



**Solution Document Concerning the
FOO Broadband Solution
Athens Olympic Games 2004**

WORK SAMPLE

*Author:
Gordon Gus Gustafson
Entriq Solutions Engineer*

Table of Contents

1.	Introduction	1
2.	Critical Milestones:	1
3.	Project Organization and Support	2
4.	Summary of the IOC Guidelines	3
5.	Viewer Experience.....	4
6.	Technology Components	5
7.	Project Timescales	7
8.	Digital Rights Management using Entriq's Media Authorization Network.....	8
9.	Frequently Asked Questions:	11
10.	Contact Information	14

1. Introduction

This document concerns a technical solution identified by the European Broadcasting Union to ensure compliance with the International Olympic Committee "Internet Video Streaming Guidelines for the 2004 Athens Games".

The solution is provided by a best-of-breed partnership of two corporations: Entriq, a DRM security, billing, and customer service provider; and The CDN, the world's largest network.

Olympic content must be encrypted using Entriq's encryption tools, and then distributed via the content distribution network.

To integrate the solution, a participating FOO member will need to customize, brand and integrate html pages that contain calls to functionality within the CDN and Entriq networks. These pages (and accompanying guidelines) will be issued to Members on Monday 5th July.

In addition the FOO Member must integrate a code module that interacts with CDN's distribution network to ensure that URL's for the streams cannot be accessed except through a participating FOO Members website.

In order to ensure readiness in good time for the start of the Athens Olympics on August 13th, it is recommended that participating FOO members commence site integration shortly after the pack is released. Guidelines for integration timing are suggested in this document.

Each Member will be given a unique Entriq account so that on-line tools can be used to encrypt content and generate up-to-the-minute reports on its usage.

2. Critical Milestones:

Milestone	Date
Contract signed	29 June
Release of Information Document	1 July
Release of Integration Pack	5 July
Completion of site integration and customization	~26 July
Completion of QA/readiness for launch	8 August
Athens 2004 begins	13 August 2004

3. Project Organization and Support

Entriq and CDN are undertaking a development project to ensure that all components are ready for issue to FOO members by the 1st July. For information regarding timelines, planning or technical questions please contact:

XXX	Entriq Project Coordinator	XXX
Gordon Gus	Entriq Solutions Engineer	gus@entriq.com
XXX	CDN Technical Consultant	XXX

In addition please complete the Contact Table in the last section of this document and return to Guy Tennant by Monday 5th July.

Each participating FOO Member is responsible for ensuring that design, development and testing of the Olympic coverage portion of their website is completed in time for the event. To ensure that this deadline is achieved it is strongly recommended that each FOO Member appoint a single Project Manager, who has delivery responsibility for the overall solution.

Entriq and CDN will endeavor to comply with any timescales or tasks put forward by the FOO member subject to the overall timescales for delivery of our components committed in the project plan.

4. Summary of the IOC Guidelines

To ensure that rightsholder Territorial Exclusivities are honored, the IOC will only consider authorizing sound or moving images of Olympic action for distribution over the Internet if (1) it is in compliance with certain mandated distribution protocols, and (2) it is accompanied by an affirmative commitment to remedy any territorial breach of such content in good time, and in accordance with stipulated procedures.

