SCM MICROSYSTEMS INC
Form 425
April 14, 2009

Filed by SCM Microsystems, Inc.
pursuant to Rule 425 under the Securities Act of 1933
Subject Company: Hirsch Electronics Corporation
Commission File No.: 333-157067

ANNUAL REPORT ON FORM 10-K

On March 31, 2009, SCM Microsystems, Inc. filed with the Securities and Exchange Commission its Annual Report on Form 10-K for the year ended December 31, 2008, which is reproduced below as Appendix A to this filing.

CONSENT OF INDEPENDENT REGISTERED PUBLIC ACCOUNTING FIRM

The consent of Deloitte & Touche GMBH, the independent registered public accounting firm of SCM Microsystems, Inc., is attached below as Appendix B to this filing.

In connection with the proposed merger transaction involving SCM Microsystems, Inc. (SCM) and Hirsch Electronics Corporation (Hirsch), SCM has filed with the Securities and Exchange Commission (SEC) a registration statement on Form S-4 (No. 333-157067), which was declared effective on February 13, 2009. The definitive joint proxy statement/information statement and prospectus dated February 13, 2009 was first mailed to stockholders of SCM and shareholders of Hirsch on February 18, 2009. SCM has filed other documents regarding the proposed transaction with the SEC and may file additional documents regarding the proposed transaction as well. SECURITYHOLDERS OF SCM AND HIRSCH ARE URGED TO READ THE REGISTRATION STATEMENT, JOINT PROXY STATEMENT/INFORMATION STATEMENT AND PROSPECTUS, AND OTHER DOCUMENTS FILED WITH THE SEC REGARDING THE PROPOSED MERGER CAREFULLY AND IN THEIR ENTIRETY BECAUSE THEY CONTAIN IMPORTANT INFORMATION ABOUT THE PROPOSED TRANSACTION.

Stockholders of SCM and shareholders of Hirsch may obtain a copy of the joint proxy statement/information statement and prospectus, as well as other filings containing information about SCM and Hirsch, without charge, at the SEC s Internet site (http://www.sec.gov). Copies of the joint proxy statement/information statement and prospectus can also be obtained, without charge, from the SCM corporate website at www.scmmicro.com, or by directing a request to SCM Microsystems, Inc., Attention: Investor Relations, 41740 Christy Street, Fremont, California 94538, or to Hirsch Electronics Corp, 1900 Carnegie Avenue, Bldg B, Santa Ana, California 92705, Attention: Secretary.

In addition to the documents described above, SCM files annual, quarterly and current reports, proxy statements and other information with the SEC, which are available at the SEC s website at www.sec.gov or at SCM s website at www.scmmicro.com.

THIS FILING IS FOR INFORMATION PURPOSES ONLY AND SHALL NOT CONSTITUTE AN OFFER TO SELL OR THE SOLICITATION OF AN OFFER TO BUY SECURITIES, NOR SHALL THERE BE ANY SALE OF SECURITIES IN ANY JURISDICTION IN WHICH SUCH SOLICITATION OR SALE WOULD BE UNLAWFUL PRIOR TO REGISTRATION OR QUALIFICATION UNDER THE SECURITIES LAWS OF SUCH JURISDICTION.

SCM Microsystems and its directors, executive officers and other employees may be deemed to be participants in the solicitation of proxies from the stockholders of SCM in connection with the proposed transaction. Information about SCM s directors and executive officers is available in the joint proxy statement/information statement and prospectus and other materials referred to in the joint proxy statement/information statement and prospectus.

Appendix A

UNITED STATES SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

Form 10-K

þ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**
For the fiscal year ended December 31, 2008

or

o **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**
For the transition period from to

COMMISSION FILE NUMBER 0-29440

SCM MICROSYSTEMS, INC.
(Exact Name of Registrant as Specified in its Charter)

DELAWARE *(State or other jurisdiction of* *Incorporation or organization)*	**77-0444317** *(I.R.S. Employer* *Identification Number)*
Oskar-Messter-Strasse 13, Ismaning, Germany *(Address of Principal Executive Offices)*	**85737** *(Zip Code)*

Registrant s telephone number, including area code:
+49 89 95 95 5000
Securities Registered Pursuant to Section 12(b) of the Act:
None
Securities Registered Pursuant to Section 12(g) of the Act:
Common Stock, $0.001 par value, and associated Preferred Share Purchase Rights
(Title of Class)

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes o   No þ

Indicated by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. Yes o   No þ

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes þ   No o

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K is not contained herein, and will not be contained, to the best of registrant s knowledge, in definitive proxy or information statements or any amendment to this Form 10-K. þ

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, or a smaller reporting company. See the definitions of large accelerated filer,   accelerated filer and smaller reporting company in Rule 12b-2 of the Exchange Act. (Check one):

Large accelerated filer o	Accelerated filer o	Non-accelerated filer o (Do not check if a smaller reporting company)	Smaller reporting company þ

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes o   No þ

Based on the closing sale price of the Registrant s Common Stock on the NASDAQ National Market System on June 30, 2008, the last business day of the Registrant s most recently completed second fiscal quarter, the aggregate market value of Common Stock held by non-affiliates of the Registrant was $35,159,238.

At March 23, 2009, the registrant had outstanding 15,743,515 shares of Common Stock.

SCM Microsystems, Inc.

Form 10-K
For the Fiscal Year Ended December 31, 2008

TABLE OF CONTENTS

Page

PART I

PART II

PART III

PART IV

SCM, the SCM logo, @MAXX, CHIPDRIVE, and SmartOS are registered trademarks and Opening the Digital World is a trademark of SCM Microsystems, Inc. Other product and brand names may be trademarks or registered trademarks of their respective owners.

