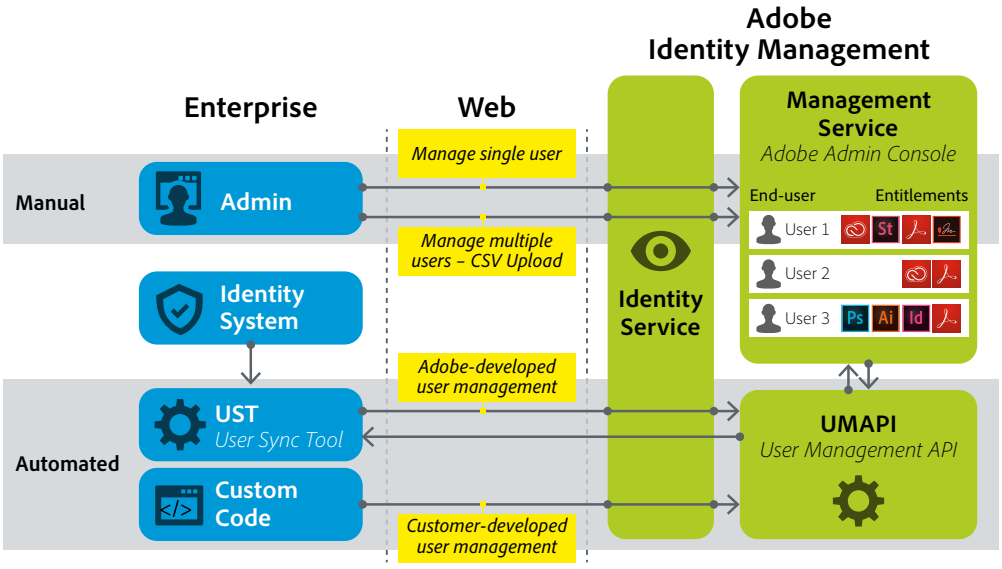


Figure 3: User Identity Management

User Sync Tool

The User Sync Tool is a set of Python scripts developed and maintained by Adobe. The UST reads user identity data from LDAP groups in the customer identity system, such as Microsoft Active Directory, and makes secure REST calls to the UMAPI (User Management API) to create, update or delete users on the Adobe servers.

Each time you run the UST, it:

1. **Requests employee records** from groups within your directory. The groups and LDAP query can be customized to fit your environment;
2. **Requests current users and associated product configurations** from the Adobe Admin Console. The UST connects to the UMAPI via REST calls over HTTPS utilizing a verified, time-boxed access token which is generated from a signed, encoded JWT (JSON Web Token);
   - **Determines which users need to be created, deleted, or updated** based on rules you have defined in the configuration files; and then
3. **Makes the required changes** to the Adobe Admin Console through the UMAPI, entitling users to the appropriate software and services.

