

Instructions - Please Read

- Remember, this is a legal document, and once approved will be attached to your UMG agreement as a technical exhibit.
- This is a high level document, so keep your replies as complete as possible while striving for brevity.
- Please fill out the questionnaire below in *Microsoft Word* format.
- If any questions do not apply to your service, do not leave blank... instead enter "N/A" for those questions.
- UMG may request revisions to some of your answers, so make sure you keep *Track Changes* turned on as it speeds up the review process.
- When you are answering a question or comment in a revision, please answer *inline* (in the main document body), not as a comment.
- Depending on your answers and the nature of your service, additional documentation may be required.

Contracting Party Contact Details

Company Name:	Song Mates, Inc
Service Name:	Press Play
Contact Name(s):	Tina Houser (CEO) Wes DeKoninck (CTO) Caitlin Alexander (CPO)
Contact E-Mail Address(es):	tina@songmates.com wes@songmates.com caitlin@songmates.com
Contact Telephone Number(s):	Tina (260) 609-5378, Wes (260) 437-0548, Caitlin (970) 576-1891
Date:	7/1/21

Due Diligence Questions

The section below is about what kind of service you have, and what kind of UMG content you wish to license for that service.

1 System Overview**Content Distribution Methods:**

☐ Permanent/A La Carte (ALC) Download (DRM-Free) (*typically audio or video tracks for consumer purchase.*)

☒ **Streaming**

☐ Offline Play (Cache/Conditional Download) (*See Section 10 for more detail*)

☐ API-based distribution to developers/partners for used in apps or games

☐ Other _____

Service Elements:**✓ On Demand**

- ☐ Internet Radio – Non-Interactive (e.g. DMCA)
- ☐ Internet Radio – Limited Interactivity
- ☐ User Upload/User Generated Content (UGC)

✓ Messaging

- ☐ Purchase Locker
- ☐ Scan/Match Locker
- ☐ Other _____

Content Types that you wish to license for your service:**✓ Full Track UMG Audio**

- ☐ Full Track UMG Video (*typically music videos*)
- ☐ Long Form UMG Video (*typically full concerts*)

✓ Audio Clips (*typically 30 second clips of full tracks*)

- ☐ Video Clips (*short snippets of UMG videos*)

✓ Full Catalog

- ☐ Partial Catalog (*specific genres or other differentiators*) _____
- ☐ Stems
- ☐ High Resolution Audio (*lossless audio better than 44.1kHz/16-bit*)
- ☐ Spatial Audio (*Dolby Atmos, etc.*)
- ☐ 4K Video (*Both UHD and DCI formats*)
- ☐ Ringtones/Ringbacktones
- ☐ GameTones/In-Game audio

✓ Metadata**✓ Images**

- ☐ Other _____

If you are licensing audio or video *clips* for your service, will consumers be allowed to cut-down or edit full length audio or video?

We're interested in this as a future feature post launch

Device Support:☐ Personal Computers (Windows PC and Apple Macintosh)☒ **Mobile Phones/Tablets**☐ Televisions☐ Over-the-Top (OTT) Devices (*AppleTV, Roku, FireStick, etc.*)☐ Smart/Voice Speakers (*Echo, HomePod, etc.*)☐ Networked Home Speaker Systems (*Sonos, etc.*)☐ Other _____

Please list any service details not identified above

1.

1.1 Please provide or attach a technical description of your system. This should describe the various system components and functional processes, including content ingest and preparation, content protection, high level description of consumer-facing and backend capabilities, etc.

Our Press Play mobile application will interact with both our internal serverless functions and data stores (for user account preferences and data) as well as make direct requests to the 7Digital API for music related user requests and tracking for reporting.

1.2 Please provide or attach a high-level architecture diagram of your system.

Attached on page 15 of this document

1.3 Please provide a **table** describing system components, who is responsible for operating each part of the service, and where it is located.

2.

3. Make sure to list **each partner company or party** who will stream, store, edit, encode or otherwise have access to UMG content. This includes CDNs.

4.

