Platform Security specifications

(Version 2.4 – Jul, 25th , 2017)

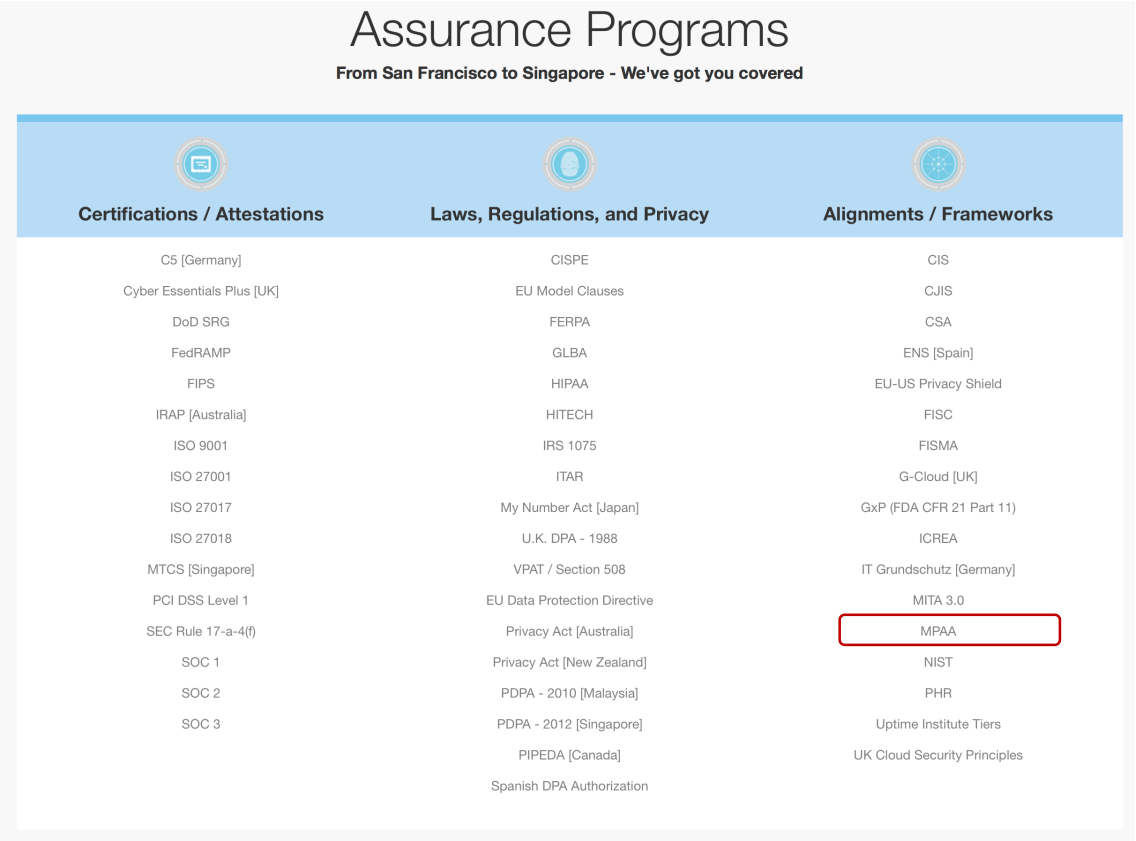
1. Platform Security

Knox Media Hub adheres to the highest levels of security for all of it systems and services. We follow industry standards and best practices, as well as continuously monitor the literature for known threats and issues pertaining to security.

2. Infrastructure Security

Knox Media Hub utilizes cloud based resources from Amazon Web Services (AWS). AWS is an industry proven platform used by countless providers. You can read more about their policies at https://aws.amazon.com/security.

AWS current certifications and accreditations are the following. Particularly important for our Industry and our clients is the certification from the Motion Picture Association of America (MPAA)



3. Instance Security

Aside from platform security we enjoy from AWS, we follow strict policies to how our instances are setup, managed, and accessed via public channels. Some of these include:

- Latest operating system releases:
- security patches applied when alerts are received.
- Strict Firewall rules: All ports closed except those needed to run our services
- Instances access only via Secure Shell (ssh)
- Utilization of Public/Private cryptography
- Password authentication disabled

4. Application and User Security

The platform of Knox Media Hub is entirely web based and uses Transport Layer Security (TLS 1.2) encryption (also known as HTTPS) for not only transmitted client data, but for all communications. This means any transmissions (data in-transit) from a client browser to our systems are sent through an encrypted data tunnel which cannot be intercepted, eavesdropped, or deciphered

The KMH platform is additionally protected from the following based on the choice of our software stack.

- Cross site scripting (XSS) protection

  XSS attacks allow a user to inject client side scripts into the browsers of other users. This is usually achieved by storing the malicious scripts in the database where it will be retrieved and displayed to other users, or by getting users to click a link which will cause the attacker's JavaScript to be executed by the user's browser. However, XSS attacks can originate from any untrusted source of data, such as cookies or Web services, whenever the data is not sufficiently sanitized before including in a page

- Cross site request forgery (CSRF) protection

  CSRF attacks allow a malicious user to execute actions using the credentials of another user without that user's knowledge or consent.

- SQL injection protection

  SQL injection is a type of attack where a malicious user is able to execute arbitrary SQL code on a database. This can result in records being deleted or data leakage.

- Clickjacking protection

  Clickjacking is a type of attack where a malicious site wraps another site in a frame. This attack can result in an unsuspecting user being tricked into performing unintended actions on the target site.

- User Authentication

  User authentication is required for all services that we offer. User Passwords are stored in a database in an encrypted format and cannot be decrypted.

- Security Auditing

  All access to services are logged and monitored in order to perform post mortem analysis if required.

5. Storage

KMH storage is based on Amazon's Simple Storage Service (S3). All client data is stored in Amazon's Simple Storage Service (S3) and is only accessible by the client owner.

Data in transit:

All data to and from S3 is encrypted in transit via SSL-encrypted endpoints.

Data at Rest:

By Default data at rest is encrypted unless a client specifies otherwise. Service-side encryption is utilized and data is encrypted using one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256).

Data access:

Access to any resource in the platform utilizes by a signed certificate which is generated for each object requested from the system at the time of access. This means all objects in storage are not accessible by anyone unless they system has fully authenticated the user and has explicitly granted access to the object in question. The access permissions of these automatically generated keys are expired after some defined period of time.