Infocomm Security Technologies for E-Commerce

Release November 2002

4th Infocomm Technology Roadmap Report 2002 - 2007

iDA INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE

Dear Reader,

Welcome to the newest revision of our Infocomm Technology Roadmap Reports.

The "Infocomm Technology Roadmap" programme serves to anticipate the macro infocomm technology trends globally and identify potential strategic technologies for adoption in Singapore. Facilitated by IDA, each "Infocomm Technology Roadmap" report is conceived and written via a collaborative effort between many parties, namely from the industry, research & academic community, as well as from government agencies.

It has been slightly over two years since we inaugurated the "Infocomm Technology Roadmap" programme via the first report on "Broadband Access and Mobile Wireless". To date, we have together travelled through four cycles of technology roadmap exercises with the support from our participants on different but strategic technology areas to Singapore.

In embarking on this intimate journey with the local infocomm community, the Technology Group in IDA is guided by the motto 'to bring technologies to better our lives' to build up Singapore's competitiveness via the infocomm cluster.

We hope that you will find our published reports useful and take your time to enjoy reading this latest version. You too can be part of the local infocomm community, if not already, just by being part of the knowledge, even as an informed user with a sophisticated demand.

Dr Brian Chen
Chief Technology Officer
Infocomm Development Authority of Singapore

The roadmap process entails a continual updating exercise. This ITR4 Release November 2002 has combined, revised, added new emerging interests and will supersede the following:

- ITR1 Release July 2000 *("Broadband Access and Mobile Wireless")*;
- ITR2 Release March 2001 *("Broadband Access and Mobile Wireless Updates", "The Connected Home", "Infocomm Security in e-commerce")*;

  ITR3 Release February 2002 *("Next Generation Optical Networks and Photonics", "Next Generation Internet Applications")* remains valid and current.

Objective of Roadmap Reports

Summary of Worldwide Technologies, Standards and Applications. A key objective of this roadmap report is to provide a good overview of past and future developments worldwide, the efforts of key standardisation bodies and industrial forums for interoperability. The report also aims to promote a good understanding of the market and technology undercurrents which are constantly evolving.

Collective Vision for Alignment of Resources. The fast changing landscapes, the multidisciplinary nature of emerging technologies, competing and converging technology standards, and heightened user expectations call for a more collaborative and managed approach to technology development. For this, the report aims to derive a common vision and directions for future work, reflective of the joint work effort between the industry, government, research community and academia. Where possible and appropriate, we would include strategic gaps and opportunities for collaborative exploitation. The roadmap exercise aims to identify synergies and complementary expertise so that we can pool our resources, leverage on each other's strengths to seize technology opportunities.

Your Feedback

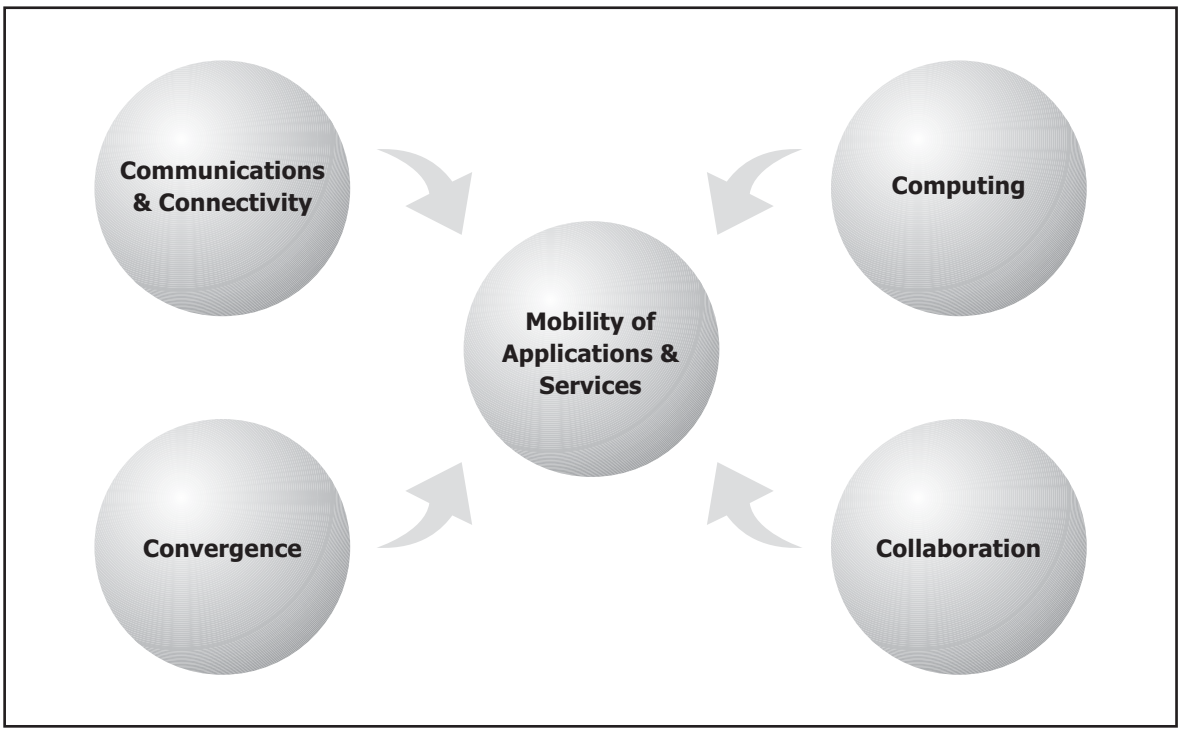
Lastly and very importantly, your feedback will be deeply appreciated on either the report itself, or on collaborative proposals for technology development via the survey form attached at the end of this report. We thank you in advance for your time and effort in doing so and this will help us produce better future roadmap reports.

You can reach us at:

Mr Raymond Lee
Deputy Director
Technology Direction
Infocomm Development Authority of Singapore
8 Temasek Boulevard
#14-00 Suntec Tower Three
Singapore 038988

Website: www.ida.gov.sg
(Click on "Technology Development", followed by "Infocomm Technology Roadmap")
Email: roadmap@ida.gov.sg

In moving towards 2007 and beyond, this ITR4 report weaves through emerging modern communication technologies for an integrated broadband infrastructure. An integrated broadband infrastructure is a multi-pronged combination of heterogeneous networks (last-mile access, mobile wireless or in-home networks), technologies and end devices closely integrated to allow the key concept of *application mobility and access* anytime, anywhere. Secured payment and authentication mechanisms, non-repudiation of services, communication between trusted parties and access management to information and services will also be an enabler of this integrated infrastructure.



The global trend towards an integrated infrastructure will facilitate three basic human needs for "communication and connectivity", "computing" and "collaboration". The "convergence" of technologies, open standards & platforms, and contents will lend to the ease of mobility of applications and services encapsulated in this infrastructure. Ultimately, working towards the mobility of applications and services regardless of the technology, network and platform used is to enable a convenient and consistent user experience. It is all about users, both consumer and corporate.

We shall now elaborate more on what we see today and the milestones ahead. Some of the technologies or applications to be described below can satisfy more than one of the three basic human needs mentioned above, hence some overlapping is to be understood.

Communication and Connectivity. Communication is a human basic need to contact each other anywhere, anytime and via various platforms and devices, and a means to stay connected. In the area of mobile wireless, we will see new varieties of services apart from simple voice calls such as rich multi-party multimedia communications, instant messaging and presence services, location based services, as well as one-to-many multimedia broadcast and mobile webcasting. This will enhance individual communication features but also open up enterprise opportunities such as in the areas of mobile e-learning, mobile seminars, corporate teleworking and marketing. Emerging 3G mobile networks could offer in Singapore average data rates of around 100 to 200Kbps while in the longer term, 4G networks could reach peak rates of 100Mbps targeting average data rates of 20Mbps at least. In fact, certain 3G standards such as HSDPA (high speed downlink packet access) for WCDMA in 3GPP Release 5 today is exploring downlink rates of up to 10Mbps, with up to 20Mbps downlink for Release 6 (but deployments are expected around 2005). This development coupled with the decreasing computational power differences between hand-held devices and desktops would facilitate the mobility of applications from wireline to wireless domain.

In the area of Broadband Access, it is about creating the necessary connectivity for communication, computing and collaboration. In our vision of 2007, we expect ADSL and cable to replace dial-up as the dominant means for accessing Internet. However, these two access technologies may no longer be considered "broadband". We believe that the access speeds offered by VDSL and fibre will set the stage for the new definition of "broadband". Lifestyle changes like teleworking will become common, resulting in increase use of applications like video-conferencing, workgroup collaboration, and productivity tools. "Always-on" broadband access characteristic is not sufficient and needs to be enhanced by QoS and symmetric downstream/upstream access speed.

Bandwidth for home area networks will even be less of an issue compared to access networks. By 2007, we could expect a home network to support applications with data rate in excess of 100Mbps, made possible by a wide choice of networking technologies, such as Ethernet, Phoneline networking and Ultra-Wideband. The preference for mobility and "no new wire" advantage will make WLAN (802.11a and beyond) and UWB the dominant choices in most homes, enabling applications with speed of 54Mbps or more. Wireline technologies such as structured wiring will be increasingly used as the high-speed backbone for in-home wireless networks. Powerline communication technology may find its niche in smart home kitchen appliances. However, for home technologies to take off, these technologies must become embedded into devices to the point that they become transparent to the users, and that the deployment of IPv6 is critical to meet the demand for addresses, QoS and security. At the same time, the plug and play ease of use is to be enabled by efforts in automatic service deployment and discovery of enabled appliances.

Security will take precedent to address a myriad of issues in diverse communication paths occurring between one-to-one, one-to-many and many-to-many in an open dynamic network. Adding to the complexity is the variety of participants in this network, from humans to machines and software agents. At the base of secured communication channels is encryption. By 2007, DES will be completely phased out and AES will be dominant over Triple-DES.

Computing. Pervasive or anywhere computing advances communications and its success pivots on the creation of more sophisticated user demand. In mobile wireless, computing applications will migrate from simplistic mobile games, rudimentary calculator functions to mobile web services, multi-party role play coloured gaming, Java enabled applications, packet based multimedia applications and mobile VPN solutions. The introduction and more widespread use of feature-rich handsets and smartphones will facilitate this migration. In addition, the development of open specifications (e.g. OSA/Parlay APIs) and IP Multimedia Subsystem specifications will work towards the vision of interoperable roaming of these services across both CDMA and GSM networks across the world.

Computing applications like web services are predicted to change the nature of computing to service based models. But regardless of the setting, in working towards end-to-end security for open and heterogeneous web services, the industry targets by 2007 to have a rather complete stack of security standards to support for dynamic and federated networks of web services. This will be the layer of security infrastructure bridging silo-computing systems.

For computing inside the Connected Home, we see today the first wave of development under the guise of data networking for sharing of resources. A second wave of development will revolve around home information and entertainment space. Towards 2007, many entertainment equipment will transit from analogue to smart digital network-ready appliances, examples are multi-services residential gateway, advanced set-top box, digital/interactive television, home media servers, and to a lesser extent, smart kitchen appliances. Most of these appliances will be integrated with one or more in-home networking technologies and adopting open standard device connectivity, with features such as easy plug and play, zero administration, automatic service delivery and discovery, quality of service and device discovery. Security and a flexible billing mechanism will be built-in to support a variety of home applications.

Collaboration. Collaboration extends communication, connectivity and computing to group interaction and team sharing. It widens the interaction scope to groups of individuals in proximity or geographically disparate around the globe. Ad-hoc networking is an important feature to allow the impromptu set up of local networking for collaborative work or resource sharing in meetings or even for multi-party entertainment and gaming.

Collaboration can also be between trusted or non-trusted parties. To enable more sophisticated user demand by 2007, we need to move towards using appropriate security mechanisms to allow communication and collaboration between trusted parties. As such, in addition to PIN and passwords, we will see the emergence of related security authentication and non repudiation technologies and services such as trust service providers, 3D Secure, PKI, biometrics and smart random tokens and chip cards.

Convergence. Convergence can occur at several levels. At the industry cluster level, it can mean working towards integrating contents across different clusters such as the media, arts and entertainment, home automation, finance, IT & communication, broadcasting, telematics, telemedicine, education or e-learning, and e-government.

At the network level, we already see the convergence of voice, text, data, multimedia video that can be delivered with a single IP based network. At the technology and standards level, convergence can mean the confluence of hardware packaging techniques (e.g. BGA, CSP, stacked packaging), movement towards globally standardised architecture, platforms, open APIs (e.g. OMA, OSA). In services, convergence can happen with aggregated contents with 3G portals, or with IP based bundled multimedia services. At home, the OSGI residential gateway represents a tool for convergence towards a multi-service model and whereby service providers can enter to make headway into the smart home via remote provisioning of new services.

Similarly, at the security level, we see efforts towards identity management, federations and single sign on. If we converge under a federated umbrella model, each partner then agrees to trust user identities issued or authenticated by other organisations, while maintaining control of the identity and preference information of its own users. This will not be easily achieved. Sharing session and authentication information across networks and across disparate application is not only difficult, but resource-intensive as well. The level of trust placed over a given client request might vary across different services. By 2007, management console to talk to any security server or client regardless of device type, brand, OS, application or location will however lend itself to support this convergence.

Mobility of Applications and Services. There can be many different networks, access devices, technology platforms but we should have only one convenient, consistent and connected lifestyle. By this, we mean that we should not need to worry about which network we are connected to, how to access different networks or be preoccupied with end to end security of applications. Increasing online applications from fixed sites mainly confined to environments such as corporate LANs or PC internet access networks (in-home or at public internet access sites) are now ported to mobile devices, leading to ubiquitous connectivity.

Security will also need to interoperate over heterogeneous environments from LAN to public, from wireline to wireless to provide the user with uninterrupted connection to the various forms of services. By 2007, single sign on solutions and portable security such as biometrics (key ones being fingerprint, iris and facial) and smart cards will gain momentum.

The above spells our vision for this report. In gearing up to this vision, the many network and enabling technologies covered in this timeframe of 2002-2007 should take a backseat when compared to the more critical issue of understanding and creating sophisticated user demand, as well as to factor in business perspectives and operational challenges. However, it is a highly volatile task for anyone to anticipate accurately trends in market factors like future user demand and business sentiments. Hence, we can at best provide a technical roadmap of technology vision and trends, and a best-effort attempt to position technology milestones in this timeframe as we collectively judged with the help of industry participants, which the reader should moderate according to prevailing market sentiments.

List of Figures and Tables

We thank the following organisations and individuals for their contributions to the *"Infocomm Security Technologies in E-Commerce"* of the fourth Infocomm Technology Roadmap (ITR4):

A-STAR	Mr. Lawrence Chen
Baltimore Technologies	Mr Tan Beng Soon
D.A.R.T	Mr Lin Yih
Digisafe P/L	Mr Andrew Chow
	Mr Lee Ser Yen
Gemplus Technologies Asia	Mr. Lee Hon Guan
IBM Singapore P/L	Mr Chin Yook Siong
Intel Technology Asia	Dr Guo Lih Shiew
	Mr Anand Rajan
	Mr Vijay Rao
Laboratories for Information Technology	Dr Yau Wei Yun
Mastercard International	Ms June Yeap
Microsoft	Mr Steven Cheah
Nanyang Technological University	Dr M Yakoob Siyal
	Dr Shum Ping
	Dr. Tan Chik How
Quantiq International	Mr Don Ng
Siemens	Mr Muljawan Hendrianto
Sun Microsystems	Ms Carol Stevenson
	Mr Cheng Jang Thye
	Ms Eve Maler
	Ms Jayne Leow
	Mr Krishnan Jagannathan
	Mr Philips Lai
	Mr Vincent Siow
VISA	Mr Sam Oon

ITR-4 Roadmap Task Force

Mr Raymond Lee
Ms Lim Chay Yong
Ms Caren Choy
Mr Adrian Ong

In collaboration with:
Mr Chan Keen Wai
Mr Richard Cheong
Mr Roi Phua
Ms Ng Geok Peng
Mr David Quay
Mr Michael Nguyen

Dr Brian Chen
Chief Technology Officer
Infocomm Development Authority of Singapore

Along with privacy, security has been cited as one of the key reasons deterring consumers and businesses from fully embracing e-business and e-commerce. This roadmap report appraises the technology trends and developments in key security technologies crucial to enable secure and trusted e-commerce, to synthesise adoption behaviour, help eliminate uncertainty and identify opportunities.

This report will start with crytography, and then present three technologies that enable the reliable verification of the identity of the participants in a transaction – Smart Cards, Biometrics and Public Key Infrastructure. Among these, smart cards deserve special mention because they provide a protected storage and processing environment for electronic credentials and other data and applications. We believe that the next wave of e-commerce will be based on XML and web services. Security has been cited as a key major hurdle against the widespread adoption of web services, and XML security technologies are highlighted as a key impetus to driving web services.

Cryptography

About Cryptography. Encryption deals with the transformation of data into an apparently random and less readable form through a mathematical process. This technology is fundamental to keeping sensitive information private whether it is being transmitted over the network or stored on computer media. In general, there are two main kinds of encryption, namely secret-key encryption and public-key encryption.

Technology Trends. Being licensed by more than 700 companies globally, the RSA algorithm is the most widely used public-key technology in the world. With the release of the algorithm into the public domain, users of RSA no longer need to pay for the use of the algorithm. This will certainly boost the adoption of RSA technology for e-commerce. ECC, an emerging cryptography technology, is gradually being accepted by the industry as a viable alternative to RSA. Although its adoption has been rather slow, the technology has evolved to be a strong and better alternative for implementing public-key cryptography, especially in mobile phones and PDAs. This will certainly create an impact on the market share of public-key technology that has been consistently dominated by RSA.

AES is the other emerging cryptography technology. It has been positioned to replace DES, which has been widely implemented in most banking and financial systems. Although Triple-DES has been used as the successor to DES in most cases despite its slower performance, it is envisaged that AES will take over to become the de facto encryption algorithm for securing commercial payment transactions.

AES is relatively simple to implement and should be easily deployed. There are many products available on AES today, and is proven to be more secure than DES and 3-DES.

Smart Cards

About Smart Cards. Today, smart card usage can be found in sectors such as telecommunication, banking, transit, government & ID, healthcare, retail etc. It provides a key enabling technology across many different industries, catalysing profitability and operational efficiencies.

Market Trends. While they may have seemed less than appealing to businesses because of high costs, lack of standardisation, interoperability issues or potential manageability problems, smart cards are finally finding a place in today's cyber and physical security infrastructure. IDC projects that by 2003 the world-wide smart card market will reach $5 billion.

E-purse and cashless vending, PC secure log-on, all-in-one employee IDs, banking and medical authorisation, and many other applications, are predicted to abound because of the smart card. Smart card technology will evolve to support this through its multi-application capabilities. A smart card's flexible storage capacity makes it possible not only to carry one card for a broad variety of applications and services both in web-based and physical environments, but also allow the user to customise the bundling of applications for each card.

Standards Developments. EMV will be the de facto basic financial standard. EMV Integrated Circuit Card Specifications was made available for debit and credit products, and were meant to ensure that minimum standards for risk control and security are applied. CEPS will be forthcoming in about 2 to 3 years' time with most current proprietary e-purse schemes providing compatibility and interoperability products with CEPS. The EMV dateline in 2005 will convert Europe into a chip card society. Fraud may shift to other parts of the world as a result, urging a worldwide movement to pursue higher security for e-commerce. SET would be slow in America and Asia Pacific but its development would be more favourable in Europe.

Technology Trends. Smart Card Operating Systems are moving towards open platforms such as Multos and JavaCard. Smart Cards will have a high security feature with dedicated on-card crypto processing and support for AES & ECC. Increasing the security of smart cards are security assurance – from none to CC/ITSEC (now known as ISO 15408) certified. They wil have faster CPUs (32 bit + & above CPU) and are increasing in memory size to 64 MB and above. Dual interface to ease multi-applications/multi-services are emerging to support both contact (ISO 7816) & contactless (ISO 14443) interface. Other technology trends discerned

in the landscape are the integration of Smart Card and Biometrics data and the movement from "Chip on Card" to "System on Card".

Biometrics

About Biometrics. The Singapore government is a long-time proponent of biometrics technology. In 1997, the Singapore Immigration & Registration (SIR) introduced the Immigration Automated Clearance System (IACS), which harnesses the use of biometrics and smart card technology to authenticate the identity of travellers through the matching of fingerprints. IACS enables SIR to facilitate immigration clearance through automated lanes at the checkpoints. Presently, the IACS is available at Changi International Airport and the bus passenger halls of the Woodlands and Tuas Checkpoints. SIR has not stopped at this but has ventured to experiment other innovative means to serve the travellers better. Currently, SIR is conducting a trial using iris recognition technology for identification of motorcyclists at Woodlands and Tuas Checkpoints.

Standards Developments. Biometric products are currently not commonplace in e-commerce. Its primary niche application remains in time-and-attendance and physical access control. Besides the cost consideration, one of the important factors is the absence of dominant standards and interoperability in the industry. There is currently no common command set for biometrics. Since the matching technology is carefully guarded by biometric companies, standardisation of these technologies will remain difficult to achieve. A unified biometric standard rallied by most biometric players is unlikely to be ready within the next two or three years. Still, the majority sees standards as the way to increase global customer base and to bring benefits to both the industry and the consumer. The ISO/IEC consortium will be the most significant player for biometrics standardisation.

Biometrics Application Developments. Right now, biometrics is used mostly in niche applications. We see that biometrics will expand its scope to areas such as Banking/Financial services as cashless payment and automated cheque cashing, Healthcare applications for privacy concern, patient information control, drug control, as well as telecommunication applications such as telephony, mobile phone, subscription fraud, call center, games etc. Another major area that has received little attention up till now is the opportunity for personalization services. For example, a mobile phone with biometric capability is able to customize the user interface, ring tone, phone diary, speed dial etc. Imagine entering a members-only golf club reception with the automated system calling your name!

Public Key Infrastructure

About PKI. A PKI user's goal to build trust and confidence in online transactions by addressing security concerns. Making a comparison of security technologies out there, PKI is by far the most robust architecture that provides the 4 key features needed of a trust infrastructure.

PKI Obstacles and Inhibitors. PKI technology has been predicted to proliferate since 1997. However, the prediction has so far failed to become a reality due to several obstacles. Inhibitors include:

- Lack of interoperability standards for cross-border certification
- High cost and complexity of installation, deployment and maintenance
- Lack of multi-vendor interoperability
- Lack of demand and (killer) application support
- The uncertain legal standing of digital certificates
- PKI relies on identification and the existence of a means whereby senders can identify themselves. This breakdown of anonymity and pseudonymity is one factor leading to the lack of privacy.

Developments. Are these obstacles insurmountable and will it lead to the death of the public key infrastructure movement? And is PKI worth the effort to circumvent these stumbling blocks? The efforts needed to strengthen and evolve PKI and their goals include:

- **A Need for Critical Mass —** Interoperability is one key barrier to achieving critical mass. One reason is the lack of interoperability among the various CAs. With the intention of achieving interoperability, a MOU was signed between the PKI associations of Japan, Korea & Singapore. Beyond the issues related to CA-CA interoperability are technology issues. The interconnection of diverse PKI from different PKI vendors is another problem. One effort towards interoperability is XKMS, an XML-based specification for protocols for distributing and registering public keys. The completion of the XKMS specification and interoperable solution based on it is predicted to appear in 2004.

- **Real World Trust Models** — The PKI trust relationship model should reflect real-world trust relationships. Hybrid PKIs are viewed as the best fit for real life as it supports the combination of both hierachical and non-hierachical models such as mesh, trust networks, and webs of trust. The PKI community is exploring a range of topologies such as bridge CAs and multiple-bridge infrastructures.

- **Service Model required for PKI** — Due to the cost and complexity involved in implementing a full PKI solution, some organisations may find it more cost-effective to outsource their PKI to an external service provider.

- **Lightweight PKI** — One criticism of full-featured PKI is that it is too heavy-weight. There is a trend towards lightening it. An effort is this area is Intel-led SPKI (Simple Public Key Infrastructure) whose charter is to develop Internet standards for an IETF sponsored public key certificate format and associated protocols.

- **Killer App for PKI** — Today's luke-warm consumer adoption of PKI is the result of a lack of convenience features. JavaCard may be the disruptive technology to hold the key to widespread adoption of PKI as it not only holds security credentials, it allows other high-security functions to be performed locally within the card. JavaCard with mobile terminals (plus J2ME) may just be the pair to make an impact.

XML Security

About XML Security. As traditional security technology works quite well for applications where you don't need "XML-level granularity", the dominant application for XML security will be web services. The various types of web services for data retrieval, data transformation, data aggregation, transactional services and collaboration will form the engine of the next wave of e-commerce. Security risks that are highlighted include: XML Vulnerability, a need for selective encryption, integraion of PKI into XML, end to end security and single sign on.