5. The table might include content handling, hosting, license serving, service delivery, content marketing and sales, commerce, and customer support. Please identify all third-party developer resources and platform providers (with business contact addresses and/or data center addresses). *All entities that handle UMG content must be identified.*

MongoDB
7digital

2 Audio and Video Assets

2.1 What codecs and formats do you make available to consumers? Please include:

- Maximum bit-rate, resolution, and channel information (e.g. MP3, 128kbps, stereo or 4k, MPEG-4, video),
- Please indicate what different formats will be used for

What audio/video formats (codecs, bitrates) are you requesting from UMG?	What audio/video formats (codecs, bitrates) are you presenting to consumers?
Likely AAC 160 and MP3 128, but will discuss best practices with 7digital and UMG	We do not have plans to alter format for delivery at this time

2.2 Are you using a UMG-approved third party supplier for audio or video, and if so, please identify whom.

7digital

3 Metadata and Production

3.1 **Metadata Feeds** UMG provides metadata in DDEX format XML files. Changes (e.g. metadata corrections) are provided on a daily basis and full metadata snap shots are provided on a weekly basis. **XML files must be handled using an automated process. Manual processing of UMG XML files is not permitted.**

6.

7. **UMG has a document called the *Asset & Metadata Guide* which details the metadata schema and content delivery process. If you haven't received it, please request.**

3.1.1 Can your system process daily updates?

We will work with 7digital to design our system to work with their tooling and knowledge of best practices in order to meet requirements set forth by UMG.

3.1.2 Are XML files handled using an automated process?

We will work with 7digital to design our system to work with their tooling and knowledge of best practices in order to meet requirements set forth by UMG.

3.2 Do you plan to use metadata from third party sources, and if so, for what?

We anticipate working exclusively with 7digital at this time.

3.3 Do you plan to modify metadata provided by UMG, and if so, for why and how?

No.

3.4 How do you separate “live” content (content available for download, streaming, or other authorized uses) from content in the production pipeline?

We will work with 7digital to design our system to work with their tooling and knowledge of best practices in order to meet requirements set forth by UMG.

3.5 How do you ensure that content is not offered for sale, streaming, or any other authorized use before the release date indicated in the supplied metadata?

We will work with 7digital to design our system to work with their tooling and knowledge of best practices in order to meet requirements set forth by UMG.

4 Service Integration and Management

4.1 **If your technology, or technology provider, supports multiple service partners/clients:**

4.1.1 Does it allow each service partner/client to have a different catalog of content?

NA

4.1.2 How are different service partners/clients managed and what can be customized per service partner/client?

NA

4.2 **Enforcement of territorial rights** – *Territorial rights enforcement is extremely important to UMG. Because of the widespread use of VPN software, UMG usually requires at least two methods of determining the user’s territory.*

4.2.1 How do you determine the territory of the user?

Location services on the device, and IP address geolocation

4.2.2 If you are doing business in multiple territories, how do you ensure that content is only made available to consumers in permitted territories, as described in the metadata?

NA

4.3 **User Accounts**

4.3.1 Do you maintain user accounts, and if so, is obtaining a user account required to access or purchase content?

Yes we do, Yes it is

4.3.2 Is login to a user account required to access content?

Yes

4.3.3 If you maintain user accounts, what other services or content types are accessible using the same user account?

None

4.3.4 How are users authenticated?

Phone # verification

4.3.5 How many logins per account do you support? What measures are in place to discourage sharing of logins?

One. User session tokens tbd.

4.4 Please list and describe the payment mechanisms that you support?

App stores, Credit Card

5 Reporting

5.1 Can your systems report according to the relevant templates for (a) financial and (b) marketing reporting from Universal Music Group? *Note: if you haven't received UMG reporting templates, please request from your UMG Business Development representative.*

Yes, through our partnership with 7digital

5.2 What type of information does your system log?

User session information, User usage information, Catalog usages through token tracking (stream tracking)

5.3 Does your system report usage by UPC and ISRC as supplied to you by UMG?

Yes, through our partnership with 7digital

5.4 Does your system track and report plays of tracks contained within compilations or soundtracks to the original ISRC of the track?

Yes, and in fact, we believe we'll need to utilize the original ISRC pretty explicitly.

5.5 Can you report sales/streaming in Universal Music Group's defined format, by the contractually required due dates?

Absolutely

6 General System Security

6.1 **Physical and network security.** For each stage in your system (content ingestion, packaging, content and license servers, reporting servers, etc.) please answer the following questions. *In particular, please make it clear how the audio and metadata are protected, and who has access to it.*

6.1.1 Who has network access to the servers at each stage in the process, and how are they protected from unauthorized uses and users?