PART I

This Annual Report on Form 10-K, including the documents incorporated by reference in this Annual Report, contains forward-looking statements within the meaning of Section 27A of the Securities Act of 1933, as amended, and Section 21E of the Securities Exchange Act of 1934, as amended (the Exchange Act). For example, statements, other than statements of historical facts regarding our strategy, future operations and growth, financial position, projected results, estimated revenues or losses, projected costs, prospects, plans, market trends, competition and objectives of management constitute forward-looking statements. In some cases, you can identify forward-looking statements by terms such as believe, could, should, would, may, anticipate, intend, plan, estimate, expect, proj
these terms or other similar expressions. Although we believe that our expectations reflected in or suggested by the forward-looking statements that we make in this Annual Report on Form 10-K are reasonable, we cannot guarantee future results, performance or achievements. You should not place undue reliance on these forward-looking statements. All forward-looking statements speak only as of the date of this Annual Report on Form 10-K. While we may elect to update forward-looking statements at some point in the future, we specifically disclaim any obligation to do so, even if our expectations change, whether as a result of new information, future events or otherwise. We also caution you that such forward-looking statements are subject to risks, uncertainties and other factors, not all of which are known to us or within our control, and that actual events or results may differ materially from those indicated by these forward-looking statements. We disclose some of the factors that could cause our actual results to differ materially from our expectations in the Customers, Research and Development, Competition, Proprietary Informatio
and Technology and Risk Factors sections and elsewhere in this Annual Report on Form 10-K. These cautionary statements qualify all of the forward-looking statements included in this Annual Report on Form 10-K that are attributable to us or persons acting on our behalf.

ITEM 1. *BUSINESS*

Overview

SCM Microsystems, Inc. (SCM, the Company, we and us) was founded in 1990 in Munich, Germany and incorporated in 1996 under the laws of the state of Delaware. We design, develop and sell hardware and system solutions that enable people to conveniently and securely access digital content and services. We sell our secure digital access products in two market segments: Secure Authentication and Digital Media and Connectivity.

For the Secure Authentication (previously referred to as PC Security[1]) market, we offer a full range of smart card reader technology solutions to address the need for smart card-based security in a range of applications and environments, including PCs, networks, physical facilities and authentication programs. Our Secure Authentication products enable authentication of individuals for applications such as electronic passports and drivers licenses, electronic healthcare cards, secure logical access to PCs and networks, and physical access to facilities. We also offer a range of smart card-based productivity solutions, which include readers and software, for small and medium-size businesses under our CHIPDRIVE® brand.

For the Digital Media and Connectivity (previously referred to as Digital Media Reader[2]) market, we offer commercial digital media readers that are used in digital kiosks to transfer digital content to and from various flash media.

We sell our Secure Authentication products primarily to original equipment manufacturers (OEMs) that typically either bundle our products with their own solutions, or repackage our products for resale to their customers. Our OEM customers typically sell our smart card reader technology to government contractors, systems integrators, large enterprises and computer manufacturers, as well as to banks and other financial institutions. In some cases, we also sell directly to system integrators and government contractors. We sell our CHIPDRIVE

[1] We revised our name for this market segment to Secure Authentication to better reflect the broader range of applications we now address, including contactless payment, electronic healthcare, logical and physical access and other applications that require secure authentication of users.

[2] We revised our name for this market segment to Digital Media and Connectivity to reflect the benefits of our readers as connectivity solutions.

solutions through resellers and the Internet. We sell our digital media readers primarily to major brand computer and photo processing equipment manufacturers. We sell and license our products through a direct sales and marketing organization, as well as through distributors, value added resellers and systems integrators worldwide.

On October 1, 2008, we entered into a Stock Purchase Agreement with TranZfinity, Inc. (TranZfinity), pursuant to which SCM purchased 10 million shares of TranZfinity common stock, or 33.7% of TranZfinity s outstanding shares (16.67% on a fully diluted basis), for an aggregate purchase price of $2.5 million. The transaction closed on October 2, 2008. We also entered into a Stockholders Agreement with TranZfinity and certain other stockholders of TranZfinity, which sets forth certain rights and privileges of SCM and the other stockholders of TranZfinity, including rights and privileges with respect to the composition of TranZfinity s Board of Directors.

On December 10, 2008, we entered into an Agreement and Plan of Merger with Hirsch Electronics Corporation (Hirsch), a privately held California Corporation that manufactures and sells physical access control and other security management systems. Our special meeting of stockholders to vote upon the merger was adjourned on March 23, 2009, and a new meeting is scheduled for April 16, 2009. We expect the closing of the proposed merger to occur once certain closing conditions have been met. Upon the closing of the proposed merger, Hirsch is expected to become a Delaware limited liability company and wholly-owned subsidiary of SCM and the securityholders of Hirsch will receive cash, shares of SCM common stock and warrants to purchase SCM common stock as consideration for the merger. For further discussion of the proposed merger, see *Growth Strategies* in Part I, Item 7, Management s Discussion and Analysis of this Annual Report on Form 10-K.

Recent Trends and Strategies for Growth

In 2006 and 2007, we directed significant attention to improving the efficiency of our operations, which resulted in a reduction in expenses from previous levels, close management of continuing expenditures and ongoing reductions in product and manufacturing costs. Top line revenue growth has been more difficult to effect, as U.S. and European government programs, which comprise a significant portion of our sales, have remained unpredictable in terms of timing and in some cases have experienced protracted delays.