XML Security Technologies. The report starts with the core of XML security: encryption and digital signatures and is followed by the technologies for key management, authorisation, single sign-on and interoperability. Security Models for XML Web Services that are highlighted in this section are SAML (Security Assertion Markup Language), WS-Security and OGSA(Open Grid Services Architecture).

XML Security Issues. "On the Internet, no one knows that you're a dog." A Digital Identity is the representation of a human identity that is used in a distributed network interaction with other machines or people. The trends in Identity Management such as the move toward federated identity and the climb towards single sign are examined in this section. Looking ahead, we see new XML Security Products emerging such as Reprogrammable Hardware to tackle the XML-processing which requires deep inspection of incoming packets and XML firewalls which go beyond the cursory inspection of traditional firewalls.

Overall Security Trends

In this report, we examine global trends and future developments of security technologies in e-commerce through the analysis of standards development, adoption status, and industry initiatives in each security technology, and draw out the following encompassing future trends.

- Standards-based end-to-end security
- Emerging service model for security
- Trends of co-ordination, convergence and consolidation in security technologies
- Emergence of specialised, dedicated appliances for enchanced performance and security

This is discussed in more detail in the conclusion chapter of this report.

The reader may refer to the accompanying roadmap chart at the back of the report, a snap overview of key developments in the timeline 2002 - 2007.

1 Introduction

Michael Porter defines the Internet as an enabling technology; a powerful set of tools that can be used wisely or unwisely, in almost any industry and as part of almost any strategy. In conformance/accordance with his interpretation, we see the Internet as a set of key structural technologies such as http, html, URI, that serve as a layer of common elements to act as a platform implemented across a range of applications. This platform may be thought as the lowest common denominator in the set of e-applications and e-services. The underlying technologies in the Internet platform need to be examined closely as developments in key structural technologies caused shifts in the applications that ride on top of this platform.

Infocomm security technologies are explored in this report as a key structural element in the set of Internet technologies that are serving as the platform base for e-commerce. We look at what security measures are required for a secure and trusted e-commerce experience and examine how competitive advantage may be gained through strategic adoption of security technologies. We report on the different security technologies and chart their trends and developments, for the next five years over the period 2002-2007. We also provide a current status quo report on the Singapore landscape and revisit our directions for this new timeline.

E-business is about using the Internet as a strategic platform and universal communication medium to redefine business models, maximise customer value. Increase effectiveness to directly affect an enterprise's relationship with its customers and its environment. Increase efficiency to affect internal structure and operating activities of the activities. Use for integration for forming inter-enterprise links. E-Commerce, defined as the buying and selling of goods and services over this digital medium may be considered as a subset under the e-business umbrella.

Global research studies show that Singapore has done reasonably well in our transformation efforts. Singapore was rated first in Asia and fifth worldwide for its e-commerce infrastructure in the World Competitiveness Yearbook 2001. The Intelligence Unit 2001 ranked Singapore top in Asia and seventh internationally for e-readiness. This indicates that Singapore's e-economy is keeping up with the global developments and is well positioned to flourish in the global ecommerce marketplace.

With this established e-infrastructure, E-commerce in Singapore has been growing steadily - both in volume and value. The finding of the Quarterly E-Commerce Survey 2001, which we recently released, shows that B2B e-commerce revenue grew by 26% from quarter one to quarter three and registered an increase of S$29m. Business-to-Consumer (B2C) activity has increased as well, with revenues growing 13% between the first quarter and third quarter of the year. For the full year 2001, we estimate total B2B and B2C sales revenues of S$112 billion

and S$2.58 billion respectively. This steady growth, in spite of the global economic downturn, is testament that e-commerce is truly established and flourishing in Singapore.

With the pervasive adoption of Internet and all the Infocomm infrastructures being interconnected globally, security for Infocomm is becoming essential. Maintaining the health of these infrastructures is what iSecurity is all about.

Security technologies include

- "firewall" to filter out unwanted intrusion from outside,
- "authentication" to identify a user to access the network;
- "authorisation" to allow the right users to access the right groups of resource;
- "encryption" to protect the data from unwanted exposure;
- "integrity" to ensure data not being altered during the transit;
- "digital signature" to enforce non-repudiation, and
- "tunnelling" solutions for secure communication between two end points through Internet.

This report will start with crytography, and then present three technologies that enable the reliable verification of the identity of the participants in a transaction (i.e. authentication) – Smart Cards, Biometrics and Public Key Infrastructure. Among these, smart cards deserve special mention because they provide a protected storage and processing environment for electronic credentials and other data and applications. We believe that the next wave of e-commerce will be based on XML web services. Security has been cited as a key major hurdle against the widespread adoption of web services. XML security technologies are highlighted as a key impetus to driving web services.

We believe that the next wave of e-commerce will be based on XML and web services. Security has been cited as a key major hurdle against the widespread adoption of web services. XML security technologies are highlighted as a key impetus to driving web services.

2 Cryptography

2.1 Overview

Just a few decades ago, the science of cryptography was employed primarily by governments to protect state and military secrets. Today, many IT systems and applications use cryptography. It can be found in all security products and solutions and serves as the underlying mechanism that addresses some of the fundamental security problems in the e-commerce world. Although not as obvious as other security technologies such as smart cards or biometrics, it is certainly one of the most essential components that cannot be omitted in order to secure any e-commerce transaction. The following sections provide an overview of two types of cryptography: Encryption and Digital Signature.

2.1.1 Encryption

Encryption deals with the transformation of data into an apparently random and less readable form through a mathematical process. This technology is fundamental to keeping sensitive information private whether it is being transmitted over the network or stored on computer media.

In general, there are two main kinds of encryption, namely secret-key encryption and public-key encryption. Secret-key encryption (also referred to as symmetric encryption) uses a single key to encrypt and decrypt a message. The main problem with secret-key cryptosystems is key management. However, the advantage of using secret-key cryptography is that it is generally faster than public-key cryptography. Examples of secret-key cryptographic algorithms are DES (Data Encryption Standard), Triple-DES, IDEA (International Data Encryption Algorithm), RC4 and the new AES (Advanced Encryption Standard).

To solve the key management problems associated with secret-key cryptosystems, Whitfield Diffie and Martin Hellman introduced the concept of public-key cryptography in 1976. The algorithm is based on two keys: one to encrypt the message and the other to decrypt the message. One of the keys, called the public key, is published, while the other, called the private key, is kept secret. The two keys are mathematically related such that the message that is encrypted using one key can only be decrypted by the other key.

Because public-key cryptography is slow, it is only suitable for encrypting small amounts of information. In contrast, secret-key cryptography is many times faster and is suitable for encrypting large amounts of information. Therefore, in practice, both secret-key and public-

key cryptography are employed. Public-key encryption is used to provide secure delivery of the symmetric encryption key to the intended recipient. The symmetric key is encrypted using the recipient's public key. Since only the recipient has the corresponding private key, only the recipient will be able to recover the symmetric key and decrypt the message.

2.1.2 Digital Signature

Besides encryption, a cryptographic mechanism known as digital signature is frequently used in e-commerce transactions. A digital signature is analogous to a hand-written signature in the real world. Instead of applying to paper documents, digital signatures are applied to electronic documents. Like hand-written signatures, digital signatures can be used to prove the authenticity of electronic documents. Someone who reads a document that is digitally signed by you can be assured that the document came from you. In addition, he is also assured of the integrity of the document, i.e. the document is complete and has not been modified in any way.

To produce a digital signature, public-key cryptography is employed. First, a small fixed-length mathematical fingerprint (called a hash code) of the original message content is created. Note that it is not possible to recover the message from the hash code. The digital signature is then created by 'encrypting' the hash code with the sender's private key. The digital signature is appended to the original message, which may be encrypted using any one of the methods explained in the previous section.

On the receiving end, the recipient verifies the digital signature using the sender's public key to 'decrypt' the signed hash code. At the same time, a new hash code can be created from the received message and compared with the original hash code. If the two match, then the recipient has verified that the message integrity is intact. The recipient also knows that only the sender could have sent the message because only he has the private key that signed the digital signature.

The following diagram illustrates the process of encryption and digital signature in a typical electronic transaction.

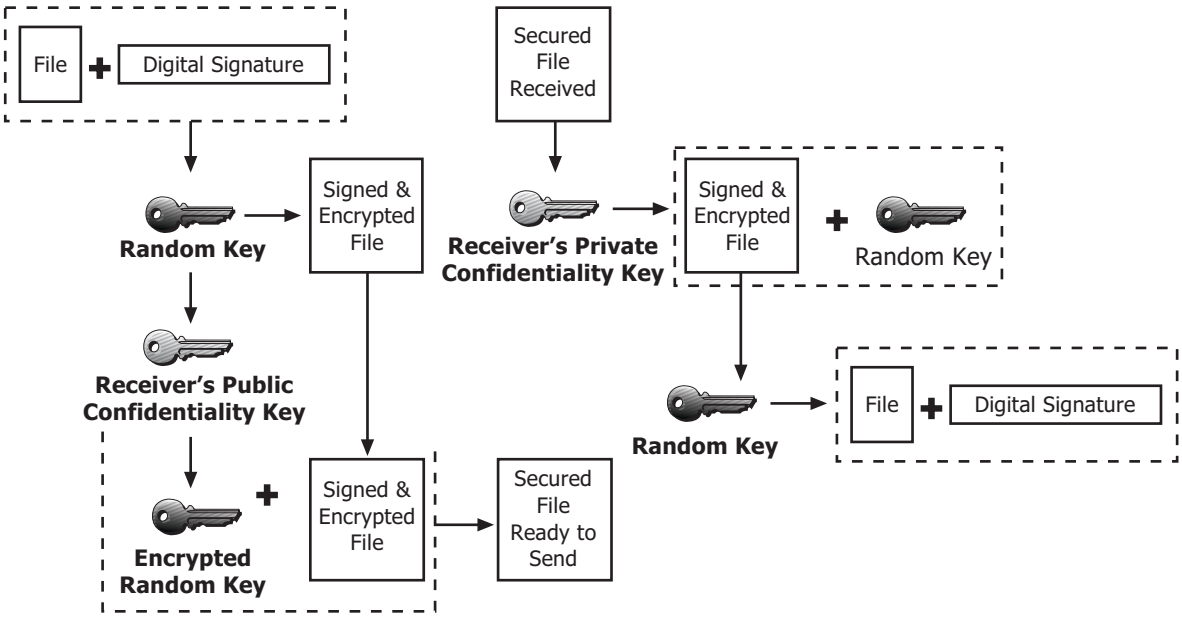


Figure 1. Process of Encryption and Digital Signature
(Source: Baltimore Technologies)

The use of public-key cryptography is growing rapidly because of its potential to resolve the key management issues. This technology has also been widely adopted to facilitate secure e-commerce over the Internet.

2.2 Technology Developments, Applications & Standards

2.2.1 RSA Cryptography

2.2.1.1 Background

The RSA algorithm is a public-key cryptographic algorithm that offers both encryption and digital signature capabilities. Developed in 1977 by Ronald Rivest, Adi Shamir and Leonard Adelman (thus the name RSA), the algorithm has been the enabling technology for computer security in the last 20 years. The strength of RSA lies in the difficulty in factoring very large prime numbers. The RSA technology was patented and was exclusively licensed to RSA Security (www.rsasecurity.com). The patent expired on 20 Sep 2000, releasing the standard into public

domain. This created for the first time a free market driving the adoption of security in applications It will possibly result in a wider adoption of security in e-commerce applications and build greater confidence in the Internet.

Due to the nature of its design, RSA has high computational overheads associated with processing. Therefore, there are few public-key implementations that can support data transmission speeds faster than 200 Kbps. In contrast, symmetric key algorithms commonly operate at 100 Mbps – nearly 500 times faster. Therefore, modern cryptographic systems usually use conventional symmetric key technology for 'bulk encryption,' and public-key technology to automate key management and distribution.

Today RSA technology is commonly used in applications such as SSL-enabled Microsoft Internet Explorer and Netscape Navigator, secure e-mail (S/MIME), virtual private networks (VPN) and secure payment systems. The algorithm is also widely used for digital signature and digital certificate in most PKI products today. With the expiration of the RSA patent, the algorithm may be used freely in any application where security is needed. As a result, a much greater number of applications are expected to be available with security built-in. For instance, open source products such as Mozilla (the open source version of Netscape Navigator) are being distributed with RSA source code. We also expect more e-commerce and m-commerce applications integrated with RSA security, as the use of RSA no longer requires a licence from RSA Security.

2.2.1.2 Standards

The RSA cryptographic algorithm has been included into many official standards worldwide. The ISO 9796 standard lists RSA as a compatible cryptographic algorithm, as does the ITU X.509 standard. The RSA system is part of SWIFT, the French financial industry's ETEBAC 5 standard, the ANSI X9.31 DSA standard and the X9.44 draft standard for the US banking industry. The Australian key management standard, AS2805.6.5.3, also specifies the RSA system. The algorithm is also found in Internet standards and proposed protocols including S/MIME, IPSec, and TLS (the Internet standards-track successor to SSL), as well as in the PKCS standard for the software industry. A number of other standards, such as IEEE P1363 and WAP's WTLS, specify the RSA algorithm as either an endorsed or a recommended system for privacy and/or authentication.

2.2.1.3 Products

The RSA cryptosystem is currently used in a wide range of products, platforms, and industries around the world. RSA is also built into current operating systems that are developed by Microsoft, Apple, Sun, and Novell. The RSA algorithm can be found in hardware devices such secure

telephones, Ethernet network cards and smart cards. According to RSA Security, RSA is being licensed by over 700 companies and the estimated installed base of RSA BSAFE encryption technologies is around 500 million. The majority of these implementations use the RSA algorithm, making it by far the most widely used public-key cryptosystem in the world.

2.2.2 Elliptic Curve Cryptography

2.2.2.1 Background

Elliptic curve cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an alternative mechanism for implementing public-key cryptography. In ECC, the public keys and private keys are defined as points on an elliptic curve.

Historically, the ECC algorithm was found to be too slow for any real implementation, although it offered greater potential security for the same key-length. Improvements in various aspects of implementation, including the generation of elliptic curves, have made ECC more practical than when it was first introduced in the mid 80s. Today, ECC has emerged as a promising new system for public-key cryptography, due to its potential to offer similar security to that of established public-key cryptosystems like RSA but using significantly reduced key-sizes. As a reference, a 160-bit ECC key is believed to offer the same level of security as a 1024-bit RSA key.

Certicom (www.certicom.com), which is founded by a team of cryptographers from the University of Waterloo in Ontario, Canada, has focused its efforts on improving the performance of the ECC algorithm. After many years of R&D, Certicom succeeded to optimise the algorithm and make it practical for industry use. To test the creditability of ECC, Certicom initiated the ECC Challenge, which offers an opportunity to create new methods of attacking the algorithm and help expose any weaknesses it may have. To date, only the 97-bit and 108-bit ECC Challenges have been solved.

To promote interoperability between disparate devices employing ECC, particularly consumer devices such as smart cards and PDAs, RSA Security has developed a new, patented technique known as 'storage-efficient basis conversion'. This technique enables efficient conversion between two ECC systems. Manufacturers designing chips to perform ECC computations generally build their hardware to be most efficient when processing only one of these numbering systems. Furthermore, the heavy storage requirement of current conversion methods has prevented the use of basis conversion, forcing manufacturers to choose one method or the other and resulting in the emergence of different, proprietary systems that create an obstacle to interoperability.

2.2.2.2 Standards

Standardisation efforts for ECC are well underway. X9.F.1, an ANSI-accredited standards committee for the financial services industry is developing two standards: ANSI X9.62 for digital signatures and ANSI X9.63 for key agreement and key transport. ECC has been incorporated into these standards:

ECC Standards	Schemes included
ANSI X9.62	ECDSA
ANSI X9.63	ECIES, ECDH, ECMQV
FIPS 186-2	ECDSA
IEEE P1363	ECIES, ECDH, ECMQV
IEEE P1363A	ECIES
IPSEC	ECDSA, ECDH
ISO 14888-3	ECDSA
ISO 15946	ECIES, ECDH, ECMQV

ECDSA - Elliptic Curve Digital Signature Algorithm
ECIES - Elliptic Curve Integrated Encryption Scheme
ECDH - Elliptic Curve Diffie-Hellman Key Agreement
ECMQV - Elliptic Curve MQV Key Agreement

Table 1. Standards Incorporating ECC

In particular, ECDSA is an analogue of the US Government's National Institute of Standards and Technology (NIST) Digital Signature Algorithm (DSA) but using elliptic curves. X9.62 will meet the unusually stringent security requirements of the financial services industry.

NIST has also extended its Digital Signature Standard (DSS) to include ECDSA as specified in ANSI X9.62. The revised standard, which is the Federal Information Processing Standard (FIPS) 186-2, is a landmark in the commercial acceptance of ECC since government agencies in the US are now able to purchase security products containing ECC without having to receive special approval. NIST is also including specifications for ECC in its Minimum Interoperability Specification for PKI Components (MISPC). NIST has developed the MISPC version 1 with industry partners: AT&T, BBN, Certicom, Cylink, DynCorp, IRE, Motorola, Nortel (Entrust), Spyrus, and VeriSign. The specification includes a certificate and Certificate Revocation List (CRL) profile, message formats and basic transactions for a PKI issuing signature certificates. The specification also defines support for multiple signature algorithms and transactions to support a broad range of security policies. This document has been formally published as NIST Special Publication 800-15.

ECC is also being incorporated into several ISO/IEC documents, including the following:

- ISO/IEC 9796-4: Digital Signature with Message Recovery, Discrete Logarithm-based Mechanisms
- ISO/IEC 14946: Cryptographic Techniques Based on Elliptic Curves

IEEE P1363, the standard specifications for public-key cryptography, has also included ECC as one of the approved public-key techniques. Besides, ECC has also been included in the Standards for Efficient Cryptography (SEC) by the Standards for Efficient Cryptography Group (SECG). SECG is a consortium comprises of leading providers of cryptography and information security solutions who have united to address the lack of interoperability between today's different cryptographic solutions – a problem that hampers developers of secure e-commerce and messaging applications.

The SECG members include 3Com, ABN-AMRO, American Express, Baltimore Technologies, BCI, Certicom, Cryptovision, Deloitte & Touche, Diversinet, Entrust, Ernst & Young, Fujitsu, Giesecke & Devrient, GlobeSet, GTE CyberTrust, Hewlett Packard, Hitachi Ltd., InterClear, Motorola, the National Institute of Standards & Technology, NTT Electronics, Pitney Bowes, Rainbow Technologies, Racal Security & Payments, Sun Microsystems, Thawte Consulting, Unisys, Visa International, VeriSign Inc, and Xcert International. This signifies support from the key players in the industry.

The SEC standard consists of two parts, namely the SEC 1 and the SEC 2 standards. These two standards define interoperable subsets of the general industry ECC standards from ANSI, IEEE and NIST. The SEC 1 standard defines a basic set of ECC functions such as MAC schemes, key derivation functions, and key agreement mechanisms. The second standard, SEC 2, provides a list of recommended elliptic curve domain parameters.

2.2.2.3 Applications

ECC is an emerging technology that is still being developed. It is not as widely implemented in applications as RSA or DSA. However, the design of ECC makes it especially useful in applications for which memory, bandwidth, or computational power is limited. It is well suited for implementation on devices that have limited memory and processing power, such as cellular phones, PDAs and smart cards. It is expected that ECC will increasingly be used in the m-commerce arena in the next five years.

2.2.2.4 Products

As of today, ECC has already been integrated into various security products. For instance, Baltimore Technologies (www.baltimore.com) has integrated Certicom's ECC technology into its entire line of security products and toolkits. Baltimore is also among the first to provide Java developers with a toolkit to work with elliptic curve algorithms. Other Baltimore products with new elliptic curve capabilities include its UniCERT CA software. Besides Baltimore's products, Certicom's technology has also been included in Xcert's CA software and NTT Electronic's software development toolkit, Nsafer.

Smart Cards in micro-payment applications will emerge with ECC capabilities and prototypes are being developed.

2.2.3 Advanced Encryption Standard

2.2.3.1 Background

The Advanced Encryption Standard (csrc.nist.gov/encryption/aes), or AES, has been developed to replace the Data Encryption Standard (DES), a secret-key encryption standard that has been widely used since 1975 when IBM invented it. The small DES key-size of 56 bits makes it relatively easy to break, considering today's computing power and thus inadequate for most present-day security applications.

From a final list of five AES candidates that includes MARS (IBM), RC6 (RSA Laboratories) and Twofish (Bruce Schneier et al.), NIST announced the selection of Rijndael as the proposed AES in Oct 2000. Rijndael was developed by two cryptographers from Belgium, namely Dr. Joan Daemen of Proton World International and Dr. Vincent Rijmen, a postdoctoral researcher in the Electrical Engineering Department of Katholieke Universiteit Leuven.

The Rijndael algorithm has been selected by NIST because of its security, performance, efficiency, and ease of implementation and flexibility. Rijndael performs very well in both hardware and software computing environments. The low memory requirements of Rijndael make it very well suited for environments with limited memory and processing power. Rijndael's operations are also among the easiest to defend against power and timing attacks. Like its predecessor DES, the AES is a block cipher symmetric-key encryption algorithm. However, unlike DES, Rijndael supports three key-sizes of 128 bits, 192 bits, and 256 bits, and is expected to provide a very high level of security for at least the next ten years.

2.2.3.2 Standards

NIST has announced that the AES has been incorporated into the Federal Information Processing Standard (FIPS), FIPS Publication 197, which specifies AES as an official encryption standard for use by US Government organisations to protect sensitive (unclassified) information. The Secretary of Commerce has approved the standard, effective from 26 May 2002. As is the case with its other cryptographic algorithm standards, NIST will formally re-evaluate AES every five years.

2.2.3.3 Applications

Hundreds of encryption products currently use DES or Triple-DES, and such systems have become almost ubiquitous in the financial services industry. According to GartnerGroup, DES will be made unsuitable for e-commerce by 2004 by advances in computing power. NIST anticipates that the stronger Triple-DES, which utilises 128-bit keys, will still be around for the next five years, although it suffers from performance issues. But DES itself will be phased out of use as it is coming near to the end of its lifecycle because 56-bit DES protected messages have already been broken. DES is currently permitted only on legacy systems in the US. Consequently, the selection of the AES may eventually affect millions of consumers and businesses.

2.2.3.4 Products

Since AES has been officially approved, conformance testing for products that implement Rijndael has been made available to the public. Conformance testing of the AES will be conducted under the Cryptographic Module Validation Program (CMVP), run jointly by NIST and the Communications Security Establishment (CSE) of the Government of Canada. Commercial, accredited laboratories test cryptographic implementations for conformance to NIST's standards, and if the implementation conforms, then NIST and CSE issue jointly signed validation certificates for those implementations. The thorough testing process for the AES should increase public confidence and eliminate suspicion of trapdoors or hidden weaknesses in the new algorithm. This will not only contribute towards interoperability, but also the credibility of the AES.

Baltimore Technologies will fully support Rijndael across its entire product range, including both its hardware and software products. RSA Security expects to make its implementation of the AES available first to RSA BSAFE customers as a standard part of software maintenance and upgrade contracts. In addition, the company also intends to make the AES a baseline encryption algorithm in the family of RSA Keon PKI products.

2.2.4 Key Management

2.2.4.1 Background

In the simplest case, when two individuals wish to communicate secretly, all that is needed is that they prearrange a key, which only they share. Using Public key cryptography, if each one generates a public key, keeping secret the corresponding private key, then only authentication of the public key, not secrecy, is required to allow the two to correspond securely.

For large pool of trusted correspondents, who wish to exchange securely a large number of secured messages with a limited resistance to cryptanalysis, it is necessary to change the key that is used in a frequent basics. Cryptographic keys must be electronically established between parties using either key agreement or key transport schemes. During key agreement, no keys are sent; information is exchanged between the correspondents that allow key computation. Key agreement schemes use asymmetric (public key) techniques. During key transport, an encrypted key is sent. Key transport schemes use either symmetric or public key techniques.

2.2.4.2 Standards

A Federal Information Processing Standard (FIPS) or NIST Recommendation will be developed to provide guidance for the life cycle management of cryptographic keys, including the generation, establishment, storage, cryptoperiod, recovery, and destruction o f key. Part of the recommendation is to define the acceptable key establishment schemes. The standard or recommendation will select Diffie-Hellman (D-H) and Menezes-Qu-Vanstone (MQV) key agreement schemes from ANSI X9.42, RSA key agreement and key transport schemes from ANSI X9.44, and Elliptic Curve key agreement and key transport schemes from ANSI X9.63. All three ANSI documents are currently in a draft form, but are expected to be adopted by ANSI in the near future. NIST intends to select a subset of the schemes specified in the draft ANSI standards. The scheme definition document will also include a specification for a key wrapping technique, whereby a symmetric key is encrypted using another symmetric key (e.g. an AES key is encrypted by an AES key).