Our system administrators have access to the servers with authorizations relevant to their respective roles. Authorization is provided through the vendor user access manager.

6.1.2 How do you protect license keys and other critical license server data?

Password license key vault available to authorized users only (such as Hashicorp or Cyberark)

6.1.3 How are your servers and networking hardware protected against unauthorized **physical** access?

All storage provided by cloud service providers. Facility access management is managed by these providers as well.

6.1.4 List the titles of the people who have physical access to these servers.

Cloud service providers only

6.1.5 How is login access to the servers controlled? List the titles of the people who have login permissions.

Cloud service providers, controlled by ssh keys

6.1.6 What firewall and other network security mechanisms do you use?

Cloud provider firewall service, authentication and authorization through auth0

6.1.7 How are your servers and networking hardware protected against unauthorized **network** access (e.g. cyber attacks, viruses, etc)?

Endpoint protection through dedicated VPN & IP Whitelisting (potentially CrowdStrike on developer machines)

6.1.8 Please confirm transaction-related data, including all data subject to contract audit provisions, and backups of this data are retained for three years.

We confirm.

6.1.9 Are non-transaction, security-related logs retained for a minimum of one year?

Yes

6.1.10 How are files containing audio and/or video assets, images, and metadata protected?

We will work with 7digital to design our system to work with their tooling and knowledge of best practices in order to meet requirements set forth by UMG.

6.1.11 List the titles of the people who have network or physical access to audio and/or video assets, images, and metadata?

7digital will have sole access to the above.

6.2 Please describe policies related to ensuring that all of your security systems are kept up to date with the latest patches, versions etc.?

Best practices as advised by our cloud providers. Third party dependencies will be auto-updated by Dependabot via GitHub and run through our standard QA testing before release..

6.3 Security Breach Monitoring and Response

6.3.1 Please describe processes for monitoring for security breaches.

Log monitoring, SIEM. Our cloud providers will provide alerts for unauthorized access.

6.3.2 Please describe the breach prevention, detection, and response plan.

Our draft incident response outline is attached

6.3.3 What technical mechanisms does your system support for handling a security breach (e.g. user account revocation, content revocation, player revocation)?

User account revocation, IP blacklisting, database read-only locking, 2FA, and any additional methods supported by 7digital.

7 Development Stage

7.1 Does your service exist today? If not, in what stage of development are you and how long until the service is fully operational?

Closed beta launching Q3 '21, Estimating prod launch Q1 '22

7.2 If the service exists today, please provide information on where it is publicly accessible (URL, app stores, etc.).

NA

8 **Permanent/A la carte Downloads (DRM-Free)** – *Typically audio or video content for permanent purchase by the consumer.*

8.1 What codec(s) and bitrate(s) will you be using?

8.2 **Download URL**

8.2.1 How is the download URL generated?

8.2.2 What prevents it from being re-used by the end user or other people?

8.2.3 What time-to-live (TTL) will it have?

8.2.4 Does it expire after one use?

8.3 What is your policy for allowing customers to re-download files?

8.4 If a download purchase locker is supported, please describe how device limits and switching rules are enforced.

9 Streaming of Audio/Video content – *audio/video content transmitted to the consumer in or near real time where no permanent copy is kept.*

9.1 What DRM or stream protection method do you use? Please specify the methods employed for each platform in the form of a table.

We will work with 7digital to design our system to work with their tooling and knowledge of best practices in order to meet requirements set forth by UMG.

9.2 If you use a proprietary or custom stream protection method, please describe it. Please specify the methods employed for each platform in the form of a table.

We will work with 7digital to design our system to work with their tooling and knowledge of best practices in order to meet requirements set forth by UMG.

9.3 Please describe the streaming protocol you will be using. Will it be “true streaming” or progressive download (HTTP/**HTTPS**)? Please specify the protocol employed for each platform in the form of a table.

True streaming through 7digital

9.4 Does your stream protection method prevent capture by (1) reuse of the media URL (e.g. captured via in-browser developer tools) and (2) capture tools such as Download Helper (downloadhelper.net), and (3) MP3 conversion websites? *Mobile browser pages must be tested against these tools on the desktop.*

Yes, it will

9.5 How are keys assigned and how often are new keys used?

We will work with 7digital to design our system to work with their tooling and knowledge of best practices in order to meet requirements set forth by UMG.