In late 2007, we embarked on a multi-pronged strategy to expand and diversify our customer base, fully capture emerging market opportunities and accelerate long-term growth. The primary component of the strategy is the development of a range of new contactless and near field communication (NFC) infrastructure products to enable fast growing contactless applications and services for the electronic transaction market (including payment and ticketing), government and enterprise customers. Additionally, we are developing programs to market our existing product offerings into new geographic regions. To ensure appropriate resources for our contactless and expansion strategies, we have strengthened our management team with the addition of marketing, engineering and product management professionals from the contactless industry to execute our contactless product roadmap, including the hiring of our CEO, Felix Marx, in October 2007. Further, we have adopted a more active approach to partnering with other companies that can provide complementary resources and strengths. For example, in mid-2008, we collaborated with XIRING, a French security solutions company, to develop a mobile eHealth terminal for the German electronic health card system. In April 2008, we began working with TranZfinity, a provider of e-payment transactions solutions, to develop our @MAXX® family of contactless readers and to provide application services for those readers; and in October 2008 we took an equity position in TranZfinity, as described above.

An additional component of our multi-pronged growth strategy is to actively seek merger and acquisition opportunities to expand our business, reinforce our market position in targeted areas and fully leverage our strengths and opportunities, such as our proposed merger with Hirsch, as described above. We believe our proposed merger with Hirsch supports our growth strategy, as we anticipate it will nearly double our revenues, diversify our customer base and position our company to better address the growing market demand for solutions that address both IT security and physical access.

We have been investing in new products, resources, programs and business development activities to support the growth strategies described above and in 2008 this has resulted in increased operating expenses year over year. We believe these investments are critical to the success of our growth strategies and we expect to continue to invest in these strategies in the future.

Overview of the Market for Secure Access and Authentication Solutions

Individuals, businesses, governments and educational institutions increasingly rely upon computer networks, the Internet and intranets for information, entertainment and services. The proliferation of and reliance upon electronic data and electronic transactions has created an increasing need to protect the integrity of digital data, as well as to control access to electronic networks and the devices that connect to them. For government entities and large corporate enterprises, there is a need to restrict and manage access to shared networks and intranets to prevent loss of proprietary data. In addition, there is a need to manage and monitor access to information stored on identification cards used in new government-driven programs around the world, such as electronic passports, driver s licenses, citizen identification and electronic healthcare cards. In some cases, there may also be a need to expand the capability of electronic networks to protect or restrict access to physical facilities for corporate employees or government personnel. Finally, for consumers and online merchants or banks, there is a need to authenticate credit cardholders or bank clients for Internet-based or other electronic transactions without jeopardizing sensitive personal account information. In each of these areas, standards- based devices that easily interface with a PC or network to provide secure, controlled access to digital content or services are an easily deployed and effective solution.

The proliferation of personal computers in both the home and office, coupled with the increasing availability of personal devices that enable access to computer networks and the Internet, have created significant opportunities for electronic transactions of all sorts, including electronic payment, ticketing, e-government, electronic healthcare access and mobile banking. In government agencies and corporate enterprises, the desire to link disparate divisions or offices, reduce paperwork and streamline operations is also leading to the adoption of more computer- and network-based programs and processes. Network-based programs are also used to track and manage data about large groups of people; for example, citizens of a particular country. While the benefits of computer networks may be significant, network and Internet-based transactions also pose a significant threat of fraud, eavesdropping and data theft for both groups and individuals. To combat this threat, parties at both ends of the transaction must be assured of its integrity. Online merchants and consumers need assurance that customers are correctly identified and that the authenticity and confidentiality of information, such as a credit card number, is established and maintained. Corporate, government and other networks need security systems that safeguard the data of individuals and protect the network from manipulation or abuse, both from within and without the system.

Increasingly, large organizations such as corporations, government agencies and banks are adopting systems that protect the network, the information in it and the people using it by authenticating each user as the user logs on and off the network. Authentication of a user s identity is typically accomplished by one of two approaches: passwords, which are codes known only by specific users; and tokens, which are user-specific physical devices that only authorized users possess. Passwords, while easier to use, are also less secure because they tend to be short and static, and are often transmitted without encryption. As a result, passwords are vulnerable to decoding or observation and subsequent use by unauthorized persons. Tokens range from simple thumb-sized objects to more complex devices capable of generating time-synchronized or challenge-response access codes. Certain token-based systems require both possession of the token itself and a personal identifier, such as a fingerprint or personal identification number, or PIN, to indicate that the token is being used by an authorized user. Such an approach, referred to as two-factor authentication, provides much greater security than single factor systems such as passwords or the simple possession of a token.

One example of a token used in two-factor authentication is the smart card, which contains an embedded microprocessor, memory and a secure operating system. In addition to their security capabilities, smart cards are able to store data such as account information, healthcare records, merchant coupons, still or video images and, in some cases, cash. Smart cards are typically about the size of a credit card and can easily be carried in a wallet or attached to a badge. Smaller cards designed for use with devices such as mobile phones are also increasingly being utilized. Depending on the application for which they are being used, smart cards can be designed to insert into a reader attached to a PC or other device, or can include wireless capabilities for contactless interface. Worldwide shipments of smart cards reached 4.5 billion in 2007 and are estimated to grow to nearly 5.4 billion in 2009 for applications ranging from mobile communications to corporate security to online banking, according to the European smart card industry organization, Eurosmart. Demand for readers used in conjunction with those cards is also expected to grow. For example, research firm Frost & Sullivan estimates that the worldwide volume of smart card reader units will grow from 15.1 million in 2007 to 37.7 million in 2011. The combination of smart cards and readers provides a secure solution for network access, personal identification, electronic commerce and other transactions where authentication of the user is critical.

