Trusted Device List (TDL) Request for Information (RFI)

CONTENTS

1 EXECUTIVE SUMMARY

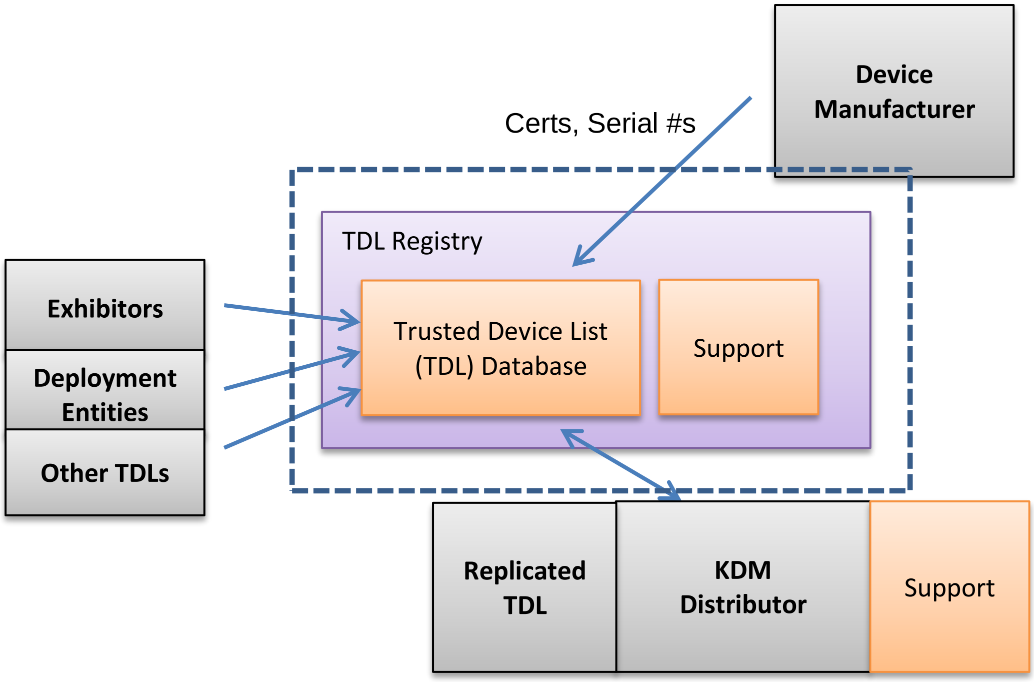
MovieLabs is working with the six major US Hollywood studios, exhibitors, distributors, deployment entities, integrators and device manufacturers to specify and build a D-Cinema worldwide centralized Trusted Device List (TDL). The team is now looking to broaden participation to include additional supporters and founders from the international community of studios, exhibitors, service providers, deployment entities, system integrators, manufacturers and other interested parties. This effort is currently in the formulation stage.

The goal of the TDL is straightforward: Develop a worldwide high availability Trusted Device List Registry for D-Cinema that is voluntary and open to all ecosystem members in a non-discriminatory manner.

The TDL will contain all information necessary for service providers and other ecosystem members to generate Key Delivery Messages (KDMs) and facilitate the delivery of Digital Cinema Packages (DCP). Information will be made available on a cost-recovery basis to authorized subscribers. The registry would not be involved in the actual KDM or DCP generation.

The TDL will receive facility list information directly via an automated FLM message, through a web interface or, when necessary, over the phone. The information will come either directly from the facility or through an authorized intermediary such as a deployment entity, system integrator, or country-specific centralized TDL. Each authorized distributor in a territory would subscribe to the TDL to take a snapshot (replicate the information) of the registry in order to generate KDMs.

Conceptually, the TDL would look something like this:



2 OVERVIEW

2.1 Trusted Device List (TDL) Overview

A reliable TDL is essential to the efficient, orderly and reliable distribution of Key Delivery Messages (KDM) and Digital Cinema Packages (DCP) to exhibitors.

The goal is to develop a world-wide high availability Trusted Device List Registry for D-Cinema that is open voluntarily to all ecosystem members in a nondiscriminatory manner.

Participants will include all parties currently involved in the distribution or consumption of Key Delivery Messages, including studios, distributors, exhibitors, service providers, integrators, centralized territory agencies, and device manufacturers.

The TDL should enable entities a mechanism to share KDM information with only one entity rather than a collection of entities. It should be easy and cost-effective to use. To achieve these goals, a high degree of automation is assumed. As there will always be exceptions that require manual intervention, the system must allow support personnel to promptly correct any KDM distribution issues that occur.

Although security is inherent in the key distribution process, some of the data managed in the TDL is sensitive to participating organizations, especially exhibitors. The system must implement access controls and have high quality security.

TDL development involves three distinct tasks: 1) the creation or building of the TDL, 2) the operation of the TDL, and 3) the Customer Support function. It is possible that one vendor could be selected for all three parts, but tasks may be contracted separately.

2.2 Purpose of RFI

The purpose of this RFI it to solicit comments on what we intend to be a subsequent Request for Proposal (RFP). We would like responses to indicate areas where we can improve the RFP that will lead to efficient and effective projects for building, operating and maintaining a TDL System.

2.3 Document Organization

This RFI is organized as follows

Section 1: Executive Summary

Section 2: This overview

Section 3: Responding to RFI – Information about responding to the RFI as well as information on how proposals will be evaluated

Section 4: Project Framework – Describes the projects that will be bid upon for the TDL

Section 5: TDL description

Section 6: Representative Use Cases – Use cases designed to illustrated TDL usage

Section 7: Notional Design – A description of some design concepts and tradeoffs

2.4 References

[DCI-DCSS]	Digital Cinema System Specification. Version 1.2. March 07, 2008
[SMPTE430-1-2006]	*D-Cinema Operations – Key Delivery Method (including Amendment 1-2009)*
[SMPTE430-2-2006]	*D-Cinema Operations – Digital Certificate*
[SMPTE430-3-2008]	*D-Cinema Operations – Generic Extra-Theater Message Format*
[SMPTE430-7-2008]	*D-Cinema Operations – Facility List Message*
[SMPTE430-9-2008]	*D-Cinema Operations – Key Delivery Bundle*
[FLM-X-Online]	*FLM-X Online documentation*, ISDCF. http://flm.foxpico.com
[ML-FLMX-DATA]	*FLM-X Data*, MovieLabs, v0.6, July 13, 2011

3 RESPONDING TO RFI

From this RFI we would like to know:

- Which companies are interested in participating in the creation of the TDL by joining an advisory group or other type of participation?
- Which companies are interested in potentially responding to the RFP, if one is issued?
- What information are we missing and which parts should we consider doing differently?

We have included questions throughout this document to prompt responses; however, we do not expect parties to respond to each of these questions. Also, feel free to add any comments you feel would be valuable to this process.

You are highly encouraged to respond, even if you are not a direct participant.

3.1 Who Should Respond

We strongly encourage all potentially affected parties to respond to the questions herein in part or whole. We also encourage additional editorial comments on the project as a whole or on topics that were overlooked. These include but are not limited to:

- Vendors who will potentially submit a proposal for one or more of the tasks defined in this RFI
- Studios
- Service Providers
- Distributors
- Exhibitors
- Integrators
- Deployment Entity
- Device manufacturers
- Any other parties who can affect or who are affected by the generation of Key Distribution Messages

Note that parties who do not respond to the RFI may still respond to the RFP.

We encourage responses from any knowledgeable party.

Any company or individual that responds to this RFI is referred to herein as a Respondent.

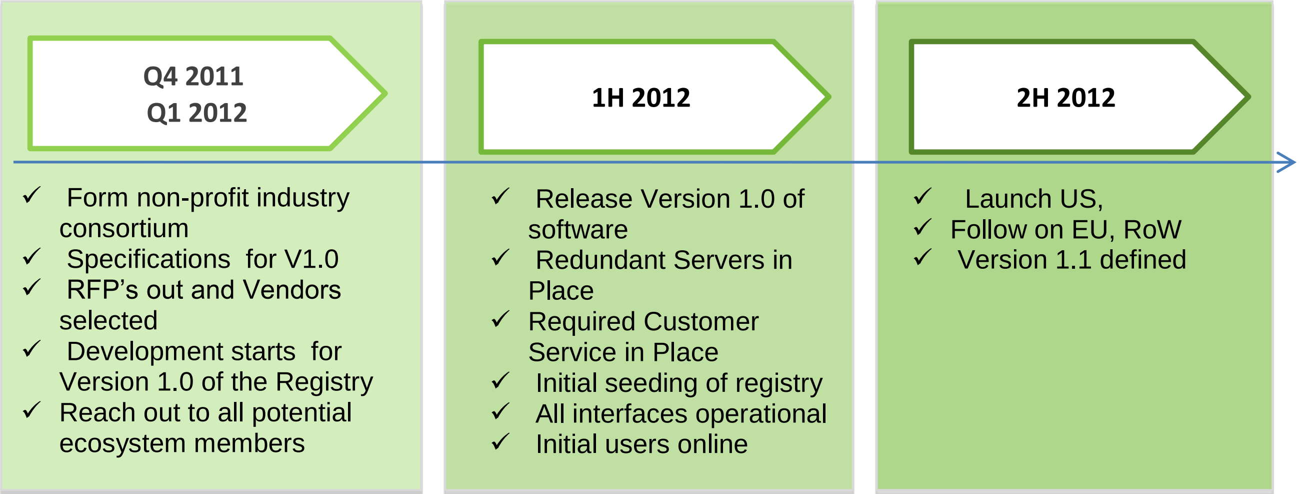
3.2 Publishing Responses

MovieLabs reserves the right, in its sole discretion, to publish or otherwise share with the community responses to this RFI, including, without limitation, inviting its member companies and their affiliates, and its and their consultants, agents and employees to participate in the evaluation of the responses to this RFI. Responses to this RFI must not involve the disclosure of confidential or other proprietary information. Responses marked confidential or proprietary will not be considered and accordingly no confidential treatment shall be given such responses. If a Respondent chooses not to answer a particular question due to confidentiality, such Respondent should note this in the response.