9.6 How is the stream rendered on the client device?

We render streams through progressive streaming via https requests. We will work with 7digital to design our system to work with their tooling and knowledge of best practices in order to meet requirements set forth by UMG.

9.7 How do you ensure that the stream cannot be captured on the client device? (All supported platforms.)

Secure transmission over HTTPS - anything stored on the device will be encrypted

9.8 How many concurrent streams per account do you allow? Please describe how device, account, and concurrent stream limitations will be enforced.

One stream per account at a time

9.9 Streaming URL

9.9.1 How is the streaming URL generated?

On request a key signed URL will be generated and tied to that user's ID.

9.9.2 What prevents it from being used/reused by the end user or by other people?

The user must be authenticated and in our system in order to generate the signed URL. We could enforce a one device login policy. We can also limit the signed URL to certain IP(s) but with mobile devices this might be more difficult.

9.9.3 What time-to-live (TTL) will it have?

The assumption in the app is once they listen on demand, so technically once the song is over we could revoke access. The question is, how long should the URL stay active if they pause/stop mid song? We could do 1 hour, 1 day, any time period.

9.9.4 What prevents direct use/reuse of the media URL?

All requests go through Cloudfront which need the correct authentication and headers.

9.10 Client Authentication

9.10.1 Please explain how you authenticate the software/hardware playback client.

The playback is part of the app and the user must be authenticated to use the app. Our app then authenticates with 7Digital to stream the media

9.10.2 Describe your procedures for verifying that authorized clients comply with the requirements.

We're unclear on which requirements you're referring to, however we will work with UMG and 7digital to design our system in order to meet requirements set forth by UMG.

9.10.3 How do you determine if the device needs to be categorized as desktop (PC/Mac) mobile (tablet/phone), or other types (TV, STB, OTT, voice speaker)?

Its a native iOS and Android app meant to run on mobile devices. Further the app collects system info on the device to determine the device type and other metrics that allow us to prevent unwanted devices from accessing the app.

9.11 Misc.

1. 9.11.1 Do you plan to support temporary (ephemeral) caching for performance or quality of service issues?

Not at this time

10 Offline Play (Cache/Conditional Download) – Typically a feature that allows consumers to save content in a secure format for offline play when not connected. Condition Downloads are not performance caching.

10.1 What mobile or device operating systems will support offline play for your service?

10.2 What DRM or content protection method do you use for offline play files?

10.3 If you use a proprietary or custom content protection method for offline play files, please describe it.

10.4 How are keys assigned and how often are new keys used? How are keys stored?

10.5 Please describe how offline play works for both general and offline playback. Please include how offline content is made unavailable upon termination of a subscription or when the application or device is kept offline longer than a subscription period. How long can offline content remain playable if the device is continuously offline for an extended period?

10.6 How do you ensure that play count data is collected from all devices? How can you be assured of its accuracy? How do you ensure that the correct number of responses are received? How do you handle cases where a license is issued (to a PC or portable device) but no play count data is received?

10.7 What is the user able to do with downloaded offline play files?

10.8 If your service allows the re-issue of licenses, please explain how this is managed and what policy you are proposing.

10.9 Will downloaded offline play content work if transferred off the device?

10.10 How are offline play files delivered to the device?

10:11 Approximately how much content will your service allow to be stored as conditional downloads on consumer devices? (Number of tracks or videos? Dynamic memory limitations?)

11 Supported Devices

11.1 What hardware devices are supported by your service?

Major Mobile Devices iOS/Android

11.2 What software players are supported by your service?

Bespoke player - built in player

11.3 What operating systems are supported by your service?

iOS & Android

11.4 What is your procedure for authorizing and de-authorizing devices? How often can authorized devices be changed?

We will be employing phone number login. There is only one device per phone number. If a user shares their phone number and one time access pin we would be able to see if that number is already logged in at the time and prevent another login attempt. We don't allow downloading of any content, so only one device can stream per account at any given time.

11.5 How do you prevent other devices, e.g. PCs from accessing the mobile parts of the service?

The app will only be available at this time via mobile app stores. Only users that have authenticated within the app will be able to make requests to our API's. Only accepted device types/models/OS's will be allowed to run the app.

12 Miscellaneous

12.1 Please describe methods for verification of student discount eligibility.

NA

12.2 Please describe methods for verification of military discount eligibility.

NA

12.3 Please describe methods for family plan verification and abuse monitoring. What are the responses to suspected and confirmed abuse?

NA