Market Opportunities

The market for secure access and authentication solutions in which we participate is experiencing unprecedented expansion, fueled by a few major trends: First, there are an increasing number of large government initiatives throughout the world, such as the Presidential Directive on Homeland Security (HSPD-12) in the U.S., the global mandate for electronic passports, national identification programs worldwide, and electronic healthcard (eHealth) programs in Germany, France and other European countries. Second, the demand for contactless devices that operate without a physical connection between the card and reader is also growing rapidly. Major deployments of contactless smart cards for payment, transport and electronic identification programs such as the forthcoming German national identification card, are driving growth in the market overall and compelling the industry to transition from the current environment of contact card interface to a contactless infrastructure. Third, NFC, a wireless connectivity technology that enables convenient short-range communications between electronic devices, is expected to become widely used on a global basis to enable contactless applications from mobile phones. This will require a major upgrade of legacy infrastructures to fully enable NFC applications such as payment, ticketing and customer loyalty/reward programs, and will create new markets for contactless infrastructure and NFC tokens.

Government Initiatives

In countries around the world, local and federal governments are utilizing smart card technology to authenticate citizens, employees or military personnel for programs such as network or physical access control, national ID, healthcare, storing digital certificates for online transactions, residency permits and visas and driver s licenses. According to IMS Research Group, more than one billion smart cards will be used in identity programs by governments and other public bodies worldwide by 2010.

To date, the largest and one of the most advanced deployments of smart cards for digital security purposes has been the U.S. Department of Defense s Common Access Card (CAC) program. Beginning in October 2000, the U.S. Department of Defense has distributed more than 17 million smart cards to military personnel and contractors. These cards are being used as the standard identification credential for military personnel, and are also being used for secure authentication and network access. In compliance with HSPD-12, since late 2006, the CAC card also has served as a standard identity credential that is both secure and interoperable across all federal agencies, regardless of which agency issued the card. To satisfy the technical requirements of HSPD-12, the National Institute for Standards and Technology developed Federal Information Processing Standards Publication 201 a U.S. federal government standard specifying personal identity verification requirements for federal employees and contractors. Under these specifications, personal identity verification cards must also include capabilities for contactless interface with security terminals at doorways and other entrances to provide secure physical access at government facilities.

In order to comply with HSPD-12, government facilities are replacing their existing access control credentials with personal identity verification cards and their existing CAC card readers with new FIPS 201-compliant smart card readers. The U.S. government s decision to deploy an integrated, agency-wide, common smart card platform will continue to raise the awareness of smart card technology, and hence increase the demand for contactless smart card proximity readers in both public and private sectors, according to IMS Research Group.

Internationally, countries around the world have been working together under the auspices of the International Civil Aviation Organization over the last several years to define and develop standards for electronic passports based on contactless smart card technology. The goal of the program is to ensure that these e-passports cannot be copied or altered, and that the biometric facial image stored on the card could be used to positively identify the holder. With implementations beginning in 2005, more than 50 countries worldwide now issue electronic passports, including Australia, Austria, Belgium, Canada, China, Denmark, France, Germany, Hong Kong, India, Italy, Japan, Korea, Macao, Malaysia, the Netherlands, Russia, Singapore, Sweden, the United Kingdom and the U.S.

Countries around the world are also utilizing smart cards as identification credentials for programs such as national identification, residency and driver s licenses. Electronic identification allow governments to better control the issuance of such identification credentials while enabling cardholders to remotely access government services. Countries utilizing electronic national identification cards include Argentina, Australia, Bahrain, China, Egypt, France, Germany, Hong Kong, India, Israel, Malaysia, the Netherlands, Sweden, Thailand and the United Kingdom. Countries issuing electronic driver s licenses include Australia, Brazil, India, Japan, Singapore, Sweden and the United Kingdom.

Many governments are also evaluating or making plans to develop electronic healthcare insurance and record systems, which would include smart card-based healthcare cards for participants. Mexico, China, India, Russia and Taiwan, as well as several European countries, including Austria, Belgium, France, Germany, Hungary, Italy, Poland, Turkey and the United Kingdom, are among the countries and regions that have already deployed or will deploy electronic healthcare cards to millions of healthcare users. These cards identify the user and store insurance and medical information that can be accessed by doctors and hospitals, among others. To date, one of the largest programs under development is in Germany, where pilot tests were set up in 2007. The German government plans to distribute 82 million new eHealth cards to citizens beginning in early 2009 and to put in place a corresponding network and card reader infrastructure for doctors, hospitals, pharmacies and other healthcare providers during 2009.

Growth in the Contactless Market

With the mass deployment of electronic passport schemes on a global basis, contactless smart chip technology has proven its maturity and reliability when incorporated in secure documents. As a result other sovereign documents like national ID, driver licenses, residence permits, weapon licenses and the like are migrating to chip-based technology. The majority of new e-government implementations around the world have chosen contactless interface. Estimates from NXP Semiconductors predict that the growth of electronic identification solutions between 2006 and 2012 will be overwhelmingly contactless (an 80% growth rate) compared to a 37% growth rate for contact electronic identification.

In the financial industry, major credit card companies in many parts of the world are embracing smart card technology as a more secure way to safeguard electronic transactions and address the problems of fraud, identity theft and protection of privacy, the cost of which can be significant. The majority of credit cards issued worldwide now comply with the Europay Mastercard Visa standard for securing financial transactions using a smart card.

Along with the move to more secure chip-based payment cards, there is an increasing preference for the convenience of contactless systems to facilitate payments. In part, this is being fueled by a desire on the part of consumers to replace cash payments with electronic payments in a number of daily transactions, particularly those of small value. Over the last two years, electronic payment programs featuring cards equipped with contactless technology, such as such as Visa® payWave^{tm} and MasterCard® PayPass^{tm}, have become widespread in Europe and Asia and are expected to generate significant demand worldwide for smart cards and related technology going forward.