If specifically requested by a Respondent, such Respondent may have its responses, or any part thereof marked anonymous. If such responses are marked anonymous, they will remain marked as anonymous if published or otherwise shared with the community. We encourage responding anonymously, if it will result in a more informative and candid response.

3.3 RFI Timeline

Project timeline is as outlined here:



Q4 2011
Q1 2012

- ✓ Form non-profit industry consortium
- ✓ Specifications for V1.0
- ✓ RFP's out and Vendors selected
- ✓ Development starts for Version 1.0 of the Registry
- ✓ Reach out to all potential ecosystem members

1H 2012

- ✓ Release Version 1.0 of software
- ✓ Redundant Servers in Place
- ✓ Required Customer Service in Place
- ✓ Initial seeding of registry
- ✓ All interfaces operational
- ✓ Initial users online

2H 2012

- ✓ Launch US,
- ✓ Follow on EU, RoW
- ✓ Version 1.1 defined

The RFI/RFP process tentatively has the following dates:

Milestone	Date
RFI Issued	1/2012
RFI Responses Due	2/2012
RFP Issued	2/2012
RFP Responses Due	3/2012
Contract(s) award (depending on negotiations)	4/2012

3.4 RFI Response Format

Responses to this RFI must include the following information:

- For any Respondent that is a company:
    - Company Name
    - Company Address
    - Company phone
    - Brief description of the company's interest in RFI or TDL
    - If the company intends to bid on projects we would like to know, although it is not necessary to indicate this at this time
    - If the company plans on participating in the project as a user of the TDL
- If Respondent is an individual, Respondent must indicate that he/she is an individual.
- One or more Points of Contact. This should be a person who can answer questions regarding the RFI.
    - Person's Name
    - Phone number
    - Email address
    - Indication of preferred contact method
- Confidentiality/Anonymity
    - If a Respondent chooses not to answer a particular question due to confidentiality, the Respondent should note this in the response. Responses to this RFI must not involve the disclosure of confidential or other proprietary information. Responses marked confidential or proprietary will not be considered and accordingly no confidential treatment shall be given such responses.
    - For each response, indicate whether the Respondent wants the response to be marked "anonymous." If the Respondent fails to indicate its desire for anonymity for any response, the response may be published with the Respondent's identity.

Comments on the RFI may be in any form. We request that specific comments reference the section and paragraph mentioned. The RFI is also available in Word format.

3.5 RFP Proposal Evaluation Process (RFP)

The RFP will cover three distinct tasks for the TDL: the creation or building of the TDL; the operation of the TDL; and the Customer Support function. It is possible that one vendor would be selected for all three tasks, but this is not required. RFP Respondents must specify which portions of the TDL they are responding to.

All proposals will be given due consideration. Proposals will be evaluated based on various criteria, including technical, management and cost factors. An RFP Respondent can bid the entire project or one of the distinct tasks (support, creation, operation).

Evaluation criteria include, but are not limited to the following:

- General
  - Does the vendor have relevant prior experience?
- Technical
  - How well does the proposal address the technical requirements?
  - How technically qualified is the vendor to achieve successful results?
  - Is software developed using environments and tools that can be transferred to a third party for continued development?
- Company and Management
  - How flexible will the vendor be dealing with changes? We strongly discourage underbidding with the idea of pricing each minor change.
  - Is there a commitment to assign qualified personnel to this project? We prefer at least some key members of the proposal team participate in the project.
  - Is the vendor culture compatible with the needs of the project? In particular, the vendor should be able to work with the parties who will be involved, including MovieLabs, studios, exhibitors, distributors, device manufacturers, and so forth.
  - Does the company have best industry practices in place for project management?
  - As applicable, does the company have best industry practices for software development, systems operations, support, and other relevant processes?
- Cost
  - What is the overall cost of the project?
  - How likely is the vendor to achieve the proposed cost?

Proposal evaluators have built and deployed numerous systems, and are familiar with industry practices. If you have particular strengths that you believe are relevant, please let us know.

MovieLabs has absolute discretion in accepting proposals, or selecting no proposals to an RFP. The selection process involves a number of factors, no single one or subset of which is necessarily determinative. As with this RFI, MovieLabs will have the right to evaluate and share the proposals in the RFP and responses to the RFP must not involve the disclosure of confidential or other proprietary information. Responses marked confidential or proprietary will not be considered and accordingly no confidential treatment shall be given such responses.

3.6 Contact Information

Responses should be sent to info@movielabs.com.

3.7 Disclaimer of Liability

- By submitting a response to this RFI, the Respondent acknowledges and agrees that MovieLabs is not obligated to the Respondent in any manner as a result of the Respondent's participation in this RFI, and that MovieLabs expressly disclaims any and all obligation to accept responses to this RFI, incorporate any responses into an RFP or otherwise engage the services of the Respondent as a result of the Respondent's participation in the RFI or RFP.

- By submitting a response to this RFI, the Respondent acknowledges that the Respondent has read and understands this RFI and agrees to its terms and conditions.
- By submitting a response to this RFI, the Respondent acknowledges that (i) its responses may be published or otherwise shared with the community, including, without limitation, with other Respondents and MovieLabs' member companies and their affiliates, (ii) its responses do not involve the disclosure of confidential or other proprietary information and (iii) any responses marked confidential or proprietary will not be considered and accordingly no confidential treatment shall be given such responses.
- The Respondent acknowledges and agrees that MovieLabs has absolute discretion in carrying out is evaluation of the responses and that the evaluation may include a number of factors which may be amended without notice to the Respondent.
- MovieLabs reserves the right to accelerate, change the dates for, discontinue or otherwise alter the RFI process or the terms of the RFI at any time, and makes no commitments, implied or otherwise, that an RFP will be issued or this RFI process or any subsequent RFP process will result in a business transaction with one or more Respondents.
- All products mentioned are included as representative examples. There is no recommendation that any particular brand or product be used; and there is no endorsement for any of these products. Furthermore, pricing is dated and may not be accurate.
- The Respondent must sign and return the General Release attached as Exhibit A to MovieLabs in conjunction with its submission.

3.8 Specific Questions for the RFI

The goal of this RFI is to improve the quality of the RFP, to improve the chances of success for the TDL, and to engage the community in the creation of the TDL.

Respondents are encouraged to respond to as much of the RFI as they desire. Even a comment or a response to just one question is valuable.

We have called out specific questions in the text, highlighting them as follows: **Question**.

4 PROJECT FRAMEWORK

The project is divided into three primary tasks: Build TDL, Operate TDL and Support the TDL. Vendors will be encouraged to bid on as many tasks as they are qualified to undertake.

4.1 Task 1: Build TDL

This Task is to create the Registry and probably be available for maintenance and upgrades of the Registry. The Vendor who builds the Registry will be responsible for the full design and implementation of the TDL. This will include the creation of the database, the front end web site, the appropriate APIs for integration with outside participants, and general installation and update procedures.

This task has the following parts

- Build TDL (or adapt internal software for use as the TDL)
- Updates to core software
- Third-level technical support (help second-level when they can't solve a problem)
- Software Maintenance (TBD) – This may be part of Build or Operate.

4.2 Task 2: Operate TDL

This Task is to operate the TDL, and includes handling the integration of new requirements, keeping the servers operational 24/7/365, integrating new participants, and general operations of the system. There is intended to be a requirement that the TDL be at least dual hosted (i.e., in two geographically dispersed locations).

This task includes the following responsibilities:

- Support TDL
  - Monitoring the health of the TDL; for example, Database integrity
  - Monitoring data feeds for problems
- Onboarding of new customers
- Maintaining bug database
- Rollout of updates to the TDL
- Providing hosting service for all TDL equipment, including colocation (space, power, cooling, etc.) and network bandwidth
- Maintaining network infrastructure, such as DNS
- Providing NOC-level system maintenance
  - Hardware replacement
  - Software installation and configuration in accordance with supplied scripts
- Troubleshooting

- Software Maintenance (TBD) – This may be part of Build or Operate.