2.2.5 Other Cryptographic Standards

2.2.5.1 IP Security Protocol

The IP Security Protocol, or IPSec, is a subset of the next-generation Internet Protocol (IP) called IPv6 (version 6). The current generation is IPv4 (version 4). IPSec offers at the network layer two security features, namely the provision of a separate authentication header and an option to encrypt the data in the payload. Taken together, the authentication and encryption services of IPSec provide a robust, standards-based security mechanism that will play a critical role in the continuing expansion of commerce and corporate operations onto the Internet.

The IPSec Working Group (www.ietf.org/html.charters/ipsec-charter.html) is a subcommittee under the IETF that is responsible for standardising IP layer security issues, such as encryption, data integrity and key management. Two other standards that are related to key management under IPSec are:

Simple Key-Management for Internet Protocols (SKIP) – An IPSec-compliant standard developed by Sun Microsystems. It is based on Diffie-Hellman technology and its purpose is to provide public encryption function at the IP level.

Internet Security Association Key Management Protocol and Oakley Key Determination Protocol (ISAKMP/Oakley) – This is another IPSec-compliant standard used for authentication and automated key exchange using Diffie-Hellman technology. IETF mandates IPSec and ISAKMP for IPv6 compliance.

Today, IPSec is primarily being used in VPN products. This will continue for the foreseeable future. However, as more IPv6 nodes get deployed (to deal with IPv4 address shortage and to fix end-to-end transparency problems due to NATs) it will become easier to deploy IPSec in the IPv6 network environments because IPSec is built-into IPv6. The industry still needs to solve some IPSec deployment issues such as lack of a robust key exchange scheme, difficulty for IT to troubleshoot network problems using packet sniffers, etc.

According to Intel, IPv6 implementations are expected to be available on PCs, servers, handheld, mobile phone devices and network processors in the near future. In the beginning these IPv6 "islands" (such as home and wireless mobile networks) connect to large IPv4 "clouds" using IPv6-to-IPv4 transition schemes built into edge devices such as routers and gateways. Some of the existing IPv4 systems may have to be upgraded to IPv6. These include network hosts and network routers. It is also generally felt that building a better understanding of the upgrade issues will help to smoothen the path of IPv6 deployment in the next 2 to 3 years.

It is expected that IPv6 will most likely be implemented in the future when the need to assign IP addresses to every individual arises, e.g. personal IP addresses for Internet-enabled mobile phones or PDAs. This will happen once the IPv6 infrastructure as well as its applications and services have been defined and established. It is also generally felt that building a better understanding of the upgrade issues will help to smoothen the path of IPv6 deployment in the next 5 to 10 years.

One such platform is the 6Bone project (www.6bone.net). The 6Bone is an IPv6 testbed that was set up to assist in the evolution and deployment of IPv6 on the Internet. The 6Bone started as a concept in 1995 and was made concrete by a formation meeting at the March 1996 IETF meeting in Los Angeles. There are currently 6Bone sites in Asia (i.e. Hong Kong, Japan, Korea, Taiwan, China and Singapore), Australia, Europe, and North America.

Japan may be the most advanced country in the world in terms of IPv6 implementation and deployment. Many of Japan's ISPs have already completed IPv6 testing and are in the final stages of deployment. Value-added services will subsequently be implemented on IPv6 networks. Furthermore, many Japanese equipment manufacturers, such as Hitachi, NEC and Fujitsu, have IPv6 routers ready for sale. The Japanese government has also announced plans to be IPv6 ready by 2005.

In contrast, in Singapore and elsewhere in the world, IPv6 related activities are still in the technology's nascent stage of development. Possible niche areas to exploit include IPv6 mobility and quality-of-service (QoS) support. IPv6 mobility support is an integral part of the IPv6 protocol stack and must be designed into an implementation from the beginning. Currently, most IPv6 implementations have not included mobility support, as that area is just being standardised. The other area to address is IPv6 mobility with QoS support.

2.2.6 Cryptographic Hardware

In response to the high processing demands of cryptography, a number of dedicated, hardware-based cryptographic accelerators have been developed. Acceleration offerings include cryptographic co-processors, chip sets, PC-boards, and PCMCIA cards.

2.2.6.1 Cryptographic Processor

At the chip level, Intel's next-generation 64-bit Itanium processor (previously codenamed Merced) provides several features that help to speed up public-key cryptography. Since public-key cryptography is the core of many security applications for e-commerce, such as SSL and

VPN, Intel believes that Itanium processors will greatly benefit the performance of these applications and enable the integration of additional security features into application software without compromising server performance. Security software companies such as RSA Security already plan to optimise their products for the new processor.

Intel currently supplies accelerators that boost SSL transaction performance at up to 200 SSL connections per second. Such an accelerator sits between the WAN router and the Web server and offloads computation-intensive SSL encryption and decryption operations from the Web server, thus boosting the overall performance of the e-commerce server.

2.2.6.2 Hardware Security Modules

Hardware Security Modules (HSM) are being developed as the fundamental technology that is essential to securing the foundations of existing and new emerging technologies such as Cryptography, Smart Cards, Biometrics, PKI, XML and their applications such as Database Encryption, Online Payment Gateway Systems, Verification Systems and Secure Time Stamping and Non Repudiation. There are two different fundamental causes that requires the existence of HSMs, the first would be the underlying weakness in current software based security, and the second would be concerning issues of trust and access.The essential function of a HSM would be the provision of a safe and trusted environment for cryptographic operations and the protection of Cryptographic keys.These HSM, also known as secure public-key–processing devices are designed to protect the creation, storage, and management of private keys. The private keys protected can include those used for additional-key generation, encryption, or digital signing. In this space, products must be designed to be certified to meet FIPS 140-1 Level 2 or 3. HSMs meeting FIPS 140-1 protect cryptographic modules from unauthorized operation and prevent unauthorized disclosure or modification of cryptographic modules and private keys.

Market leadership of the secure public-key processing devices market is held by nCipher for their nShield line of HSM devices with FIPS 140-1 Level 2 or Level 3 certified versions.There is a trend for applications to incorporate HSM as part of their integrated product offering, such as from Protegrity that specifically built their Database to interact with the nCipher HSM from the ground up. According to IDC, there will be an increase in market growth from less than US$20million at present to more than US$112.2million by the year 2005.

2.2.6.3 Trusted Computing Platform

IBM has developed the basic security technology that has been adopted by the Trusted Computing Platform Alliance (TCPA) in their Trusted Computing Platform Specifications 1.0. TCPA is a trade group representing some 145 technology companies. Compaq Computers, Hewlett Packard, Intel, IBM and Microsoft are among the group's sponsors. The specification defines how to design one of these trusted computing platforms and how to incorporate them. The IBM's security chip, an integral component of the specification, resides on a computer's motherboard. The hardware provides a security mechanism that uses both public and secret-key cryptography for creating digital signatures. The security chip is expected to add only about US$2 to the cost of a system, but costs may vary, depending on how manufacturers adopt the specification.

2.2.6.4 Others

Atalla is perhaps the most established provider of board-level hardware accelerators. Besides Atalla, Intel and IBM, Infineon Technologies, Baltimore Technologies, Rainbow Technologies and several others also offer hardware accelerators that help improve the performance of cryptographic processing. These hardware cryptographic devices are able to support various encryption algorithms such as Triple-DES and RSA, and some, like Baltimore's newer products, even support ECC and AES. Hardware solutions that boost the performance of SSL on Web servers are also available from these vendors.

2.2.7 Cryptographic Key Strength

Today, entry-level secret-key encryption generally starts with 40-bit keys. Although a higher level of security can be provided by increasing the key-length, a more realistic approach balances the cost of encryption with the level of risk. For example, while 40-bit and 56-bit encryption may be good enough for short-lived, time-sensitive information, they offer weak protection for long-lived, time-insensitive information such as trade secrets (e.g. the formula for Coca-Cola).

It should be noted that 56-bit DES keys have been cracked in less than three days using a US$250,000 computer[1]. The consensus among cryptography experts is that the minimum key-length for 'reasonably strong' security is 128 bits for secret-key cryptography, while a more conservative view maintains that commercial grade encryption will require up to 256 bits.

1 The US$250,000 DES Cracker was built by the Electronic Frontier Foundation (EFF). It broke RSA Security's DES Challenge II in 1998 and Challenge III in 1999, the latter in collaboration with Distributed.Net, a worldwide coalition of computer enthusiasts. Details are available at www.eff.org/descracker/.

For public-key cryptography, 512-bit RSA keys have similarly been cracked in five months using a distributed array of computers[2]. Consequently, the recommended minimum key-length for 'reasonably strong' security is 768 bits, while most commercial grade encryption will require up to 2,048 bits. For ECC cryptosystems, a 160-bit key is believed to provide equivalent security compared to a 1,024-bit RSA key.

When public-key cryptography is used for the secure delivery of the symmetric key, the size of the public key required is not directly proportional to the symmetric key size. For RSA cryptosystems, a minimum key size of 2048-bit is recommended for the secure delivery of a 112-bit symmetric key.

Security Level (in Bits)	Symmetric Scheme (Key Size in Bits)	ECC-based Scheme (Size of n in Bits)	DSA/RSA (Modulus Size in Bits)
56	56	112	512
80	80	160	1024
112	112	224	2048
128	128	256	3072
192	192	384	7680
256	256	512	15360

Table 2. Cryptographic Key Sizes

Currently, RSA 1024-bit key is considered as the standard key size. Many commercial products have already provided RSA 2048-bit key capacity. According to the security model proposed by Lenstra and Verheul, one should use RSA 2048-bit key for a commercial application in which the confidentiality or integrity of the electronic information has to be guaranteed until the year 2020. This might lead to much larger size keys for enhanced keys, keys even as 4096-bit long. Whenever the key size is double, RSA cost increased by a factor of eight. This means that the cost of doing RSA-computation for 4096-bit key would be around sixty-four time that of the current RSA implementation for 1024-bit key. In contrast, the ECC with equivalent security for RSA-4096 would require only ECC key of only 220-bit length. This is only 60-bit increase from the current standard length of 160-bit. This hardly affects the cost of the ECC cryptography.

In the current smart card, the implementation of RSA with 1024-bit key with a crypto-coprocessor requires 0.15 second for RSA computation. In the same smart card, the ECC implementation uses approximately one second for RSA computation without a crypto-

2 The RSA-155 (512-bit) Challenge was completed by an international team of researchers in 1999 using 292 individual computers located at 11 different sites around the world. Details are available at http://www.rsasecurity.com/rsalabs/challenges/factoring/rsa155.html.

coprocessor. Using the above model, the computation of RSA with 4096-bit key and ECC with 220-bit key will take about ten seconds and four seconds respectively in the same chip. Note that here the RSA figure is given using a crypto-coprocessor while the ECC figure is given without one.

2.3 Future Developments and Outlook

2.3.1 Market Trends

Being licensed by more than 700 companies globally, the RSA algorithm is the most widely used public-key technology in the world. With the release of the algorithm into the public domain, users of RSA no longer need to pay for the use of the algorithm. This will certainly boost the adoption of RSA technology for e-commerce.

ECC, an emerging cryptography technology, is gradually being accepted by the industry as a viable alternative to RSA. Although its adoption has been rather slow, the technology has evolved to be a strong and better alternative for implementing public-key cryptography, especially in mobile phones and PDAs. This will certainly create an impact on the market share of public-key technology that has been consistently dominated by RSA.

AES is the other emerging cryptography technology. It has been positioned to replace DES, which has been widely implemented in most banking and financial systems. Although Triple-DES has been used as the successor to DES in most cases despite its slower performance, it is envisaged that AES will take over to become the de facto encryption algorithm for securing commercial payment transactions.

2.3.2 Technology Developments

In this conclusion section, we would like to highlight the following trends and developments in cryptography to the technology innovators in the local Infocomm industry.

ECC Emerging. ECC adopted standards since 2000. Current research focuses on the implementation efficiency of these algorithms. We expect to see more security protocols being designed and proposed based on ECC, especially in wireless communication where small key size and low power consumption is favourable, e.g. authentication and identification protocol.

Developments in PKC. The latest development in private-key and public-key cryptography concentrates on its security proof and the formation of the security proof mechanism. The other area on public-key cryptography is to search for other methods that can be used to construct PKC besides factorisation, discrete logarithm and elliptic curve discrete logarithm.

Quantum Cryptography. This has generated a lot of interest and attention. The quantum properties of photons could make encrypted messages absolutely secure. Central to the technique are the strange laws of quantum mechanics that govern the universe on the smallest scale, and the ability to exploit physics on this scale has generated huge interest. Already experimental messages encrypted using quantum mechanics are being sent over tens of kilometres of optical fibers and received securely.

Identity-Based Cryptography. One of the most promising areas is identity-based cryptography, which was introduced in 1984 by Ali Shamir. Identity based means that the public key is the user identity, for example, user name, email address, IP address, telephone number, and etc. It is only very recent that the researchers solve a practical ID-based encryption based on ECC in 2001 (by D. Boneh and M. Franklin), but it uses a super-singular curves which is not a standard in ECC. For ID digital signature, there is an efficient scheme introduced by L. Guillou and J. Quisquater in 1988. With the identity-based cryptography, there is no need to have public key infrastructure at all. It only requires a few trusted centre authorities. The ID-based cryptography can be used to solve the key escrow and recovery problem. The current and future research emphasises on the studies of ECC security and its characteristics to build better ID-based protocols.

The other area of cryptography research is on theoretical proof of security and finding other hardness problems suitable for public key cryptosystem.

Assessment of the Various Cryptography Technologies. We would also like to highlight the following analysis in the area of cryptography for the consideration of adopters in the use of technology for competitive advantage.

AES is relatively simple to implement and should be easily deployed. There are many products available on AES today, and is proven to be more secure than DES and 3-DES. Compared to AES, ECC adoption may be less dramatic as it depends very much on its efficiency and scalability. However, ECC has got great potential for many products that handles with fixed size and curve pattern. The development efforts to make cryptography more efficient in terms of processing speed and performance by hardware design techniques and choosing an efficient algorithm, for example, FFGA, ASIC design and etc.

3 Smart Cards

3.1 Overview

Today, smart card usage can be found in sectors such as telecommunication, banking, transit, government & ID, healthcare, retail etc. It provides a key enabling technology across many different industries, catalysing profitability and operational efficiencies. As the world is moving toward globalisation, a common interoperable secure transaction framework for businesses and consumers would better bring e-commerce to the masses in both B2C and B2B sectors.

With $3.9bn in B2C and B2B e-payment value by 2005, merchants and banks are investing in new technologies to cope with the growing volume of transaction whilst maintaining payment and processing cost efficiency. New payment channels such as Internet, mobile phones and digital TV also emerge with the advancement and convergence of fixed and wireless technology. The growing concern on magnetic stripe cards cannot provide the protections necessary to thwart fraud and security breaches may propel smart card technology to the forefront of business transactions. The declining cost of smart cards is also one of the driving factors of the growing interest in smart cards.

Developing compelling applications for e-payment via wired and wireless payment channel would encourage consumer usage, improve their lifestyle and productivity, and in turn, encourage businesses to adopt e-commerce as one of their strategies to extend market reach regardless of geographical boundaries among other benefits such as customer retention. Yet, consumer confidence in e-commerce is still lacking today. Besides promoting awareness, there is a need to implement better security technologies and, more importantly, cheaper technologies so that businesses would be more willing to deploy them. There is also a need to look at the system risk and liability management, conducive legal support and monetary regulation, among other factors.

With the growth of e-commerce, card-based payment systems such as credit cards and e-purse for micro-payments are and will remain the most common online payment method. An estimated 400 million online sites accept payment by card. e-Visa, Visa's Internet unit, expects 10% of Visa's overall transaction volume to come from Internet purchases by 2003, up from 2% today. However, most of such card payment services entail only credit card numbers or PINs and do not exploit the technological benefits of a smart chip card that can work hand-in-hand with advanced security technologies such as digital certificates or biometrics.

3.2 Technology Developments, Applications & Standards

3.2.1 Types of Smart Cards

3.2.1.1 Cryptographic Cards

FIPS 140-2[3], the US federal standard for cryptographic modules includes four levels of requirements for environmental aspects, physical characteristics, software and operating system, key management and storage, and security of the cryptographic algorithms (e.g. RSA, DSA).

All operations are kept internal to the chip including key generation and secure storage, authentication, signature, encryption, one-way hashing, random number generation, etc. RSA smart cards are still widely adopted by the market. The downside to cryptographic cards is that the performance is still relatively poor for high-speed application usage.

3.2.1.2 Contactless Cards

Contactless cards are prevalent in the 1990s while development began back in the 1980s. Contactless cards are fast becoming the de facto smart card standard due to its convenience, speed of use, durability, increasingly capability in asymmetric cryptography and boosted by mass adoption via micropayment applications such as transit and others like door access. Contactless cards are especially well suited for the transport application, where 'the cards are many and the readers few'. Today, contactless technology is also finding its way into national ID card projects such as Japan's national ID programme that will be launched in August 2003, with typically dual interface (contact and contactless Type B) cards. Infineon estimates the worldwide market for chip cards to reach up to 4.5 billion cards in 2006, about 25 percent of which equipped with contactless technology.

Amongst the ISO 14443 standards for contactless proximity cards, there are 2 types of normative standards: type A and type B. Type A originated from patented Mifare technology from Philips and the popular commercial version is based on an enhanced proprietary version called type A Mifare – in which the contactless interface is based on hardwired memory logic. Type B is newer than type A standard and is oriented towards processor friendly applications. Type B is gaining

3 FIPS 140-2 is Federal Information Processing Standards that specify the security requirements for cryptographic modules. Please refer to section 4.3.4.1 for more details.

popularity as there is no license fee involved. However, command set specifications for type B to ensure interoperability between applications are still lacking in ISO 14443 specification.

There are many other proprietary types not accepted currently into ISO 14443 which are type C to G such as Sony's type C which is implemented in transit systems in Hong Kong and Singapore. More recently, there Philips and Sony have joined forces to develop 'Near Field Communication' products which are A and C compliant.

Type C cards are currently being used in the Hong Kong Octopus transport card and in Singapore Ez-link transport card. Amongst the advantages of Type C are faster speed (typically deployed at 211kbps while A and B types operate at 106kbps, theoretical speeds for A, B and C can be higher). Octopus cards are also used as a payment medium at selected fast food outlets, parking, vending machines, phone booths and loyalty programme. The established productivity and business benefits of contactless card technologies for ticketing and tolling are now spreading out from high-profile mass transit applications in major cities to numerous smaller-scale projects in mid-sized cities and towns. In the short term the transit sector will grow at a compounded annual rate of 24 percent to 2006 when there will be approximately 153 millions cards in circulation around the world according to Datamonitor.

There is also ISO 15693 for vicinity contactless cards that operates at longer ranges than proximity cards which is the more popular standard for tagging applications, such as in industry assembly lines, book tagging, CD tagging, for cargo and container fleet monitoring or for tagging rare species of fishes.

Contactless technology is also increasingly converging into platforms that have the following features:

- Dual interface to ease multi-applications/multi-services;
- Multi-Application Operating Systems (i.e JavaCard, Multos etc);
- Higher security than 3DES symmetric capabilities to further include asymmetric capabilities such as on-card crypto processing such as with ECC, especially when transit cards evolve into retail payments.

3.2.1.3 Hybrid & Combi Cards

Dual interface cards such as hybrid and combi cards are smart cards that provide both a contact and a contactless interface on the same card. Combi cards share the same processor and central circuitry but with two I/O interfaces (contact pads and contactless antenna), while hybrid cards contain two geographically separate processor/circuitry and I/O interfaces for

each contact and contactless functions. Type A Mifare cards are for example hybrid cards, whereby the contact interface rides on a CPU while the contactless interface runs on simple hardwired logic without a CPU (mainly for simple door access applications).

Cost of implementation remains to be an issue for deployment for dual interface cards. As such, dual interface cards are being adopted only at the organisational level and mainly for identification and door access, and to store digital certificates. Financial security standards today are also mostly built for contact chip cards, and hence to support legacy and financial applications, the contact interface is needed. In future, as contactless standards and products mature offering the same level of security as contact cards for example with asymmetric crypto-capabilities, we may fully migrate to pure contactless technology.

3.2.1.4 Mobile SIM Cards

SIM cards today offer up to 64 KB of memory. A typical GSM functionality would occupy about 8 KB of memory, with the rest of the memory space available for sale to other applications. With the advent of advanced mobile networks and data applications, SIM cards will evolve to USIM cards. The track on Mobile Wireless Roadmap has described in detail the evolution and trends in SIM cards.

The success of the SIM concept in GSM has ensured a steady and standardised evolution path to becoming an 'intelligent' SIM. The move to open platform like JavaCard technology will lead to hardware and software elements of smart cards becoming unbundled. The smart card and its success within the GSM network and from now on until 3G, continues to offer the operator a vital platform from which services can be deployed to help reduce churn, retain customer relationships and increase average revenue per user.

In the 3G world, the opportunities for developing and introducing more complex and sophisticated 'intelligent' SIMs will depend on the demand for new applications. The 2G world focused on technology-based solutions rather than customer-driven services. For 3G, the focus will be on how consumers interact with technology, how they will personalise their service bundles and how payment for services will be made. 4G will focus more on security requirements especially when data applications would have stabilised after the 3G era and the SIM card will be an important enabler to make improvements to security.

3.2.1.5 USB Dongles

USB ports are now a standard feature on PCs. Products such as iKey from Rainbow Technologies (www.rainbow.com) and eToken from Aladdin Knowledge Systems (www.ealaddin.com), have raised eyebrows. These hardware tokens works by plug-and-play into a USB port and can carry as many as up to four different X.509v3 digital certificates on average, providing hardware cryptography such as 1024-bit RSA. They are usually Microsoft PC/SC standard compliant and compatible with Windows 98, ME, XP, NT and Windows 2000. They can also be carried on a key ring together with your house-keys. The communication rate between a USB dongle and the PC is also many times faster than that between a smart card and the PC. The iKey, for instance, runs up to 160 times faster than a smart card.

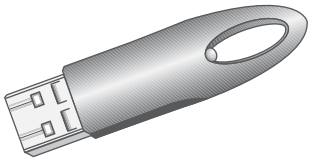


Figure 2. USB dongle from Rainbow Technologies

Among its first implementations were e-government applications over the Internet for interaction with consumers and commercial businesses. Some are taking into consideration the trend of reader-less solutions such as USB tokens, which provide a scalable, economical, secure and portable means of authentication. However, the current price tag is still quite high and can cost up to S$100 per token. Manufacturers are also increasing the memory capacity of such tokens, with current capability up to 32 Kbytes of memory.

The current ISO7816 for contact cards is undergoing amendment to integrate USB2.0 speeds of up to 480Mbps. This will help to produce standardised products for USB tokens that can offer not only high storage capacity but also much faster transaction speeds when compared to current speeds of typically 9.6kbps.

3.2.1.6 Software Smart Cards

Web browsers such as Internet Explorer and Netscape Navigator now provide PKI support where the private keys and certificates are typically stored on a disk. Because keys stored in software on a disk (or even inside a PDA) can be easily copied and stolen, the security of the private key therefore relies on the password that is used to protect it. These keys are extremely vulnerable to offline cryptanalysis and could be easily cracked by performing a dictionary-search, especially if the password used to protect the keys is easily guessable.

To address this weaknesses of software-based keys, Arcot Systems (www.arcot.com) has pioneered and patented an innovative technique called cryptographic camouflage that camouflages keys in a manner that makes it difficult to determine if a decrypted key is the correct one. The only way to verify this is to try the key on the authentication server, which will fail if the key is indeed incorrect. The system can be set up to monitor these repeated authentication failures and 'lock' the particular account, just like in the case of a smart card.

Arcot claims that this 'software smart card' technology is almost as secure as hardware smart cards and is able to provide the requirements for two-factor authentication. It has incorporated this technology in its product family (i.e WebFort, AccessFort & TransFort) that is designed to work with digital certificates and keys issued by a CA and provides roaming support for the online download of digital certificates and camouflaged keys.

This solution essentially enables digital certificates to be used without the need for secure hardware storage such as smart cards and USB dongles. While the technology does not provide the same security as smart cards, it does offer a reasonably strong, yet very convenient and less costly solution for online authentication, with all the features offered by a regular PKI.

3.2.2 Smart Card Standards

Within ISO, the standards on smart cards reside primarily in ISO 7816 (for contact cards) and ISO 14443 (for contactless cards).