Contactless transactions are being made more convenient with the emergence of mobile phones as a logical and leading platform to enable secure electronic payments. With smart device capabilities, the mobile phone enables consumers to purchase goods and services electronically and conveniently, while ensuring security through individual authentication of the user. In effect, the mobile phone becomes an electronic wallet. Integration of contactless payment technology into mobile phones is expected to further spur demand for contactless technology over the next several years. According to the research firm Gartner Group, the number of consumers using mobile payment services via mobile phones and other devices is expected to grow from 32.9 million users in 2008 to 103.9 million in 2011.

There is significant long-term opportunity for companies that can provide contactless solutions that enable mobile phones and other personal devices to support secure electronic payment and banking transactions.

Major contactless technology standards include ISO14443 A and B, MIFARE^{tm}, FeliCa®. In Japan, the contactless technology standard known as FeliCa is widely used for applications such as payment, transport, loyalty and mobile communications. Developed by Sony, FeliCa is the most mature contactless technology in the world today. Growth in FeliCa-enabled devices both within and beyond Japan is expected to be significant over the next several years.

Growth in Near Field Communication Market

As noted above, mobile phones are emerging as the preferred platform to enable contactless applications, in particular secure electronic payments. NFC is fast becoming the preferred technology to enable secure short-range wireless connectivity for mobile phones and other personal mobile devices. Based on the 13.56 Mhz frequency, NFC is a wireless connectivity technology with a short-range of one to four inches. An NFC device can communicate with both existing ISO 14443 smart cards and readers, as well as with other NFC devices, and is thereby compatible with existing contactless infrastructures already in use for public transportation and payment. According to ABI Research, the volume of NFC-enabled chipsets supporting the mobile phone market will grow from zero units in 2005 to 419 million units in 2012, an average annual growth rate of 161%.

Smart USB Tokens

As a result of the major trends driving growth in secure access and authentication solutions described above, there is complementary and growing demand for small, portable tokens that bridge the gap between NFC-enabled mobile phones and a notebook or desktop PC. Smart USB tokens combine mobility with the ease of a USB interface to PCs and other computing devices and the capability to accept a smart card in either standard size or the smaller SIM card format. Such tokens secure authentication for applications including banking, payment, access control and data storage.

SCM s Secure Authentication Products

We offer a full range of smart card reader technology solutions to address the need for smart card-based security for a range of applications and environments, including PCs, networks, physical facilities and authentication programs. Our products include both contact and contactless smart card readers and terminals, USB tokens, application specific integrated circuits (ASICs) and small office productivity packages based on smart cards, sold under our CHIPDRIVE brand. We sell our readers and terminals, tokens and ASICs primarily to PC OEMs, smart card solutions providers and government systems integrators to support specific programs, such as e-health cards, secure mobile banking or the U.S. government personal identity verification program; as well as to OEMs that incorporate our products into their devices, such as PCs or keyboards. We sell our CHIPDRIVE small office productivity packages primarily to end users via retail channels and the Internet. Sales of our Secure Authentication products accounted for approximately 84% of our total revenue in 2008, approximately 80% in 2007 and approximately 71% in 2006. Additional discussion of our Secure Authentication business is contained in Item 7, Management s Discussion and Analysis of this Annual Report on Form 10-K.

Smart Card Readers

SCM is one of the world s leading suppliers of smart card readers for security-oriented applications. Our smart card readers are hardware devices that connect either externally or internally with a computer or other processing platform to verify the identity of, or authenticate, the user, and thus control access. Much like a lock works with a key, SCM s readers work with a smart card to admit or deny access to a computer or network, or to authenticate the card holder for identification and access to facilities, programs or services. They offer incremental levels of protection against unauthorized use, from simple PC Card reader devices to more complex PIN entry systems, which require both a smart card and a user s personal identification number to authenticate the user. Our readers are utilized to authenticate users in order to support security programs and applications for corporations, financial institutions, governments and individuals. These security programs and applications include secure network logon; personal identification for programs such as healthcare delivery, driver s licenses and electronic passports; secure mobile banking; digital signatures; and secure e-commerce.

SCM s reader devices employ an open-systems architecture that provides compatibility across a range of hardware platforms and software environments and accommodates remote upgrades so that compatibility can be maintained as the security infrastructure evolves. We have made significant investments in software embedded within our products to enable our smart card readers and components to read the majority of smart cards in the world, regardless of manufacturer or application. Our smart card readers are also available with a variety of interfaces, including biometric (fingerprint), wireless/contactless, keypad, USB, PCMCIA, ExpressCard® and serial port, and offer various combinations of interfaces integrated into one device in order to further increase the level of security.

SCM s smart card reader product line includes:

Contact Smart Card Readers/Writers: include internal and external Secure Card Readers that require only a smart card to provide secure authentication and external Secure PINpad Readers with a numeric PINpad that utilize a smart card in conjunction with a personal identification code to ensure two factor authentication of the user.

Contactless Readers and Dual Interface Readers: internal and external readers that address the demand for contactless interface used in many security programs based on smart cards, for example public transport, e-banking and e-passport personalization and verification. We are currently working to add NFC and FeliCa functionality to our entire range of dual interface and contactless solutions.