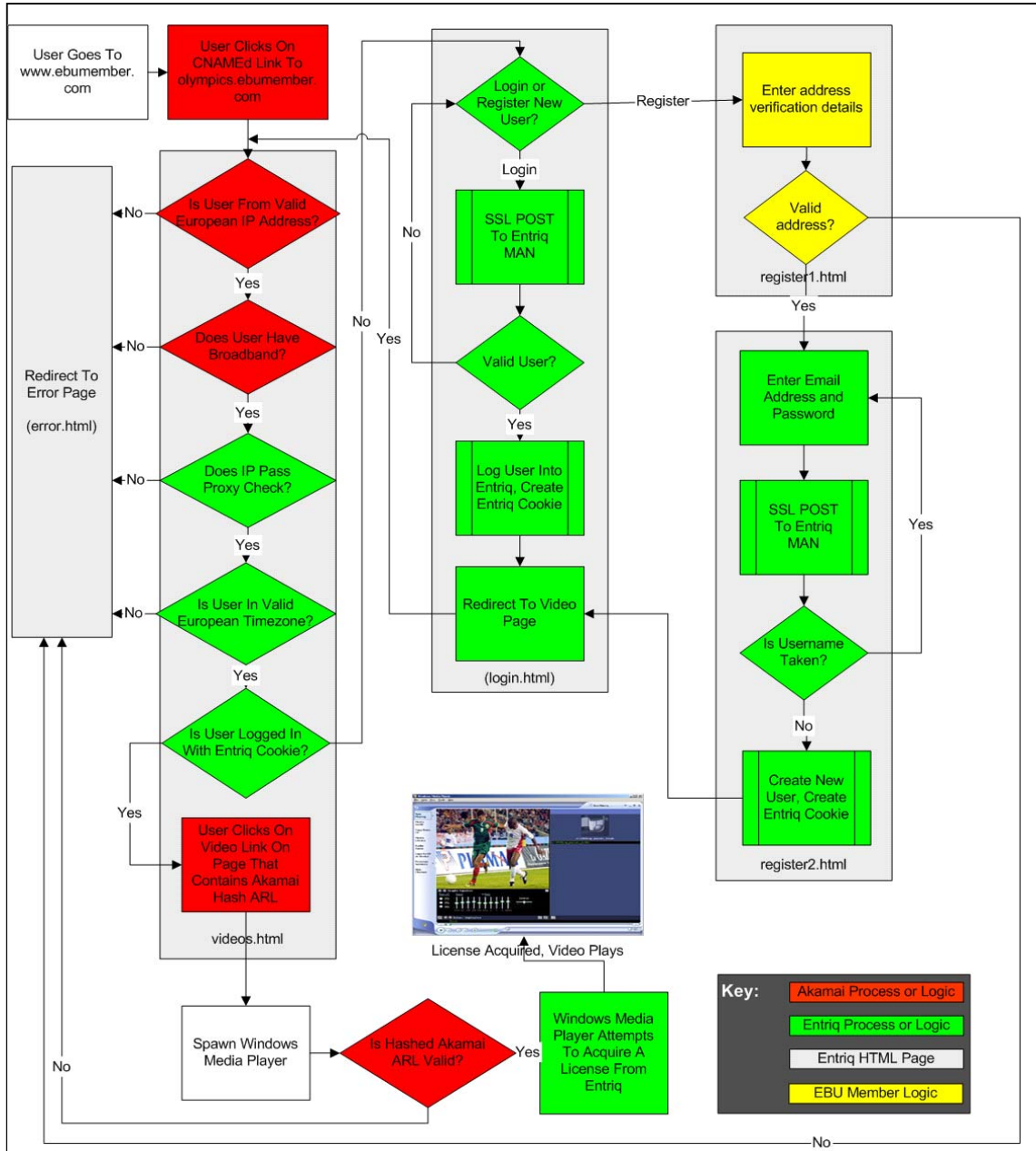
In short the protocols require:

- A territorial check to ensure that a viewer is located within Eurovision territory, which shall include: recording and geo location of a viewer's IP address; validation of their system clock time zone; and confirmation that their connection speed exceeds 100kbit/s.
- Viewer registration which must include some form of address verification.
- Stream link control to ensure that only viewers referred from authorized FOO Member websites can access Olympic streams.
- Content encryption to ensure that streams cannot be recorded and forwarded to bypass territorial checks and to enforce any commercial terms that may be imposed.
- A blacklist mechanism for IP addresses identified as being the source of abuse, which must be updated within 4 business hours of notification of any breach.
- A proxy detection mechanism capable of limiting the number of simultaneous streams per IP address, which will be augmented with an Exclusion list for known and agreed proxies.

5. Viewer Experience

The following diagram illustrates the viewer experience and the underlying sequence of tests that are executed when the Olympic content is accessed.

- Note: The pages supplied by Entriq assume the use of a Standalone Windows Media Player i.e. where the player opens independently of the web page. To modify the HTML to accommodate embedded media players please see FAQ's.



6. Technology Components

Validating territory:

- A viewer requesting an object (e.g., video link) from CDN will be subjected to a geographic location test based on an IP address lookup. CDNs are integrated with most major ISP networks worldwide and consequently have an unequalled database of IP address and network information. The check will be completed using Edge Side Include (ESI) code embedded on the video webpage (which must be hosted on the CDN network) so that rejected viewers can be redirected to an error page explaining that the content on the website is not available for viewers outside of that territory.
- A PC time zone check, implemented in javascript, which will redirect the rejected viewer to a similar page if the timezone offset is found to be outside of the Eurovision territory.

