

SecureDIMM

Protect Sensitive Data

As laser printers assume an expanding role, they are often called upon to print proprietary, confidential, or otherwise sensitive documents.

Accounting, Engineering, Human Resources, Marketing, Payroll, Production, and Sales - every department within your organization is using laser printers to print an ever-growing array of sensitive data. From market strategy to client information, much of the information printed on corporate printers is confidential in nature. If this data is diverted into the wrong hands, corporate competitiveness and success can be irreparably damaged. If it is being used to output checks, drafts or other financial documents, modifications to the data stream (for example, altered check values) can translate into immediate and direct financial losses.

Most corporations have established security programs to protect the databases where their sensitive data resides in its raw form. The data however, is usually still vulnerable to unauthorized access and modification as it travels to a printer. The most ironic part of this security hole is that it exists at the precise point in time when the data is often formatted in a manner to be most useful to a nefarious party. This vulnerability can seriously impair corporate security and even expose an enterprise to unnecessary legal liability.

The Capella Technologies SecureDIMM

The Capella Technologies SecureDIMM is an integral component of a comprehensive solution that protects sensitive print job data using advanced encryption technology. When a document is printed the data is often stored in spool files, where it can be viewed, or even altered, with tools as simple as the Microsoft Windows Notepad program. More technically savvy users can even intercept the data directly from the network as it travels to the printer. Even simple mistakes such as directing a print job to the wrong printer can unintentionally expose sensitive data.

SecureDIMM makes it possible to protect sensitive print job data by encrypting it and thus making it indecipherable to humans and printable only by specific printers.

SecureDIMM contains firmware that is executed by the microprocessor in the LaserJet printer. This firmware extends

the printer with sophisticated data decryption capabilities. Encrypted data is decrypted at its final destination, inside the printer.

In the absence of the decryption commands, the printer continues to function like any standard LaserJet printer, providing maximum investment efficiency. Both encrypted and standard jobs have complete access to other optional printer enhancements such as fonts, page description languages and other Capella Technologies printer enhancement filters.

Advanced Encryption Technology

The SecureDIMM utilizes the Rijndael encryption algorithm. The National Institute of Science and Technology (NIST) has selected Rijndael as the new Advanced Encryption Standard (AES). The NIST is an agency of the United States Commerce Department's Technology Administration.