3.2.2.1 ISO 7816

Contact cards are standardised through ISO 7816. These standards describe for example the chip's physical characteristics, dimension and location of contacts, signal and transmission protocol, inter-industry commands for interchange, numbering system and registration procedure for application identifiers, inter-industry data elements, inter-industry commands for Structured Card Query Language, security related inter-industry commands, inter-industry enhanced commands (under draft), and signal protocol for synchronous cards.

There are new initiatives to develop ISO 7816-11 on personal verification through biometric methods, ISO 7816-12 on USB electrical interface and operating procedures and ISO 7816-15 on Cryptographic Information application.

3.2.2.2 ISO 14443

Contactless cards can be classified into three classes: close coupled, proximity cards or vicinity cards. The common contactless smart cards are proximity cards (ISO 14443) while RFID tags used mainly in industrial and car-parking facilities are vicinity cards. The distinction is made mainly by their read/write operating distance. As such, close coupled cards work at distances below 2 mm, proximity cards at about 10 cm maximum, and lastly vicinity cards at about 70 cm to 1 m. Our focus is on proximity cards.

ISO 14443 (parts 1 to 4), which has been completed as an International Standard in Dec 2000, is based on ISO 7816. It describes RF power and signal interface, initialisation and anti-collision for multiple card presence and the transmission protocol. Recently, a new project was proposed to work on ISO 14443-5, specifies compatibility guidelines for proximity cards, with contact card protocol developed under ISO 7816-3 and ISP 7816-4.

3.2.2.3 PC/SC

Core members of the PC/SC Workgroup (www.pcscworkgroup.com) include Apple, Gemplus, Hewlett Packard, Intel, Microsoft, Schlumberger, Philips, ingenico and Toshiba. The PC/SC specification is independent of PC platform and OS, but it has so far mainly been implemented on Windows.

As of today, most smart card readers already conform to the PC/SC standards. This would encourage interoperability for smart card readers. Windows 9x, XP, NT and 2K already incorporates smart card reader drivers. Current readers for smart card and biometrics come in a variety of interfaces: RS232 (serial port), PCMCIA, PS/2, USB port, etc.

3.2.2.4 Smart card reader APIs

The SS 467: 1999 Specification for Smart card reader APIs was initiated at a time before PC/SC was established, and there was a need for standardization. While that effort achieved some level of standardization, it did not quite address multi reader and multi vendor support. This standard attempts to address these limitations, and at the same time, address the issue of running PC/SC readers on old applications. It extends and replaces the SS 467:1999, a preceding specification for Smart card reader APIs.

This standard is not meant to compete or replace PC/SC. In fact if there is a need to write a new Windows based application, and the smart card readers selected are compliant with PC/

SC API standard, then PC/SC API is the logical and best choice. This extended API is meant for adapting old applications to work with PC/SC compliant readers with little change, or needs to operate with both old (SS 467:1999) and new (PC/SC). At the same time, this extended standard can be used, in areas where PC/SC API does not apply.

This standard is aimed at Smart Card Reader (SCR) Suppliers who need to supply drivers, and application developers who need to develop software that operate with SCRs. The reader API we do is similar to efforts in Europe on FINREAD (financial reader) initiative under the EU Smart Card Charter trailblazers where the objective is to provide a standard to harmonise across different card reader manufacturers, so that the intended application can be supported by multi-vendor readers.

3.2.2.5 OpenCard Framework

The OpenCard Consortium (www.opencard.org) includes members such as 3-G International, Amex, Bull, Giesecke & Devrient, First Access, Gemplus, IBM, Toshiba, Visa, Towitoko, Schlumberger, Sun Microsystems, UbiQ Inc, Siemens and XAC Automation. The consortium has released the OpenCard Framework (OCF), which is an object-oriented software framework for smart card access, essentially built on the Java programming language. Within the Windows environment, OCF can utilise the PC/SC smart card reader drivers. OCF aims at achieving transparency for the application programmer with regards to smart card OS, card terminals and card issuers. In contrast, PC/SC primarily addresses transparency with regards to card terminals and card OS (to a limited extent), but neglects the role of the card issuer.

3.2.3 Multi-Application Card Standards

3.2.3.1 Java Card

In terms of security certification, Java Card platform has compliance with FIPS 140-1. Generally, most of the Java Card vendors are focusing on an attainable security level of common criteria EAL 4 as specified in the smart card protection profile[4]. Java Card vendor, Sun Microsystems, is underway to strengthen the security of the Java Card and the new Java Card Specification version 2.2 was released on April 2002 include support for both AES and Elliptic Curve cryptographic algorithms. It is important to ask for the evaluation report when a vendor claims to achieve a certain level of security assurance. Java Card technology's compatibility with

4 Please refer to Smart Card Protection Profile at section 4.3.4.2 for more details.

existing smart card standards ranges from organizations such as the internationally recognized ISO to industry-specific standards bodies such as GlobalPlatform, Europay-MasterCard-Visa (EMV), European Telecommunications Standards Institute (ETSI) and the Third Generation Partner Project (3GPP).

Java Card Security	
Advantages	**Disadvantages**
• No dynamic class loading • Ttransaction atomicity • No threading • Applet firewall • Cryptographic signing & authentication	• Applets added post issuance • No sandbox • Native method calls • No garbage collection • Object sharing complexity • Out of band verification

Table 3. Java Card Security Features

Financial institutions in Europe, Asia and the United States such as American Express, Citibank and Visa have deployed millions of Java Card technology-based smart cards that support value-added services including stored value, Europay MasterCard Visa (EMV) debit/credit, loyalty, and Internet public key authentication.

Government agencies in US are currently issuing Java Card technology-based smart cards as their new identification cards to replace existing "paper" identification cards. Most recently the US Federal Aviation Administration (FAA) named Java Card technology as the platform of choice for the Transportation Workers (TW) card, the first national identity card for transportation workers. The Department of Defense is issuing a Common Access Card to 4.3 million active duty U.S. military personnel and eligible contractors. The Government of Taiwan will deploy a Java Card technology-based smart card as their new health insurance identification card to all 24 million residents.

Telecommunications carriers such as China Mobile, France Telecom, Hong Kong Telecom, Orange, Swisscom, Telecom Italia Mobile and Telefonica have deployed millions of Java Card technology-based SIM cards worldwide. Java Card technology-enabled SIM cards allow operators to provide secure, innovative services on mobile devices.

One of the largest contributions to the development of Java Card technology came from the Java Card Forum (JCF at www.javacardforum.org), founded in 1997 by the smart card manufactures, issuer and smart chip manufacturers. The primary purpose of JCF is to promote Java as the preferred programming language for multiple-application smart cards. There is also new task force looking into integrating biometric with Java card, thus proving a secure

platform for enrolling and managing biometric data. The new Java Card 2.2 Biometry API Proposal was published on April 2002.

3.2.3.2 MULTOS

MULTOS (www.multos.com) stands for Multi-Application Operating System and is driven by MAOSCO, a consortium comprising in the core 12 companies namely Aspect Software, Dai Nippon Printing, Discover Financial Services, Europay International, Fujitsu Group, Giesecke & Devrient, Hitachi, Infineon Technologies, Keycorp, MasterCard International, Mondex International and SchlumbergerSema.

I.Life card by Pacific Century, Hong Kong's incumbent telco, and HSBC, the largest retail bank in Hong Kong has launched a multi-application 16 KB MULTOS MasterCard with functions such as credit/debit, Mondex e-purse, loyalty, calling card, digital ID using PKI (only digital ID and Mondex is on the chip). A merchant's website needs to be set up to authenticate I.Life cardholders. Pacific century and HSBC will issue free card readers to encourage the use for e-commerce.

The following is a schematic example of some possible multi-applets on the MULTOS platform.

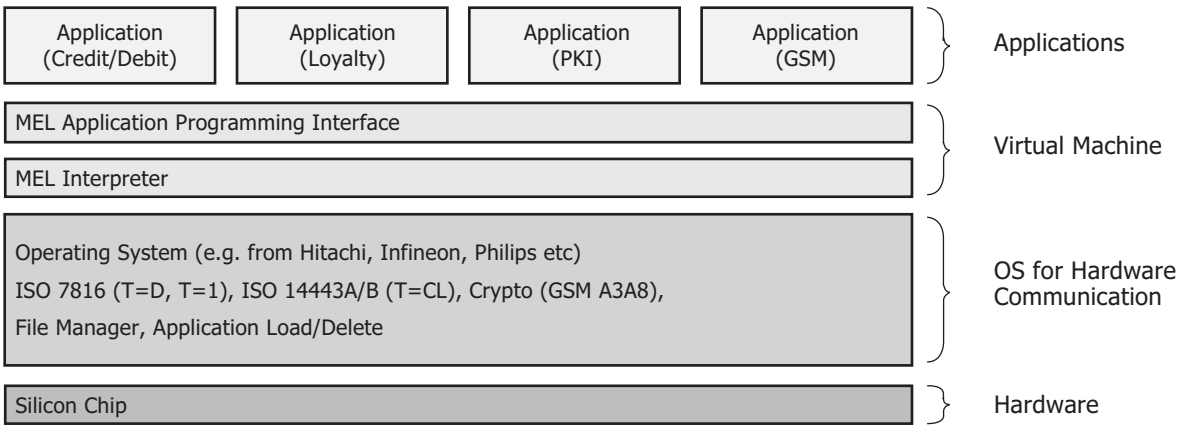


Figure 3. MULTOS Multi-layered Architecture

MULTOS provides application firewalls, secure load and delete mechanisms and memory management, and is the only smart card to be certified ITSEC E6 (equivalence to EAL 7), the highest level of security assurance under the ITSEC security evaluation scheme. It follows an issuer centric business model that allows control over which applications can operate over which interface. An RSA co-processor may be available in contactless mode (implementation

specific) for loading and deleting MULTOS applications over the air. A PKI applet would occupy about 5.2 KB on EEPROM on MULTOS. MULTOS is positioning itself strongly in the financial and mobile fields thanks to its strong security.

There is currently no royalty cost for MULTOS implementation. However, an ITSEC E6 security evaluation may cost over US$600,000. A licence for implementer would be around £250,000 upfront and £50,000 per annum. A MULTOS chip costs about US$7 with RSA co-processor. Similarly, this cost increases with if more application space is required. There is, however, a fixed CA cost for MULTOS of US$0.04 per application per card and per load or deletion.

MAOSCO is marketing MULTOS to be the only operating system that supports all high-level languages. SwiftCard Technology is developing a Visual Basic-to-MEL translator, while earlier in 2000, it announced the Java Compiler SwiftJ to convert Java applets into MEL. MEL is the assembly language used for writing applications in MULTOS cards. Visual Basic is used by Microsoft Windows for Smart Card. It is worthwhile noting that Chipper International, which used to have its own proprietary Chipper ServiceBoX operating system has completed the porting to the MULTOS platform.

3.2.3.3 Windows for Smart Cards

Although Microsoft's Windows for Smart Cards (WfSC) had a very strong initial impact, It was hampered by early performance and architectural problem. Microsoft now does not directly support this product.

3.2.3.4 Global Platform

Global Platform (previously known as Open Platform) is establishing standards for smart card infrastructure that enable issuers to capitalize on the power and promise of this new technology. Visa first developed the Global Platform card and terminal specifications (www.visa.com/nt/suppliers/open/main.html) to promote the use of smart cards and ensure their interoperability. In 1999, together with several other companies, Visa founded GlobalPlatform Inc., a cross-industry association with the objective to promote and further develop the Open Platform standards. Members of GlobalPlatform include Amex, JCB, Microsoft, Sun Microsystems, telcos such as BT and Telstra, chip manufacturers and system integrators.

Global Platform version 2.1 defines card specifications, terminal specifications and support infrastructure for multi-application smart cards. It is ISO 7816 and EMV compliant, uses

firewalls to separate applications on the card and runs an on-card manager in charge of commands and dispatch, content and security management. It is now compatible with Java Card and MULTOS.

3.2.4 Payment Standards

There are several means of payment possible such as cash, cheques, GIRO and electronic fund transfers, wire transfer services, operator billing, loyalty points, virtual cards, payment cards such as credit, debit and e-purse micro-payment cards. E-commerce can occur via a PC, an Internet enabled point-of-sale terminal, ATM, Internet appliances and kiosks, digital TV, mobile devices (e.g. PDAs, handsets), set-top boxes and even vending machines.

The horizontal core standard for financial applications is the EMV, initiated by Europay, MasterCard and Visa. It provides a building block for other specific standards such as SET/ C-SET (chip SET), 3D-SET (Three Domain SET) and wallet servers. Building on both EMV and SET is the CEC (Chip Electronic Commerce) standard. Finally, in the particular vertical domain of e-purse applications for micro-payments compliant to EMV, we have two dominant standards, namely CEPS (Common Electronic Purse Specification) driven by Visa against Mondex by MasterCard.

3.2.4.1 EMV

Representatives from Europay, MasterCard and Visa came together in 1993 to collaborate on a global industry specification for chip cards, terminals, and applications to ensure consistent, secure interoperability for payment systems. In June 1996, the first release on EMV Integrated Circuit Card Specifications (EMV 96) was made available for debit and credit products. The specifications were meant also to ensure that minimum standards for risk control and security are applied. Visa then customised these specifications to address the unique requirements of Visa Smart Debit and Visa Smart Credit by creating Visa Integrated Circuit Card Specifications (VIS). The EMV specifications were followed by various banking implementations with country specific customisation throughout 1997.

Europe's deadline for EMV chip card migration for banks is 1 Jan 2005, while the tentative deadline for Asia Pacific as 1 Jan 2006. There are implications for mobile payments, smart card payments if you need to be compliant to accredited financial industry standards. EMV 2000 version 4.0 is the latest version available since Dec 2000. The EMV migration currently affects the card platform specification for the contact interface. Hence, any chip card or SIM card that needs to be compliant to credit/debit functions will be implicated. EMV currently

does not endorse contactless chip cards but have in plans to define specifications for contactless cards as well as low voltage chip cards.

The EMV movement would indeed have favourable impact on the deployment of smart cards for more secure financial transactions. All ATMs in Europe would be EMV compliant by the 1st January 2005 or banks will bear the consequences of liability shifts in case of fraud. The migration has already started and is expected to meet the deadline. Many countries in Asia have also started implementation, but Visa expects 90% of Asia Pacific's card issuers and merchants to migrate only by 2008.

To date, Visa has issued five million EMV chip payment cards in Asia Pacific and has launched a number of initiatives to accelerate migration, with the purpose of making the change from magnetic stripe to chip as smooth as possible for financial institutions, cardholders, members and vendors. These initiatives include introducing cost-effective chip cards starting from just 99 US cents, as well as new global standards. Visa and its members have also contributed US$25 million to support banks, vendors and industry partners in their migration towards chip cards.

EMV 2000 version 4.0 is the latest version available since Dec 2000. The EMV migration currently affects the card platform specification for the contact interface. Hence, any chip card or SIM card that needs to be compliant to credit/debit functions will be implicated. EMV currently does not endorse contactless chip cards but have in plans to define specifications for contactless cards as well as low voltage chip cards.

There are currently two levels of EMV certification or type approval. Level 1 consists of certifying the terminal chip card interface. Terminals can include not only integrated POS, standalone POS, ATMs but also mobile phones, set top boxes and unattended payment terminals. The level 1 testing involves electromechanical characterisation, logical interface testing, and transmission protocol testing. Level 2 consists of certifying the payment application according to the credit/debit specifications of EMV. This includes the testing of the Application Kernel in an EMVCo accredited laboratory - the application kernel is the part of the terminal payment application that deals with EMV specific functions. This testing does not necessitate testing on the acquirer infrastructure – note that this means that payment systems are not included in level 2 testing.

There are currently only 9 accredited laboratories for EMV certification. There is only one accredited laboratory for Asia Pacific region which is located in Tokyo for both level 1 and 2 testing. Companies can apply to be an accredited laboratory to EMVCo. The rest of laboratories are in Spain, France, England, Germany and Denmark (offer both level 1 and/or 2 services).

Asia Pacific	Europe	Americas
• All new acquiring bank-owned smart card terminals are required to be compliant with industry-wide EMV specifications effective on Jan 2003. • Priority markets - Japan, Taiwan, Korea & Malaysia. • Japan – Card fraud focus and multi-application preferred. 6 mil cards and several thousand terminals in 2002. • Taiwan – Card fraud driven. Bankers Association migration underway and First Commercial Bank already issuing. • Korea – Product differentiation driven: multi-applications/ contactless focus for mobile credit cards, citizen's and loyalty cards. • Malaysia – Card fraud driven. Migration plan in 2002/2003. • Australia – ANZ launched EMV cards in 2001.	• UK – World's first EMV migration project. Currently 30 mil EMV cards, 300 K terminals and 20 K ATMs. • France, Spain, Germany, Italy – major migration to be completed by 2004. • Planning underway in Greece and Sweden. • Critical mass should be achieved by end 2004.	• USA – Six major issuers of EMV cards with 8 mil cards currently and expecting 20+ mil by end 2002 • Canada – expected to start migrating in 2003. • Latin Americas was migrating aggressively. Brazil started (2 mil cards and 500K terminals). Mexico, Venezuela, Chile, Colombia and Argentina aim to start in 2002.

Table 4. MULTOS roadmap from 1997 to 2002
(Source: Asia Pacific Smart Card Association) Chip Electronic Commerce)

3.2.4.2 Chip Electronic Commerce

The EMV Chip Electronic Commerce (CEC) specification defines the use of EMV-compliant debit or credit chip cards for payment transactions in the e-commerce environment using the SET protocol. It leverages on 2 existing specifications, EMV 96 version 3.1.1 and SET version 1.0. Compliance with EMV 96 ensures that chip cards will operate in all chip readers regardless of location, financial institution, or manufacturer. It also provides key features for online card authentication using cryptograms and for cardholder verification through an optional cardholder PIN. SET provides confidentiality, data integrity, interoperability, and merchant authentication, facilitating secure debit and credit card payments for e-commerce based purchase transactions.

EMV Chip Electronic Commerce is organised as follows:

Part I: System Architecture. Definition of the components of the EMV/SET system and the requirements placed on each;

Part II: Transaction Processing. Definition of the requirements for and manner in which transactions are to be processed in the EMV/SET system.

SET has not picked up due to the cost of implementation amongst other possible reasons. In fact, Visa's strategy is now shifted to "Verified By Visa" and 3D Secure. Some of these payment trends are already described in Mobile Wireless Roadmap under the Wireless Payment and Charging chapter.

3.2.4.3 Common Electronic Purse Specification

Common Electronic Purse Specification (CEPS) is a comprehensive set of specifications that enables domestic and international interoperability for electronic purse (e-purse) schemes worldwide. It is undergoing enhancements to include support for a contactless smart card interface.

CEPS appears to hold the promise of bringing interoperability to e-purse micro-payment schemes worldwide. If so, it will deliver significant benefits to consumers. There are currently many proprietary e-purse schemes or stored value programmes implemented such as VisaCash, Europay CLIP, Proton World's Proton, Singapore NETS CashCard, Germany's Geldkarte to name a few. However, all these standards and about 90% of e-purse schemes are committed to CEPS migration, except Mondex. Most will also be EMV-compliant. Basic services provided would be purchase, load, unload (optional), currency exchange (optional), subsequent debit, cancel last purchase, and purchase reversal.

To date, Visa has developed the Visa Cash Electronic Purse Specifications, which comply with the Common Electronic Purse Specifications (CEPS). With Visa Cash CEPS, Visa Cash can be used across borders, virtually anywhere, anytime. The number and range of devices that can accept electronic purse cards are increasing rapidly from vending machines to cellular phones to PCs. It enables card issuers to offer cardholders the ability to use their cards overseas, eliminate the need to carry coins and bills in multiple currencies for traveller. There are more than twelve million Visa Cash cards worldwide used in 50+ Visa Cash programs operating in 17 countries and on the Internet.

With the promise of more CEPS products to come and the fact that the security of CEPS could be enhanced by the use of digital certificates, CEPS is most likely to enter the market in a more aggressive manner in the near future.

3.2.5 Major Initiatives

3.2.5.1 e-Europe

The eEurope Smart Cards initiative aims to accelerate and harmonise the development of smart cards across Europe and to establish them as the preferred mobile and secure access key to citizen information society services. As outlined by the eEurope Smart Cards (eESC) initiative, Smart cards is an essential component of the eEurope Action Plan to bring the benefits of the Information Society to all Europeans.

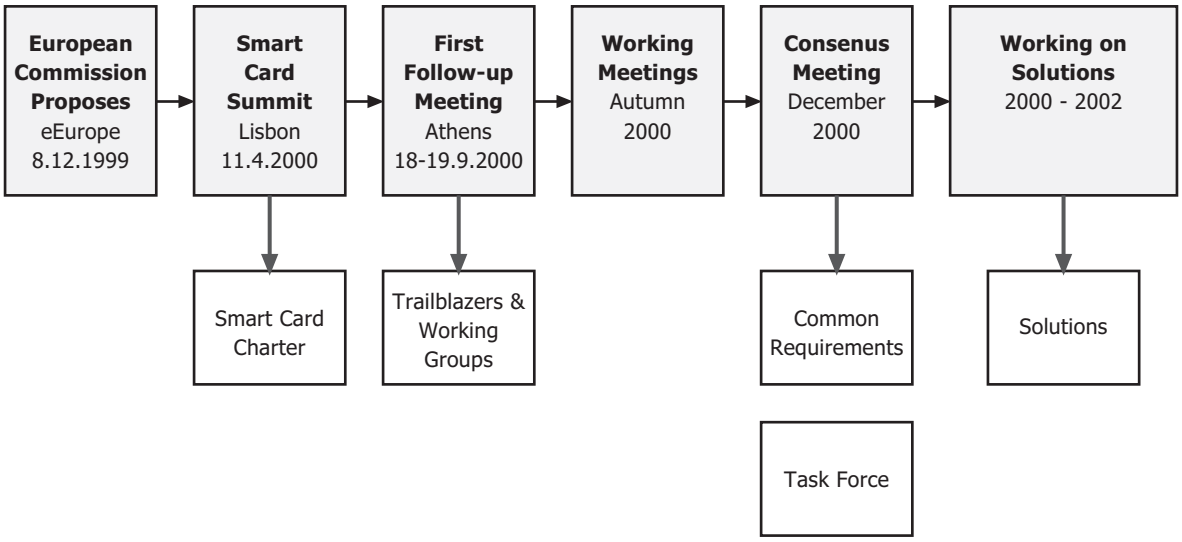


Figure 4. Roadmap of the eEurope Smart Card Initiative
(Source: European Commission)

Established in spring 2000, the work of eESC initiative has resulted in (among others) an emerging smart card infrastructure and a maturation of the generalised common specifications to a interoperability framework. The eESC stated that the future of the smart card is dependent on interoperability, which includes the use of smart cards in secure public identification and authentication, e-government, e-payments, health, transportation. Technical issues such as interoperability, security certification, card readers, multi-application, contactless cards and

consumer requirements for ease of use are also under consideration. Emerging trends such as "Systems on Cards" and single multi-application cards are progressing to a future where the user will have the ability to customise the applications on his card. With this in mind, the eESC has released the "Global Interoperability Framework for Identification, Authentication and Electronic Signature with Smart Cards" in August this year. In addition, in June this year, the EU endorsed the Commission eEurope2005 Action plan to extend the initiative to 2005.

In a parallel effort, eESC has issued a call in to establish an FP6 network of excellence for the eEurope2005 programme for the clustering of EU funded smart card projects. A network of excellence is broadly to provide a communication and cooperation infrastructure for a specific, strategically important area of information technology. Networks contain a number of members, such as active researchers in both academia and industry. The aim is to avoid unnecessary duplication and foster the sharing of ideas about matters of common interest across application domains.

One of the projects in the above network of excellence cluster is Finread. Finread, a consortium of major European operators of the electronic payments and finance sectors, supported by the European Committee for Standardization, develops technical specifications for smart card readers that allow electronic payments on a PC via the Internet. It has released the first technical specifications for a smart card-reading device to be connected to the Internet through a personal computer. Referred to as FINREAD, this EMV compliant chip card reader is explored to secure payment transactions, and to authenticate and protect the confidentiality and integrity of sensitive personal data transfers. Examples of applications for Finread include E-government and access to social welfare systems.

3.2.6 Local Standards

3.2.6.1 Cards & Personal Identification Technical Committee

In Singapore, the Cards & Personal Identification Technical Committee (CPITC) at www.itsc.org.sg/tc/5th_term_compo/cpitc.html) evolved from the former Smart Card Technical Committee (SCTC). The former SCTC is the industry group responsible for setting, standardise and promoting smart card standards. It is one of ten committees set up under the Singapore IT Standards Committee (ITSC at www.itsc.org.sg), which spearheads the development of infocomm standards in Singapore. To date, The CPITC has established a common API for card readers to ensure interoperability between readers in Singapore, prior to the existence of the PC/SC specifications. It has also released an extension to ISO 7816 Part 4 to accommodate the e-purse specifications used by the NETS CashCard.