Validating connectivity:

- A connection speed check will be performed by ESI code based on a test run from the CDN EdgeServers. Connection determined to be under 100kbps will be redirected to an error page (carrying the logo of the FOO Member) explaining that connection speed has been determined to be below the minimum threshold required.

Viewer registration:

- The viewer will be required to register the first time that content is accessed in order to verify their address. Entriq will provide HTML pages that manage the registration of a unique email address and password, with tools to change or resend the password if it is forgotten.
- The FOO member must ensure that further information is captured that validates the user's physical address based using an appropriate mechanism within each FOO member territory. The implementation must be local to each member as there is no pan-European function available.
- Further attempts to access content from the viewer's PC outside of a 2-hour time window will require the viewer to login again.

File Encryption:

- Encryption of content occurs within the FOO member's domain on designated machines running Windows 2000, 2003 or XP. The encrypted file will include a unique item name as well as the URL of Entriq's globally distributed license server network. A viewer's media player will seek a license from this URL when attempting to access the file. If the user has a valid Entriq session cookie (that was obtained as a result of completion of the territorial and login checks) a license containing the secret key to decrypt the content will be sent to that player.
- Content encryption is a simple process using Entriq's on-line tool Media Manager. The tool encrypts files within a nominated directory (based on an ActiveX DLL downloaded to that PC automatically).

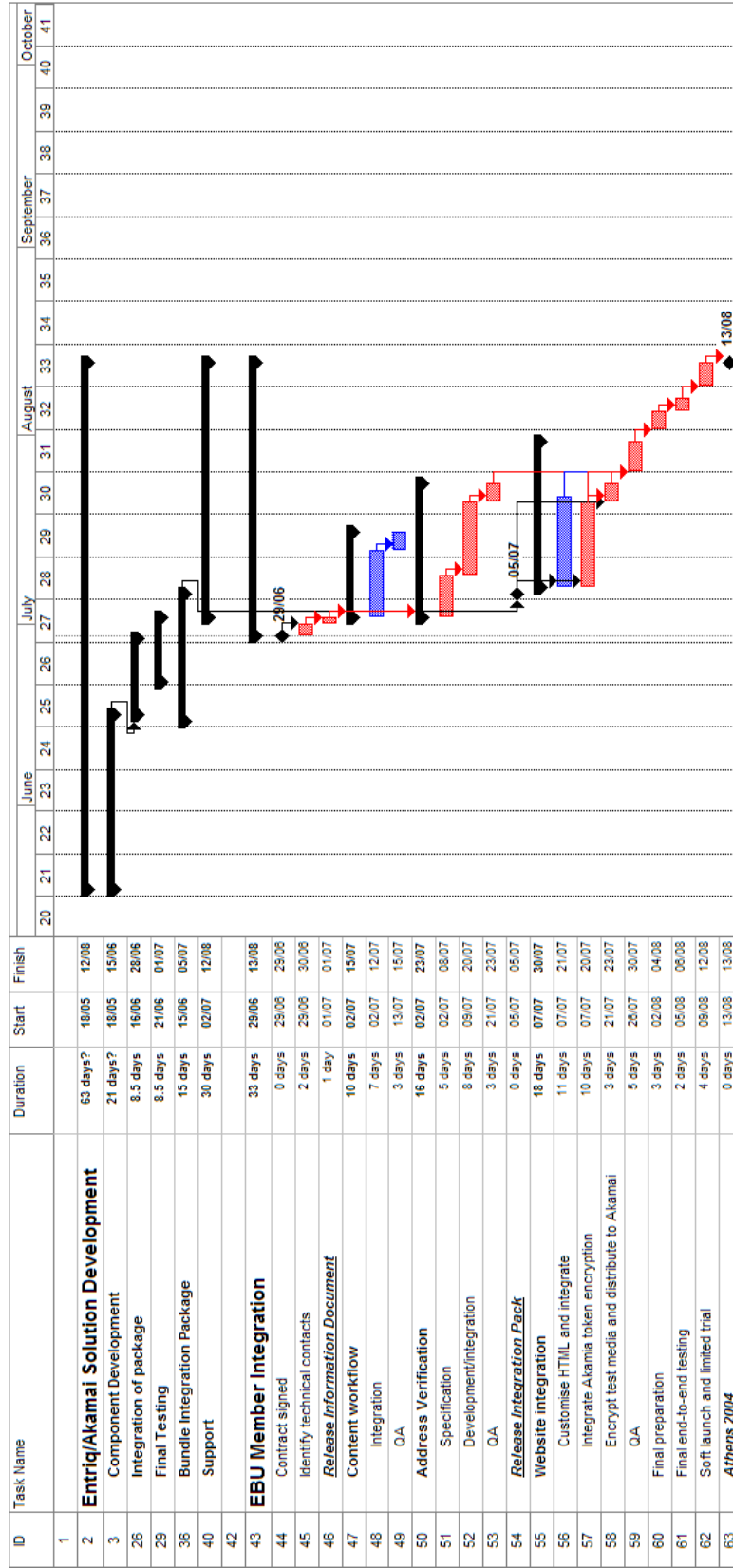
IP Proxy management:

- In order to comply with the IOC guidelines, Entriq is providing a central registry of Blacklisted IP addresses. If Entriq is so advised, IP Addresses will be added to this database within 4 hours of notification.
- Entriq will monitor the number of streams on a given IP address and will impose a maximum limit if the IOC advises that it is to be imposed (at the time of writing the Guidelines stated the IOC's intention not to impose this limit). Rejected users will be redirected to a customizable error page hosted on the FOO member's network.
- An Exclusion List exists so that known and approved proxies can be exempted from the global maximum.

URL restriction:

- CDN will provide code for integration into the FOO Member's website facilitating the use of the Streaming Authentication Service. The code appends a timestamped hash to the viewer's request, which proves that the viewer was referred by the FOO Member's site (and not cut-and-pasted into an IM chat, email or posted on a blog). The code can be provided in Perl, C, jsp or asp. Detailed information will be provided by the designated CDN contact person.

7. Project Timescales



Notes:

1. The minor timescale in the Gantt chart is shown in weeks numbered from 1st January 2004.
2. This document is shown as Task 46 in the plan and is intended to:
 - a. Suggest guideline timescales,
 - b. clarify the encryption process for the content management system workflow
 - c. allow time for finalization of the address verification mechanism in each territory
3. The Integration Pack will contain at least the following items:
 - a. Framework code for pages: video.html, error.html, login.html and Javascript to manage the tests described in this document.
 - b. Documentation describing the pages
 - c. Contact information for technical support
4. The timescales are provided as guide only. It is up to the FOO Member to ensure adequate resources are provided to facilitate the branding and layout of the html pages, integration of the CDN URL, Protection code, and performance of appropriate Quality Assurance procedures prior to launch.
5. It is suggested that the FOO Members plan to complete all works and testing before the beginning of August if possible.

8. Digital Rights Management using Entriq's Media Authorization Network

Entriq provides a security service on an Application Service Provider basis to content providers seeking to monetize their assets on the internet. Entriq's Media Authorization Network offers a set of internet based tools for setting up media policies to implement a wide variety of business models, such as subscription, syndication, and pay-per-minute/day/play etc. Access to content can be restricted by fields like geographic region, site membership, and media player or device. A wide variety of reports can then be obtained to monitor and analyze actual usage.

A content provider can integrate Entriq's encryption process into their content production and encoding workflow, and use Entriq to manage users and report on actual usage or revenue earned broken down by country, syndicator, content item or genre, referring website, and a variety of other categories depending on the business model selected.