4.3 Task 3: TDL Support

This Task is to provide support to the ecosystem worldwide. There will be a requirement to provide multiple language support either via a translation service or directly. There are two basic categories of support, one for bringing new ecosystem members into the System and keeping them operational (Operational Support), and the second for keeping the integrity of the data up to date (Data Support). Under the current operational model Operational Support is a first-line activity, and in most cases mostly an extended-business-hour type activity. Data Support should be assumed to be a second-line of support issue is also an extended-business-hours support activity. Data Support is provided as a second-line activity behind Service Providers, Deployment Entity, and System Integrators. Support will be primarily by email with secondary phone support. The actual business hours of support will probably change as the system goes online in new territories.

Data Support is intended to be a second-line activity as the Service Provider/Distributor will issue corrected KDMs based upon support calls themselves with their updated corrected data and facilitate the correction of the Registry for the future.

Support includes the following

- Email and Phone Support (**Question**: What level of support is required and how many hours per day would constitute extended-business-hours work for Operational Support?)
- Second-level phone support for Data Support
  - Help with database data errors
- First-level phone support for Operational Support
  - administration (e.g., account management, onboarding of new members, initial integration and operation)
  - any operational problem with the TDL (e.g., problem accessing REST web services APIs)
  - special interfaces and integrations with partners
- Bug reporting
  - Identify and report bugs that become evident in the support process
  - Assist developers isolate bugs.
- User and company account management
  - Create new accounts; delete expired accounts
  - Help users recover credentials
- Monitor the system for security or integrity problems in accordance with procedures

5 TRUSTED DEVICE LIST

This section describes a nominal design for the TDL. The design provided is for illustrative purposes and does not imply that the TDL be designed in this manner, It is intended to give people a general idea where this project is heading.

5.1 Context

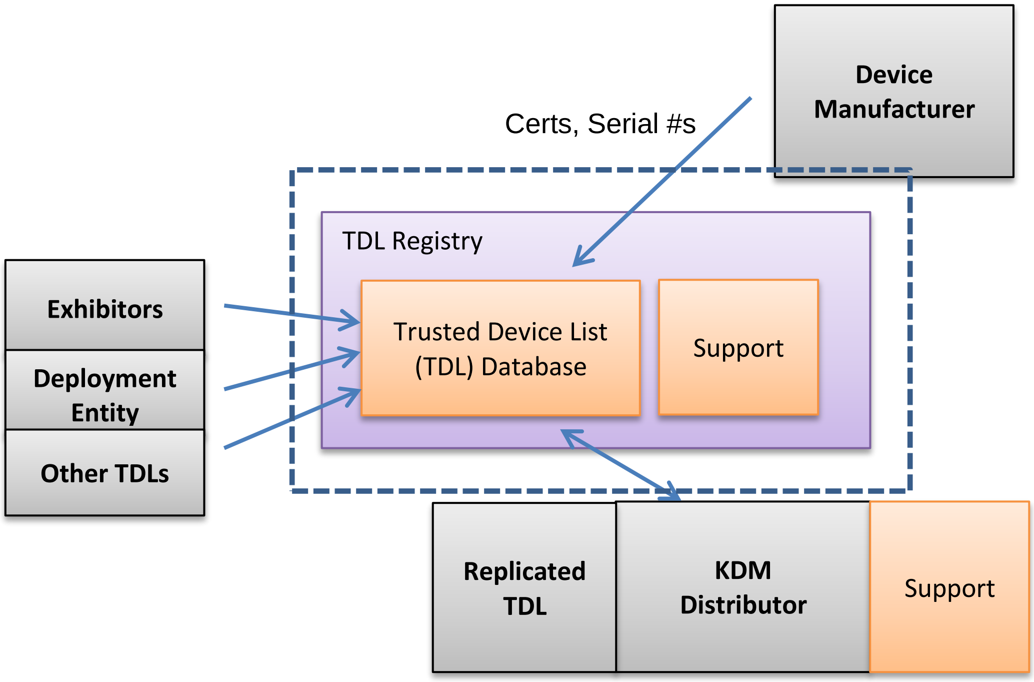
This project is in the context of Digital Cinema as defined by the Digital Cinema Initiative (DCI) as defined in *Digital Cinema System Specification*, Version 1.2, March 7, 2008 [DCI-DCSS], and various SMPTE specifications (see References)

Digital Cinema Packages (DCPs) are delivered to Theater Systems. Theater Systems require key information delivered in the form of Key Delivery Messages (KDM) for decryption of DCPs to allow presentation. To issue KDMs, a distributor needs information about the Devices containing Security Managers (SMs) that are being authorized for presentation.

The Goal of a Trusted Device List (TDL) system is to maintain timely and accurate information on participating auditoriums so that participating subscribers can obtain information needed to issue KDMs.

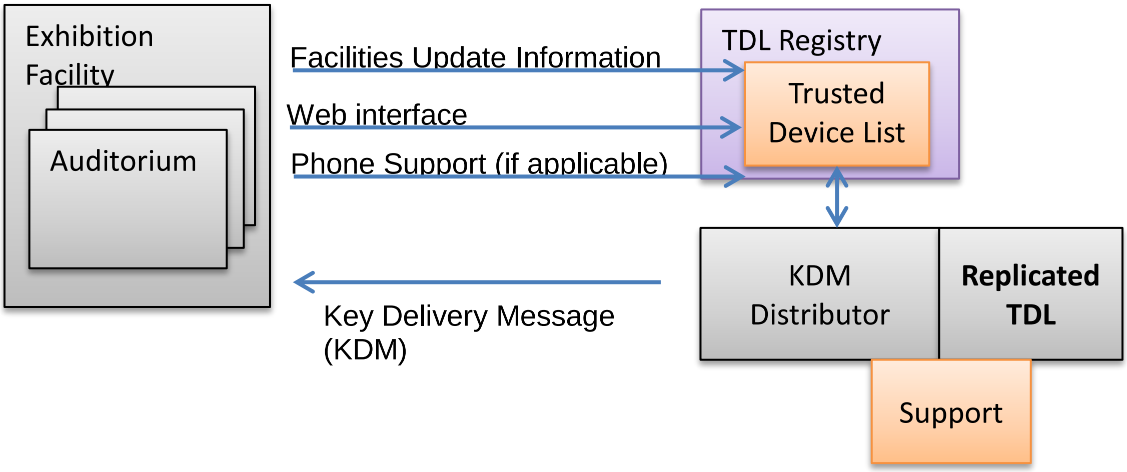
5.2 System Architecture

The following is a conceptual model used to describe and discuss the TDL.



Information about how devices are deployed into auditoriums and facilities, the core of the TDL data, comes from Exhibitors, Deployment Entities, Integrators or other TDL sources (joint ventures, regional authorities, etc.).[1] Device manufacturers optionally submit additional device information into the database for use validating data from other sources. The TDL maintains this information. KDM distributors query the database with the assumption they maintain a replicated copy of the TDL. A support function maintains operations.

The following diagram provides additional information on interfaces.



5.3 Basic Part of the TDL

The TDL is made up of the following basic pieces:

- Data functions – those are for putting information into and getting information out of the database
- Access Controls – these are permissions for readers and writers of the database to control where a writer can put information and who is allowed to access/read the information

5.4 Data Functions

The TDL is first and foremost a database, and therefore has typical database functions. The system will have to maintain the following sets of information:

- TDL information
- Authorized Users detailed information and associated permissions
- Unique Naming Convention/Service for Exhibitor, Facility, and Screen
- Historical Logs – information on changes to the TDL

5.4.1 Data Sources

The TDL has several data sources: Device manufacturers, Exhibitors, Deployment Entities, Integrators, Service Providers (interacting with Exhibitors), regional authorities, and Support.

[1] We feel at this time given the limited size of the database and the simplicity of the information that a federated system is not required although open to a discussion on this issue.

5.4.2 Database Interfaces

There are two main interfaces directly to the database: a REST API for automated management of the database, and a Web/HTML interface for direct interaction with the TDL. There is also direct support for bulk ingest of TDL information and bulk download of the TDL. Additional support for receiving an RSS feed for TDL updates is a potential capability.

5.4.2.1 REST API

REST API is defined online at [FLM-X-ONLINE].

5.4.2.2 Web (HTML) API

There will be a user-friendly web interface provided by the TDL.

The TDL web interface will include functionality equivalent to the REST API, offered in a manner more suitable to a browser interface. The TDL web interface will provide functions for

- Data entry, retrieval and management (e.g., modification, deletion).
- Data Access controls
- Account Management
- Historical Log Information
- Data Conflict Task List – Data integrity problems, Stale TDL Entry or Unverified TDL Data bug list for an exhibitor.
- Additional, to be defined.

Access levels assigned on a per-user basis will determine which functions a user may access. For example, only administrative users will be able to add users.

Details of the web interface will be defined during the design process.

Question: Any additional major requirements we should mention now?

5.4.2.3 Other Input into system

5.4.2.3.1 No Data Input via email

Due to difficulty in validating information, email is currently not considered acceptable means of updating the TDL. It is possible for an agent or a designated agent to receive email and then use one of the interfaces to update the information

5.4.2.3.2 No Data Input via phone – directly by TDL Support Function

There is no first-line Data update support currently offered by the TDL. First-line support offered by authorized parties such as service providers deployment entities, and integrators may use the web API for updates. Note that there is phone support to address administrative issues and TDL functional problems.