3.2.6.2 Asia Pacific Smart Card Association

The Asia Pacific Smart Card Association (www.smartex.com), APSCA, promotes a closely knitted smart card community in the Asia Pacific region covering countries like Hong Kong, Malaysia, Taiwan and Singapore, with plans in 2001 to include China, Japan and Korea. The members of APSCA come from varied sectors of smart cards from suppliers to users, including consultant firms and software developers, a smart card service directory is provided by the organisation for users in the region including Singapore. It is the interest of the whole Asia Pacific region to promote awareness of smart card development, dialogue, co-operation and interoperability in the realm of smart cards where often or not, exclusive business partnerships spur a fragmented market and customer base.

3.2.7 Global Standards

3.2.7.1 FIPS PUB 140-2

FIPS 140-2 (as last updated on Oct 2001) is the revised standard based on FIPS 140-1 and the new requirements needed to meet the technological and economic change. As of May 26, 2002, NIST and CSE will only accept validation test reports for cryptographic modules against FIPS 140-2 and the FIPS 140-2 DTR. However, FIPS 140-1 validated modules may continue to be procured. Please refer to the following URL for a comparison of the security requirements in cryptographic module in FIPS 140-1 and FIPS 140-2 at csrc.nist.gov/publications/nistpubs/800-29/sp800-29.pdf.

3.2.7.2 Common Criteria: Smart Card Protection Profile

This Smart Card Protection Profile (SCPP) at csrc.nist.gov/cc/sc/Scsug.pdf (released on September 2001) describes the IT security requirements for a smart card to be used in connection with sensitive applications, such as banking industry financial payment systems. This Protection Profile (PP) is applicable to both contact and contactless smart cards, without special regard for form factor or physical card security features. This PP does not cover security requirements for card terminals or networks interfacing with them. It is anticipated that application-specific PPs or security targets could be developed that would incorporate the requirements in this PP as their foundation. In addition to the security requirements specified in this protection profile, individual applications may have additional security requirements specified in their own protection profiles.

NIST and the US General Services Administration also establish a Government Smart Card Interoperability Specification (GSC-IS at.smartcard.nist.gov) aim in providing an open and standard method for using smart cards.

3.3 Future Developments and Outlook

3.3.1 Market Trends

While they may have seemed less than appealing to businesses because of high costs, lack of standardisation, interoperability issues or potential manageability problems, smart cards are finally finding a place in today's cyber and physical security infrastructure. From network authentication and physical access to securing transactions taking place over the Internet, smart card-based applications are predicted to continue their march on the global market. For instance, analyst firm IDC projects that by 2003 the world-wide smart card market will reach $5 billion. E-purse and cashless vending, PC secure log-on, all-in-one employee IDs, banking and medical authorisation, and still other applications, are predicted to abound because of the smart card.

Smart card technology could, quite easily, solve this dilemma through its multi-application capabilities. A smart card's flexible storage capacity makes it possible not only to carry one card for a broad variety of applications and services both in web-based and physical environments, but also allow the user to customise the bundling of applications for each card. With this in mind, a business traveller could customise his or her card to hold all travel-related data, such as corporate credit accounts, frequent flyer, hotel and rental car memberships, etc. Another card could contain all Internet and online account passwords and credit card information.

Smart Card Applications that are moving towards multi-applications and multi-services card are in Transport, Telecom, Banking, Healthcare, Retail, Nation IDs card, E-payment via E-commerce, M-commerce & T-commerce and IT security (such as Cyber & Physical access).

3.3.2 Standards Developments

EMV will be the de facto basic financial standard. CEPS has progressed very slowly although most current proprietary e-purse schemes providing compatibility and interoperability products with CEPS. The EMV dateline in 2005 will convert Europe into a chip card society. Fraud may shift to other parts of the world as a result, urging a worldwide movement to pursue higher security for e-commerce.

Open platforms are growing in market share and will require more powerful engines. However, proprietary platforms will still have biggest market share in the next few years. In several closed environments, proprietary standards are seen as more secure and scheme owners need not risk sharing data with interoperable applications, thus in full control of their customer data and transactions. Proprietary standards will still exist simply because companies that have strong technology offers would like to maintain their status quo. Multi-application platform standards are yet to be unified but there are increasing collaboration and interoperability between the main contenders.

Most of the standards trend will require the migration of infrastructure. Vertical industry standards are still necessary to customise basic horizontal standards into useful implementations for that particular industry sector. As such, interoperability between cross-disciplinary alliances is sometimes pursued for the benefit of all in a bid to increase customer base.

Acceptance of applications and standards will also depend on the convenience for users. As smart card technology booms around the world, some of the most popular applications include:

- Financial - credit, debit, stored value
- Government - staff ID, secure access and authentication, healthcard, passport and citizen ID with both biometric and smart chip
- Healthcare- patient ID, portable patient information and network access/authentication in smart chip
- Schools - student/staff ID and multipurpose campus cards
- Transit- electronic payment for public transportation and toll roads
- Telecom - subscriber ID and mobile e-commerce
- Retail - payment, loyalty and e-commerce
- Corporate- ID, secure access and authentication

Application	Volume by 2005 (in millions)
Prepaid Phonecards (using Eurochip)	5
Transport Cards	4
Mobile SIM Cards	4
Banking Controller Cards	3

Table 5. Market Forecast for Smart Cards in Singapore
(Source: Infineon Technologies)

3.3.2.1 Technology Trends

Smart Card Operating Systems are moving towards open platforms such as Multos and JavaCard.

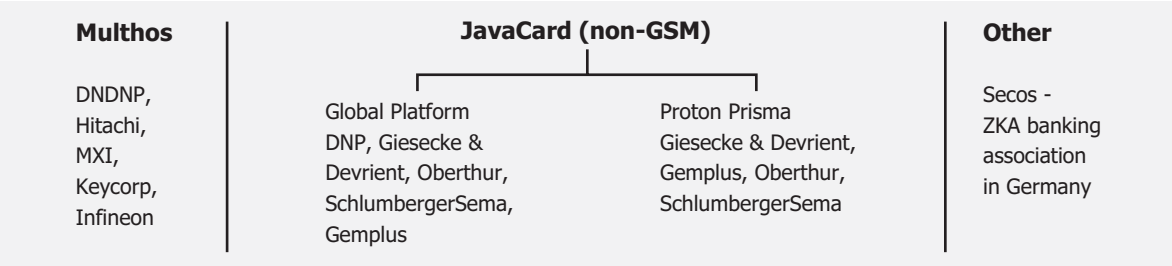


Figure 5. Industry Support for SCOs
(Source: Asia Pacific Smart Card Assosciation – In Toouch June 2002)

Smart Cards will have a high security feature with dedicated on-card crypto processing and support for AES & ECC. Increasing the security of smart cards are security assurance – from none to CC/ITSEC (now known as ISO 15408) certified. They wil have faster CPUs (32 bit + & above CPU) and are increasing in memory size to 64 MB and above. Dual interface to ease multi-applications/multi-services are emerging to support both contact (ISO 7816) & contactless (ISO 14443) interface. Other technology trends discerned in the landscape are the integration of Smart Card and Biometrics data and the movement from "Chip on Card" to "System on Card".

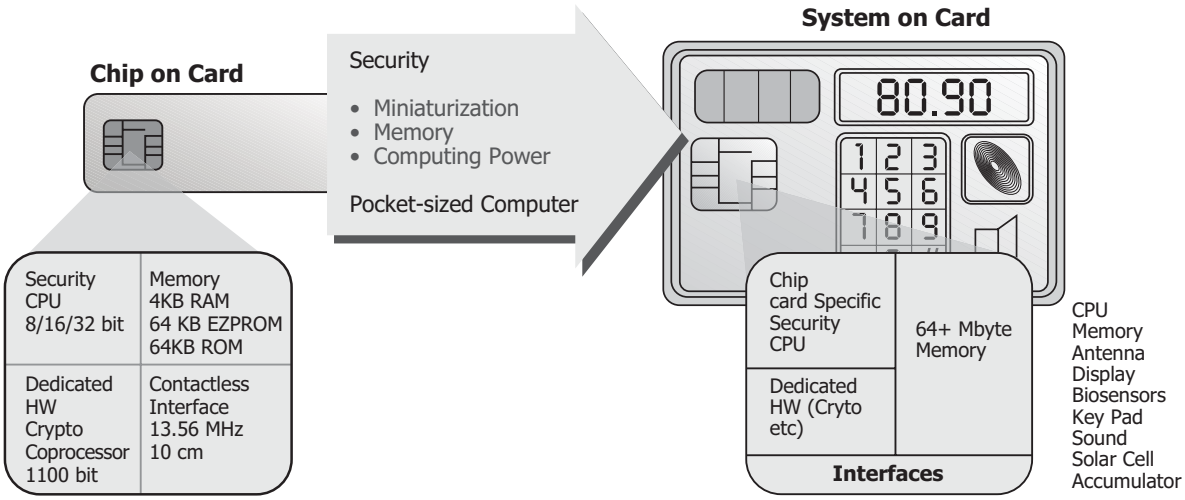


Figure 6. "Chip on Card" Movement to "System on Card"
(Source :Infineon Technologies 2001)

4 Biometrics

4.1 Overview

Today, passwords or PINs are the most popular means of authentication. However, passwords are easy to steal and crack, especially with the availability of a wide variety of password cracking tools that can be downloaded from the Internet. Organisations are now realising the need for stronger authentication than simple passwords. There are three possible 'factors' in authentication:

- Something you know (e.g. a password or PIN)
- Something you have (e.g. a smart card or token)
- Something you are (e.g. biometrics)

Among the three factors, biometrics remains the only security technology that can reliably prove you are who you are. Forrester Research reported that 40% of all helpdesk calls were from users who needed to reset or be reminded of their passwords or PINs. While there are unfortunate numbers of fake identity cards, passports and credit cards, it is extremely difficult to fake, steal, lose or forget one's biometric traits.

Essentially, biometrics identifies a person by using that person's unique physiological or behavioural characteristics. Examples of measurable biological and behavioural biometrics are fingerprint, iris, retina scanning, face geometry, hand geometry, DNA (genetic fingerprint), brain neurology patterns, dynamic hand signature, voice, keyboard strokes, finger Doppler signal and ultrasonic responses. Stability, repeatability, ease and cost of deployment, and non-invasiveness to health would be the natural criteria for the choice of a good biometric.

For any biometric system, there are four steps in the entire process:

- Enrolment, where one or more of the user's biometric samples are registered into the system.
- Capture, where the user's biometric sample is recorded.
- Matching, where the captured biometric sample is compared against samples of one or more enrolled users in the system.
- Output of matching result.

There are generally two modes in which biometrics is used: verification and identification. Verification or authentication (also called one-to-one matching) compares a sample of the user's biometric to the biometric reference template of the user whose identity is being claimed.

This requires an accompanying user name, ID, or card, so that the user's reference template can be retrieved for the comparison to be made. In contrast, identification (also called one-to-many matching) compares a sample of the user's biometric against the biometric reference templates of all the users enrolled in the system. Identification is therefore a much harder problem than verification. For this reason, the vast majority of consumer applications (including those for e-commerce) use mainly verification and not identification.

Since the extraction of biometric data at the enrolment stage and later at the capture stage can never be perfectly identical at each time, it is up to the virtue of a good adaptive biometric system to correctly determine whether results are close enough to render acceptance or not. Much depends on the choice of the statistical threshold value used to determine a correct match.

4.2 Technology Developments, Applications & Standards

There are several biometric technologies in use today with a few more technologies being investigated in research laboratories world-wide. Nevertheless, all the technologies share a common process flow as follows:

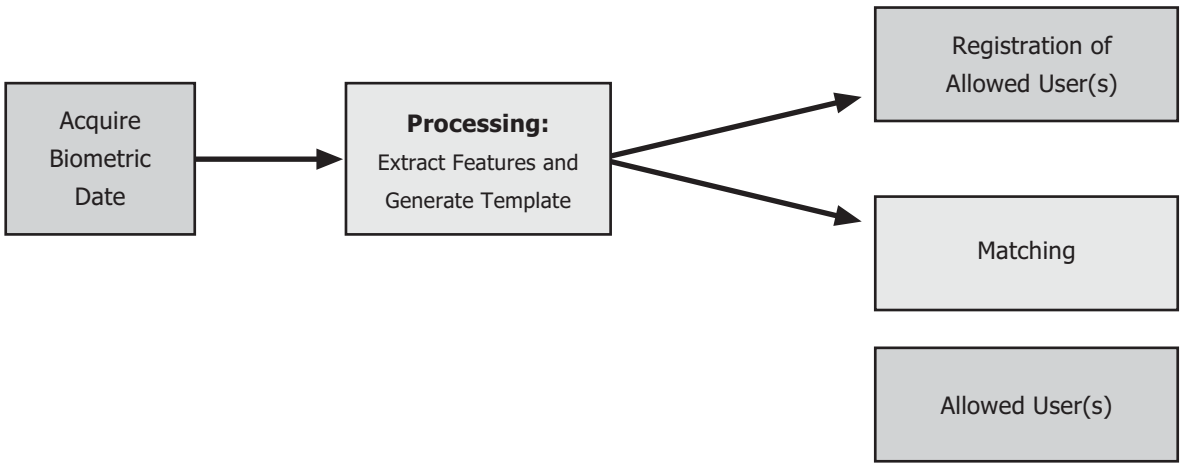


Figure 7. Biometrics Common Process Flow

A sensor is required to acquire the biometric data that will then be processed by a processor which could be processor which is a part of an embedded system or a PC. The processing involves enhancing the data, removing noise and segmenting out the crucial data. From such conditioned data, the unique features are then extracted and a template is then generated to represent the biometric data. This template will be the basis in which the uniqueness of the

data is associated with the identity of the user. Subsequently, if it is the first time the user is using the biometric system, then the template will be stored as a reference of an allowed or known user of the system. Other information associated with the user may be included as well. If the user wanted to gain access to the system, then the template generated will be compared or matched against the reference of allowed user(s). If the matching is made in such a way that it is compared against a claimed identity, the matching process will be a one to one comparison between the generated template and the stored reference template. Such a matching process is called a verification process.

There are many ways to claim an identity, such as by entering name, telephone number, PIN or password and using token such as smart card or contactless card. Another possible mode of matching is to compare the generated template against a list or database of allowed users where the reference templates are stored. Such a process involves one to many comparison and the matching process is called an identification process. The type of matching process used in a biometric system will depend on the nature of application where the biometric system is used and the biometric technology involved as not all biometric technology is suitable for identification. The following sections will discuss the common biometric technology such as face, fingerprint, hand geometry, iris, and voice.

4.2.1 Types of Biometrics

4.2.1.1 Fingerprint

William Herschel first introduced fingerprint identification in the late 1850s. Since then, fingerprint verification has become the most widely used biometric technology. Fingerprints are now used universally for forensic investigation by law enforcement agencies. A wide range of commercial products are integrated with fingerprint capture capabilities, including computer keyboards, mouse, laptops and point-of-sale terminals. There are also mobile devices such as PDAs and mobile phones that are equipped with an embedded fingerprint sensor. Both contact and contactless smart cards enabled for fingerprint applications are available. The worldwide market is supported by many biometric vendors and associated developers.

This market is generally split into the different types of sensors, of which there are four popular types: capacitive sensors, electric field sensors, optical sensors, and thermal sensors.

Optical Sensors. The majority of the optical sensors available today are based on the principle of total internal reflection, employing a prism and a lens to focus the image onto an imaging chip. The imaging chip can be based on CMOS or CCD technology, depending on the cost and

quality of the fingerprint image desired. When a finger is placed on the prism surface, the oil, moisture, etc. on the finger cause a change in the refraction index. As a result, the light on the point where the finger meets the glass surface will not be properly reflected. The pattern, when focused onto the image acquisition device will produce the fingerprint image. The advantages of this technology are that unlike other types of sensors there is no electrostatic discharge problem (since there is optical isolation between the imaging chip and the finger), that it yields large imaging surface (typically 1 inch by 1 inch), and that it has longer usage history. As the imaging chip is not close to the surface, it is more robust against scratches and impact at top surface. Vendors supplying such solutions include SecuGen (www.secugen.com), Cross Match Technologies (www.crossmatch.net/), Digital Persona (www.digitalpersona.com/html/), and Identix (www.identix.com/).

Capacitive Sensors. A capacitive sensor consists of a large array of tiny capacitors etched onto a small piece of silicon. It works by using the capacitors to measure the difference in capacitance caused by the difference in height of the finger's ridges and valleys. Capacitive sensors are typically cheaper to implement and much smaller than optical sensors. Leading suppliers of capacitive sensors include Fujitsu (www.fujitsu.com), Infineon Technologies (www.infineon.com), ST Microelectronics (www.st.com) and Veridicom (www.veridicom.com).

Electric Field Sensors. An E-field sensor is a solid-state sensor that applies a small signal and then measures the resultant E-field generated by the live layer underneath the skin of the fingerprint. It is therefore immune to skin conditions such as dirt, oil or dryness. A good example of such a sensor is Authentec's EntréPad sensor (www.authentec.com).

Thermal Sensors. This type of sensor works by sensing the differences in temperature of the finger's ridges and valleys. It measures the rate of heat transfer and not absolute temperature. In the valley areas, since air is a bad conductor of heat, a lower heat transfer will be measured in comparison with the ridges. Since the heat transfer will be constant if the finger is stationary, thus this sensor is also constructed in a stripe form. The image is acquired when the user swipe the finger passes the sensor. This technology may be limited by the surrounding climatic conditions. One example is FingerChip from Atmel (www.atmel.com). In 2002, Atmel aims to provide on-chip processing integrated with the sensor. By 2005, Atmel aims towards single chip integration including on-chip analogue to digital conversion and on-chip microprocessor processing.

Other potential sensing technology employed in the acquisition of the fingerprint includes ultrasonic, pressure and variations such as direct optical sensing using fiber optic. In addition to the touch sensors, swipe sensors similar to the thermal sensor but using the other technologies described are in active development.

Although there are plans to incorporate fingerprint sensors onto the smart card itself for portability, there is currently no such solution implemented in accordance to the standard ISO thickness of 0.76 mm for the card. There are also obvious issues of incompatibility when used with an ATM machine, simply because the card would not be present for the sensor to be used. Cost would be another obstacle for the mass deployment of such a product. As such, it would be more economical to install a fingerprint reader at the point-of-sale for all cardholders. Yet, efforts to miniaturise the fingerprint hardware implementation and algorithm processing are important for embedded applications because these can bring down cost considerably. One important trend is to port the biometric algorithm processing within the reach of a smart card chip processor so as to offer better user friendliness, privacy and security (such that the template never leaves the card). There are already some commercial solutions available in this area of fingerprint matching on smart card, such as Veridicom's Match-on-Card and Laboratories for Information Technology's BioJavaCard. However, realization of sensor on the smart card with complete fingerprint processing is still a research challenge.

A major area of focus for fingerprint verification is to counter the possibility of fraud using a fake or dead finger, especially at unattended terminals. Fake fingers are easier to differentiate compared to dead fingers. Although there are improvements in the technology to detect such fraud, no system can be assured of 100% security. In addition, other biometric features such as iris, face, hand and voice, are also prone to fraudulent verification and this is not peculiar only to fingerprint. Hence, in applications where high security is needed, it may be necessary to complement biometrics with other safety features in a total security approach.

4.2.1.2 Iris

Iris recognition is a non-intrusive biometric technology that relies on a biometric feature that does not change with time. The system takes a normal video image of the iris and produces a circular image template. It uses the pattern of furrows, crypts, corona, filaments, pits, freckles and striations of rings contained in the eye.

The patented software recognition technology provided by Iridian Technologies (www.iridiantech.com) reveals 266 independent degrees-of-freedom of textural variation. This makes it very accurate such that no two persons are supposed to have the same iris patterns.

Some of the video acquisition technology works through glasses (including Sunglasses), under dark lighting conditions and contact lenses (even those with patterned lenses) at a distance of about 1 meter. There is also desktop-based iris acquisition device that works at a distance of about 10cm to 20cm. Usually the recognition technology is provided by Iridian

Technologies. The company is also planning to improve the reliability and accuracy of the system by using both irises instead of one.

4.2.1.3 Retina

While iris recognition compares patterns in the iris based on the exterior, visible coloured part of the eye, retinal scanning examines the vascular patterns inside the eye found on the retina. This technology is deemed to be the most accurate. However, it can intrude into personal privacy space in terms of what is revealed such as medical conditions. Typically, a micro laser beam is used to scan the retina and a 3D image is reconstructed based on the reflected light. Algorithm developments help to improve the 3D image in terms of resolution. Other approach to image the retina includes shining light (include infra-red) and using normal video camera to capture the retina image.

Disadvantages of retinal scanning include the need for fairly close physical contact with the scanning device, the fact that trauma to the eye, pregnancy, drugs and certain diseases can obscure the retinal pattern, and concerns about public acceptance.

4.2.1.4 Voice

Voice identification measures both physiological and behavioural characteristics. Most methods concentrate on analysing the time between sound waves crossing the zero spectrum, not just the tones that an individual is creating (i.e. voice recognition). However, the quality of voice may suffer in noisy environments and be affected by the physical state of health of the user and influence of alcohol. One example of a voice recognition product is Domain Dynamics' (www.ddl.co.uk) TESPAR (Time Encoded Signal Processing and Recognition) technology.

4.2.1.5 Face

Face recognition is a non-invasive biometric technology that relies on detecting the different facial features on the face from a photographic image. Visionics' (www.visionics.com) FaceIt face recognition software detects the intrinsic shape and features on the face, with high resistance to skin tone, facial hair, eyeglasses, lighting, expression and pose, through the use of proprietary software algorithm compensation. Another approach developed by Imagis Technologies (www.imagistechnologies.com/Default.htm) uses a combination of spectral analysis and 3-D modeling to locate and fit a face, identifying over 115 facial descriptors in the process, giving it high accuracy.

4.2.1.6 Hand Geometry

Hand geometry systems measure finger length, hand thickness, palm shape and skin translucency. Recognition Systems (www.recogsys.com) is the primary supplier of hand geometry products and its HandPunch and HandKey products are used in 90% of the nuclear power plants in the United States, and in airports, banks, schools, hospitals, police and law offices. Biometric characteristics such as finger length, width, height and palm width are used. Hand geometry can only be used for one-to-one verification.

4.2.1.7 Hand Signature

Hand signature systems measure the speed of the pen, pressure, direction in signature and other related characteristics. LCI Technology of Netherlands has a product called SmartPen (www.lcismartpen.com). It is a ballpoint pen that doubles as a sensor and mini PC capable of transmitting handwriting wirelessly. While writing, the built-in sensors are able to register the dynamics (speed, pressure, angles) of the act of signing. The information is then encrypted inside the pen and wirelessly transmitted to a computer system that verifies the authenticity of the signature. This technology can be used for verifying credit card signatures electronically.

Another company, Cyber-SIGN (www.cybersign.com), provides solutions for enterprise biometric signature verification. A digitising tablet is used to capture the user's handwritten signature. The data is then encrypted and sent to a server for verification. In particular, this technology is compatible with Adobe Acrobat/PDF, Windows and Lotus Notes, and can also be used on PDAs.

4.2.1.8 Comparison

The chart in the following page illustrates how the various biometric technologies rank against one another in terms of accuracy. According to this chart, iris scan leads in terms of accuracy, followed by fingerprint recognition. Close behind it is voice and hand signature recognition. In addition to this chart, the International Biometrics Group (www.biometricgroup.com) also provides a good comparison between the different biometric technologies in terms of cost, intrusiveness, accuracy and user effort required. Its Zephyr Analysis also provides a concise ranking of the various biometric technologies.

