

The logo for Authentica, featuring the word "authentica" in a lowercase, sans-serif font. A vertical blue bar is positioned to the right of the text, partially overlapping the letter 'a'.

## Authentica Content Server

### Key applications

- **HIPAA**  
Adopt ARM internally or with trusted partners, while providing a Web based delivery solution for remote doctors and offices where IT support is limited and client desktops cannot be affected.
- **Executive Communications**  
Protect, deliver and manage sensitive, proprietary content to external recipients securely from the desktop without client-side requirements.
- **New Product Introduction**  
Protect, deliver and share sensitive specifications, pricing information, and other intellectual property with partners and suppliers easily.

Authentica's patented Active Rights Management (ARM) solution provides digital rights management software for securing business intellectual property. Designed for enterprise environments, ARM combines strong content security and digital rights management, and scalability in a client-server architecture. With ARM, information is always encrypted no matter where it's distributed and the author dynamically controls what recipients can do with this information after they have it. Recognizing that organizations cannot always control a recipient's message environment, Authentica has designed Content Server to provide an alternative secure delivery solution.

Integrating Authentica's MailRecall, PageRecall, and NetRecall protection technologies and the Authentica Policy Server, Content Server provides a single content delivery application. Content Server extends MailRecall by enabling customers to optionally deliver messages securely to external recipients without requiring client-side software. Furthermore, it extends PageRecall by providing a simplified Web solution for end users to protect and apply ARM protection policy to documents, deliver them to recipients, and then track document access activity after delivery. Authentica Content Server (ACS) enables organizations to address their security problems with investment in a single architecture.

### Choosing Active Rights Management or Secure Delivery

ACS wraps Authentica's patented technology in an easy to use Web-based application for securing, distributing and managing electronic content. ACS offers a choice between Authentica's full Active Rights Management (ARM) protection and simpler secure delivery on a file-by-file basis. Employing a Web mail interface to send and protect content, ACS enables users to simply manage their content permissions from the Web thereby minimizing administrator involvement.

ACS offers users the convenience of two delivery options. In the tradition of Active Rights Management, ACS can provide after delivery control of e-mails, electronic documents, and Web content if a corresponding Authentica client is installed on a recipient's desktop. However, for communications where an Authentica client is not or cannot be present, ACS offers a SSL secure delivery option.

- **Active Rights Management** – provides persistent information protection and encryption, the ability to recall documents or messages anytime after delivery control over message or document forwarding, life-cycle tracking of recipient activity, enforcement of print and copy rights on documents and messages even after content is downloaded to recipient's machine.
- **Secure Delivery** – provides file encryption, user authentication, secure file delivery, automatic read receipt and automatic delivery notification.

### How Content Server Works

ACS enables individual senders and applications to protect and deliver content to external recipients without IT administrator involvement. The server automates the delivery process by sending a delivery notification using a standard e-mail message. The message contains a URL reference to the protected information stored on the ACS. Recipients select the link and download content using their Web browser over a Secure Socket Layer (SSL) session. If the delivery is protected with ARM permissions, the recipient downloads the protected content and Authentica's Web Viewer or PageRecall plug-in

authenticate to the Authentica Policy Server to view it. In this mode content is always encrypted and ARM permissions are enforced even on a recipient's desktop. If ARM permissions are not applied, recipients authenticate and access content via their Web browser. The content is decrypted on the server and then passed to the recipient's browser over a SSL protected session.

Content can be delivered using three methods:

- **Individual Sender**

Senders login to a personalized Web page to access the ACS features. From this Web page, they can manage existing deliveries or compose new ones. When composing a delivery, the user selects a Send Message option which opens a Web mail interface. From here, the user defines recipients, creates messages, and uploads attachments. Once the delivery is created, the user selects the security method and associated permissions to apply; Secure Delivery or Active Rights Management. After the security options are set ACS sends delivery notifications to all the recipients.