5.4.2.3.3 Operational Input via phone – directly by TDL Support Function

There is an Operational Support function that can receive phone input to correct problems.

Question: What is the best operational model around this? How do we authenticate phone users?

5.4.2.4 Bulk Ingest

Bulk ingest involves the initial acquisition of data into the TDL database. An interface will be provided for bulk ingest of TDL data already in existence with exhibitors, service providers and other parties.

The system will make available the ability to take a complete download of the applicable parts of the database via an authenticated FTP transfer.

Question: Is this the best method? What is the granularity of the downloads?

5.4.2.5 Updated Data Feeds

Replication via query is core to the TDL design. Whether or not there is a subscription or 'push' mechanism for TDL data is TBD. The update feeds will make available to an authorized reader of the TDL only those portions of the TDL that they are specifically authorized to receive.

The current mechanism is documented in [FLM-X-Online] as the "SiteList" mechanism. A query of the SiteList returns information about which FLM-X data are updated allowing a query of just the changed data. This is a polling mechanism equivalent to RSS, but more adapted to this application.

Question: Is SiteList sufficient for all needs, or is subscription mechanism required?

5.4.2.6 Verification Notices

When a change is made to the TDL in response to a KDM problem, there is interest in knowing whether the update resulted in successful KDM generation. In this model, a verification notice would be generated when the TDL update resulted in a valid KDM being generated. Note that KDM generation is *not* part of the scope of the TDL.

Question: Is this function required? When is a KDM considered verified (sent, received, installed, playing, etc.)?

Question: Are there other scenarios where verification notices would be valuable?

5.4.3 Automated Reporting

Ideally, servers and TMSs report Device status directly to the TDL. This avoids many of the problems associated with humans in the loop (e.g., reads serial number from Media Block rather than a possibly incorrect barcode on the outside of a chassis), while introducing other problems (e.g., high reliance on Internet connections).

This would likely require changes to devices and operations. It would also have implications for facilities that have private networks.

Question: We are interested in your thoughts on automation.

5.5 Data Integrity

Driving forces behind the TDL are increased data integrity; and greater ease and lower cost to achieve that integrity. This section outlines some methods that improve data integrity.

The general goal is to work toward the exhibitor or their proxy to work toward automating and actively keeping their data in the TDL accurate. It is assumed that when a problem is found the agreed upon notification and correction policy will remedy the situation. The web UI will also provide a mechanism for an exhibitor to also track problems with their TDL entries.

5.5.1 Consistency Checks

Data on input into the ecosystem will be validated for integrity. The integrity checks will include checks for duplication of data, data inconsistencies, and blacklisted (e.g., stolen) equipment.

Question: What other data inconsistency checks should be performed?

Question: What logs should be kept? Should historical logs for facilities be kept?

Question: What level of data integrity override should be permitted?

5.5.2 Conflict Resolution

The system will perform basic data integrity checks when messages are received. Those items found in conflict will be flagged and a correction protocol will be followed on automated updates to the system, apparent errors will trigger an external conflict resolution procedure. If the entry is manual via the web interface the error will be flagged on entry and not accepted until resolved.

Question: When bad data is received by the system, what mechanism to resolve these issues should be followed?

5.5.3 Database Inconsistency Resolution

When a distributor or other ecosystem member finds errors in the TDL, they are required to flag that the information is “stale” and potentially provide the updated information as an “unverified update” which the TDL will log and work to resolve the problem. The TDL then will contact the facility/their proxy to resolve the issue so that subsequent updates are correct and don’t reintroduce the same error. This synchronization of coordinating participant’s discovery of a problem and the subsequent validation of the fix so that other TDL participants receive corrected information is a key function that the TDL will provide. We are investigating the best methods to coordinate these database updates.

Question: When distributors find bad TDL information what should be the process for correcting the information? Unless distributors have proxy rights for exhibitors, the most they can do is mark the data “stale” or inconsistent and have exhibitors or their proxy agents deal with it after the fact.

5.6 Access Controls

The general access model is that companies entering data have controls over which companies can access their data. Exhibitors specify which companies have rights to look at their data. The system will provide an Exhibitor the ability to provide default groups of companies to read their data on a territory-by-territory basis.

Exhibitors may grant other organizations authority to act on their behalf. For example, many exhibitors will grant or have delegated to integrators or deployment entities the ability to update TDL information on their behalf. If Exhibitors are receiving assistance from service providers, they may wish to grant them TDL update authority, as well

Question: Do we need access control at a more sophisticated level down to specific facilities or even to the granularity of a subset of the FLM-X?

Question: Our assumption is that device information would be available to all participants, with the possible exception of other device manufacturers. Are any controls necessary? Note that controls may become more complicated when companies have more than one role.

5.7 Operations Functions

5.7.1 Account Administration

Policies must be developed for the following

- Adding and removing companies
- Adding and removing users

Question: How do we determine which companies and users are allowed to join? What is the initial list?

The system should use best industry practices for

- Authenticating users
- Authenticating systems authorized to access the TDL
- Account recovery (lost username and/or password).

The system should be monitored for unauthorized access to the system. This should be a combination of both automated tools and audits.

Administrative support will likely be required for username and password support. The means to authenticate the party at the other end of an email or phone call must be part of the system design.

Question: How do we authenticate initial contacts at participating companies?

Question: How do we identify and authenticate facility personnel?

Question: How do we authenticate phone contacts?

5.7.2 System Administration

Systems require general administration. Some examples of this administration include

- Issuing certificates for access to the TDL
- Controlled conventions, naming and vocabularies, particularly around identities (e.g., unique exhibitor names)

5.7.3 User Support

Online resources should be available to users to avoid the need to contact support. These can include

- Training
- Help with specific support topics (e.g., account recovery)
- Question: Other?

5.7.4 Site Operations

A site operations interface is required for efficient operations. We anticipate that collocated equipment will be monitored in a Network Operations Center (NOC). The implementation must provide interfaces that support efficient monitoring.

Interfaces should be provided in the following areas:

- Site Operations/Managed Services
- Software Maintenance
- Security and Anti-Fraud

5.8 Data

The TDL database will maintain all FLM-X data. The database will also maintain information about TDL participants, access control information and other administrative data.

FLM-X data is described in more detail in [ML-FLMX-DATA].

5.8.1 Facility Data

5.8.1.1 FLM Data

The TDL will store all FLM messages, plus additional administrative data including at least when and how the data arrived at the system (e.g., via message, web or REST interfaces).

In addition to FLM message, the following data will be maintained:

- Date and time that data arrives or is entered at TDL. Note that IssueDate from the FLM-X structure takes precedence because messages may be delayed
- Method of update: email, web, REST, etc.
- Authority (e.g., username)
- Question: What other data must be maintained? Do we need to keep information on email source, IP addresses, and other identification information?

5.8.1.2 Notes and Log

Information should be kept concerning the history of the facility data including errors found and potentially corrected (but not verified) by distributors.

5.8.1.3 Data Integrity

Information about the validity of the entry might include that the data has been found to be stale or in error, or that an alternative set of data has been submitted but not verified as complete, or that this data is in error for being on a black list or a duplicate of other information. These data should be available as part of the TDL.

5.8.1.4 Theater Validation Data (TBD)

There has been some discussion that when TDL information is added, the system be capable of generating test DCPs and KDMs to promptly test and validate devices in theaters—the digital cinema version of email validation. This could be useful for exhibition to ensure data is correct, and also to increase data integrity in problematic territories.

If implemented the TDL must keep track of the status of the testing. State might include validated, DCP sent, DCP received, DCP results confirmed, DCP results failed.

- **Question**: How valuable is this capability, how likely is that this would be used, and under what conditions would it be applied?
- **Question**: Would it be valuable for Exhibition for initial testing and integration?

5.8.2 Participant Data

Information will be maintained on participants, including exhibitors, device manufacturers, studios, service providers, distributors, deployment entities, integrators and their representatives.

Some organizations act on behalf of others. For example, a Service Provider may act on behalf of certain studios to issue KDMs.

5.8.2.1 Participating Organization data

The following information is maintained on each organization participating

- Organization information
  - Unique organization ID
  - Organization type
  - Name
  - Address
- Points of Contact
  - Contractual
  - Technical
- Proxies (who can they act on behalf of)
  - Organization ID
  - Allowed functions (e.g., issue KDMs)

5.8.2.2 Individual information

The following information is maintained on each person with access to add or retrieve information from the TDL. People are associated with participating organizations.

- Personal information
  - Name
  - User ID
  - User credentials (login information)
  - Contact information
- Associated organization
  - Organization ID
  - Role in organization (primary POC, technical, administrative, etc. TBD)
- Privileges and access rights
  - May enter data on behalf of organization
  - May retrieve information on behalf of organization
  - May update company information
  - Others TBD

5.8.3 Device information

Device information may be submitted by manufacturers independently from FLM data. This allows cross checking and provides supplemental information to KDM generating organizations if necessary.

Device information is a subset of DeviceType. The particular elements and attributes are:

- DeviceTypeID
  - scope
- DeviceSerial
- ManufacturerID
- ManufacturerName
- ModelNumber
- SoftwareList
- KeyInfoList
- WatermarkingList

5.8.4 Access Control Data

TDL data is only accessible to those who have been granted access. All data entered is tagged with the organization entering those data.