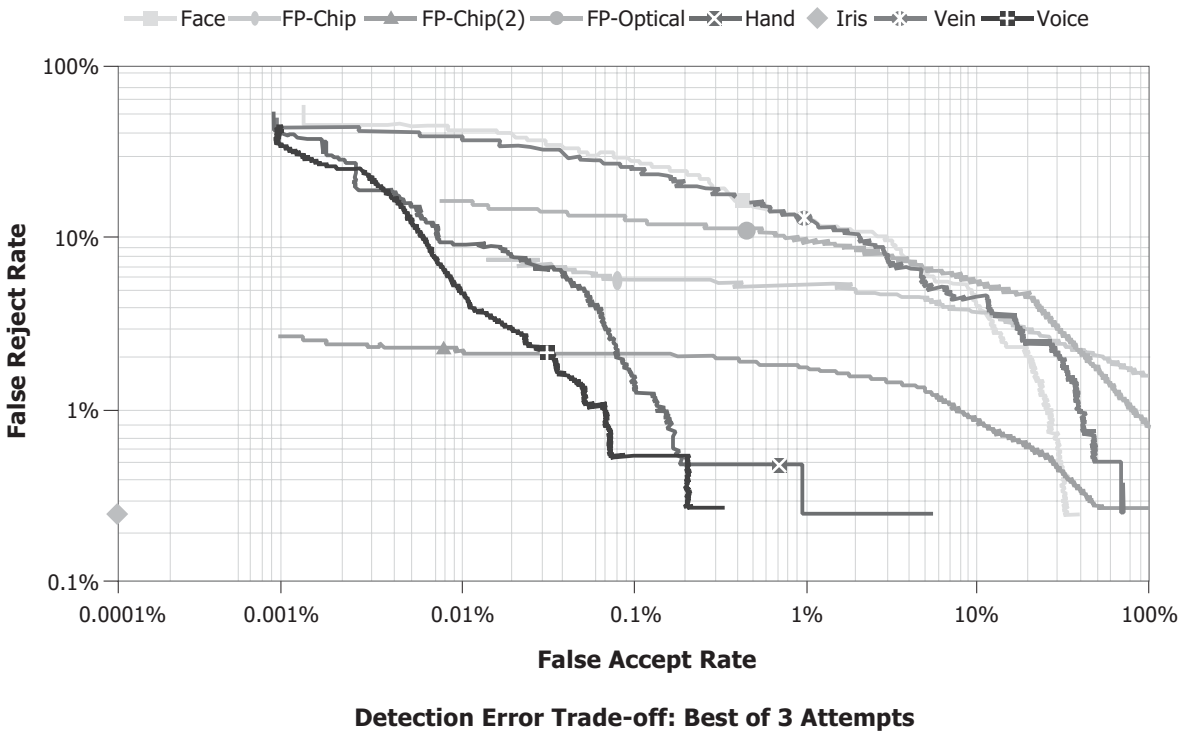


Figure 8. Comparision of Biometrics Technologies
(Source: Courtesy of National Biometrics Test Center)

4.2.1.9 Multi-Layered Biometrics

A multi-layered biometrics system combines a number of biometric features such as face, voice and fingerprint to achieve maximum security, reliability and user friendliness. Due to their inherent complexity, such systems are obviously more costly and more challenging to implement.

In an article by John Daugman of Cambridge University entitled "Combining Multiple Biometrics", it is mentioned that a strong biometric is better alone than in combination with a weaker one. In short, to ensure that multi-layered biometrics do indeed offer better security than a single biometric, we should exercise caution in system implementation to exploit the benefits and flexibility of multi-modality such that intruders cannot make use of the weaker biometrics to compromise the security of the entire system.

A number of biometric vendors are beginning to provide such systems. Among them is Keyware (www.keyware.com) with its LBV (Layered Biometrics Verification) technology that

is able to combine the security of smart cards, digital certificates and biometrics such as face, voice and fingerprint.

4.2.1.10 Biometric Adoption

Biometric technologies relieve users from the need to remember PINs and passwords. To date, fingerprinting is the most popular form of biometrics used for identification, because of its low cost of implementation, non-invasiveness and high accuracy. With faster and smaller processors, on-chip processing and verification will offer the highest security for fingerprint recognition.

Overall, there are two differing views from the participants regarding the future trend in biometric adoption. On one hand, consumer privacy concerns would hamper the growth of biometrics. Privacy concerns could be the fear that unknown parties might be able to trace the activity of a person through a central database, because every time access is required, a request to the central database is needed. There is also the fear that you lose the means of control over something so unique and personal to you. To promote biometrics, there is definitely some user assurance and education to be accomplished beforehand. Yet consumers are still feeling insecure about e-commerce with the current situation, thus may be willing to accept biometrics more easily in the near future with recent outcries of Internet fraud especially in Internet banking and credit card fraud for on-line purchase. However, the cost of deploying and maintaining a biometric system is still likely to surpass other technologies such as smart cards, although it has gradually decreased over the past decade. The cost for biometrics has not reached the price level for mass commercialisation. Standards are still lacking and many solutions are proprietary. As such, for the next five years, biometrics may be more suitable for niche markets such as access controls, time-and-attendance, immigration, welfare right systems, and in enterprise implementations.

On the other hand, others strongly believe that biometrics would be a good compromise for security and convenience. This is because the highest security is as good as the weakest point and usually the latter is not at the entry part. Biometric technologies can provide trust, prevention and effective deterrence to identity fraud, rather than an absolute guarantee of infallible security. A good fraud prevention and deterrence system in place using biometrics, for example, could suffice to surmount the threshold level of fear to boost business prospects for e-commerce, in addition to the currently available bank and credit card guarantees of zero or minimal loss statements. Many biometric vendors tend to oversell their products based on their security features and, if not properly taken into perspective, many users or potential users would be disappointed. As in the case of Britain, where thousands of stores are requiring customer fingerprint manually in addition to the use of credit card due to high fraud rates, some also believe that fraud in credit cards would continue to escalate, especially for e-

commerce. Biometrics would be a good and viable technology to reduce such fraud cases and it might even happen sooner than five years. The principle or driving force for its adoption in e-commerce would be fraud prevention and not the emphasis on high security.

4.2.2 Standards

Biometric products are currently not commonplace in e-commerce. Its primary niche application remains in time-and-attendance and physical access control. Besides the cost consideration, one of the important factors is the absence of dominant standards and interoperability in the industry.

There is currently no common command set for biometrics. With regards to an open architecture for sensors, matching algorithms and applications, there are only guidelines (even from US National Institute of Standards and Technology), but few published open standards. Since the matching technology is carefully guarded by biometric companies, standardisation of these technologies will remain difficult to achieve. However, we can possibly look forward to a blueprint and preliminary specification for data inter-exchange conversion. The current efforts in standardisation fall into three categories, namely:

- API standards
- File format standards
- Other related standards such as testing and evaluation, security management and communication standards as well as best practises.

The relationship between these areas is best illustrated with the following diagram.

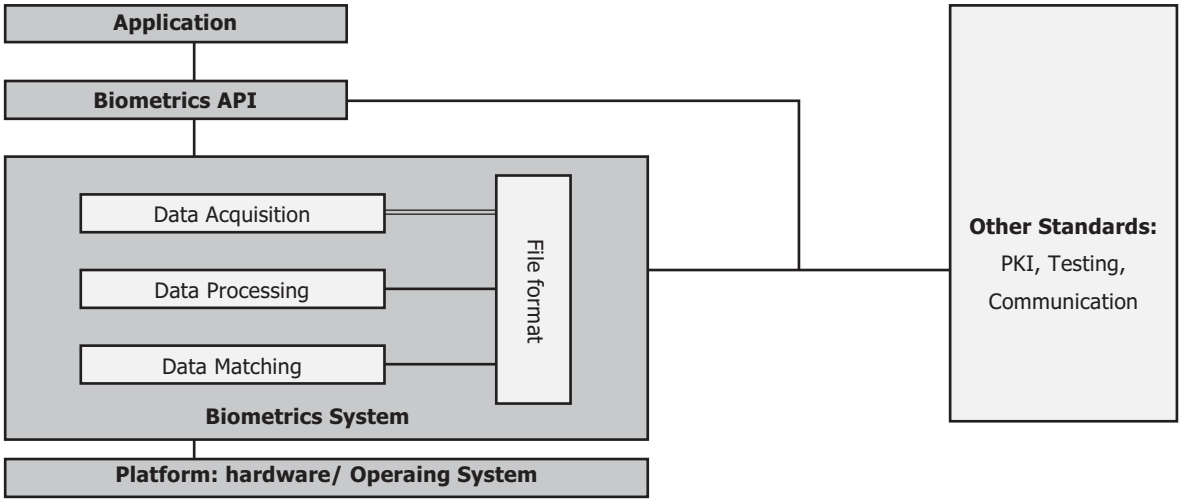


Figure 9. Framework for Biometrics Standardisation[5]
(Source: Laboratories for Information Technology)

4.2.2.1 API Standards

Biometrics API standards are key in the adoption of biometrics technology. Not only they facilitate competition among vendor to develop standards-compliant products, they also reduce the risk to users, as they are not locked to a single vendor. In the early days, API standardisation effort was fractured into SVAPI, BAPI, HA-API and BioAPI, with each standard driven by different key groups of companies. In recent years, the various standard groups came together and decided on a unified standard. This eventually led to the merger of both BAPI and HA-API with BioAPI. With this, BioAPI appears to be the biometric standard that is likely to dominate the market in the future.

SVAPI. Development of the Speaker Verification API (SVAPI) began in 1996 supported by a consortium of biometric technology developers and users. Version 1.0 of the API was released in 1997 and has since been made available free to software developers and manufacturers for use in applications of secure communications and information access that make use of speech verification. SVAPI members include Citicorp, IBM, ITT Industries, Motorola, T-Netix, SRI/Nuance, Massachusetts Institute of Technology and Lincoln Laboratory, as well as the Internal Revenue Service, the US Department of Defense, the Immigration and Naturalisation Service, and several other companies and consultants. Novell chairs the committee and has

5 "Biometrics: Emerging Market needs Standards", Dr Huang Wei Min, Laboratories for Information Technology (LIT), Singapore.

played a pivotal role in the API's development. The open standard API is positioned to expand the market for speech verification solutions by allowing developers to engineer applications that will be compatible and interoperable with compliant systems from different vendors.

BioAPI. The BioAPI is an open standard for biometrics developers and integrators that is driven by the BioAPI Consortium (www.bioapi.org). The consortium was formed in Apr 1998 and comprises four key companies: Compaq, IBM, Microsoft and Novell. Currently, it has about 80 over members. Its goal is to work with industry biometric solution developers, software developers, and system integrators to leverage existing standards to facilitate easy adoption and implementation; to develop an OS independent standard; and to make the API biometric independent. BioAPI will provide a set of functions that supports the following:

- Simple application interfaces
- Modular access to biometric functions, algorithms, and devices
- Secured and robust biometric data management and storage
- Methods of differentiating biometric data and device types
- Operating in distributed computing environments

Version 1.0 of the BioAPI was published in March 2000, and the Reference Implementation was released in September 2000. Version 1.1 of both the Specification and Reference Implementation was released in March 2001. The BioAPI WG is still working on the Conformance Test Suite that that will enable confirmation that applications and BSPs will conform to the BioAPI Specification. The main difference between BioAPI and other biometrics API is that BioAPI is flexible in deployment of biometrics across platforms and operating systems. The International Committee for Information Technology Standards (INCITS), a standards committee accredited by the American National Standards Institute (ANSI), has approved the BioAPI Consortium's BioAPI Specification, Version 1.1. This specification is designated as ANSI/ INCITS 358.

CDSA/HRS. The CDSA/HRS is an extension to the Open Group's Common Data Security Architecture (CDSA) developed by Intel. Its basic purpose is to verify the identity of a person based on some combination of password knowledge and biometric measurement. Access control decisions (to such things as: smart cards, cryptographic keys, persistent data objects, and web accounts) can be made on the basis of this identification. The Human Recognition Services (HRS) extension is based on BioAPI Standard version 1.1. Different independent software vendors in Asia Pacific are making an effort to customise CDSA for mobile computing devices such as mobile phones and PDA. The biometric component of the CDSA's HRS is used in conjunction with other security modules (i.e., cryptographic, digital certificates, and data libraries) and is compatible with the BioAPI specification and CBEFF.

4.2.2.2 File Format Standards

Biometrics file format standards enable reusability and interchangeability in different biometrics systems. Examples of standardisation efforts include:

WSQ. Wavelet Scalar Quantization (WSQ) Gray-scale Fingerprint Image Compression Algorithm is a file compression format defined by the US Federal Bureau of Investigation (FBI) for fingerprint image compression.

ANSI. A proposal of data format (ANSI/NIST 1-2000) developed for the interchange of biometrics data by the American National Standards Institute (ANSI) and the National Institute of Standards and Technology (NIST). ANSI/NIST-ITL 1-2000 Data Format developed by American National Standards Institute (ANSI) and the National Institute of Standards and Technology (NIST) for the interchange of biometrics data (fingerprint, facial, scar, mark, and tattoo). It was approved as an American National Standard in July 27, 2000.

CBEFF. A Common Biometrics Exchange File Format (CBEFF) proposed by NIST and the US government's Biometrics Consortium in Feb 1999 to establish a universal file format recognisable by various applications. It is in fact more difficult to define a file format standard for biometrics than for the API because different vendors use different algorithms to extract features and for processing. In January 2001, NIST published the "*Common Biometric Exchange File Format (CBEFF)"* as NISTIR 6529.

XCBF. XML Common Biometrics Format (XCBF) proposed by Organisation for the Advancement of Structured Information Standards (OASIS) in March 2002 to define a common set of XML 1.0 encoding for "Common Biometrics Exchange File Format" (CBEFF) – the current generic standard for biometric data format. The basis in XML is to facilitate the transfer of biometric information across the Internet.

ISO. Recently the International Organization for Standardization, ISO/IEC, is also actively pursuing the standardization for biometrics. The subcommittee for biometrics, JTC1 SC37, was established in July this year for the standardization of generic biometric technologies to support interoperability and data interchange between applications and systems. In May 2002, the working group WG11 under JTC1 SC17 is established to work on standardization of biometrics applied to cards and travel documents.

Standards Analysis. A unified biometric standard rallied by most biometric players is unlikely to be ready within the next two or three years. While specifications are being drafted and refined, we will certainly see many proprietary implementations. In fact, in some countries where personal privacy is a major concern, there are also movements against a unified biometric

standard. Some may hold on to proprietary standards because of security concern, not wanting to share their application or are unwilling to share their existing customer base.

Still, the majority sees standards as the way to increase global customer base and to bring benefits to both the industry and the consumer. The ISO/IEC consortium will be the most significant player for biometrics standardisation.

4.3 Trends And Developments In Biometrics

4.3.1 Market Forecast

GartnerGroup predicts the biometrics market to grow to US$1 billion in 2005, mainly driven by the applications in corporate PC and network security, B2B e-commerce, healthcare, national ID and banking.

According to International Biometric Group's latest market report, "Biometric Market Report 2003 - 2007", the biometrics revenues is expected to grow from US$600 million in 2002 to US$4.04 billion in 2007. This phenomenon is largely driven by PC manufacturers who integrate fingerprint sensors to peripheral devices (such as mice and keyboards). It also reveals that on a 2-4 year timeline, biometrics will become a more common consumer-facing solution, and many new biometric revenue models based on transactional authentication will begin to emerge.

This above figure is consistent with the market report released by the International Biometric Industry Association (IBIA). IBIA predicted that revenues for the manufacturer and developer level would rise to $1 billion by 2004, and $2 billion by 2006.

IBIA also give a snapshot of Biometric applications between now and in 4 years time (2006). Over the four years, self-contained biometric will be a key driving market factor. This trend will be largely adopted by the telecommunication industry for their new line of telecommunication equipment (such as mobile phone, PDA, etc) to identify the identity of the bearer.

Biometrics Application	2002	2006
Physical Access Control	51%	24%
Logical Access Control	40%	11%
Time Attendance	9%	5%
Telecommunication	-	56%
Automotive	-	4%

Table 6. Segmentation Trends in Biometrics Applications
(Source: International Biometric Industry Association)

In the International Biometric Group report, Fingerprint-scan commands the biometrics market with a 52.1%. This is followed by Facial-scan at 12.4%, and Hand-scan at 10.0%. Iris-scan dominates at a mere 5.9%, largely due to its high cost of implementation cost despite the fact that it is the most reliable biometric tech among all.

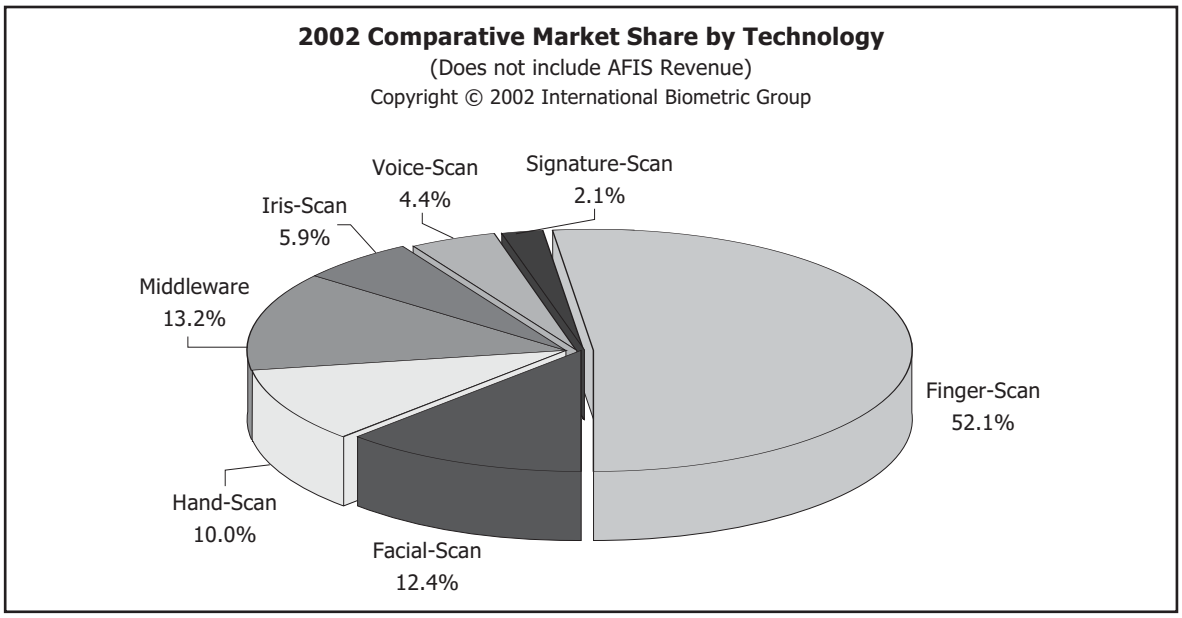


Figure 10. Biometric Technology Market Share Segmentation
(Source: International BiometricGroup)

Right now, biometrics is used mostly in niche applications. We see that biometrics will expand its scope. Possible areas where biometric technologies could make a significant impact include:

- Banking/Financial services such as ATMs, payment terminals, cashless payment, automated cheque cashing etc.
- Computer & IT Security such as Internet transactions, PC login etc.
- Healthcare such as privacy concern, patient info control, drug control etc.
- Immigration such as border control, frequent travelers, asylum seekers etc.
- Law and Order such as public ID card, voting, gun control, prison, parole etc.
- Gatekeeper/Door Access Control such as secure installations, military, hotel, building management etc.
- Telecommunication such as telephony, mobile phone, subscription fraud, call centre, games etc.
- Time and Attendance such as school and company attendance
- Welfare, including health care services and benefit payments
- Consumer Products such as automated service machines, vault, lock-set, PDA etc.

Another major area that received little attention up till now is the opportunity for personalization services. For example, a TV remote control with biometric capability can automatically select the channel of interest of the user together with the preferred volume and brightness settings. Similarly, a mobile phone with biometric capability is able to customize the user interface, ring tone, phone diary, speed dial etc. Imagine entering a members-only golf club reception with the automated system calling your name – it will surely impress you and your guests!

4.3.2 Issues and Challenges

Having had a glimpse of the basics of biometric technology, this section attempts to highlight the issues, potential and challenges faced by biometric technology. In selecting a specific biometric technology, there are several issues to consider:

- Size of user group
- Place of use and the nature of use (such as needs for mobility)
- Ease of use and user training required
- Error incidence such as due to age, environment and health condition
- Security and accuracy requirement needed
- User acceptance level, privacy and anonymity
- Long term stability including technology maturity, standard, interoperability and technical support
- Cost

There are major challenges to the wide roll-out and adoption of biometric systems, such as lack of user education, especially since there are several biometric technologies to choose but

not every technology is suitable for all application scenario and the impact to privacy on the use of such technology. Over expectation, either due to ignorance of the users or exaggerated by the over-zealous sellers in the capability of biometric will also slow the market adoption as the system will not perform as "expected" in the eye of the users, causing lack of trust in the technology. Lack of interoperability and standard is also a challenge preventing wide-scale adoption since users especially corporations will not want to invest in a technology that will soon obsolete or lack of technical support. In this area, several international standardization efforts have been pursued, including the BioAPI for biometrics application programming interface, CBEFF for common biometric data exchange format and very recently formation of groups at ISO/IEC to look into biometric standardisation. Some of the biometric technology is also less mature and will need more time for research and trial testing before the performance can be enhanced to suit the market need.

Biometrics is an emerging area with many opportunities for growth. The technology will continue to improve and challenges such as interoperability solved through standardization. This will lead to increase in the market adoption rate and the technology will proliferate. Hopefully, in the near future, you will not have to remember PINs and passwords and keys in your bags or pockets will be things of the past.

5 PKI

5.1 Overview

Public-key cryptography has emerged over the past 20 years from the secret intelligence agencies into publicly available commercial products. Financial institutions are among the first adopters for public-key technology back in the 1980s for securing the funds transfer networks. Other early adopters included government agencies and telecommunications companies. The security need for using the Internet for commercial purposes has also created a huge demand for public-key encryption technology.

Public key infrastructure, or PKI, is the whole system of encryption and digital signature technologies, digital certificates, certification authorities, registration authorities, as well as the processes and policies that govern the issuance, revocation and management of these certificates. A PKI is an enabling infrastructure that has no intrinsic value but is necessary to provide a framework to identify the participating parties of an electronic transaction on the Internet. It is able to provide the following fundamental security requirements prevalent in e-commerce transactions.

- **Data Confidentiality**, which means that no one but the intended recipient of the message can read the message.
- **Strong Authentication**, which means that users can securely identify themselves without resorting to sending passwords over the network.
- **Data Integrity**, which means that users can verify whether a message has been tampered with.
- **Support for Non-Repudiation**, which means that the user who sends a message cannot deny having sent the message.

The challenge for all businesses today is to build an infrastructure that can be trusted. PKI has frequently been cited as a crucial element in establishing trust on the Internet and promoting end-user confidence in conducting e-commerce. Proponents of PKI predict that, over the next few years, all businesses large or small will be dependent on digital signatures and digital certificates. This is opening up new opportunities for businesses in finance, insurance, mortgage and other industries to execute paper-based business transactions electronically. PKI technology achieves all this because it employs the use of advanced encryption techniques and digital signature schemes. These services enable a wide variety of applications that can be deployed securely over the Internet.

5.2 Technology Developments, Applications & Standards

5.2.1 Technology

Public-key technology is a combination of encryption algorithms, protocols, and derived tools designed for secure communications, such as digital certificate, certification authority and registration authority, directory service and authentication device. These components, when applied concertedly, form the basis for information, transaction, and communications security and are the foundations of the PKI. Typically, a complete PKI solution will also provide automatic key update, backup and recovery, as well as a secure means of checking the validity of a digital certificate.

5.2.1.1 Digital Certificate

A digital certificate is similar to a passport or driver's licence in that it allows the identity of a person to be verified by a recognised authority. It contains the public key of the user as well as information about the user and the certificate, such as the user's name and the certificate's expiry date. It is digitally signed by a trusted third party known as the certification authority. Its main purpose is to enable the validation of the user's public key, thus proving that the key actually belongs to the user.

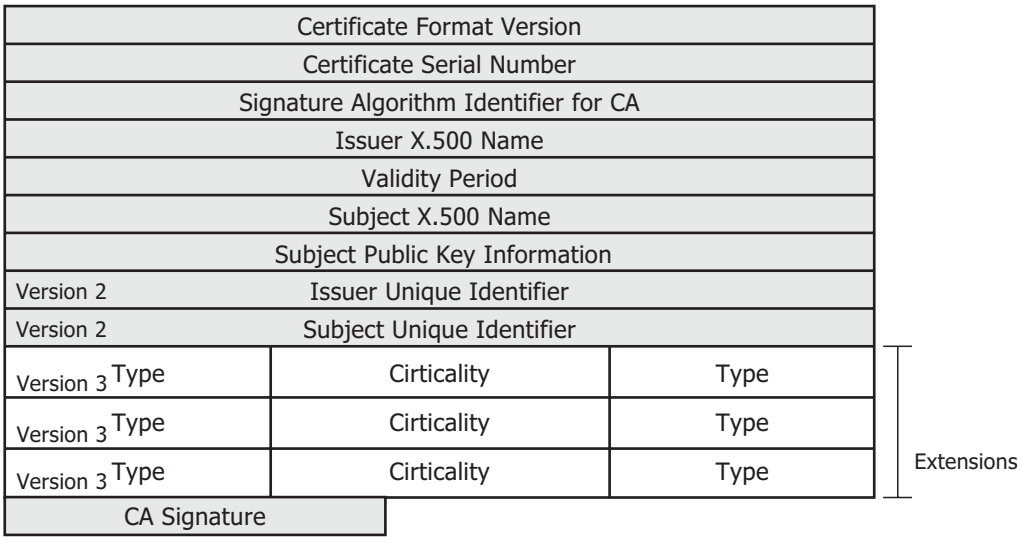


Figure 11. Format of a Digital Certificate
(Source: Entrust Technologies)

The portability and scalability of a digital certificate supports a wide variety of applications. For example, digital certificates and private encryption keys can be loaded onto smart cards. Over time, digital certificate-configured smart cards will likely become the standard for credentials such as passports, driver's licences, and credit cards.