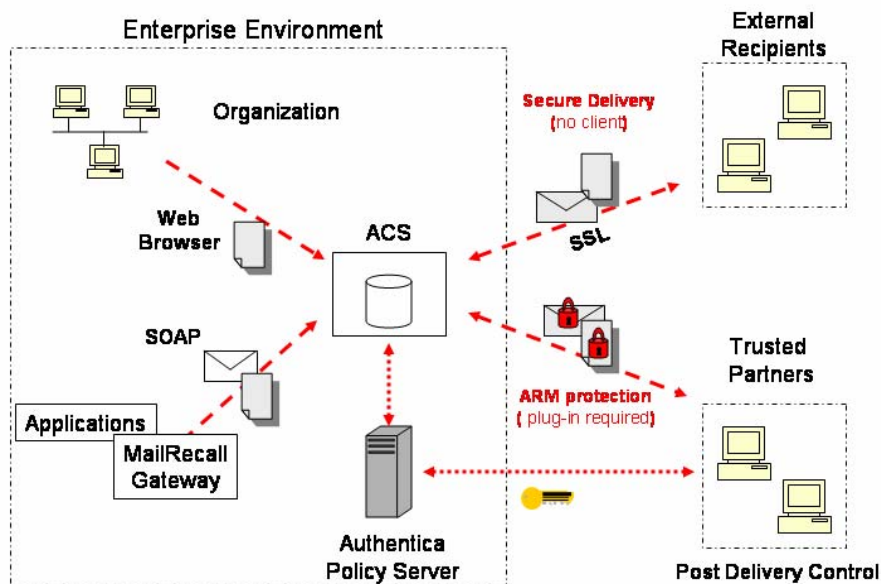
- **MailRecall Gateway Extension**

MailRecall Gateway is a plug-in to Baltimore/Content technologies MAILsweeper server. MAILsweeper scans and filters content prior to being protected by MailRecall Gateway. The gateway can protect e-mail messages on MAILsweeper and deliver the encrypted messages directly to the recipients. ACS extension provides MAILsweeper administrators an alternative secure delivery method for environments that cannot support client-side plug-ins. The extension allows e-mail messages to be channeled to ACS. This process can be made transparent to the sender. This alternate delivery method allows secure delivery of e-mail without a client plug-in.

- **SOAP API**

ACS provides a Simple Object Access Protocol (SOAP) API to allow any application to programmatically "push" content to the server to protect and deliver content.

**Figure 1: Authentica Content Server System**



## Features and Benefits

Features	Benefits
Option for Active Rights Management or Secure Delivery	<ul style="list-style-type: none"> <li>▪ Protect intellectual capital from loss or disclosure</li> <li>▪ Ensure confidentiality and privacy</li> <li>▪ Track activity of all access and use</li> </ul>
E-mail notification with embedded URL to secure content	<ul style="list-style-type: none"> <li>▪ Deliver secure content using recipient's existing Web browser and e-mail client</li> </ul>
Client-less solution for secure messaging and document delivery	<ul style="list-style-type: none"> <li>▪ Share documents securely without dependence on recipient desktop environment</li> </ul>
Automatic enrollment of external recipients	<ul style="list-style-type: none"> <li>▪ Register and view secure content without sender or administrator involvement</li> </ul>
Encrypt and deliver any type of content with secure delivery option	<ul style="list-style-type: none"> <li>▪ Deliver all data types securely: CAD data, worksheets, etc.</li> </ul>
Delivers large files	<ul style="list-style-type: none"> <li>▪ Reduce review-cycle time and resources</li> <li>▪ Leverage time and cost benefits of electronic information sharing</li> </ul>
Automatically generate read receipt	<ul style="list-style-type: none"> <li>▪ Prove content was accessed by authenticated recipients</li> </ul>
Web-based delivery management	<ul style="list-style-type: none"> <li>▪ Send, track, and manage content delivery from a personalized Web page</li> </ul>
Digital certificates, NT domain, LDAP directories for authentication	<ul style="list-style-type: none"> <li>▪ Meet a variety of deployment security requirements with ACS capability</li> </ul>
Recipient can reply to Web messages	<ul style="list-style-type: none"> <li>▪ Enable secure collaboration without recipient client requirements</li> </ul>
MailRecall Gateway can pass e-mail messages to ACS for secure delivery	<ul style="list-style-type: none"> <li>▪ Apply secure delivery or ARM protection based on recipient environment</li> </ul>
Java based Web server application utilizes the Authentica Policy Server	<ul style="list-style-type: none"> <li>▪ Transparent and secure encryption key management</li> <li>▪ Authentication and policy management capabilities</li> <li>▪ 128-bit encryption strength and data integrity</li> </ul>
Utilize MS SQL Server or Oracle for internal database	<ul style="list-style-type: none"> <li>▪ Scale system to meet high load or failover needs</li> </ul>

### Specifications:

Authentica Content Server: MS Internet Information Server 5.0, iPlanet Web server, Enterprise Edition 6.0 on Microsoft Windows 2000

Authentica Policy Server: Microsoft Windows NT/2000, Sun Solaris 2.6 and 8

**Contact: ReSoft International - 203 972 8462 - [www.re-soft.com](http://www.re-soft.com) - [info@re-soft.com](mailto:info@re-soft.com)**