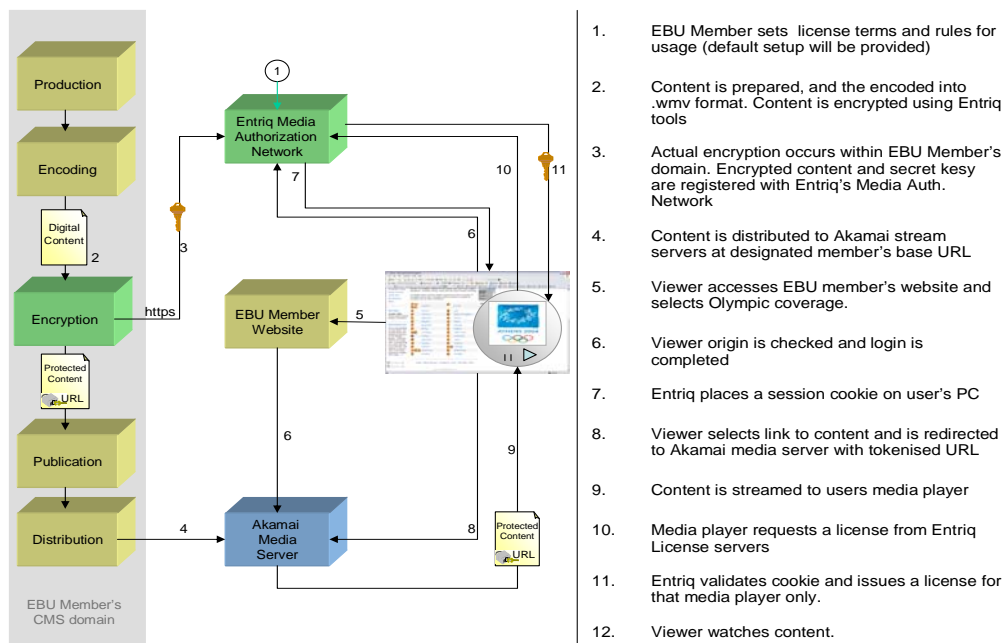
Integration with the Media Authorization Network is usually accomplished through a well defined and powerful XML (over http) API that is easy to incorporate into any website, whatever technology is used. This is the recommended mechanism for integration with an operator who maintains their own user database and controls the login procedure.

Public broadcasters who do not maintain a database of registered users have a more simple option available – integration of the html based login calls that execute on the client and cause the appropriate API calls to be made on the Entriq server side.

Entriq operates multiple license servers in fully redundant (no single-point-of-failure) peering facilities worldwide. This ensures that the network is robust, scalable, and reliable so that a content provider's business operation is never disrupted.

The Media Authorization network is format and DRM agnostic, providing common functions and reporting capability across multiple distribution channels and technologies.

Overview of Digital Rights Management Process:



Content Encryption using Entriq tools:

System Requirements:

- Encryption is accomplished using Entriq's on-line tool, the Media Manager. Encryption occurs locally i.e. the content files are never transferred out of the FOO Member's network.
- The machine used to access Media Manager must be running Windows 2000, 2003 or XP. Internet Explorer 6 must be used to ensure that the ActiveX encryption controls are downloaded from Entriq.
- In addition Windows Media Player version 9 must be installed on this machine to ensure that the latest DRM libraries are accessible.

Using Media Manager to encrypt a file:

Set Entriq up as a trusted site:

1. Start Internet Explorer.
 2. Select **Internet Options** from the **Tools** menu
 3. Select the **Security** tab, and click on the **Trusted Sites** icon.
 4. Select the **Sites** button immediately below and to the right.
 5. Make sure that the "**Require server verification (https:) for all sites in this zone**" flag is not checked
 6. Add <http://www.entriq.com> and <http://secure.entriq.com> to your trusted sites.
- NOTE: https will be made available on these domains before the Olympics commences. Entriq will announce the availability of https by notifying each FOO Member at a time to be determined around mid-July.

Accessing Media Manager

The Media Manager tool is accessed through an Entriq customer account, which can be found at the following URL: <http://www.entriq.com/support/members.html>.

1. Enter the user name and password
2. Select the **Media Manager** option from the menu on the left.
3. Click on the drop down menu next to the word "Register" on the blue header line and select **Windows Media Files**.
4. The first time that the tool is accessed the encryption and registration DLL will be downloaded from www.entriq.com. This utility is automatically downloaded and stored in the Windows directory on that system, and has no function other than to encrypt the media files nominated and then register the file name, ID, metadata and secret keys on the Entriq Media Authorization network. The encrypted file will remain on that system and will not be distributed to Entriq.
5. Thereafter a dialogue asking "if you wish to run an Active X control on this page" may appear, depending on the security settings of the machine. Select "yes".
6. Select a Channel ID. For the purposes of testing, Entriq has set up a simple free-to-air policy that will issue a license each time a request is made. This channel is called Test (free to air).
7. Check "yes" next to **Encrypt (DRM)**. Do not check **Access Control** which requires an Entriq plug-in to run on the media server (this functionality enables Pay Per Time business models and is not required for the Olympics).
8. Use the **Browse** button to locate the Windows Media Video (.wmv) file you wish to encrypt.
9. If batch encryption of all files in a directory is required, simply enter the directory name in the Input Directory box provided.
10. By default the encrypted file will be renamed and placed in the same directory. If you wish the file to be placed elsewhere, modify the URL of the output folder. The original media file will remain unchanged.
11. Select **Process and Register** to encrypt and register the file.
12. A pop-up should show a message that reads:

Registration Complete.	
Total Files Processed:	1
Successes:	1
Errors:	0

Confirming the Encryption Process Works

An encrypted file will be stored in the output folder setup in Media Manager, under the name E-<FOO_Member_name>-<Channel_Name>-<***original_file_name***>. It is almost the same size as the unencrypted file.

