

## **Marlin Simple Secure Streaming (MS3)**

THE MARLIN DEVELOPER COMMUNITY, INCLUDING, INTERTRUST, PANASONIC, PHILIPS, SAMSUNG AND SONY MAKE NO REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, CONCERNING THE COMPLETENESS, ACCURACY, OR APPLICABILITY OF ANY INFORMATION CONTAINED IN THIS DOCUMENT. THE MARLIN DEVELOPER COMMUNITY, INCLUDING, INTERTRUST, PANASONIC, PHILIPS, SAMSUNG AND SONY DISCLAIM ALL LIABILITY OF ANY KIND WHATSOEVER, EXPRESS OR IMPLIED, ARISING OR RESULTING FROM THE RELIANCE OR USE BY ANY PARTY OF THIS DOCUMENT. THIS DOCUMENT IS PROVIDED TO YOU "AS IS".

THE MARLIN DEVELOPER COMMUNITY, INCLUDING, INTERTRUST, PANASONIC, PHILIPS, SAMSUNG AND SONY MAKE NO REPRESENTATIONS CONCERNING THE APPLICABILITY OF ANY PATENT, COPYRIGHT OR OTHER PROPRIETARY RIGHT OF A THIRD PARTY TO THE INFORMATION CONTAINED IN THIS DOCUMENT OR ITS USE. THE RECEIPT OR ANY USE OF THIS DOCUMENT OR ITS CONTENTS DOES NOT IN ANY WAY CREATE BY IMPLICATION, ESTOPPEL OR OTHERWISE, ANY LICENSE OR RIGHT TO ANY PATENT, COPYRIGHT, TRADEMARK OR TRADE SECRET OF THE MARLIN DEVELOPER COMMUNITY, INCLUDING, INTERTRUST, PANASONIC, PHILIPS, SAMSUNG AND SONY, WHICH ARE OR MAY BE ASSOCIATED WITH THE IDEAS, TECHNIQUES, CONCEPTS OR EXPRESSIONS CONTAINED HEREIN.

# Marlin Simple Secure Streaming (MS3)

## Introduction

Marlin Broadband is a full-featured DRM technology that easily scales from simple to complex business models, supports downloading or streaming content, subscription or purchase-to-own usage, and deployments to devices or to domains, to name but a few of the options.

However, many content distribution use cases simply require the content to be streamed to a (trusted) client, grant access to the content for one-time use only, and signal minimal constraints such as media output controls.

For such use cases, Marlin has developed the MS3 specification, focused solely on secure access to streaming content to authorized clients, and designed specifically to make integration into existing services as simple as possible.

Beyond offering a secure, but low-cost/low-complexity solution for Services to get to market with streaming content, other key benefits include:

- Authentication/authorization of clients even for unprotected content delivery.
- Easily supports emerging HTTP-based adaptive streaming technologies like Microsoft's Smooth Streaming or Apple's HTTP Live Streaming.
- Common content packaging formats supports both MS3 and Marlin Broadband deployments
- Content is protected prior to streaming, instead of being streamed over a protected channel, thus minimizing overhead for CDNs and enabling advanced caching strategies
- Lastly, MS3 is an open standard that can be implemented by anyone.

## What is MS3?

MS3 specifies a simple mechanism for services to authenticate trusted clients and securely issue content keys or authentication tokens so these clients can access streamed content. Content can be clear or protected using any of a variety of content protection schemes.

