THE CLIPPER GROUP

Navigator™

Navigating Information Technology Horizons℠

Published Since 1993 Report #TCG2004102 December 23, 2004

Authentica Active Rights Management — Rights That Go with the (Data) Flow

Analyst: Anne MacFarland

Management Summary

Active data has a restless, peripatetic lifecycle. It is distributed here and there, copied onto thumb drives, and forwarded as an attachment, always in a good or justifiable cause. **However, in many cases, the enterprise, at some point, loses control of the use of its data.** Authentication of users, and file system and database dataset locking are great as long as the information is stays in the application or is stored in a file system or database. But, these days, that is by no means assured. Common presentation applications make it relatively easy to open from data from wherever, and people certainly do. Data copying is a routine that has been optimized for speed and transparency, and is often done by end users for convenience without regard for security considerations. Now, data is exposed to still more risks via new enterprise data initiatives for collaboration, data integration, and enterprise search that export from the protective environment of the application that generated it, plus more frequent collaboration with folks outside the bounds of enterprise IT systems. The enterprise may not anticipate these risks, but it will be held responsible for any misuse of data that occurs. *Creator beware!*

To add fuel to the fire, **the concept of the enterprise is expanding**. Joint projects, temporary alliances, increasingly close relationships with fickle customers are becoming a normal part of business life. The need to close deals and generate revenue demands that information be promptly shared. Even in the halls of academia, there is a new impatience with the unwillingness of researchers to share information before the proper journal articles have been published. And in today's highly competitive business environment, you don't want stumbling blocks of paranoia to poison your relationships with the partners upon whom you depend for essential services, and for entry into new markets. **You do not always have time to build dependable trust relationships.**

You need to safeguard your sensitive data. Government regulations may demand that you do so, and be able to prove that you have. **Many enterprises in the paranoid branches of government and industry are well aware of this peril, and have concluded that the risk cannot be mitigated by only a centrally managed system, but must be complimented with protection that moves with the data.** Enterprises like these form the initial customer base of Authentica, Inc., based in Lexington Massachusetts. For more details of Authentica's products, read on.

IN THIS ISSUE

Enterprise Use of Data

Enterprises' use of data is changing.

- There are more significant partners with whom intellectual property must be shared.
- An enterprise has more supply and distribution relationships where access to the needed information (but not more than the needed information) is key to prosperity for all involved.
- Enterprises have more initiatives and projects whose documentation must be controlled and, at the end of the project, retired from distribution.
- More of the data that is shared is *changing data* (inventories, etc.) where the use of stale data must be prevented.
- And, for many enterprises, more interaction with competitors is common.

It is not enough that you have to be able to search your email files for evidence of wrongdoing. **Proper governance demands that confidential information be protected and the intellectual property rights not be compromised.** Government regulations, where applicable, add immediacy to that demand.

Authentica

Authentica has taken its concept of a robust policy server and a powerful enforcing data-based agent and produced an *Active Rights Management (ARM)* platform that addresses the specific data risk exposures of Financial Services, Government, Health Care, and Manufacturing. It has recently launched Authentica Secure Office to help enterprises more securely share Microsoft *Office* files.

These different offerings all use the same enforcement mechanism. The Policy Server is where digital rights are set and evolved as situations change, and where users are authenticated[1]. The local agent initiates authentication and subsequently enforces limitations on what an authenticated user may be able to do with a document – the ability to view, edit, copy, print, and forward. An authenticated user may be enabled to use a document while offline. In that case, the agent will send a usage log to the server when a connection to the Internet is restored. The policy server generates an audit log of who has accessed the document and what was done with it.

The creator of a document controls the enablement and expiration of the watermark. The creator may choose to change the rights profile of a document over its lifecycle, or the rights of a specific user, upon termination of employment, for example. When the local agent contacts the policy server before opening a document, the policy changes will be enforced. This is useful for controlling the information access of terminated employees. It also ensures that stale data will not be used inappropriately.

If a document is printed, a watermark of where and when it came from prints out. If it is scanned, the watermark persists. Screen scraping does not remove the watermark either.

The digital rights capability is what most if not all enterprises, large and small, need to do data protection properly. That alone will increase an enterprise's ability to share information freely when it is appropriate. It lets enterprises work effectively with entities they do not trust.

The audit trail is what many enterprises need to meet the end-to-end documentation involved in compliance with government regulations. The visibility it gives into internal business processes and information flows is a side benefit whose value may only become evident over time.

If content creation is your business, you may need a *use trail.* Authentica can tell you what actually has been read and how profligately it has been forwarded. This can guide what you produce and how you adjust your business model to ensure both customer satisfaction and profitability. Moreover, of

[1] Authentica supports multiple authentication systems (digital certificates, user ID, etc.) in order to leverage existing user environments.

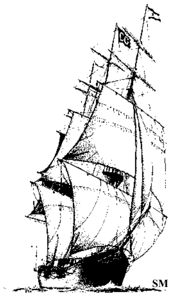
course, Authentica's Active Rights Management can prevent unwarranted re-distribution.

How to Deploy

Authentica's Active Rights agent plugs into Adobe (*Acrobat*), Lotus (*Notes*), Microsoft (*Explorer* Web browser, *Office*, and *Outlook*), and the Netscape's Web browser. The Policy Management Server application is integrated with Content Management Solutions from Documentum, eRoom, Filenet (*Content Manager)*, Hummingbird (*DM),* IBM/Lotus (*Notes Domino*), and Microsoft (*SharePoint*). Services for implementation (fixed fee), customization (consultancy), and technical support (8 x 5 or 24 x 7) are available.

Conclusion

If data is sensitive or worthy of regulated access, there is an obvious need for Authentica's kind of local, data-centric control. If you wish to have any control over the content you produce, the need is just as clear. Moving from simple authentication to active data rights management is similar to the move from increasingly inadequate firewalls to a multi-faceted approach to security. Your systems deserved the improved security. Your data deserves no less.



About The Clipper Group, Inc.

The Clipper Group, Inc., is an independent consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 25 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

- ***The Clipper Group can be reached at 781-235-0085 and found on the web at www.clipper.com.***

About the Author

Anne MacFarland **is Director of Enterprise Architectures and Infrastructure Solutions for The Clipper Group.** Ms. MacFarland specializes in strategic business solutions offered by enterprise systems, software, and storage vendors, in trends in enterprise systems and networks, and in explaining these trends and the underlying technologies in simple business terms. She joined The Clipper Group after a long career in library systems, business archives, consulting, research, and freelance writing. Ms. MacFarland earned a Bachelor of Arts degree from Cornell University, where she was a College Scholar, and a Masters of Library Science from Southern Connecticut State University.

- ***Reach Anne MacFarland via e-mail at Anne.MacFarland@clipper.com or at 781-235-0085 Ext. 28. (Please dial "1-28" when you hear the automated attendant.)***

Regarding Trademarks and Service Marks

The Clipper Group Navigator, **The Clipper Group Explorer**, **The Clipper Group Observer**, **The Clipper Group Captain's Log**, and *"clipper.com"* are trademarks of The Clipper Group, Inc., and the clipper ship drawings, *"Navigating Information Technology Horizons"*, and *"teraproductivity"* are service marks of The Clipper Group, Inc. The Clipper Group, Inc., reserves all rights regarding its trademarks and service marks. All other trademarks, etc., belong to their respective owners.

Disclosure

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.

Regarding the Information in this Issue

The Clipper Group believes the information included in this report to be accurate. Data has been received from a variety of sources, which we believe to be reliable, including manufacturers, distributors, or users of the products discussed herein. The Clipper Group, Inc., cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.