Physical Access Control Terminal: designed to address the requirements of the U.S. government for secure access to facilities. The physical access control terminal combines new technologies such as contactless and biometric interface with existing control systems as well as CAC and newer personal identity verification credential cards, to provide support for new connectivity options going forward.

eHealth Terminal: specifically designed to meet the requirements of the German Health Card, to support Germany s intended rollout of healthcare cards to 82 million citizens. SCM s eHealth100 terminal reads and operates both with Germany s current memory card-based health card as well as the new chip-based card, and is compliant for use with three different card types: the electronic health card, the health professional card, and the Secure Module Cards used for secure data communication.

ePassport Readers: designed to read all electronic passports currently in use or planned for distribution. Ranked among the highest in interoperability and versatility in international interoperability tests. We offer both complete ePassport readers and ePassport modules that can be incorporated into customer terminals and designs.

Mobile Readers: unconnected devices that enable secure network access and user authentication by generating one-time passwords.

Keyboard Readers: reader interfaces that are designed to be embedded into a computer keyboard at the manufacturer.

SCM s smart card readers are developed in compliance with relevant industry standards related to the applications for which they will be used, including PC/SC, Europay Mastercard Visa, FINREAD and Common Criteria. For example, many of our readers, including the SCRx31 Secure Card Reader line, conform to Europay Mastercard Visa international standards for financial transactions. We typically customize our smart card readers with unique casing designs and configurations to address the specific requirements of each customer.

Smart USB Tokens

SCM s @MAXX family of personal contactless tokens is designed to securely support a broad range of applications. When connected to a PC, the tokens support the establishment of a secure channel to content and services available on the PC or a remote system. Unplugged, they fully leverage existing contactless infrastructures by enabling multiple services and applications such as contactless payment, contactless public transport ticketing or access to facilities. A planned NFC version of the @MAXX token is designed to enable legacy infrastructures (such as PCs or point of sales terminals) to become NFC enabled devices and, for example, enable smart phones that are not equipped with NFC to become NFC-enabled mobile devices, provided there is a USB connection.

ASICs/Chip Sets

SCM s ASICs provide smart card interface capabilities for embedded platforms, such as desktop computers or keyboards. We offer two levels of ASICs to provide both basic smart card interface capability and support for multiple interfaces and reader devices. All of SCM s ASICs comply with all relevant security standards for applications in the smart card industry. In addition, our advanced chip allows on-board flash upgrades for future firmware and application enhancements. We have a unique position in the market, with the ability to offer dedicated smart reader/writer, single chip solutions with embedded FLASH for secure firmware upgrade in the field (to prevent obsolescence) for our own products as well as to be integrated in PCs, keyboards and other devices.

CHIPDRIVE Productivity Solutions

We offer several CHIPDRIVE packages, consisting of smart cards, readers and software applications, for small and medium-sized businesses. These products support applications such as smart card-enabled logon to Microsoft® Windows® and smart card-based, secure electronic time recording.

Overview of the Market for Digital Media Connectivity Solutions

Digital cameras have rapidly saturated the consumer market over the last few years, with 80% of U.S. households predicted to own a digital camera by 2010, according to Gartner Group. Camera phones have also gained rapid popularity; in fact, 15% of consumers declare their phones to be their primary picture-taking device, according to an October 2007 survey from InfoTrends. InfoTrends estimates that U.S. output of digital photo prints will grow from 13.2 billion prints in 2005 to 16 billion by 2009. Digital flash media cards, which store digital images on the majority of digital cameras and some camera phones, are the key driver behind digital print growth. Higher capacity memory cards allow digital camera users to take more pictures before having to download images or swap out the card. As card capacities increase, more time is needed to download images. This uses more of the camera s battery life, which already may be insufficient for many camera owners. To print without draining the camera battery, the digital flash media card can be removed and inserted into a card reader on a PC, printer or kiosk to download and print images.

Retail photo kiosks and minilabs, which give instant, high-quality printouts of digital images, make printing photos more convenient for the consumer and typically provide higher quality prints than home printers. As flash memory card capacities increase and digital cameras continue to proliferate, SCM believes consumers will increasingly use photo kiosks and minilabs to download and print their digital pictures. Each photo kiosk or minilab requires a variety of media card readers to download images from the various media cards in use in digital cameras on the market.

SCM s Digital Media and Connectivity Products

SCM offers digital media readers that provide an interface to the various formats of digital media cards to download digital images and other content. We sell our digital media readers primarily to photo kiosk manufacturers. Our digital media readers allow photo kiosk makers and others to build digital flash media interface capabilities into their products and provide interface capabilities for all major memory card formats, including PCMCIA I and II, CompactFlash® I and II, MultiMediaCardtm, Secure Digital Card®, SmartMedia^{tm}, Sony Memory Stick® and xD-Picture Card^{tm}. Sales of our Digital Media and Connectivity products accounted for approximately 16% of our total revenue in 2008, approximately 20% in 2007 and approximately 29% in 2006. Additional discussion of our Digital Media and Connectivity business is contained in Management s Discussion and Analysis of this Annual Report on Form 10-K.

SCM s digital media readers leverage our interface chips to enable each reader slot to read multiple types of cards. Our digital media reader product line includes:

Preconfigured Drives: SCM s 3.5 inch 5- and 6-bay drives provide plug-and-play interface for photo kiosks and mini labs. Marketed as Professional Card Drive (PCD) or Modular (gMOD and PCD-zMOD) readers, these drives are designed to support heavy commercial usage and support multiple media card formats in either an integrated or a modular form factor.

Single Board Drives: SCM s single board drives provide flexible interface solutions for print kiosks, photo labs and other applications requiring digital flash media interface. Single board drives can be configured using any combination of media interface and drive placement to address the specific requirements of each kiosk or other product environment.