The policies regarding access control are to be determined, however, the mechanisms described here will support various policies.

Access Controls are granted by one organization to another organization.   Granularity of access controls are based on general classifications of information, region and time.

An access control grant contains the following information (TBD)

- Organization granting access
- Organization given access

- Start/End time. Absence of start, end or both implies unbounded (earlier, later or all respectively)
- Region. Absence of region implies worldwide.
- Access rights
  - May access FLM data
  - May access Device information from manufacturer (granted by manufacturer)
  - May view company information, including point of contact
  - Other, TBD

5.8.5 Log Data

Logging will be a passive function that will allow the operators to determine what actions happened to the system. Incoming messages and actions will be tagged and stored. Logs should be kept for a minimum of a year. Tagging will include

- Time received
- Source (individual and/or organization)
- Method (REST, web, etc.)

5.8.5.1 Log Data Visibility

An authorized user shall have access to view the log data. The log data will be available in the UI.

5.8.6 Fraud and Malicious Behavior Detection Data

The TDL will maintain data for the purposes of detection malicious behavior on the TDL, either from participants or outside intrusion. These data are TBD.

6 DEPLOYMENT ASSUMPTIONS

6.1 Sizing Estimates

The following are not meant to be accurate numbers but are provided for sizing and capacity planning purposes.

Parameter	Value
Total Facilities	100,000
Auditoriums per Facility (average)	2
Digital Screens	200,000
Devices/Screen	2
Total Devices	400,000
Data/Device	5,000B
Total Active Data	2GB

Table 1. Facility Parameters

Parameter	Value
Device change rate in auditorium changes/day	1%
Auditorium updates/day	1,000
FLM Updates/Day (2x because 2 auditoriums/facility)	2,000
Rate of update	1.4/minute
Size of FLM(5K/device * 4 devices)	20KB
Size of FLMs updated per day (2,000 * 20KB)	40MB

Table 2. Change Parameters

Parameter	Value
KDM generation entities (database readers) [Note Assuming readers have access to full database.]	200
Number of queries if each reader queries once/minute	200/minute
Size of reads if full query sent to each KDM generator (200 * 2GB)	400GB
Size of database query if each KDM generator queries once/day (200 * 40MB)	4GB
Assumed size of all queries/day	450 GB
Average (450/365/60/60 * 8)	41Mbps (assumes even loading all day)

Table 3. Query Volumes

Following are values we believe are reasonable estimates based on the numbers above. These values are based on reasonable future growth. Initial configuration does not need to support these volumes.

Parameter	Value
Database	4GB
Bandwidth	at least 100Mbps, better at 200mps
Outbound volume	500GB/day or 15TB/month
FLM Archive growth rate	40MB/day, 1.2GB/month, 14GB/year
Database update rate	1.5/minute
Database query rate	~200/minute.(3.5/second)

Table 4. Bandwidth and Database Size

Question: Please comment on the sizing requirements?

6.2 Availability Requirements

Overall system availability is 99.99%. That is, critical functions are available 99.99% of the time. We need to better define what constitutes critical functions. The working model is that readers of the database (KDM generation entities) will always keep a separate version of the database and will only depend on the TDL for updates.

Question: The base assumption is that the entire system has 4-nines availability. Are there functions we can carve out with lower availability?

6.3 International Rollout

Our plan is to deploy the TDL first in the United States and Canada. Once operations are stabilized, our tentative plan to next move to Europe followed by Asia Pacific, the Middle East, Central and South America, and Africa (not necessarily in that order).

The exact rollout order will be determined at a later date and depends on factors such as the scope and pace of digital rollout in each region, and any logistical issues that affect our ability to deploy such as the number of languages that must be supported.

Question: Can you provide any guidance on rollout order or issues affecting rollout in any region?

Question: What languages must the web interface natively support?

6.4 Phased Functionality Rollout

We are considering rolling out the TDL in phases. Although the ultimate goal is for the TDL to be a trustworthy authoritative source, this would be difficult to achieve immediately upon launch.

The phase outlined below illustrates how the TDL might be phased to achieve increasing levels of functionality towards the goal.

Example phases:

- Phase 1: Clearinghouse for KDM generators. In this phase the TDL provides a mechanism to share current TDL data between organizations that generate KDMs. The goal is to avoid duplication of troubleshooting. These organizations would not change how they currently collect data, but by sharing anomalies they can generate KDMs more accurately. At this time we would also create a unique naming convention for all facilities and screens.
- Phase 2: Authoritative source. Once sufficient experience is gained resolving conflicting data submissions, the system will be given the ability to accept inputs from various sources and resolve ambiguities. In this phase, the TDL might offer additional Support capabilities to aid with resolution.

6.5 TDL Alternative Mechanism

There has been discussion that KDM generation should move to a fully automated on demand model, complementing the concept of Theater Key Retrieval (TKR). In this model, a facility will directly request their KDMs from the distributor by first authenticating themselves, providing FLM-X data, and then requesting a KDM for their facility. The distributor will respond on demand by creating the KDM and returning it to the facility. This idea is a completely automated mechanism. This mechanism assuming that each facility has the ability to generate either directly or indirectly KDM requests with the proper facility information and that the facility has the ability to query its equipment to automatically gather the correct facility information.

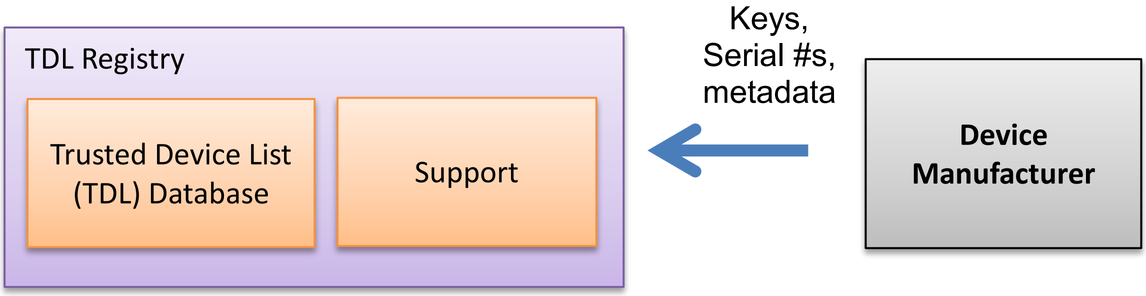
Question: Should we look to facilitating and putting in place a supporting infrastructure for the move to this on-demand model for fully automated facility to distributor KDM request?

7 REPRESENTATIVE USE CASES

The following Use Cases illustrate the basic operation of the TDL.

7.1 Manufacturer provides information

A device manufacture provides information to the TDL.

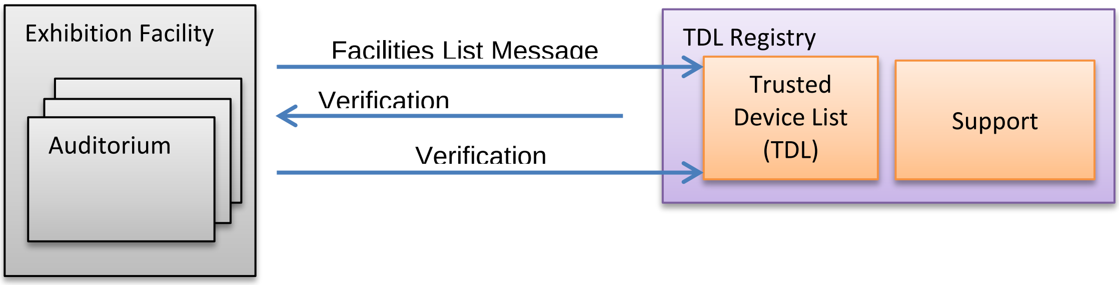


Steps are as follows

- Device manufacturer makes information available to Registry upon manufacture
- This data is used later to ensure data integrity

7.2 New or changed auditorium (automated)

This is a typical change that may occur either through a new installation or changed equipment.

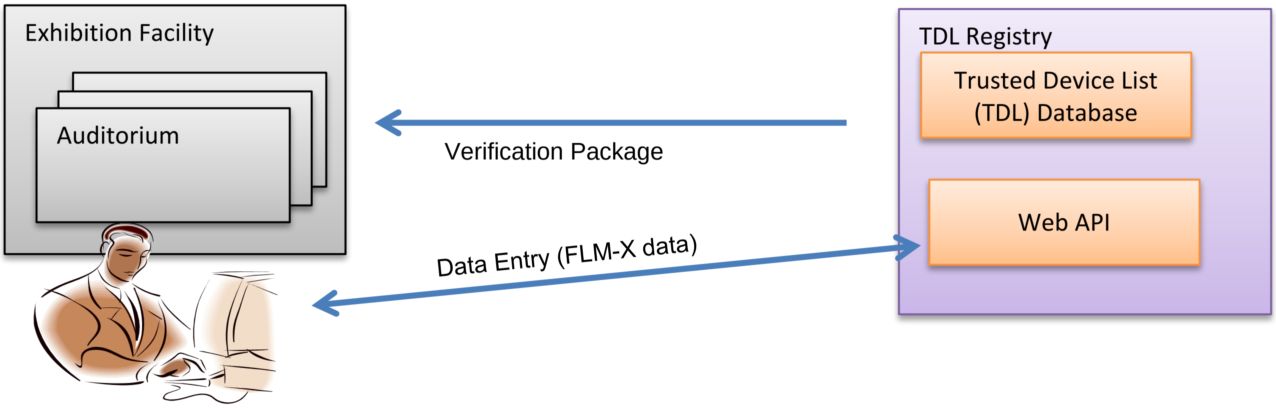


Steps are as follows:

- FLM is generated at Exhibition Facility
- Authenticated at TDL Registry
- Optional - Verification Package (test DCP and KDM) sent to Facility
  - Verification package includes verification information
  - Operator in Auditorium plays DCP and records information
  - Information sent to TDL Registry
  - If everything checks out, incorporated into TDL

7.3 New or changed auditorium (Web)

This is a case where automation is not implemented at the exhibitor. However, the exhibitor has web access and updates accordingly.