Compact digital certificates will become the emerging technology for PKI. Vendors are currently developing compact certificates so that they will be suitable for mobile and handheld devices where limited memory and processing power are the main constraints. Elliptic Curve Cryptography (ECC), which has a superior cryptographic strength in constrained environments, will most likely be adopted as a good alternative public-key algorithm to the traditionally dominant RSA public-key cryptosystem.

5.2.1.2 Certification Authority

A certification authority (CA) is the trusted party that creates and manages digital certificates, and issues lists of revoked certificates. By electronically signing a digital certificate, a CA vouches for the certificate owner's identity. Just as the government issues and guarantees the identity of the passport bearer, a CA acts as the guarantor of the validity of the digital certificate. It is expected that a network of trusted and independent CAs will emerge to support a wide variety of e-commerce and secure communications applications. It is anticipated that the PKI will consist of a trusted web of CAs that includes corporate, public, government organisation, and national CAs. Over time, certain CAs will cross-certify with one another and be able to validate certificates issued by other CAs.

In certain implementations, a service interface is created to handle the process of applying for a certificate. This user interface, better known as the Registration Authority (RA), captures and authenticates the identity of the users and submits the certificate request to the CA. Regardless of whether the CA or RA handles the user registration process, the quality of this authentication process determines the level of trust that can be placed on the certificates issued by the CA. The CA will therefore require some proof of identity prior the issuance of a certificate. The procedures that the CA uses are codified in a document called a Certification Practice Statement (CPS).

5.2.1.3 Certificate Directory

Directories are primarily used for reading information rather than transactions or complex queries. In a CA system, directories are used to store and distribute digital certificates, keys, cross-certification lists and entries for distribution of certificate revocation lists (CRLs) and to retrieve keys.

The enabling directory technology for CA systems is the Lightweight Directory Access Protocol (LDAP). The IETF-developed LDAP standards were designed specifically for use in the Internet Protocol (IP) environment. The legacy directory protocol, X.500, is very comprehensive but is more suitable for smaller systems and desktop client-server architectures. LDAP is interoperable with and incorporates many of the features of X.500 while offering the advantages of being more compact, more flexible and easier to implement. The latest version of LDAP utilises Secure Sockets Layer (SSL) to create a secure connection between the client and the LDAP directory. Prominent LDAP providers include ISOCOR, Novell, Banyan Systems, Microsoft, Netscape and Sun Microsystems.

Siemens (www.siemensmeta.com) has also developed a directory technology, called DirX Meta Directory, to provide reliable and scalable directory services for large-scale PKI deployment. DirX Meta Directory supports both LDAP version 3 and X.500. It supports 'chaining' whereby the directory server automatically forward queries based on a pre-defined sequence instead of returning the query back to the client when the server cannot respond.

5.2.1.4 Certificate Revocation & Validation

E-commerce requires that digital certificates be validated before they can be trusted. Certificates can be validated using certificate revocation lists (CRLs), certificate revocation trees (CRTs) or online certificate status protocol (OCSP).

CRL. CRLs are simply lists containing all certificates that are no longer valid. Each CA would maintain and update the list in a timely fashion so anyone can check a digital certificate against the list and validate a certificate issued by a CA. CRLs work well for small-scale implementation. However, for large-scale implementation, which involves geographically dispersed organisations with several hundred thousand employees, management of CRLs can be quite cumbersome.

To make the management of CRLs more scaleable, Entrust Technologies (www.entrust.com) developed CRL Distribution Points that allow smaller segments of a CRL to be maintained at unique distribution points in the directory system. This allows for greater system scalability and lower bandwidth consumption.

The issuance and distribution of CRLs and the process of certificate revocation management remain the focus of attention. For one thing, checking the validity of a certificate is not straightforward; the user must open a network connection to the issuing authority, find the CRL and submit the certificate for validation. Companies such as ValiCert (www.valicert.com) offer certificate validation and revocation management tools and services that make this process a lot simpler.

CRT. Certificate revocation trees (CRT), developed by ValiCert, mitigate the issues of update delays and scalability in certificate validation. This method hashes the serial numbers of revoked certificates and reduces the volume of validation data as well as verifies the integrity of the revocation tree.

To meet the certificate revocation requirements of m-commerce, VeriSign has developed a technology that utilises short-lived wireless server certificates – a new generation of wireless compact digital certificates that provide both strong authentication and real-time certificate validation for handheld devices.

OCSP. VeriSign (www.verisign.com) and other vendors are also working on the proposed Online Certificate Status Protocol (OCSP) that allows an automatic check on a certificate's status. OCSP is meant to provide real-time validation for certificates. However, there is concern that OCSP could require too much bandwidth because it establishes an additional network connection to the certificate revocation server to check on a certificate's status as part of each transaction. Currently, an IETF working group has defined methods for using OCSP with HTTP, FTP or SMTP.

Netscape's support for OCSP is available in Netscape 6. Sun Microsystems will also incorporate certificate revocation checking mechanism in the Java Software Development Kit (JDK). The JDK supports manual verification since version 1.2, which was released in 1998. It will be able to support automatic verification with the next version of Java 2.

5.2.2 Applications

With growing demand for secure communications and trusted commerce in an online world, it is anticipated that the market demand for PKI will accelerate as standards mature and initial systems are implemented. Applications driving PKI today include secure e-mail, SSL-based e-commerce, secure payment, and secure mobile commerce.

5.2.2.1 Transport Layer Security

The Transport Layer Security (TLS) protocol is a proposed IETF standard that provides enhanced communication privacy and security features at the transport layer. Release 1.0 of TLS is based on SSLv3.1 and offers additional options for authentication such as enhanced certificate management, improved authentication and new error detection capabilities. Three levels of server security include server verification via digital certificate, encrypted data transmission and verification that the message content has not been altered. The advantage

of TLS is that it is application protocol independent and offers extensible framework so new encryption methods can be incorporated as needed. Future versions will be able to support Kerberos authentication, ECC and AES.

5.2.2.2 Wireless Application Protocol

The Wireless Application Protocol (WAP) is designed to work within wireless devices with limited display capabilities and simple user interfaces. These devices also have limited processing power, battery life and storage capabilities. In addition, network provision is inherently less reliable relative to the wired world of the Internet.

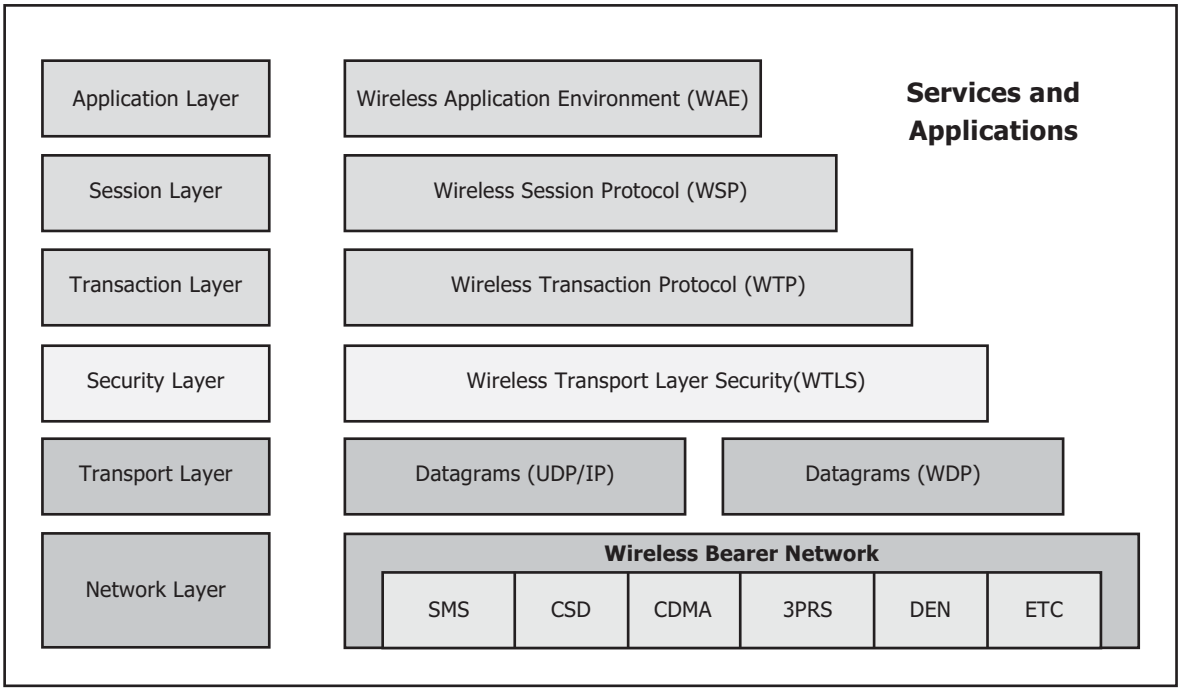


Figure 12. Security within WAP is provided by WTLS

Wireless Transport Layer Security (WTLS) provides the mandatory security within WAP. It provides key security elements of confidentiality, integrity and authentication. WTLS is the wireless version of TLS, which has been heavily modified to support datagrams in a high latency, low bandwidth environment. To operate within this environment, WTLS provides an optimised initiation of a secure session through dynamic key refreshing that allows encryption keys to be updated on a regular and configurable basis during a secure session. This not only provides a higher level of security, but also provides considerable savings on network bandwidth

by shortcutting the relatively costly handshaking procedure. The additional security elements of verified authentication, authorisation and non-repudiation are provided by integration with a PKI in the back-end.

The current focus is on the WAP 2.0 specifications, which are intended to provide much greater end-to-end interoperability between WAP devices and the Internet in general. To this end, existing Internet security specifications like TLS and IPSec are being examined.

The likely outcome is that WAP Forum's Security Group (WSG) will specify profiles of these specifications (i.e. subsets) which WAP 2.0 devices will implement. WSG will also seek to influence the further development of these Internet specifications so that the needs of wireless devices are handled better. For example, the certificate URL concept can provide benefits to wired, as well as wireless client devices. In addition, WSG is examining the needs for additional application layer security functionality. For instance, it is possible that more functions like signText() will be defined for the WAP Cryptographic API. In terms of the impact on wireless PKI, a similar approach may be expected, aiming at interoperability with current Internet specifications and attempting to influence the evolution of those specifications.

5.2.3 PKI Assessment

For a PKI user's goal to build trust and confidence in online transactions by addressing security concerns, an important consideration is that PKI is only one of the many security options to reach this end goal. In addition, not every security need would require a full-fledged implementation of PKI. Instead, individual risk tolerance, good security and risk management policies (i.e. insurance coverage, daily transaction/transfer limits) could help to balance security risk with the security need without having to implement a PKI. However, PKI remains the most suitable solution where all four elements of security: authentication, confidentiality, integrity and non-repudiation are required, and adoption will continue to grow in selected sectors, and for applications that require these four elements of security. This section presents the assessment of PKI versus its alternatives to support this point.

The three main security models are:

- **TLS -** Transport Security is the most commonly used. Existing technologies such as secure sockets (SSL/TLS) provides simple point-to -point confidentiality and integrity for a message. Authentication is provided only through the use of an additional user token (ie password, biometrics, hardware token).

- **PKI -** At a high level, the PKI model involves certificate authorities issuing certificates with public asymmetric keys and authorities that assert attribute properties other than key ownership. Owners of such certificates may use associated keys to express a variety of claims including identity. It is considered an end-to-end solution that provides confidentiality (symmetric & asymmetric key encryption), integrity (digital signatures), authentication (a certificate and associated key is unique to individual) and non-repudiation (strong binding of certificate and public key to user (who holds the private key) with accompanying legal commitments and time-stamps).

- **Kerboros -** The Kerboros model generally regarded as an authentication services that relies on communication with the Key Distribution Center (KDC) to broker trust between parties by issuing symmetric keys encrypted for both parties and "introducing" them to one another. It provides the following features of confidentiality, integrity and authentication but little non-repudiation benefits due to the lack of strong binding of user to the key.

Making a comparison of security technologies out there, PKI is by far the most robust architecture that provides the 4 key features needed of a trust infrastructure i.e. confidentiality, integrity, authentication and non-repudiation and backed by legislation as a means of making binding commitments. Nevertheless, technology is only as strong as its weakest link and as such, PKI is only as robust as its strongest security policies that are in place for correct PKI implementation.

Technology aside, however, risk management can be counter-balanced by having good security policies (i.e. limited liability) and as such, even weaker but cheaper technologies other than PKI can be counter balanced by the use of a well thought out security policy. (i.e. banking is secure with pin/password as long as transaction limits are limited).

	Rating	Assessment
PKI	• Confidentiality • Authentication • Integrity • Non-repudiation (strong legal binding)	• Comprises a full suite of services that the ensure integrity of the whole value chain of the transaction • Cost: High • Maturity: Medium • Scalability: High
VPN/SSL Encryption with Hardware Token	• Confidentiality • Authentication • Integrity • Non-repudiation (weak legal binding)	• Gaining popularity for enterprise use • Moderately secure, but • Hardware token and password can be stolen • Cost: High • Maturity: Medium • Scalability: Low
VPN/SSL Encryption with Biometrics	• Confidentiality • Authentication • Integrity • Non-repudiation (weak legal binding due to lack of maturity)	• Mainly use for door access and PC log-in • Cost: High • Maturity: Low • Scalability: Low
Kerboros (an authentication service available in Win 2000)	• Confidentiality • Authentication • Integrity	• Moderate adoption • Used within universities and enterprises • Moderately secure except password can be • compromised and does not support non-repudiation • Cost: Medium • Maturity: Medium • Scalability: Medium
VPN/SSL Encryption (with user ID & password)	• Confidentiality • Authentication • Integrity	• Widely adopted • Fairly secure, but • Password and ID are easily compromise • Does not support non-repudiation • Cost: Medium • Maturity: High • Scalability: High
Password/PIN	• Authentication	• Popular • Fast, but insecure • Low consumer confidence • Audit mechanism: none • Cost: Low • Maturity: High • Scalability: High

Table 7. Comparison of Security Technologies

5.2.4 PKI Obstacles

5.2.4.1 Market Inhibitors

PKI technology has been predicted to proliferate since 1997. However, the prediction has so far failed to become a reality due to several obstacles. Based on IDA's findings of a consultation paper released in Sep 2000, the industry generally feels that the main market inhibitors for PKI are as follows:

- General lack of awareness of PKI and security issues (education)
- Lack of interoperability standards for cross-border certification
- High cost and complexity of installation, deployment and maintenance
- Issues related to ease of use and convenience
- Lack of consensus on cross-border legal issues
- Lack of multi-vendor interoperability
- Lack of demand and (killer) application support

5.2.4.2 Implementation Difficulties

The technical and policy issues that are obstacles to the implementation of PKI include:

- A hierarchical model of trust which results in a spiral of dependencies for trust verification

- One obstacle to the acceptance and use of digital signature in PKI is their uncertain legal standing. There is limited assurance provided by the CA and liability is often disclaimed during registration and limited during operation, this compromises the value of transactions which PKI can support.

- One need is for the CA to liable if incorrect verification is made.

- PKI relies on identification and the existence of a means whereby senders can identify themselves. This breakdown of anonymity and pseudonymity is one factor leading to the lack of privacy.

- Another disadvantage of PKI is that the standards still developing, which presents a shifting target to interoperability. Although X.509 standard defines digital certificates, it can be implemented in different ways. Furthermore, there is no standard PKI implementation, and problems exist with interoperability between disparate vendor solutions.

- Operation and Management difficulties are also common. A typical PKI implementation can take a long time to complete and requires strong planning and a strong project team. After the initial effort of implementing a new PKI system, the following administrative and operational are consuming. Lack of a common framework and common set of protocols to do certificate and key management is another hindrance. Best practices also vary between PKI models.

5.3 Future Developments and Outlook

5.3.1 Technology Issues

In the previous section, several inhibitors to PKI are outlined. Are these obstacles insurmountable and will it lead to the demise of PKI? And is PKI worth the effort to circumvent these stumbling blocks? This section examines what is needed on the road ahead to strengthen and evolve PKI.

5.3.1.1 Critical Mass Needed

The value of PKI is inherent in the size and reach of the community. A critical mass of networked PKI identities creates positive externality as they acquire more members. This is embodied in Metcalfe's Law which stipulates that the value of a network is proportional to the square of the number of nodes on the network. Interoperability is one key barrier to achieving critical mass.

One reason is the lack of interoperability among the various CAs. With the intention of achieving interoperability, a MOU was signed between the PKI associations of Japan, Korea & Singapore. The main objectives of this initiative are:

- To establish an international e-commerce infrastructure in Asia with the aim of interoperability between countries;
- To investigate technical, institutional and operational issues on PKI-based applications ranging from e-government to private sectors in each country;
- To explore how the nationally certified CAs can be interoperable with each other;
- To develop a test-bed, conduct experiments and demonstrate a proof of concept of an inter-working PKI framework;
- To publish a recommended "Technical Profile" to facilitate PKI interoperability.

Beyond the issues related to CA-CA interoperability are technology issues. The interconnection of diverse PKI implementation that are based on technology supplied by different PKI vendors

poses another problem. One effort towards interoperability is XKMS, an XML-based specification for protocols for distributing and registering public keys. One goal of XKMS is to enable disparate PKI systems have open exchange and validation of certificates across PKI web services. The completion of the XKMS specification and interoperable solutions based on it is predicted to appear in 2004.

5.3.1.2 Key Management

Private Keys are highly susceptible to a wide range of risks, such as illegal discovery, copying or invoking of private keys, in memory or on disk, even if they are protected by cryptographic measures. The higher level of protective measures that may be applied to private keys such as chipcards and dongles; directly connected device-readers, biometrics, ATM-style PIN-pads are not scalable or widely adopted as yet.

PKI is built on the capstone of Public Key Encryption, based on the fundamental assertion that the possessor of a key pair, would be the only entity that possess knowledge of the private key. Digital Signatures and Chain of Trusts are also all based on the absolute secrecy of the private key. The role and importance of the Root Certificate Authority within a PKI is paramount as trust is delegated through a chain of Digital Certificates. Compromise of the private key of the CA causes significant issues of trust, perception, and liabilities.

There are two scenarios that would lead to the compromise or loss of the confidentiality of the Private Key. One is termed "Rubber Hose", for the use of non-digital means to extract the Private Key, physical force, bribery or coercion is usually sufficient to induce individuals with access to duplicate a copy of the Key. This ties in to the growing prevalence of attacks arising from insiders within an organization. The second is the insecurity of software based cryptography. The private key of the CA is commonly kept on the hard disk in an encrypted format. However for use, for example in a certificate signing process, the key must be made available for use in the memory space of the CA server. Attacks are possible through the creation of a process to read into the memory space of a process that is performing cryptographic operations, or by triggering a core dump which would entail the writing of memory content to a file. Once the key has been compromised, every single certificate issued/ signed by the root CA would have to be revoked which is a major effort.

Secure public-key–processing devices, also known as hardware security modules (HSMs) have emerged to counter this vulnerability. HSMs are designed to protect the creation, storage, and management of private keys. The essential function of a HSM would be the provision of a safe and trusted environment for cryptographic operations and the protection of Cryptographic

keys. With reference to the CA example above, the private key of the root CA would be kept within the confines of the HSM, any cryptographic operations would be performed within the HSM only.

The Monetary Authority of Singapore's (MAS) "Internet Banking Technology Risk Management Guidelines Version 1.2" Section 4.14 also recommends the usage of HSM or tamper-device for secure encryption and decryption functions. IDC predicts that PKI software vendors will bundle secure public-key processing devices for root key protection and that HSM devices will be required for digital signing of ecommerce transactions as people must be able to trust that signing operations are secure. HSM devices will also be required for the validation of certificates associated with business transactions.

5.3.1.3 Trust Model

Verisign describes PKI as "the interface between the Internet and the Real World." The PKI trust relationship model must reflect real-world trust relationships. PKIs can be structured in different ways and this structuring determines the trust relationships. The traditional hierarchical PKI model are usually more appropriate for hierarchical organisations, and non-hierarchical PKI models such as mesh, trust networks and webs of trust for dynamic organisations such as the collaborative teams and virtual organisations.

Hybrid PKIs are viewed as the best fit for reallife as it supports the combination of both hierachical and non-heirachical. This is enabled by means of bridge CAs. The PKI community is exploring the range of topologies for a multiple-bridge infrastructure and potential challenges.

5.3.2 Technology Developments

5.3.2.1 Service Model

Due to the cost and complexity involved in implementing PKI, some organisations are outsourcing their PKI to an external service provider. In the market today, there are an increasing number of service providers who can provide such services to organisations who wish to outsource their PKI.

Outsoucing service providers include IBM Global Services, Baltimore Technologies's Managed PKI Service; Entrust Technologies's Entrust@YourService and VeriSign's OnSite. IDC expects that this trend of outsourcing PKI will drive the growth of managed services, with the market growing from $720 million in 2000 to an estimated $2.2 billion by 2005.

Earlier in this section, XKMS was introduced as an XML-based with a goal of interoperability between diverse vendor PKI offerings. Another feature of XKMS is that it is built on a service-based model. XKMS is based on Web Services standards WSDL and SOAP, is designed to be implemented as a Web service, and will operate as an application that provides services such as key registration on request.

5.3.2.2 Wireless PKI

Widespread mobile Internet users have brought the development of mobile Internet technology and rapid expansion of mobile Internet service. These are main factors that increase the importance of security issues in mobile Internet. In order to protect user's private information in mobile E-commerce services such as banking, stock exchange, shopping, implementation of security technology is essential. Korea Information Security Agency (KISA) has defined the Wireless PKI Technology Criteria and Specification to assure of interoperability for certificate generation and management and to maintain the international compatibility within the scope of Wireless Digital Signature Certification Management Infrastructure which will be built on the Digital Signature ACT.

5.3.2.3 Lightweight PKI

One criticism of full-featured PKI is that it is too heavy-weight. There is a trend towards lightening it. An effort is this area is Intel-led SPKI (Simple Public Key Infrastructure) whose charter is to develop Internet standards for an IETF sponsored public key certificate format and associated protocols.

SPKI expands PKI from the use of an ID PKI to the use of delegable, direct authorisation in a role-based security model. SPKI was designed as a standard form for digital certificates whose main purpose is authorisation rather than authentication. These structures bind either names or explicit authorisations to keys or other objects. The binding to a key can be directly to an explicit key, or indirectly through the hash of the key or a name for it. This forms a distributed security infrastructure, which combines a simple public-key infrastructure design with a means of defining groups and issuing group-membership certificates.

Another example is PKI-lite, which is based on a relatively simple certificate profile and a policy framework. PKI-lite avoids the lengthy policies, user identity verification, and practices framework typically associated with a full-featured PKI, Instead, works on a simple certificate profile and a policy framework. This effort is undertaken by HEPKI-TAG (Higher Education PKI Technical Activities Group).

5.3.2.4 JavaCard as Disruptive Technology for PKI

One view of PKI is that it is cost effective only in high value or high volume scenarios. Today's luke-warm (or cold) consumer adoption of PKI is a result of lack of convenience features. JavaCard may be the disruptive technology to hold the key to widespread adoption of PKI as it not only holds security credentials, it allows other high-security functions to be performed locally within the card, offering another level of convenience not previously available (eg. offline authorization, personalized transaction record like having a POSB passbook in your mobile phone). JavaCard with mobile terminals (plus J2ME) may be the killer pair.

5.3.3 Market Forecast

PKI technology has matured over the last few years and is ready for widespread implementation. With the strong security provided by public-key technology, it is anticipated that PKI will eventually become the mechanism underlying most e-commerce transactions. Increasingly, the financial community is adopting public-key tools such as digital signatures and digital certificates to secure business transactions against forgery, fraud and denial-of-service.

Nevertheless, PKI is still an evolving market and standards in this area are still evolving. Businesses are advised to consider their business requirements and risk assessment before making a decision to adopt PKI as an enterprise security solution. Moreover, in order to protect investment and avoid future interoperability headaches, it is vital to source a PKI that is completely open and built to the most common and advanced commercial standards. This needs to be considered by the organisation at the design stage to ensure seamless integration with the rest of the organisation's IT infrastructure.

