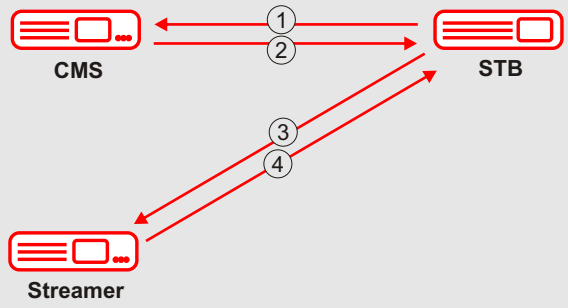
Digital Rights Management and Encryption

Industrial Solution

SysMaster provides advanced encryption and DRM procedures to guarantee the security of all distributed content:

Work Flow Scheme



1. STB sends an encrypted SSL 128 AES request to the Content Management System (CMS) that contains: PIN, STB IP, Time Stamp Key, Media Object ID

2. CMS Returns to STB the IP of the Streaming Server along with the session key that has time based expiration. The key is used to decrypt the content.

3. STB sends a streaming request to the Streaming server that contains PIN, STB IP, Time Stamp Key, Media Object ID, Session key.

4. Streaming server encrypt the media content using 128 AES SSL encryption based on the following parameters: PIN, STB IP, Time Stamp Key, Media Object ID, Session key.

Transmission Encryption

The system uses advanced SSL AES 128 bit packet encryption that utilizes the following parameters:

- PIN Number of the subscriber

  The PIN number uniquely identifies each subscriber and does not allow the subscriber to have access after balance depletion. In addition the PIN number is used to allow a single session per subscriber thus preventing the media to be accessible by multiple parties using the same PIN number.

- Time Stamp

  This parameter is used to disallow authentication based on cached access control data. If the request is not within the designated time parameters of the centralized server it will be ignored.

- Packet Sequence

  The parameter allows unique encryption of each packet individually, thus providing rotating encryption that is virtually impossible to capture and decrypt.

- Client Device IP

  The parameter provides a filtering mechanism to ensure that the client is properly identified and processed. The device IP is also used for encryption purposes to ensure that multiple clients can not access the services from behind a NAT Router improperly.

- Media Object ID

  This is the id of the media stream that needs to be accessed. The ID guarantees that only clients with privileges over the media can access and stream it.

Authentication and Authorization

The system ensures that all clients are properly authenticated and authorized using advanced authentication and authorization methods such as:

- PIN Authentication

  All subscribers have a unique PIN number that is built into their STB, This PIN is captured in encrypted format and is never transmitted in clear text

- IP Based Authentication

  The subscribers can also be differentiated based on IP addresses to guarantee that multiple clients behind NAT do not have access to the same service.

- Time Based Authentication

  Every single subscriber request must carry a proper time stamp. This will guarantee that the request is correct and is recently generated, thus avoiding the reuse if cached or old captured requests for authentication purposes.

- Content Plan Authorization

  Every subscriber has access only to his content plan thus allowing geographical and demographical separation of subscribers. Subscribers will have access to only authorized content at all times.

- Streaming Server Authorization

  Every subscriber has access to only a selected group of streaming servers to ensure that all content is not distributed randomly over the network.

Digital Rights Management

The system will keep track of all accessed content, including the time the content was retrieved, and the subscriber that retrieved it. The report can then be used to generate Digital Rights Management reports to the company that has ownership of the content. In addition, if required, all content can be interfaced with a proprietary or third-party DRM server that will act as a Certification Authority for every content access attempt. Content owners can easily retrieve the billing reports online using the advanced web interface. The DRM System has the following features:

- Certification Authority

  The system can be interfaced with a specialized server that will act as a CA for every content access.

- Advanced Real-Time Content Reports

  The system allows the content owners to log into the reporting interface and retrieve reports for all content accessed, as well as all other required data such as the time it was accessed and the subscriber count.

- Content Statistics

  The system will generate comprehensive content statistics that will show content access, subscriber count, average time viewed, and other important statistical information on historical as well as real-time basis.

- Centralized Recording Management

  The system enables and disables centrally all content recording on the STB level. The administrators can disable recording by checking the proper option for every media object thus not allowing the subscribers to record content via digital or analog means.

Set Top Box Security

The STB has multiple security features that make it one of the most advanced devices in the industry. The STB has the following security options:

- Encrypted PIN Support

  Each STB supports a unique 16 digit PIN (Personal Identification Number) that is stored in encrypted format in the STB memory and is used to authenticate the subscriber and the STB before the server. The PIN is never displayed in unencrypted format.

- HDCP Interface Support

  This is part of the HDMI interface and is required to provide control over the HDMI interface of the device.

- Macrovision Analog Interface

  This is part of the A/V Analog interface and is required to allow control over the analog interfaces.

SysMaster
2700 Ygnacio Valley Rd, Suite 210
Walnut Creek, CA 94598
United States of America
Email: sales@sysmaster.com
Web site: www.sysmaster.com