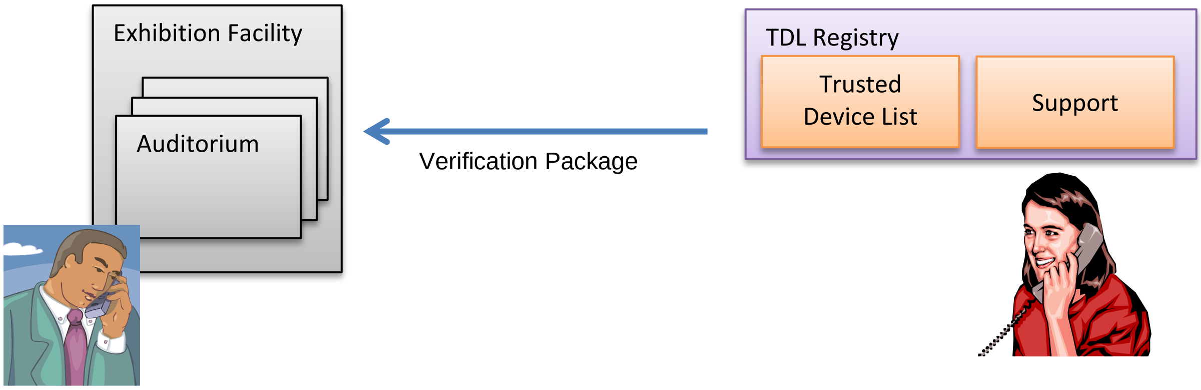


Steps are as follows:

- Theater operator to TDL Registry Support
- Verbal authentication (TBD)
- TO provides information equivalent to FLM
- Optional Verification Package (test DCP and KDM) sent to Facility
  - Operator in Auditorium plays DCP and records information
  - Information provided to TDL Registry Support
  - If everything checks out, incorporated into TDL

7.4 New or changed auditorium (phone) (This option is under discussion)

This is a case where automation is not implemented at the exhibitor and the exhibitor does not have Internet access. Phone support is necessary.



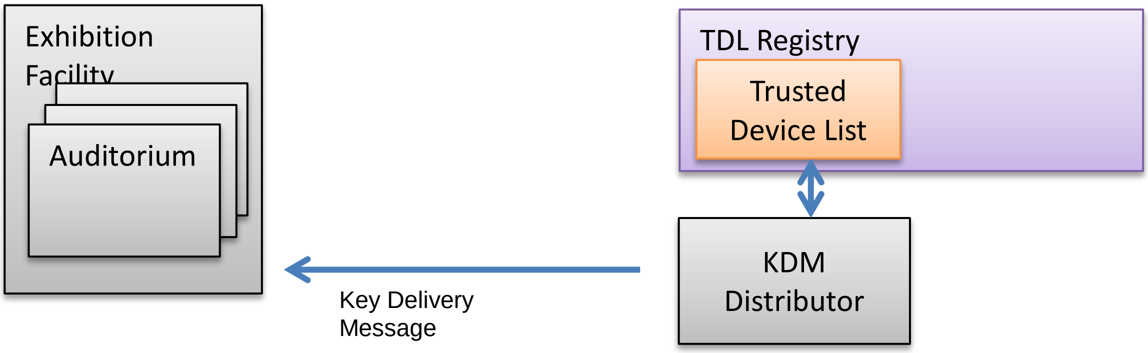
Steps are as follows:

- Theater operator to TDL Registry Support
- Verbal authentication (TBD)

- TO provides information equivalent to FML
- Optional Verification Package (test DCP and KDM) sent to Facility
  - Operator in Auditorium plays DCP and records information
  - Information provided to TDL Registry Support
  - If everything checks out, incorporated into TDL

7.5 KDM Generation

KDMs are generated from a distributor to the Exhibitor. This is outside the scope of the system, although relevant to the overall process.

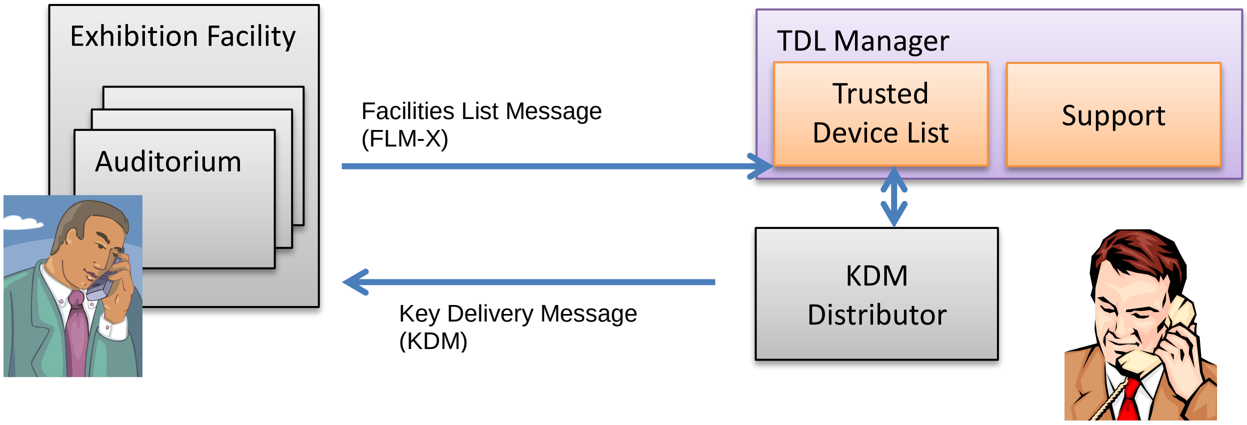


Steps are as follows:

- KDM Distributor obtains information from TDL by using own version of the database
  - Theater information
  - Device information, including certificates
- KDM issued
- Showing proceeds on schedule

7.6 Emergency KDM Generation

This is one of many emergency scenarios. In this scenario, an exhibitor calls support at the Distributor with a problem. It is determined that the TDL information is incorrect and the Distributor's support updates the TDL.



Steps are as follows:

- Problem with KDM
- An exhibitor calls KDM distributer
- The distributor refers the exhibitor to update the TDL Registry
- If the distributor has been given proxy update privilege by the exhibitor the distributor will update the TDL accordingly. If the distributor does not have proxy update privilege it shall flag the TDL entry as a stale entry and update the Registry with unverified corrected data.
- Distributor updates local copy of TDL and issues KDM
- Presentation proceeds

There is no default permission for the any part to act on behalf of another party, so in this scenario the Distributor cannot update the TDL unless it has been granted permission to do so by the Exhibitor. Once the TDL is updated, the corrected information is available to all.

Question: Do you think that in cases where the distributor is not permitted to update the TDL by proxy, that marking the TDL entry as stale and that a follow up is required is a good solution?

Question: Another option is that a distributor updates the information regardless and the information in the TDL is marked "unverified update" and is subsequently handled by the TDL support function to update the information permanently. Is this a better approach?

Question: If a distributor updates the TDL, is that the definitive record? How do we manage inconsistencies between Distributor reported data and Exhibitor reported data which has been superseded and potentially subsequently continues to be transmitted improperly? What about two distributors updating the information but differently for the same TDL entry?

Question: Should we have a mechanism for distributing a message that indicates that there has been an equipment change and new KDMs need to be generated? This could be forced out to the appropriate KDM generation entities.

8 APPENDIX A – GENERAL DESIGN THOUGHTS

This section describes a potential design for the TDL. It is not complete and does not necessarily meet all requirements; although it should provide the reader with a basic understanding of the requirements.

8.1 Design Approach

The TDL database is relatively small with a small transaction rate. Speed will not be an issue. However, the system has challenging reliability requirements. Delays in distributing FLM information will result in incorrect KDMs, and ill-timed downtime will result in dark theaters. Data loss is unacceptable as KDMs will be incorrectly generated.

Therefore, design should focus on data integrity and availability.

Please note that all products and pricing are examples only. We do not recommend or endorse any products listed and pricing may be old and inaccurate.