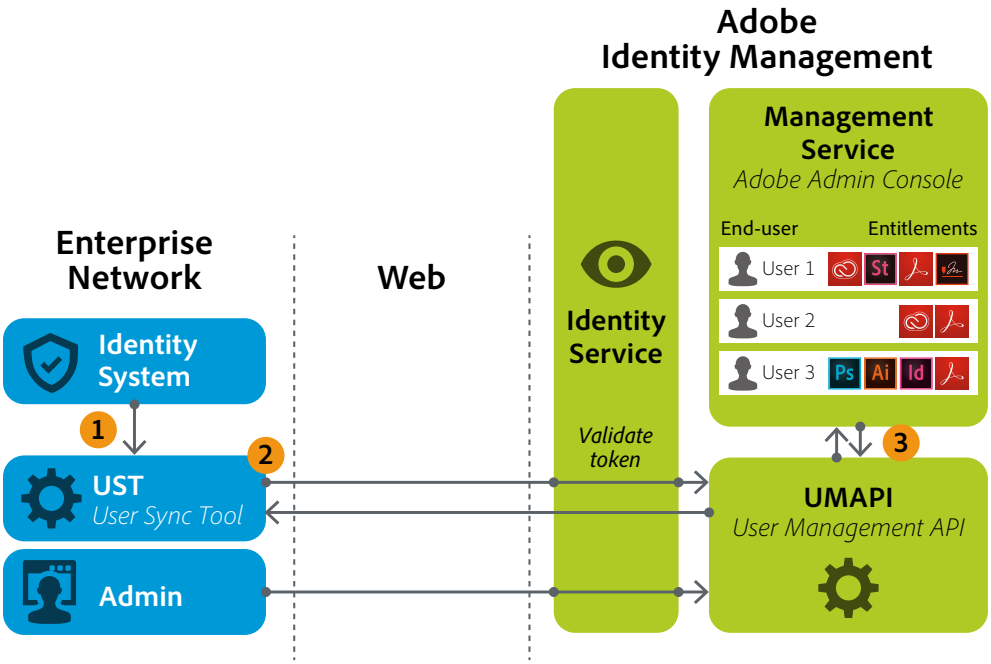


Figure 4: User Sync Tool

The UST can automatically keep your enterprise users's Adobe entitlements in sync with their groupings in your Identity System. For example, if you add a user to your LDAP directory, the next time the UST runs, it pulls that user's information and adds them to the appropriate group within the Adobe Admin Console via the UMAPI. If you change or remove a user from your LDAP directory, the UST will call the UMAPI and perform the appropriate action in Adobe Admin Console.

For detailed instructions about how to install, register, and run the UST, please see the Adobe product support website.

User Authentication and Authorization Data Flow

Adobe enables user authentication and authorization in two ways:

- **Interactive** authentication and authorization occurs when a user explicitly signs into an Adobe desktop application or an Adobe cloud service and enters his/her information into a dialog box. In this case, authorization occurs seamlessly and, to the end-user, appears to be part of the authentication process.
- **Automated** authentication and authorization occurs after an end-user has been authenticated using interactive authentication. Automated authentication utilizes a unique identification token so that the end-user does not have to log in again, and authorization occurs seamlessly as well. Any time an end-user interacts with an application or service and is not required to explicitly log in, that end-user is taking advantage of automated authentication. Authorizations are, however, re-checked with each interaction to verify access rights.

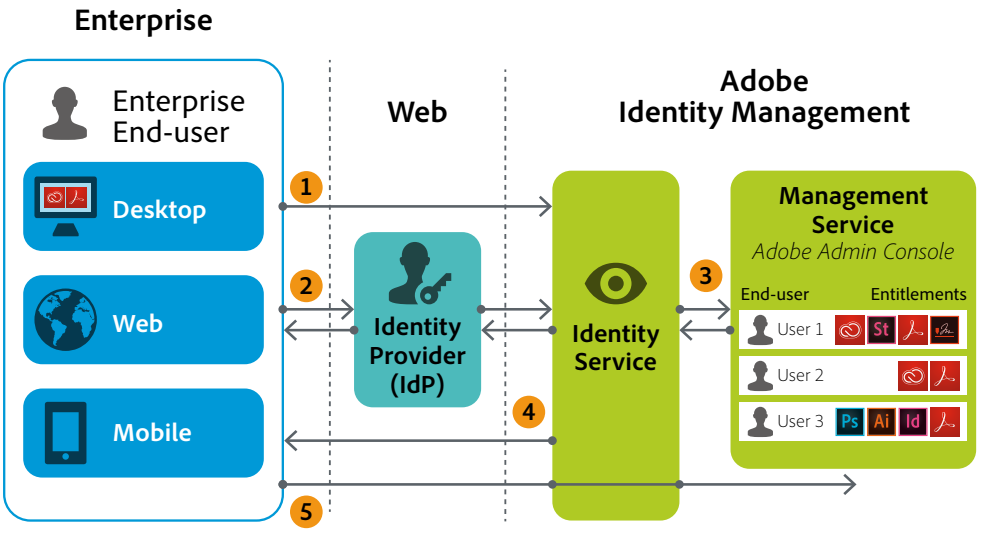


Figure 5: User Authentication Data Flow

The data flow of user authentication depends on which User Identity Type (see above) the end user is attempting to authenticate with. The authentication process essentially follows the diagram above with the following steps:

1. An end-user in your organization launches a desktop application or requests access to an Adobe cloud service for the first time. If they are using an Adobe ID or Enterprise ID, they log in directly with the Identity Service.
2. If a user inputs his/her email address or just the domain (e.g., @companydomain) of his/her email in the username field and the organization uses Federated ID, then the Identity Service initiates a SAML Request which redirects the end-user to their Identity Provider (IdP), and the end-user logs in using their corporate credentials.
3. Once the user is properly authenticated, Adobe IMS then conducts the required entitlement and policy enforcement checks and redirects the user to the appropriate Adobe cloud service or enables appropriate desktop application licensing.
4. Adobe IMS stores a DeviceToken on the end-user's computer. IMS uses the DeviceToken to generate an Access Token, which is like an application session token, and uses both of these to generate a signed license for the application, which is stored, with the DeviceToken, in an encrypted state in the end-user's per-user settings. The token is not affected by operating system logout or login. This means that if the user reboots their system, they can launch a desktop application or use a cloud service without manual re-authentication.

For more information:

- Single Sign-On / Common questions
- Set up identity
- Configure Microsoft AD FS for use with Adobe SSO
- Manage Users
- Administrative roles
- View Federated ID event logs

5. The end-user can now interact with any Adobe desktop application or cloud service without manually re-authenticating him/herself (e.g., the user can concurrently use Dreamweaver and Photoshop without logging into each application separately). This is **automated authentication**. When a desktop application is launched, it contacts the Identity Service and exchanges DeviceID and a DeviceToken with for an AccessToken. Policy checks and entitlement confirmations occur during this process.

If a user's access rights or entitlements are changed or revoked, AccessTokens and DeviceTokens become invalid.

Identity Data

What data do we collect and why?

Adobe collects identity data ensuring each end-user has a unique ID. This enables Adobe to verify end- users for license entitlement purposes and allows for password protection of those entitlements, and the User Generated Content (UGC) stored in connection with them. For identity data, Adobe collects:

- **User Name and domain** – An identifier for the user that is usually in an email address form e.g. - user@domain format. Usually a valid, primary email address. For Adobe ID types and most Enterprise ID identity types, the full user name is required to log into the Adobe system. Some enterprises use user names that don't match their email address, e.g. SOMEUSER vs. the email address (user name and domain), but this is controlled by the enterprise. For Federated ID identity types, either the full email or just the @domain portion is required in order to pass control to the proper Identity Provider.

- **UID (Federated IDs only)** – A unique identifier associated with the user (usually the email address). Adobe uses the UID as a key from the Federated Identity Provider to look up the end user in the Adobe system

- **Password** (Adobe ID and Enterprise ID only)

- **Date of Birth** (Adobe ID only. Required for COPPA, GDPR and age verification for website access.)

- **Country** – The ISO Alpha-2 Country Code for the user, which is gathered when the identity profile is created. Adobe generally uses the Country Code to determine the regional asset storage location for the end user's stored content. Enterprise and Federated ID's locations are defined by the organization.

- **First and Last Name** – Gathered when the identity profile is created. For Enterprise and Federated ID identity types, the UID, Country, First and Last Name fields are configurable by the IT administrator when creating the user accounts, and the Admin can choose how much or how little user information is included in those fields.

Where do we store your identity data?

Regardless of the geographic location of the customer, all identity data is stored in multi-region, load-balanced, cloud infrastructure providers with data centers located in US-East (Virginia), US-West (Oregon), EU-West (Ireland), and Singapore. Identity data is replicated across all data centers.

How secure is our identity data while stored?

All identity data is secured at-rest using AES-256 bit encryption in compliance with Adobe's Common Compliance Framework and meets our internal policies for encryption and storage of sensitive data.

How long do we keep it?

Content is replicated to and backed up within each data center, in other data centers within the region, and in cross-region data centers for load balancing and redundancy. Data center backups for identity data occur daily and are stored for seven (7) days. Adobe also complies with applicable laws regarding cross-border data transfers.

Adobe ID accounts are created, owned and controlled by the individual user. Accordingly, the individual user controls the lifecycle of the account and it remains active as long as the individual user chooses to keep it active. Adobe deactivates Adobe ID accounts and deletes the personal information, hashed password, and payment data associated with it upon request by the individual user or after 48 consecutive months of inactivity.