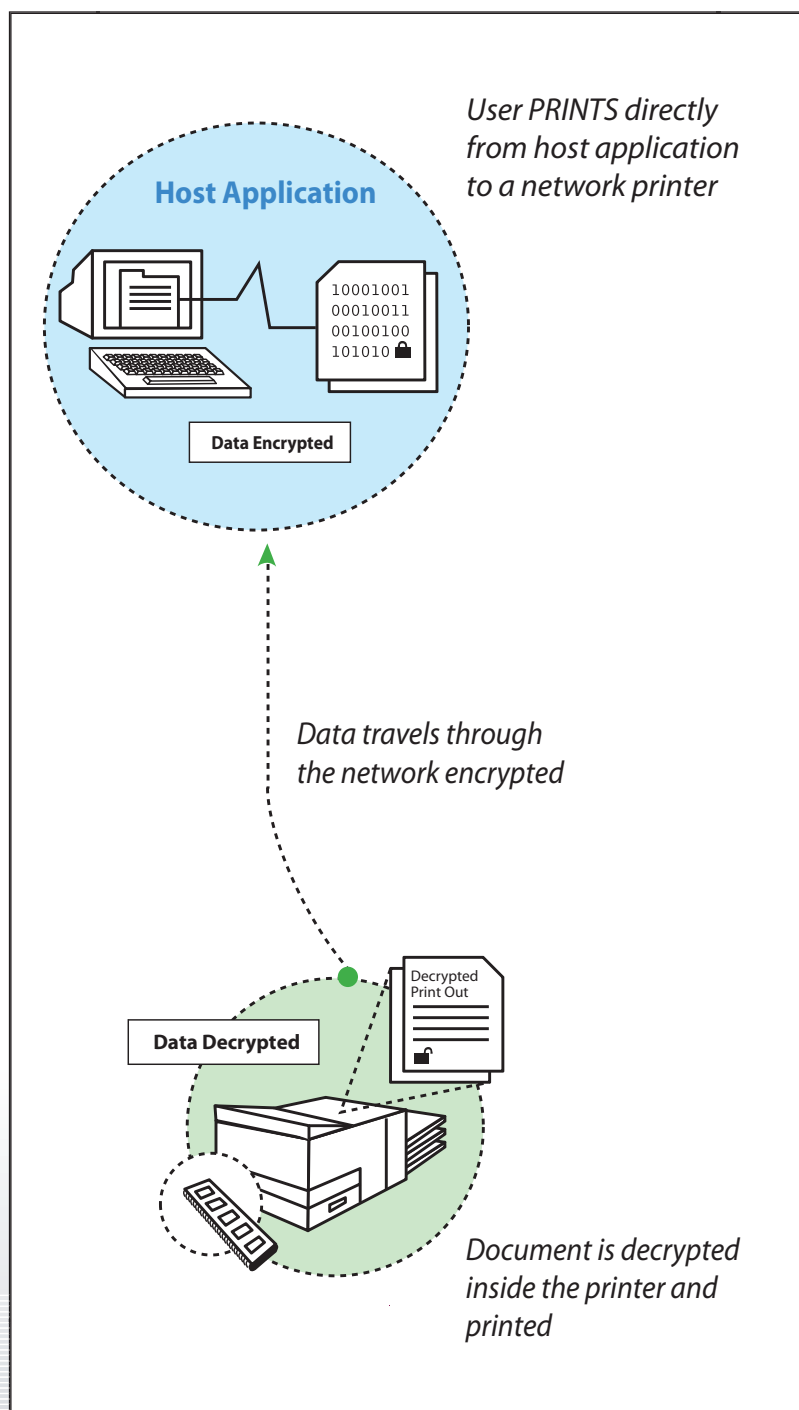
Incorporating the SecureDIMM into a Complete Encryption Solution

The SecureDIMM itself is only half of the equation. Before the DIMM can decrypt data, the data must first be encrypted. Capella Technologies offers a variety of methods for accomplishing this task.

For users operating in the Microsoft Windows environment, a port monitor is available to provide a transparent encryption capability available to all programs.

For users of other operating systems, Capella offers a simple encryption filter. As a print job is passed through this filter, it is encrypted and wrapped with the special decryption commands used by the SecureDIMM.

For the greatest level of security, Capella supports incorporating encryption directly into the application programs that create printer data streams. Capella can assist corporate customers and software developers with modifying their applications specifically for this purpose.



Conclusion

At the enterprise level, we go to great lengths to guard our corporate data resources. We secure the physical access to our buildings with locks and employee badges. We protect our computers and databases with passwords. The Capella Technologies SecureDIMM extends protection to our data when it is most vulnerable - as it is being printed. By immediately encrypting print jobs at their source and decrypting them only within the printer, we eliminate one of the weakest links in the typical corporation's security scheme and insure the privacy of its confidential information. Indeed, an effective output encryption strategy is essential to any enterprise that values its printed data.

Capella Technologies Quality and Experience

Capella Technologies, Inc. specializes in Output Management solutions that enhance, track and secure your documents. Capella Technologies can help your organization review and improve your processes around business to business transaction documents. Our products can help you to;

- Improve efficiencies
- Reduce cost
- Improve customer service
- Improve your corporate image
- Improve document print security

About Capella Technologies, Inc.

Capella Technologies provides Document Output Management & Job Accounting products which enable companies to format, print, monitor, allocate, archive, distribute and secure business-critical documents in the most cost-effective way possible.

To learn more about Capella Technologies' Secure DIMM or other products, please visit our website at www.capellatech.com or email sales.info@capellatech.com.

*The information contained in this document is subject to change without prior notice.
All trademarks and registered trademarks are the property of their respective companies.*