8.2 High Availability

8.2.1 Reliability Assumptions

The following are the assumptions used to drive the high-availability architecture. It is useful to specify down time in terms of end results as a validation of more conventional availability statistics. Such data also provide guidance in design tradeoffs.

- The most stringent availability requirement emergency KDM issuance, consisting of a single FLM update followed by a FLM query.
    - At any given time, there should is a target of 0.0001% chance of failure (four nines)
- Routine FLM Update
    - TBD. **Question**: Any recommendations?
- Routine Database query
    - It is presumed that people will cache the database, so frequent queries are not necessary.
    - TBD. **Question**: Any recommendations?

8.2.2 High Availability Approach

High availability and reliability require addressing all potential sources of failure. Typically, the most likely causes of failure in high reliability systems are power, network, operations and software. Hardware is the most likely element to fail, but it's also but due to relatively simple design techniques it is the least likely to cause a system failure. The following outlines how we address each point of failure

- Power and cooling
    - High availability colocation
    - Dual-power to each device

  - Multi-site failover
- Network
  - Dual carrier at each site
  - Multi-site with different carriers
  - High-availability DNS
- Hardware
  - Redundancy
  - Fast failover on local server failure (either high availability cluster or load balancer)
  - Multi-site failover
- Software
  - KISS—Keep It Simple Stupid
  - Testing approach
  - Considering failsafe
- Operations
  - KISS
  - Detailed procedures, especially for managed services (in colocation facility)
  - Authentication is likely a high source of failure (cannot access functions because of authentication failure)
- Other
  - Modem? How many lines? Where is POP? Availability?

8.3 Interfaces

The TDL will accept input and queries via two methods: Web and REST (web services).

There may be an event notification.

8.3.1 Web Interfaces

The TDL will offer a web interface that will support at least the following functions

- FLM-X equivalent updates. That is, information that is in a FLM-X message can be updated through the web
- Queries. A distributor wishing to generate a KDM can query the database for information. As part of this query, the user will be able to download certificate information. **Question**: Is this necessary or is REST interface sufficient?
- Support interfaces. An authorized support agent will be able to override information provided in FLM-X messages to correct errors.

Question: What reports are required? Reports might include usage reports, or the results of particular queries.

The User Interface must be internationalized and localized. A list of languages and countries will have to be defined.

Question: What languages are required for the UI?

8.3.2 REST Interface

REST is a very simple and straight forward web services interface approach. It uses basic HTTP functions which the TDL combines with XML for to create, modify, query or delete 'resources.' FLMs map nicely onto REST's resource model making the TDL interface both conceptually and structurally simple.

8.4 Authentication

Authentication is necessary to ensure the integrity of the system. However, authentication failures are, from the user's perspective, system failures.

Both users and systems (e.g., TMS) need to be authenticated.

8.4.1 Threats

There are numerous threats that can compromise the integrity of the TDL. The system's design must consider these threats and include countermeasures.

- Denial of Service, either at the system level or FLM level
- Cause KDMs to be generated for unintended devices for unauthorized use.

The following is a partial list of threats to the TDL

- Data
    - Unauthorized access by non-participant
        - Creation, modification or deletion of data
            - More serious threat is substituting data to cause KDMs to be generated for incorrect devices either as a denial of service, or to an unauthorized a device for use in piracy.
        - Query of data
    - Unauthorized access by participant
        - Creation, modification or deletion of another party's data
        - Access to data not specifically authorized
    - Disgruntled employees with access (particularly exhibitors)
- System
    - Denial of Service (DoS)
    - monitoring data between TLD and other parties (man in the middle attack)
    - Intercepting transactions (man in the middle or DNS redirection)

8.5 Reliability Calculations

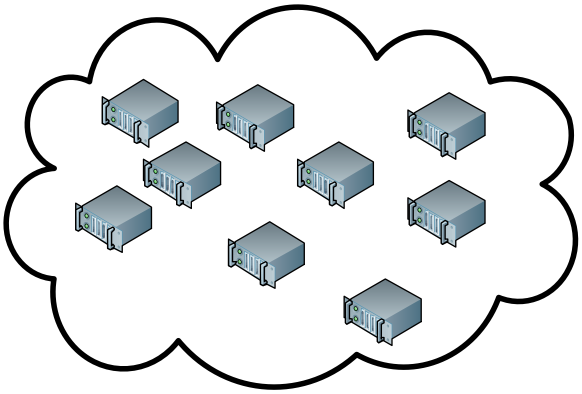
Mean Time to Repair (MTTR) is the amount of time to repair after a failure. MTTR is important in the TDL because downtime over a couple of minutes blocks emergency KDM issuance.

Availability is uptime divided by total time. This is a function of both failure rate and MTTR. For example, something that fails once every 100 days for 1 day (0.99 availability) has the same availability as failing every 50 days for ½ day. Unfortunately, you can't go directly from availability to MTTR.

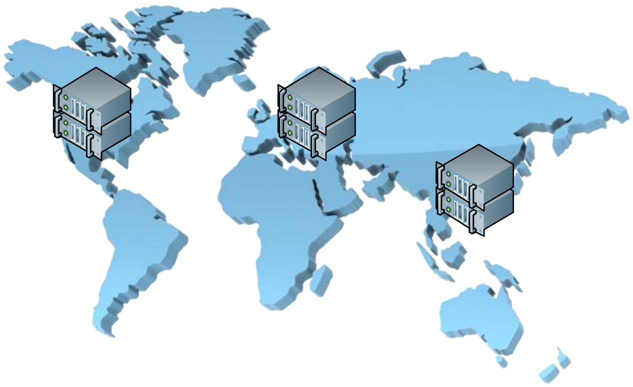
8.6 Site and Hardware Options

To meet availability requirements, a reliable hardware configuration is required. Options have been narrowed to two:

- Hosted Clusters – small number of sites geographically distributed with high-availability clusters.
- Servers in the Cloud – large number of low-availability servers. From a network standpoint, the cloud configuration can also be thought of a large number of low-availability sites.



Servers in the Cloud



Hosted Clusters

In all cases, it is necessary for anyone accessing the TDL to find a working site.

8.6.1 Servers in the Cloud Option

As high-availability servers are not available in the cloud, this approach uses a large number of low-availability servers.

8.6.1.1.1 Amazon EC2

The Amazon Elastic Cloud Computing (EC2) offering allows individual servers to be allocated from their pool of resources.

Amazon SLA is 99.95%, but that does not mean we will see that availability. This SLA is based on "regional unavailability" meaning that they measure whether their region is operational, rather than whether you instance is running. Individual failures don't count and should be assumed to be higher. http://aws.amazon.com/ec2-sla/ E2C has five regions, with an unknown number of availability zones in each region.

Therefore, even with systems distributed across availability zones, there still needs to be many instances to achieve high availability.

Regarding storage, Amazon's high durability option is Simple Storage Service (S3). People often cite the "durability" number of 99.999999999%, however, the availability is cited as 99.99%. http://aws.amazon.com/s3/#protecting. It is attractive for archiving, but if used operationally, this feature alone would cap availability at four nines. Amazon Reduced Redundancy Storage (RRS) is more cost-effective, but offers the same availability (99.99%). For our small data volume, S3 makes more sense.

Amazon offers a service called Remote Database Service (RDS) which claims some high availability features. However, they offer no SLA making it unclear what availability is achievable.

8.6.1.2 Pros and Cons

The advantages of this approach are:

- The cloud service owns equipment. No capital outlay. Equipment upgrades over time with no intervention.
- The cloud service operates equipment. Not contractor or staff to manage.

The disadvantages are:

- High failure rate, with potential downtime during switchover
- Likely increased software complexity to address frequent failover
- It is questionable whether high availability can be achieved using Amazon Cloud services.

8.6.1.2.1 Cloud Costs

We have minimal computing demands, so the smallest E2C is likely adequate. Pricing with a 1 year purchase ("reserved") is $227/year or $18/month. If we need a large instance it is $75/month.

Bandwidth is $0 for in (from Internet to instance). Outbound traffic is $0.09 up to 40TB/Month. 15TB/Month would be $1350/month.

S3 cost is $0.154/GB per month. Even with full archiving, database would be less than 20GB after a year, with a rate of $3/month. Transactions would cost about $1000. Data would be $1080.

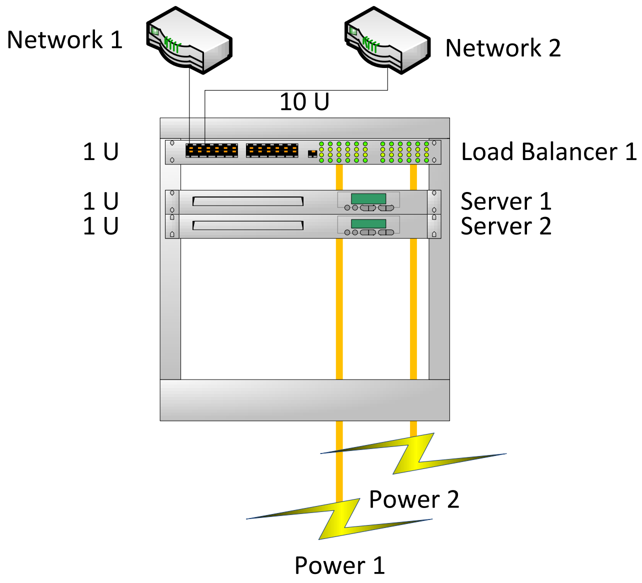
8.6.2 Hosted Clusters Option

The hosted option involves two or more sites. It is not practical to have a large number of sites outside of cloud services, so the hosted uses high-availability clusters within each site.