Double click on the file to open the Windows Media Player. The player will detect that the file is encrypted and will automatically seek a license at the URL embedded within the file during the encryption process. Entriq operates a network of license servers at this URL and upon receiving a license request will check the policies associated with that media item. If the item is associated with a free-to-air policy, and the user has been logged in and obtained a valid session cookie, the license will be issued. If the user is unknown, Entriq will redirect to a page hosted by the FOO member, called DRMconsole.html.

While the license is being acquired the media player will show the text "acquiring license..." just above the Play button. The media should play automatically once the license has been acquired and the media file decrypted, unless the viewer has disabled the "Acquire licenses automatically for protected content" flag in the players Security Settings, in which case the viewer will be prompted to accept the license.

Encryption Performance:

Processors clocked in excess of 2Ghz should encrypt at rate of 3MB per second or more.

9. Frequently Asked Questions:

Who supports end users/viewers and what is the path of escalation?

The FOO member is expected to provide the 1st line of customer/end user support. CDN and Entriq will provide 2nd line support to the FOO members in line with the Service Level Agreement. Final details and escalation procedures will be clarified in the week of the 19th July.

Will access to FOO coverage be restricted between members?

The FOO has recommended that FOO coverage is restricted to Europe but that any European may access any FOO Member's site that offers coverage.

Can the media access policies be changed to force a viewer to purchase content?

Please note that the Entriq-FOO Agreement calls for the Olympic content to be issued free of charge unless there is an additional agreement between Entriq and the FOO member that chooses to sell content.

What IOC Guidelines exist on address verification?

The IOC does not recommend a mechanism but requires that such a mechanism is implemented:

"Once a viewer passes the technical territorial validation, the viewer needs to be registered within an authorization database. The viewer must be asked to provide registration information to validate their residency. Examples of information which could validate residency include credit card billing, internet service provider billing, or cell phone billing."

In the US this will take the form of verification of credit card billing address. It is up to the FOO Member to propose a viable mechanism for their country.

How can an FOO Member track usage?

Each participating FOO Member has an Entriq account at <http://www.entriq.com/support/members.html>. Within the account Media Manager, User Manager and Channel Manager provide a variety of reports on number of licenses issued, number of unique users registered etc. that can be broken down by content item, or country.

A number of reports (e.g. financial) will only work when more complex business models are involved or when Entriq plug-ins are operating on the media servers.

Can a license cap be established so that variable costs can be contained within limits?

Entriq provides reporting capability based on statistics compiled from the live system database. Using these tools, an FOO Member can monitor the number of licenses issued to end users and can take action based on this data.

In order to contain variable costs associated with license generation, a member could modify the business rules associated with encrypted content without modifying the content files themselves. This would have an immediate effect on the end user seeking a license to view that content, who would be redirected to a URL of the FOO Member's choosing. The page at that URL would be generated by the FOO Member and could clarify the reasons for license denial.

Do I need to get an SSL certificate?

All login and register posts to Entriq are performed via SSL, so the page hosting the form does not need to be SSL to ensure secure submission. However an FOO Member is at liberty to protect the login and register pages by hosting them via SSL if they so wish.

The Integration Pack provided by Entriq assumes that the Windows Media Player will be standalone. How can the Integration Pack be adapted for sites where an embedded Windows Media Player is used?

The best practices associated with embedding a player on a web page are beyond the scope of the integration pack, and are best handled by suitably skilled web developers.

If such a format is desired, consideration will need to be given to such matters as:

- the inclusion of the geographic and proxy checks provided in the Entriq example code;
- the location/domain of the Entriq cookie;
- the placement of the login and address verification pages in the user flow;
- the mechanism used to load the embedded player with new encrypted media;
- compatibility with browsers other than Internet Explorer.

Please notify Entriq of your intentions so that more detailed discussions can be set up.

Many viewers will attempt to access the coverage from work. Please provide details on VPN Detection and IP Blocking.

In line with the IOC's "Internet Streaming Guidelines for the 2004 Athens Games" Entriq will provide a reporting mechanism that will identify instances where multiple streams are being accessed from one IP address simultaneously. This information will be provided to the FOO member and the IOC upon request.