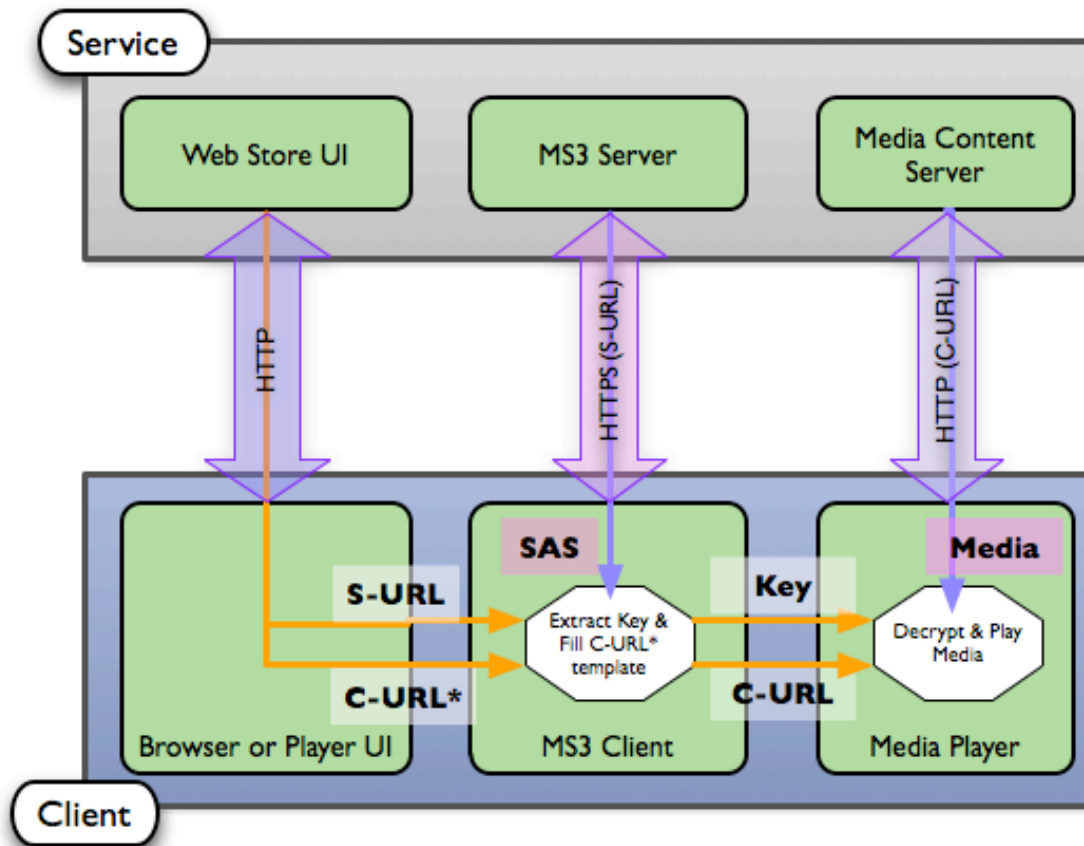


Figure 1: Typical MS3 Deployment Configuration

In an MS3 deployment, a Media Service supplies a client with content location information (C-URL) and the location of an MS3 Service (S-URL) where the authorization to access the content may be obtained. The MS3 Service provides this authorization via Stream Access Statement (SAS) to authorized clients.

In a typical scenario, this client contains a web browser for accessing the media service and acquiring a S-URL and C-URL. The client also includes a hardened component responsible for establishing a TLS session with the MS3 Service, retrieving the authorization to access (and the key to decrypt) the content, and feeding the content to the media-rendering pipeline in a manner consistent with the content rules.

MS3 specifies the following 3 elements:

1. a container (SAS) that contains a content encryption key and output control flags delivered over a secure channel. SAS's are typically discarded at completion of the playback session for the content item they authorize access to.
2. a simple TLS profile for client authentication and for establishing the secure protocol over which the SAS is delivered. MS3 Services may use a TLS certificate issued by a certificate authority of their choosing, while an MTMO signed certificate is necessary to authenticate an MS3 Client.

3. HTTP binding for processing the two URLs defined above. These URLs can be delivered to the client in multiple ways, several examples of which are included in the specification. Although no single one of the mechanisms listed in the specification is mandated, choosing one of them, the simplest for instance (the compound URL method), will help overall interoperability among clients and services.

## MS3 Content Formats

MS3 is silent on content formats. It is designed to support authorization of trusted clients to access both clear and encrypted content, notably all Marlin content formats. As such, the PDCF (OMArLin) and the Marlin Broadband Transport Stream (BBTS) specifications are perfectly suitable for deployment. Other content formats are under development.

A key design point of MS3 is that only the content key is delivered over a standard, secure TLS connection, since the content is already encrypted, it can be stored anywhere, and delivered using a variety of methods including http.

This makes MS3 ideally suited to HTTP based adaptive streaming deployments like those using Microsoft's Smooth Streaming or Apple's HTTP Live Streaming.

## Implementing MS3 functionality

MS3 specifications are available to Marlin Adopters or Participants from <http://www.marlin-community.com>

Intertrust provides both MS3 client and server module implementations as part of its Wasabi Media Suite. The server module is available as a small Apache module or CGI executable, and the client functionality is an integral part of the media client modules that also support Marlin Broadband functionality.

## Deploying MS3

MS3 Services require nothing more than a TLS certificate and a simple server module to generate SAS containers, along with readily available tools to encrypt and package content.

MS3 Clients need to be trusted by the service to comply with Marlin robustness rules in order to be allowed to access content keys. MS3 Clients that are also Marlin Broadband clients (as in Intertrust's implementation) can simply use the credentials issued to them by an existing MTMO authorized Trust Service Provider such as Seacert.