Technology

Many of the markets in which we participate are in their early stages of development and it is expected that they will continue to evolve. For example, early markets typically require complete hardware solutions, but over time requirements shift to critical components such as silicon or software as OEM customers increase their knowledge and sales volumes of the technologies being provided. We are committed to developing products using standards compliant technologies. Our core technologies, listed below, leverage our development efforts to benefit customers across our product lines and markets.

Silicon Strategy

We have implemented a number of core interface and processing technologies into our silicon chips. We have also selected what we believe to be the best available silicon from outside suppliers based on desired functionality, and have embedded our core interface and processing technologies in order to meet time-to-market requirements. We currently utilize the foundry services of external suppliers to produce our ASICs for smart cards readers, and we use chips and antenna components from third-party suppliers in our contactless smart card readers. We expect to continue to maintain a balance between our own silicon and the use of third-party devices.

Firmware and Drivers

For our Secure Authentication products, including contact and contactless readers, we have developed interface technology that provides interoperability between PCs and smart cards from many different smart card manufacturers and with many different operating systems. SCM s interoperable architecture includes an International Standards Organization-compliant layer as well as an additional layer for supporting non-International Standard Organization-compliant smart cards. Through proprietary integrated circuits and firmware, our smart card readers can be updated electronically to accommodate new types of smart cards without the need to change the reader s hardware. For our Digital Media and Connectivity products, we have developed interface technology that provides interoperability and compatibility between various digital appliances, computer platforms and flash memory cards. For complex terminals for electronic healthcare and other markets, we have chosen to use Linux®-based embedded firmware, which helps to provide the base layers for writing higher levels of application software. All SCM products are offered with the necessary device drivers for major operating systems, including Microsoft Windows, Windows Vista^{tm}, Linux and MAC OS®.

Complete Hardware Solutions

We provide complete hardware solutions for a range of secure digital access applications, and can customize these solutions in terms of physical design and product feature set to accommodate the specific requirements of each customer. For example, we have designed and manufactured smart card readers that incorporate specific features, such as a transparent case and removable USB cable, to address the needs of specific OEM customers.

Customers

Our products are targeted at government contractors and systems integrators, as well as manufacturers of computers, computer components, consumer electronics and photo processing equipment. Sales to a relatively small number of customers historically have accounted for a significant percentage of our total sales. Sales to our top ten customers accounted for approximately 58% of revenue in fiscal 2008, 61% of revenue in fiscal 2007 and 53% of revenue in fiscal 2006. In 2008, Tx Systems, Inc and Flextronics America, LLC (formerly Solectron) each accounted for more than 10% of revenue. In 2007, Envoy Data Corporation accounted for more than 10% of revenue. In 2006, Flextronics America, LLC accounted for more than 10% of revenue. We expect that sales of our products to a limited number of customers will continue to account for a high percentage of our total sales for the foreseeable future. The loss or reduction of orders from a significant customer, including losses or reductions due to manufacturing, reliability or other difficulties associated with our products, changes in customer buying patterns, or market, economic or competitive conditions in the digital information security business, could harm our business and operating results.

Sales and Marketing

We utilize a direct sales and marketing organization, supplemented by distributors, value added resellers, systems integrators, resellers and Internet sales. As of December 31, 2008, SCM had 38 full-time employees engaged in sales and marketing activities. Our direct sales staff solicits prospective customers, provides technical advice and support with respect to our products and works closely with customers, distributors and OEMs. In support of our sales efforts, we conduct sales training courses, targeted marketing programs and advertising, and ongoing customer and third-party communications programs, and we participate in trade shows.

Backlog

We typically do not maintain a significant level of backlog. As a result, revenue in any quarter depends on contracts entered into or orders booked and shipped in that quarter. Sales are made primarily pursuant to purchase orders for current delivery or agreements covering purchases over a period of time. Our customer contracts generally do not require fixed long-term purchase commitments. In view of our order and shipment patterns, and because of the possibility of customer changes in delivery schedules or cancellation of orders, we do not believe that such agreements provide meaningful backlog figures or are necessarily indicative of actual sales for any succeeding period.

Collaborative Industry Relationships

We are a contributor in various national and global standardization bodies and industry consortia, and are party to collaborative arrangements with a number of third parties. We evaluate, on an ongoing basis, potential strategic alliances and intend to continue to pursue such relationships. Our future success will depend in part on the success of our current arrangements and our ability to establish additional arrangements. These arrangements may not result in commercially successful products.

DIN SCM is a member of DIN, the German Institute for Standardization, which develops norms and standards as a service to industry, the state and society as a whole. A registered non-profit association, DIN has been based in Berlin since 1917. DIN s primary task is to work closely with its stakeholders to develop consensus-based standards that meet market requirements. Some 26,000 experts contribute their skills and experience to the standardization process. By agreement with the German federal government, DIN is the acknowledged national standards body that represents German interests in European and international standards organizations. 90% of the standards work now carried out by DIN is international in nature.

NETC@RDS SCM is a member of the NETC@RDS initiative, which is devoted to establishing improved health care access and administration procedures for mobile citizens in the European Union (EU), using the electronic European Health Insurance Card. We are a technology provider to the NETC@RDS project and have participated in market validation tests which included 85 pilot sites in 10 EU member states.

NFC Forum SCM is a principal member of the NFC Forum and was recently named chair of the NFC Forum s Devices Working Group. The NFC Forum is a non-profit industry association whose mission is to advance the use of NFC technology by developing specifications, ensuring interoperability among devices and services, and educating the market about NFC technology, which is a type of radio frequency technology that allows for secure transference of data between a card and reader over distances of not more than a few inches, and is an important technology for contactless payment applications. The NFC Forum consists of 150+ global member companies, including leading mobile communications, semiconductor and consumer electronics firms. NFC Forum members are currently developing specifications for a modular NFC device architecture, protocols for interoperable data exchange and device-independent service delivery, device discovery, and device capability.