For both Enterprise ID and Federated ID, the account deletion schedule is determined by the enterprise customer and can be controlled within the Adobe Admin Console. When you no longer want a specific Enterprise or Federated ID associated with your organization's account, an authorized administrator can remove it within the Admin Console. More details on managing users with the Admin Console can be found on the Adobe product support website.

How does the identity management service handle logging?

Adobe logs each time a user signs into their applications and services, when they activate their software, when they open an Adobe application on their desktop or mobile device, and when they use cloud storage or services. Log data collected may include the ID of the user, their email, their IP address, and event tracking data.

Adobe may also log analytics data related to the application and services usage.

In addition, for Adobe ID identity types, Adobe may collect product usage data from their desktop and mobile applications. Adobe does not collect or store any user-identifiable product usage data tied to Enterprise ID or Federated ID identity types.

Adobe ID users can change their desktop data collection preference at any time by visiting their Account Management page on Adobe.com or from within the Settings menu in mobile versions of Adobe applications. Any user may opt out of analytics collection at any time. IT Administrators can download content logs directly from the Admin Console to view how their users are interacting with company-owned assets. These content logs include user data such as user name, user email and IP address.

Who can access my identity data?

At Adobe, only authorized Adobe personnel have access to this data and only on an as-needed, least-privileged basis, consistent with Adobe's ISO 27001 certification. Data logged by Adobe's identity management services is considered "most privileged" and is only accessible by an even more restricted number of Adobe personnel.

Adobe Common Controls Framework

Adobe's Identity Management Service follows the Adobe Secure Product Lifecycle and is designed to protect from the software layer down. To protect from the physical layer up, Adobe implements a foundational framework of security processes and controls called the Adobe Common Controls Framework (CCF) designed 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 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 ~290 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.

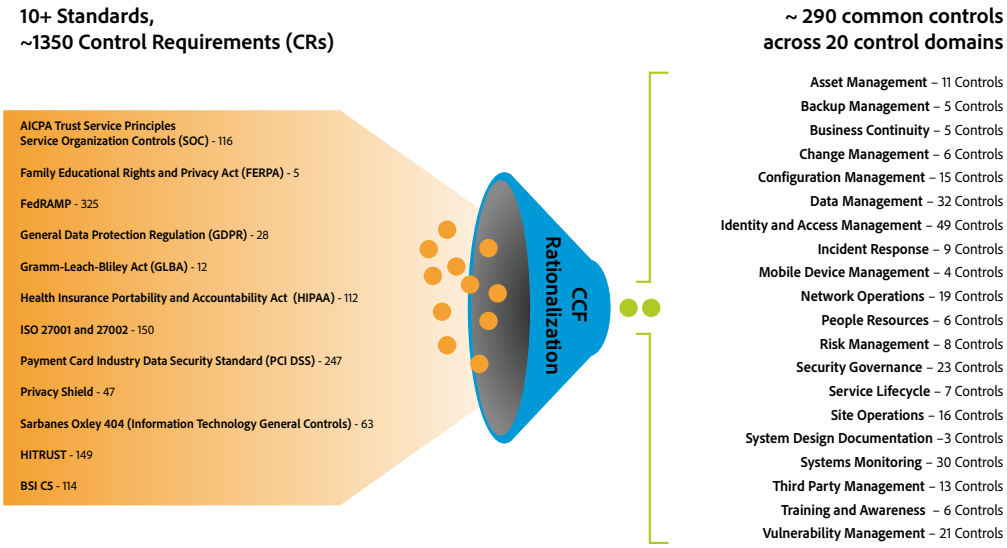


Figure 6: The Adobe Common Controls Framework

Security compliance

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 services are under continuing self review to ISO 27001 standards and the Shared Cloud underlying services infrastructure has a SOC 2 – Security certification.

Adobe complies with several compliance certifications and standards across its product lines. Please refer to our "Current List of Certifications, Standards, and Regulations" for the latest information on approved certifications for Adobe Cloud Platform.

Customer Data Confidentiality

Customer data is treated as confidential data by Adobe. 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 Adobe Identity Management Services and your identity data. At Adobe, we take the security of your digital experience seriously and we continuously monitor the evolving threat landscape endeavoring to stay ahead of malicious activities and help ensure the security of our customers' data.

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