Entriq may be mandated to impose a global limit on the number of streams that can be accessed per IP address. This value will be determined by the IOC.

The IP addresses of known corporate or ISP proxies, e.g. AOL or ZDF, can be entered into an Exclusion List which will exempt them from the global limit.

If so requested, Entriq will append any IP address where abuse is suspected to a Blackout List, which will disallow any further streaming to that site.

Is there an operating system check in the validation process?

There is no requirement to provide a check in the IOC guidelines. Individual FOO Members may choose to include object code that checks the OS in their web pages, and/or specify it in the FAQ and Terms and Conditions. The operating systems supported by Microsoft Windows Media Player 9 using DRM v7 are: Windows 98, Windows 2000, Windows Millennium Edition, Windows XP

What is Player Individualization?

A Windows Media Player will be individualized the first time that a license is received. The process converts the player to a unique entity with its own cryptographic keys that are used to ensure secrecy of the keys used to decrypt a media file when they are provided in a license. The process may involve the upgrade of some DRM components, which in some cases can generate messages for the user. Some broad guidelines for client facing FAQ's will be provided in Entriq's Integration Pack, but it is the responsibility of the FOO Member to provide FAQ's for and URL's for obtaining WMP 9 from Microsoft.

Where can I find info on Microsoft Windows Media Player 9?

For a list of WMP 9 FAQ's see:

<http://www.microsoft.com/windows/windowsmedia/9series/player/faq.aspx>.

Can the Real Player be used?

The Entriq/CDN solution for the Athens 2004 Project is only based on the use of Windows Media Player v7-v9.

Can we provide coverage to Apple Macintosh users?

Microsoft has a Media Player for the Macintosh, however the DRM library is based on the first version (v1), which cannot handle silent license delivery, offers a poor user experience, and is not as secure as DRM v7. Given IOC sensitivities to security and territorial restriction, Entriq would recommend that Mac coverage is not provided.

What about Linux?

No protected format has gained industry acceptance on the Linux platform at the present time.

Please provide some indication of benchmarks for the encryption process

As a guideline, a sample .wmv file encoded at 640x480, 1000kbps, duration 16:30s results in a file size of 130MB. This encrypts using Entriq's Media Manager tool in 50 seconds on a 1500Mhz Pentium M processor – an effective encryption rate of 2.6 MB per second.

File size is the prime determinant of encryption time. A reduction in bit rate and resolution to 350kbps and 340x288 respectively, encrypts on the same machine at the same effective rate.

Is there any way to operate the encryption process automatically?

Entriq has developed an Automated Registration Service (ARS) to facilitate the automatic encryption of content as part of a CMS workflow. The tool is currently only available as a Beta release.

It is intended to automate content encryption in production environments where a high number of files are produced frequently. The utility monitors a single directory and automatically encrypts any file dumped there by an upstream process (such as Encoding). Configuration of the utility is managed under the guidance of the Media Manager on-line tool, which is accessed from the FOO Member's Entriq account (see previous section). Once configured, the utility automatically loads whenever the server is booted.

For further discussion on the use of the ARS utility, please contact Entriq using the details provided in this document.

What is the Media Authorization Network (M.A.N)?

The Entriq global network for media authorization is a secure, reliable service accessible to any organization or individual that wants to distribute and sell online media.

Highlights:

- Average response time: 0.001 seconds per authorization
- High availability through use of redundancy and clustering, providing smooth handling of peak events
- Main and standby sites
- Co-location with high-speed direct connectivity to multiple Tier-1 network providers
- 24x7 system monitoring & services
- SSL-based system interfaces
- Access control to guarantee 1 (or n) streams per authorized user to prevent stream theft

Where can I find additional information on the Entriq M.A.N?

Information can be found on the Entriq website www.entriq.com and within the FOO Member account, where details of the API can be obtained in the Developer's section. In-line help and user manuals are provided for each tool.

10. Contact Information

Please complete the following table and return to XXX by email by no later than the 5 July.

Project Manager	Name: Email: Tel: Mobile:
Technical Lead	Name: Email: Tel: Mobile:
URL of FOO Member website	
Webserver technology platform and web development language	
Do you intend to use an embedded Windows Media Player? If so, have you already implemented it on your website?	
Do you have a user database? If so, what database technology do you use?	
What scheme do you propose for address validation?	