PCMCIA SCM is a member of the Personal Computer Memory Card International Association, or PCMCIA, an international standards body and trade association with more than 100 member companies. We have been a member of PCMCIA since 1990. PCMCIA was founded in 1989 to establish standards for integrated circuit cards and to promote interchangeability among mobile PCs.

PC/SC Workgroup SCM is an associate member of the PC/SC workgroup, a consortium of technology companies that seeks to set the standard for integrating smart cards and smart card readers into the mainstream computing environment.

Share Security Formats Cooperation (SSFC) SCM is a customer partner of SSFC, an alliance of leading Japanese technology companies that aims to establish a securely shared new data format for contactless smart cards, enabling multiple security applications to be managed using a single smart card.

Silicon Trust SCM is a member of Silicon Trust, an industry forum sponsored by Infineon Technologies that focuses on silicon based security solutions, including smart cards, biometrics, and trusted platforms.

Smart Card Alliance SCM is a member of the Smart Card Alliance, a U.S.-based, multi-industry association of member firms working to accelerate the widespread acceptance of multiple applications for smart card technology. We are also a member of Smart Card Alliance s Leadership Council.

Teletrust SCM is a member of Teletrust, a German organization whose goal is to provide a legally accepted means to adopt digital signatures. Digital signatures are encrypted personal identifiers, typically stored on a secure smart card, which allow for a high level of security through internationally accepted authentication methods. We are also a member of the smart card terminal committee of Teletrust, which defines the standards for connecting smart cards to computers for applications such as secure electronic commerce over the Internet.

Other SCM is also a member of several digital flash media card organizations, including CompactFlash Association, Memory Stick Developers Forum, MultiMediaCard Association, SD Card Association, SSFDC SmartMedia Forum, xD-Picture Card Forum, Photo Marketing Association International and USB Implementers Forum.

Research and Development

To date, we have made substantial investments in research and development, particularly in the areas of smart card-based physical and network access devices and digital connectivity and interface devices. Our engineering design teams work cross-functionally with marketing managers, applications engineers and customers to develop products and product enhancements to meet customer and market requirements. We also strive to develop and maintain close relationships with key suppliers of components and technologies in order to be able to quickly introduce new products that incorporate the latest technological advances. Our future success will depend upon our ability to develop and to introduce new products that keep pace with technological developments and emerging industry standards while addressing the increasingly sophisticated needs of our customers.

We focus the bulk of our research and development activities on the development of products for new and emerging market opportunities. Research and development expenses were approximately $3.9 million for the year ended December 31, 2008, $3.1 million for the year ended December 31, 2007 and $3.8 million for the year ended December 31, 2006. As of December 31, 2008, we had 73 full-time employees engaged in research and development activities, including software and hardware engineering, testing and quality assurance and technical documentation. The majority of our research and development activities occur in India.

Manufacturing and Sources of Supply

We utilize the services of contract manufacturers in Singapore and China to manufacture our products and components. We have implemented a global sourcing strategy that we believe enables us to achieve economies of scale and uniform quality standards for our products, and to support gross margins. In the event any of our contract manufacturers are unable or unwilling to continue to manufacture our products, we may have to rely on other current manufacturing sources or identify and qualify new contract manufacturers. Any significant delay in our ability to obtain adequate supplies of our products from current or alternative sources would harm our business and operating results.

We believe that our success will depend in large part on our ability to provide quality products and services while ensuring the highest level of security for our products during the manufacturing process. We have a formal quality control program to satisfy our customers requirements for high quality and reliable products. To ensure that products manufactured by others are consistent with our standards, we manage all key aspects of the production process, including establishing product specifications, selecting the components to be used to produce our products, selecting the suppliers of these components and negotiating the prices for certain of these components. In addition, we work with our suppliers to improve process control and product design. As of December 31, 2008, we had 9 full-time employees engaged in manufacturing and logistics activities, focused on coordinating product management and supply chain activities between SCM and our contract manufacturers.

On an ongoing basis, we analyze the need to add alternative sources for both our products and components. Even so, we rely upon a limited number of suppliers for some key components of our products. For example, we currently utilize the foundry services of external suppliers to produce our ASICs for smart cards readers, and we use chips and antenna components from third-party suppliers in our contactless smart card readers. Wherever possible, we have added additional sources of supply for mechanical components such as printed circuit boards or casing. However, a risk remains that we may be adversely impacted by an inadequate supply of components, price increases, late deliveries or poor component quality. Additionally, components may not be available in a timely fashion or at all, particularly if larger companies have ordered more significant volumes of the components, and if demand is great, higher prices may be charged for components. Disruption or termination of the supply of components or software used in our products could delay shipments of our products, which could have a material adverse effect on our business and operating results. These delays could also damage relationships with current and prospective customers.

Competition

The Secure Authentication and Digital Media and Connectivity markets are competitive and characterized by rapidly changing technology. We believe that competition in these markets is likely to intensify as a result of anticipated increased demand for digital access products. We currently experience competition from a number of sources, including:

Advanced Card Systems, Gemalto (formerly Gemplus and Axalto), O2Micro and OmniKey in smart card readers, ASICs and universal smart card reader interfaces for PC and network access;

AMAG Technology, Bioscrypt, BridgePoint Systems, HID, Integrated Engineering, Precise Biometrics, XceedID and XTec in physical access control terminals; and

Atech, Datafab, OnSpec and YE Data for digital media readers.