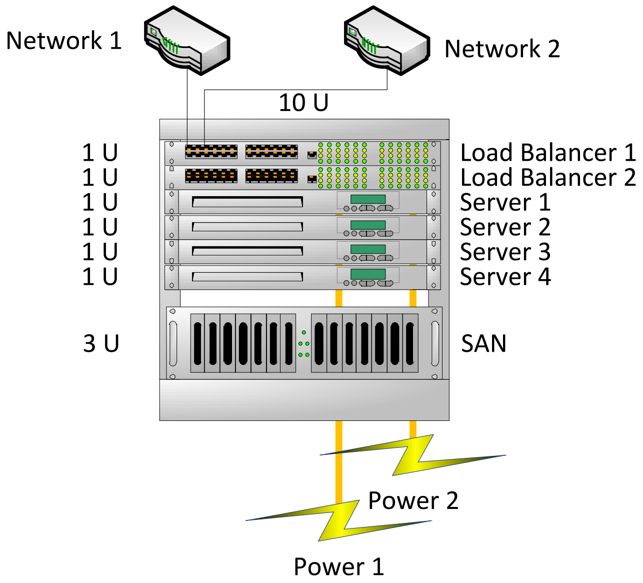
8.6.2.1 Configuration

There are various ways to achieve high availability in a cluster, but the most common and straightforward is to put two or more servers behind a load balancer. These each component take power from two sources and has network interfaces connected to distinct carriers.

The following shows two configurations using this model. Both are high-availability, but the Extended Configuration has higher availability and higher cost.



Basic HA Cluster



Extended HA Cluster

These configurations would be replicated across multiple sites, geographically dispersed with independent ISPs.

Intra-site failover handled via load balancer. Load balancer failure will bring down site, unless we use redundant load balancers.

8.6.2.2 Hosted Cluster Costs

There are many hardware options, but higher availability requires high quality maintenance. Most enterprise dealers offer 4-hour hardware replacement. In other cases, it makes sense to have spares available onsite. In the following, representative hardware is listed based on quality of equipment and service.

Some representative hardware with cost estimates:

- Load Balancer
  - F5 BIG-IP 1600 Series (smallest). Standalone $18,000. HA (dual) $34,000 [list]
  - KEMP LM-3600, Standalone $10,000, HA $20,000 [dell.com]
  - Barracuda, Model 440, $6,000 (may not include necessary options)
  - KEMP LoadMaster DR might work too ($1600 on dell.com)
- Server
  - Supermicro, Intel Core i7-950, 6GB, LSI MegaRAID, 4x3TB drives in RAID 5. $3400
  - Dell PowerEdge C1100, 1xXeon E5620, 12GB DRAM, 4x2TB HDD, $5,000
  - Dell PowerEdge R710, 1xXEon E5649, 12GB DRAM, 4x2TB HDD, $5,300

The cost is a function of what availability is desired. Generally, a 99.999% system requires every available resource, in particular the Extended HA Cluster shown above; although a 99.99% system could possibly use the less reliable Basic HA Cluster configuration.

Configuration for 4-5[2] nines:

- 2x F5 BIG-IP 1600 Series Global Traffic Manager ($34,000)
- 4x Dell PowerEdge, C1100 ($2000)
- Total/site: $54,000
- Four sites: $216,000

Configuration for 3-4 nines:

- 1x Kemp Loadmaster DR ($1600)
- 3x Supermicro ($3400)
- Total/Site: $11,800
- 2 sites: $23,600

For comparison:

- 4 instances in Amazon EC2
- Total/year: $3600

8.6.3 Inter-site/Server failover

Inter-site failover applies to failures of servers within a cloud, or site failures. In cloud services, failover would happen frequently. In hosted clusters, failures are rare.

There are three methods for handling failover

- Load-balancer based DNS – Some load balancers include DNS nameservers and can direct traffic to working sites.
- Hosted high-availability DNS (e.g., Level 3) – hosted DNS monitors whether sites or servers are up and supplies DNS results for servers that are up.
- Obtain Autonomous System Number (ASN) and handle at Border Gateway Protocol (BGP) level. This option is technically the superior, but would require applying for an ASN and placing our service on the Internet backbone. It will not be considered fully.

The DNS-based approaches rely on resolving hostnames to functioning IP addresses. This works ultimately, but even with a short DNS time to live (TTL) it takes time to detect that a host is down and to try an alternate. Generally speaking, a failed host could cause applications and browsers to be unable to locate a working site for a small number of minutes.

Applications (REST clients) can be designed to retry appropriately. In some cases, web users will be required to hit ‘reload’ on their browsers.

[2] When we refer to 3-4 nines, or 4-5 nines we are indicating a general range. The exact value would depend on many factors.

8.7 Preliminary System Design

8.7.1 Hosting

The chosen approach is multiple (minimum 2, but ideally 3-4) sites in high-availability configurations.

There is little confidence the Amazon Cloud can provide sufficiently reliable service for high-availability on-line service. The absence of relevant SLA commitments combined with recent Cloud failures implies it is a poor choice. However, Amazon S3 is likely a good choice for archive.

8.7.1.1 Site Location

We recommend two sites initially. These would be in two geographically separated cities in the US.

The system would be designed to expand, presumably to a site in Europe and a site in Asia.

Any single machine would be capable of processing the full system load.

8.7.1.2 Network

Each site would obtain network access via two independent carriers. This is a standard option most hosting facilities.

8.7.1.3 Power

Our rack would be supplied from two independent high-availability power sources. This is a standard offering at most hosting facilities.

8.7.1.4 Rack Space

Current configurations would require no more than ½ rack.

8.7.2 Equipment/Server Design

As failures cause temporary outages during switchover, it is preferable that individual sites fail as infrequently as practical. To achieve this, sites will have no single point of failure.

8.7.2.1 Load Balancer

Load balancers will run in redundant configuration with automated failover.

One might consider handling DNS failover either in an external name service or by hosting nameservers in the load balancer. External services would maintain a heartbeat with applications, and there is like no load balancer involvement. If DNS is hosted in the load balancer, they will run in global load balancing configuration, sharing information with peers at other sites. The feature is available in many load balancers such as F5 BIG-IP.

Load balancers can be a TLS/SSL endpoint. This may be advantageous.

8.7.2.2 Server Hardware

Servers are commodity high-availability servers with dual (at least) network interfaces, dual power and hot-swappable disks in redundant configuration (probably RAID 5 or 6).

MTTF on such hardware is generally in the 2-5 year range.

8.7.2.3 Long-term data retention

Amazon S3 provides the most cost effective and practical solution for long-term storage. The complication is that to access S3 it is necessary to run an EC2 instance. This is not expensive, but it adds complexity.

Other options are to be determined.

8.8 Software

The software is notionally partitioned into the following major components

- Database – includes both storage and replication
- Web front end
- REST interface
- Applications
  - Data entry and retrieval
  - Administrative Tools

8.8.1 Database

Some candidate database management systems (using the term loosely) include:

- Apache Cassandra – This system is designed for high-availability replication. It applies techniques for weak consistency, with eventual consistency. It does not attempt to resolve conflicts, leaving that to the application. Conflict resolution is where traditional weak consistency replication systems typically fail. Cassandra comes from social networking sites and is used in many high-profile applications.
- MySQL – Very popular in applications of this type, MySQL has replication capabilities. However, it replicates master-slave, a configuration inherently more difficult to reconstruct after a failure. Amazon RDS supports MySQL.
- Oracle – As an industrial strength database management system, Oracle is expensive and difficult to manage. Many shy away from it because it's difficult to configure correctly. Oracle offers several replication methods.

8.8.2 Web front end

We conceive the web user interface as a front end to the REST interface. Functions include:

- Exhibitor
  - Query FLM data
  - Update FLM data
  - Manage rights to access FLM data

  - Manage 'account' (e.g., users)
- Device maker
  - Query device information
  - Create/update device information
  - Manage rights to access device data?
  - Manage account
- KDM generator
  - Query device information
  - Query FLM information
  - Manage account
- Administrator/Support
  - TBD

8.8.3 REST front end

A REST front-end is documented online at [FLM-X-ONLINE].

Agents should be able to make queries using GET if-modified-since model for updates

8.8.4 Subscription Model

Subscription model is under discussion.

8.8.5 Application

We anticipate that applications are mostly custom code developed for the TDL database.

The application lives behind the REST interface. It responds to CRUD (Create, Read, Update, Delete) requests and interfaces with the database accordingly.

It must resolve conflicts between updates occurring in different locations as a consequence of failure.

It must respond to all aspects of failover (not including those occurring at network layer).

It must monitor the system for failures and suspicious behavior and respond accordingly.

It must generate reports for participants.

8.8.6 Administrative Tools

The system must include administrative tools the perform functions associated with policy and operations (TBD).