The lack of application support has been a problem plaguing PKI since its inception. However, META Group predicts that this situation will improve in the next 18-24 months as promising new players addressing application support for PKI through middleware tools (e.g. SHYM, Ubizen) combined with VeriSign's recognition of the application problem and new releases of software development kits to enable access to advanced PKI services.

Moreover, there needs to be more user transparency and ease of use to the end-user in order for PKI to be widespread and readily adopted. On this aspect, the Web browser support for client certificates will need to mature. Microsoft Windows 2000's support for a full range of PKI-based security services may increase the likelihood of the ubiquitous use of PKI on the Windows platform.

In the coming years, market leaders will begin to exert their influence on PKI. We believe that the market opportunity for PKI will span from established vendors of computer systems, software applications, and financial and information services to new start-ups. Companies that grab the high ground will be able to leverage their market strength into expanded product offerings and long-term market success.

GartnerGroup's Dataquest estimates that the digital certificate software and CA service market is set for a compounded annual growth rate of 80% between 1998 and 2002. Another GartnerGroup report predicts that PKI technology will be used to secure business relationships in the emerging B2B e-market arena, which is expected to grow to US$7.3 trillion by 2004.

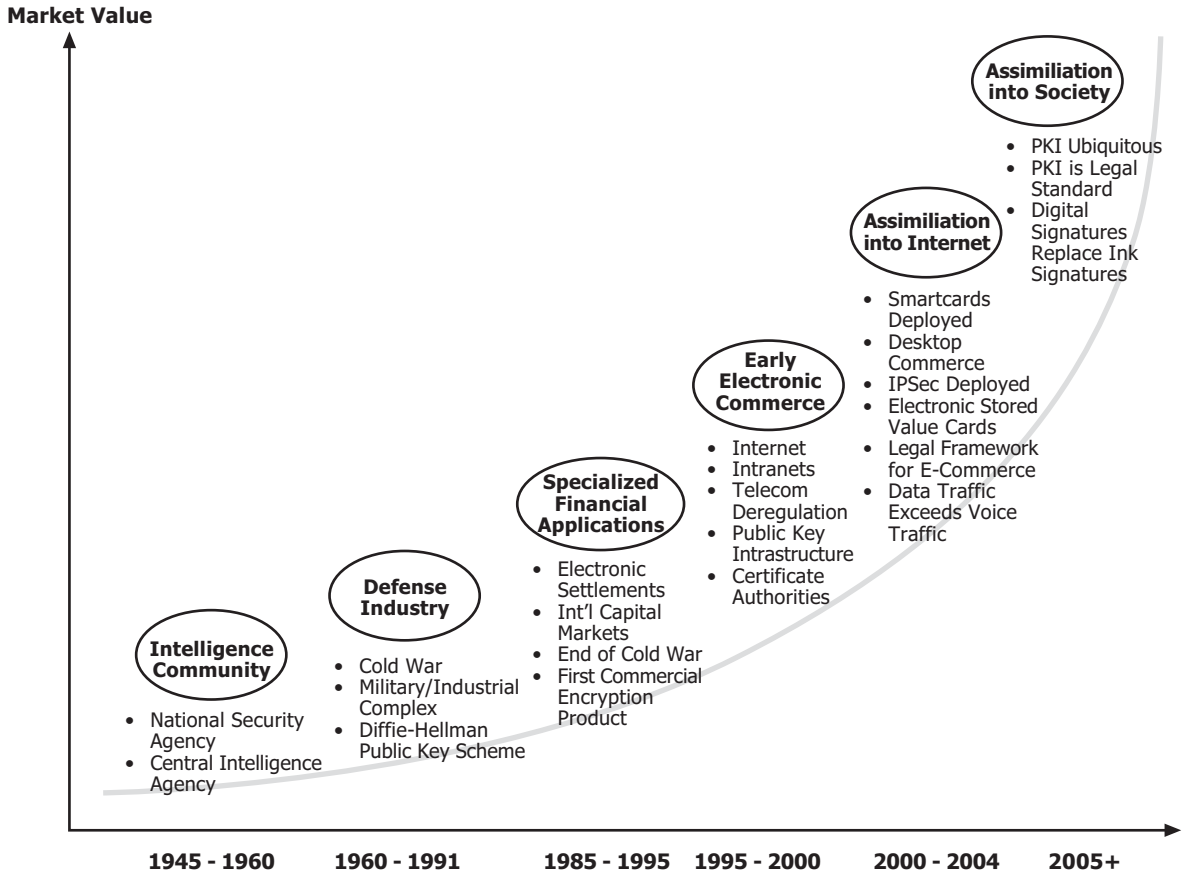


Figure 13. PKI is at an Inflection Point in Its Lifecycle
(Source: Hambrecht & Quist)

According to IDC, by 2002, PKI software products growth will begin to slow some, but the massive force of e-commerce will continue to push the market to US$586.3 million by 2003.

META Group believes that increasing deployments of B2B functionality by PKI vendors and third parties to solve applications support problems will result in increased implementation of advanced PKI functionality. META Group also predicts that by 2002/2003, the support for the creation and audited storage of digitally signed records (or digital receipts for payment transactions), which includes secure time stamping, will be enabled within applications. Furthermore, dispute-resolution processes that enable businesses to examine the secure record store as required will be enacted.

6 XML Security

6.1 Overview

In this chapter on XML security, we look at the impact of XML on secure e-Commerce. XML is used in a variety of ways, such as standards for industry data formats and to enable industry registries and ontologies. In web services, it is used to enable open distributed computing over multiple trading partner networks. The various types of web services for data retrieval, data transformation, data aggregation, transactional services and collaboration will form the engine of the next wave of e-commerce.

This chapter begins with an overview of the security risks and vulnerabilities posed by XML applications. This is followed by a section on XML security technologies. The core XML security standards for encryption, digital signatures, key management and access control are discussed before delving into the more specific security models such as SAML, WS-Security and OGSA. This is followed by an analysis of the more encompassing security issues such as end to end security and identity management. A highlight on trends and developments concludes this chapter.

6.2 XML Application Security Risks

In the emerging landscape of XML based e-commerce, a characteristic computing architecture would be one that is decentralised and heterogeneous with connections across multiple communities interweaved with peer-based architectures that are all open to the public Internet. This is contributing to a new paradigm in the use of technology and how we think about security.

Any of these characteristics presents challenges to the overall security of the system. One challenge is the enforcement of a single security policy across multiple heterogeneous systems. Another is ensuring that security policies are enforced with decentralised administration. The increase in vulnerability exposed by forming web services-based networks with trading partners (that are weak in security) is another issue in the upcoming wave of distributed computing. Adding web service functionality to a legacy application that was never designed to be exposed to the public Internet also increases security risks.

Security risks such as the vulnerabilities highlighted above are cited as the most significant obstacle against the use of web services. These risks as well as other security issues are overviewed in this section:

- XML Vulnerability
- Need for selective encryption
- Integration of PKI into XML
- End-to-end Security
- Single sign on

6.2.1.1 XML Vulnerability

The greatest vulnerability is in the informative and readable nature of XML itself. Message formats using self-describing metadata clearly show the data elements and the data is transmitted in human-readable form. And critical information may be exposed to anyone who is able to get access to the XML data stream.

Not only is XML data stream more readable compared to the traditional binary stream, an attacker also has more information available to them as the Web Services stack consists of layers for description and discovery. WSDL files and UDDI entries are informative, providing detailed information that may enable a hacker to gain entry. In addition, XML Web Services traffic may be tracked for activity trails, pattern recognition and auditing. Security and monitoring tools being built need to be able to keep up with the constant advances in hacking.

6.2.1.2 Need for Selective Encryption

XML is a meta-language that is used as a data description facility. An XML document is a text file that contains the data enclosed within data definition tags. Using existing encryption technology, the XML document as a whole may be encrypted. But this then raises the question of how to control authorised viewing of different groups of elements. An XML document may be moved from hop to hop, in a network of trading partners to fulfil a single transaction. For example, the logistics partner may need to know a customer's name and address but doesn't need to know the various details of any credit card such as account limits.

In addition, encrypting the whole document hides the tags that give XML its semantic quality. One of the strengths of XML languages is that it allows semantic searching. The schema provides information as to the meaning of a tag. If a document subsection, including tags, is encrypted as a whole, then the ability to search for data relevant to those tags is lost.

The existing encryption model works by a sender encrypting a file before sending it to a receiver. However, Web Services applications require support for a finer and more granular level of handling (from file to data element level) and multiple signers with different access levels.

6.2.1.3 Integration of PKI into XML

Standards based on XML are emerging to integrate PKI with XML. This is to address several issues in the area of key management in web services application environments.

The first issue is the need to provide developers with a standard way to integrate authentication, digital signature and encryption services, such as certificate processing and revocation status checking into applications.

The second issue is the need to manage keys. Security for web services applications will need to manage the private keys used for authentication in a heterogeneous distributed environment spanning several organisational domains.

The third issue is interoperability. Certificate servers from different vendors for PKI are mostly not compatible and enterprise deployment of PKI has to deal with the problem of different certificate servers working together. There are several different aspects to compatibility such as the ability to mix and match off-the-shelf PKI products, how to unify diverse PKI systems as well as how to share PKI certificates and key pairs between PKI applications.

6.2.1.4 End to End Security

End-to-end security is the safeguarding of information in a networked system by cryptography from origin to destination.

Traditionally, network-level security, such as those provided by firewalls, was the main line of defence against outside intrusion. Firewalls offer protection for Web services that are deployed internally and not exposed to the outside world. However this is a perimeter based security model of providing security between the entry and exit points of a particular network and the external environment. In the case where web services are integrated with partner services, which reside outside the firewall and are accessed via open networks, alternative security measures are needed.

6.2.1.5 Single Sign On

Web services are moving from a many-to-one to many-to-many model and may not be available in a single server or network. This has serious impact on current security methodologies. Web services sharing session and authentication information across networks and across disparate application is another issue.

As service-driven architectures evolve, it becomes important to distinguish a partner's request from that of an outsider. The common security infrastructure will extend to allow community based models and virtual organisations to have shared privileges and access rights, and towards federated identity. An even more complex scenario is the vision of dynamic Web service federations for dynamic open virtual communities.

Single sign-on plays an important role in Web Services environments to achieving federations. Diverse systems need to communicate with each other and it is impractical for each system to maintain each other's access control lists. This issue is explored further in the section on identity management.

6.3 XML Security Technologies

In the previous section, selected security risks and vulnerabilities that are emerging in the XML web services application environment are highlighted. In this section, we outline the XML security technologies and standards that are being developed and drafted. We will begin with the core of XML security: encryption and digital signatures. This is followed by the technologies for key management, authorisation, single sign-on and interoperability.

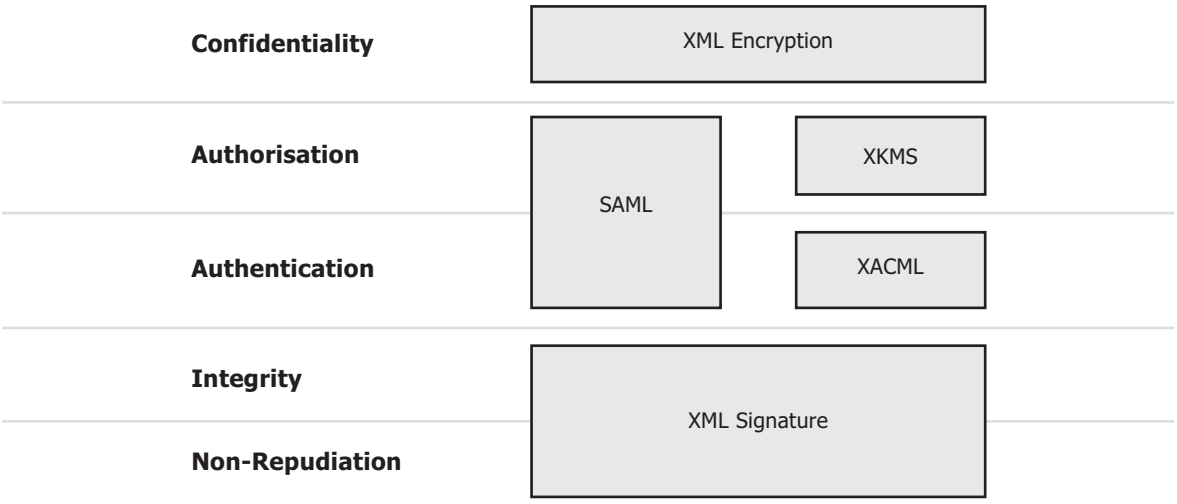


Figure 14. The Core XML Security Technologies

The figure above lists the security technologies that this report will highlight. As shown, they fit together as a foundation for the five basic security requirements, namely, confidentiality, integrity, authorisation, authentication and non-repudiation. With relation to XML security, these may be briefly summarised as the following: confidentiality to protect information against

unauthorised access, authentication so that the provider knows who is requesting the service, authorisation and access control to allow specific users to access the service, non-repudiation to prevent denial of transactions and integrity to assure non tampering.

In this chapter, we examine how the 6 selected XML security technologies form the foundation for a secure e-Commerce experience.

XML Encryption	• A process for describing how to use XML to represent a digitally encrypted Web resource, encrypting data and representing the result in XML. The data may be arbitrary data (including an XML document), an XML element, or XML element content. The result of encrypting data is an XML Encryption element which contains or references the cipher data.
XML Digital Signatures	• A method of using XML syntax and processing rules to associate a key with referenced data.
XKMS	• A specification for protocols for distributing and registering public keys, suitable to be used in conjunction with the proposed standards for XML Signatures and XML encryption.
SAML	• An XML-based security standard for exchanging authentication and authorisation information.
XACML	• An XML specification for expressing policies for information access over the Internet.
WS-Security	• A specification that forms the necessary technical foundation for higher-level security services.
OGSA	• A proposed specification for security for open grid services.

These technologies are examined in more detail in the following section. The following working groups drive these security technologies.

	IETF	W3C	OASIS
XML Encryption		W3C Working Group	
XML Signature	IETF/ W3C Joint Working Group		
XKMS		W3C Working Group	
SAML			Security Services TC
XACML			XACML TC
WS-Security			WS-Security TC

Table 8. Working Groups driving XML Security Standards

6.3.2 Core XML Security Standards

6.3.2.1 The W3C XML Encryption Specification (Xenc)

It is important for businesses to make sure that sensitive data is transferred from one point to another in a secure manner over public networks. Cryptography can help us achieve this goal by making messages unintelligible to all but the intended recipient.

Cryptography now does far more than merely conceal information. Message digests confirm text integrity, digital signatures support sender authentication, and related mechanisms are used to ensure that a valid transaction cannot later be repudiated by another party. These are all essential elements of remote trading, and mechanisms for handling complete documents are now fairly well-developed.

Who is Driving This. XML encryption is driven by the XML Encryption Working Group. This is a W3C working group led by Microsoft, Entrust, IBM, Motorola and includes participants such as Verisign, RSA, webMethods and Sun. They are working on the following specifications in the area of XML encryption.

- XML Encryption Requirements
- XML Encryption Syntax and Processing
- Decryption Transform for XML Signature

The charter of this working group is to develop a process for encrypting/decrypting digital content, including XML documents and portions thereof and an XML syntax used to represent the encrypted content and information that enables an intended recipient to decrypt it.

About This Standard. Besides being able to use standard methods of encryption when transmitting XML documents, the W3C and IETF propose a standard for encrypting the XML data and tags within a document. This standard will allow selective encryption of XML elements. This would let you encrypt portions of a document, with the idea that only sensitive information needs to be protected. Encrypting portions of a document with different keys would allow you to distribute the same XML document to various recipients, but the recipients would only be able to decrypt the parts relevant to them.

6.3.2.2 XML Signature

Digital Signature is a method for determining the data integrity of a message. A key is used to sign a message or part of a message. The resulting signature is often attached with the message. The receiver can then perform a similar operation. If the resulting signature does not match the sent signature, then the message has been tampered with. This ensures their authenticity, data integrity, and gives support for non-repudiation

Who is Driving This. The XML Signature specifications are driven by a IETF/W3C joint working group led by Microsoft, Entrust, Citicorp, Motorola and includes participants such as IBM, Sun, Baltimore and Verisign. They are working on the following specifications in the area of XML signatures.

- Signature Syntax and Processing
- Canonical XML
- Exclusive Canonical XML
- XPath Filter
- XML Signature Requirements

XML Signatures are specific XML syntax used to represent a digital signature and are designed for use in XML transactions. The standard defines a schema for capturing the result of a digital signature operation applied to XML as well as non-XML data. Unlike non-XML digital signature standards such as PKCS, XML signature has been designed to both account for and take advantage of the Internet and XML.

About This Standard. A fundamental feature of the XML Signature is the ability to sign only specific portions of the XML tree rather than the complete document. This is in alignment with a key requirement for XML security to support partial and selective security in XML documents. An XML signature can sign more than one type of resource, such as HTML, JPG, and different granularities of XML from the whole document to specific sections in an XML file.

6.3.2.3 XKMS (XML Key Management Specification)

It is strategically important for businesses to establish trust on the Internet as they become more involved in electronic commerce. Security breaches and loopholes have serious implications on the enterprise. Standards based on XML are emerging to address the need to integrate PKI with XML.

Who is Driving This. This is driven by a W3C working group, originated by VeriSign, Microsoft, webMethods and includes endorsements by Baltimore Technologies, Entrust, HP, IBM, IONA, PureEdge, and Reuters. They are working on the following specifications in the area of key management and the integration of PKI into XML.

- XML Key ManagementRequirements
- XML Key Management Specification
- XML Key Management Specification - Bulk Operation

About This Standard. The XKMS protocol is a proposed standard that defines a way to distribute and register the public keys used by the XML-SIG specification. XKMS is made up of two parts: the XML Key Registration Service Specification (X-KRSS) and the XML Key Information Service Specification (X-KISS). X-KRSS is used to register public keys, and X-KISS is used to resolve the keys provided in an XML signature.

One aim of XKMS is to have ease of use for PKI, and encourage it to become second nature for the end user. There is a need to integrate PKI features into applications, so that it becomes just another function in a developer's toolkit. To enable the use of keys in establishing trust for web services, developers must enable application level support for handling digital keys and digital signatures via the use of toolkits offered by a range of software vendors.

Another issue is the trend towards Managed Security Services (MSS) including PKI. Many organisations have decided that the technical implementation and administration of a PKI is too burdensome, and are outsourcing the certificates and other specialist activities to MSS providers such as VeriSign. This issue is aligned with another XKMS aimto implement PKI function as a web service.

XKMS is compatible with the emerging standard for XML digital signatures. Designed to be implemented as a Web service, XKMS is built upon Web Services standards WSDL and SOAP. The XKMS specification revolutionises the development of trusted applications by introducing an open framework that enables virtually any developer to easily incorporate trust services directly into the application. Currently, with the new XKMS specification, those functions instead reside in servers that can be accessed via easily programmed XML messages.

6.3.1.4 XACML

In the current enterprise environment of heteregneous and distributed systems, it is becoming increasingly difficult for an enterprise to obtain a consolidated view of the policy across a distributed heterogeneous environment. There is a need to create co-ordinated policy statements over a wide variety of information systems and devices.

Who is Driving This. XACML is driven by the OASIS eXtensible Access Control Markup Language TC. They are working on an XML specification for expressing policies for information access over the Internet.

About This Standard. As systems get increasinly distributed, the task of analyzing and controlling the security system infrastructure in a consistent manner across an entire enterprise becomes increasinly complex. The objective of the OASIS XACML TC is to address this need by defining a language capable of expressing policy statements for a wide variety of information systems and devices. The XACML specifications propose to consolidate current practices for access-control and then to extend a platform-independent language (i.e. XML) with suitable syntax and semantics for expressing those techniques in the form of policy statements.

6.3.2 Security Models for XML Web Services

As traditional security technology works quite well for applications where you don't need "XML-level granularity", such as SSL/TLS and signing a whole document, the dominant application for XML security will be web services. This section outlines several security models relating to xml-based web services.

6.3.2.1 SAML (Security Assertion Markup Language)

Web services will most likely be used in automated transactions that involve multiple business partners and be distributed over a heterogeneous environment. These distributed services will be aggregated into composite web services. A composite web service should ideally be presented as a single virtual service to the user, and allow this user (be it a human user, another web service or a application) to have a single sign on across these multiple Web services from separate but affiliated sites.

SAML is a protocol for asserting authentication and authorisation information. SAML compliant servers will house the authentication and authorisation data, allow secure exchange of profile information and act as an interoperability bridge between disparate security systems.

Who is Driving This. SAML is a standard that evolved from the convergence of AuthXML and S2ML, and is managed by an OASIS XML-Based Security Services Technical Committee that includes participants such as Baltimore, Cisco, Entrust, HP, Verisign and WebMethods.

About This Specification. Single sign-on plays an important role in Web Services environments for achieving federations. In a federation, distributed and diverse systems will need to communicate with each other and manage access control lists between themselves. SAML encodes authentication and authorisation information in XML format. A Web Service can request and receive SAML Assertions from a SAML compliant authority to authenticate and authorise a service requestor.

The aim of SAML is to deliver interoperability between compliant Web access management and security products. Users should be able to have their security credentials transferred automatically between disparate domains. Heterogeneity, distribution and different ownership should be transparent to the user.

SAML addresses this need by having a unified framework that is able to convey security information for users who interact with one provider so they can seamlessly interact with another. It provides a standard way to define user authentication, authorization and attribute information in XML documents. This unified framework is based upon a set of XML-based messages that contain details on whether users are authenticated, what kind of rights, roles and access they have and how they can use data and resources based on those rights and roles. These XML messages are the assertions. SAML defines the following three kinds of assertions.

Authentication Assertions:	require that the user prove his identity.
Attribute Assertions:	contain specific details about the user, such as his credit line or citizenship.
Authorisation Decision Assertion:	Identify what the user can do (for example, whether he is authorized to buy a certain item).

These assertions are represented as XML constructs and have a nested structure, whereby a single assertion might contain several different internal statements about authentication, authorization, and attributes. SAML-compliant security policy engine provides the base-level information to build SAML-enabled applications that interact across systems, and works over cross-domain authentication and cross-domain authorisation.

Developments. Of particular interest in the area of SAML, is its use in Federated Identity Management. There is currently some overlap between efforts by the Liberty Alliance and Microsoft. The Liberty Alliance Project is a group of vendors and corporate users which includes

SUN. They have released their federated identity management specification, which is based on SAML. This is outlined in more detail in the following Security Issues section.

For now, WS-Security is regarded as the messaging language and SAML as the security language. Sun supports SAML 1.0 in the form of the Sun ONE Identity Server. Microsoft announced that it would add support for SAML tokens, as well as Kerberos and X509 certificates in its WS-Security technology and specifications. More detail on the relation between WS-Security and SAML is included in the following Security Issues section.

6.3.3.2 WS-Security

First and foremost, SOAP does not directly provide any mechanisms for dealing with access control, confidentiality, integrity and non-repudiation. Such mechanisms can be provided as SOAP extensions using the SOAP extensibility model to enable secure web services. Security is crucial, to provide SOAP with the facilities for securing the integrity and confidentiality of the messages and for ensuring that the service acts only on requests in messages that express the claims required by policies.

Beyond providing security, another issue is to allow the use of existing security infrastructure to be used in the framework for secure web services, maximising current investments and leveraging on the maturity of existing security solutions. This requires interoperability between the different vendor's security solutions.

The WS-Security specification is a general messaging model of claims, policies and security tokens, that subsumes and supports several more specific models such as identity-based-security, access control lists, and capabilities-based-security. It allows use of existing technologies such as X.509 certificates, Kerberos tickets and password digests. It also provides an integrating abstraction allowing systems to build a bridge between different security technologies. The general model is sufficient to construct higher-level key exchange, authentication, authorisation, auditing, and trust mechanisms.

Who is Driving This. WS-Security is a proposed specification for a web service security standard that has been submitted to OASIS by Microsoft, IBM and Verisign for standardisation in the OASIS Web Services Security Technical Committee. These specifications are a convergence from previously proposed specifications by IBM and Microsoft such as SOAP-Security, WS-Security and WS-License. This technical committee includes participants such as SUN, Intel, Cisco and Baltimore.

About This Specification. WS-Security defines a set of SOAP headers that can be used to implement security measures for Web services. The base WS-Security specification describes how to add encryption and digital signatures to Web services to support XML-Encryption and XML-Signatures. WS-Security also defines a general mechanism for passing around arbitrary security tokens.

The initial specifications for WS-Security describes how to attach signature and encryption headers, as well as security tokens such as binary security tokens, X.509 certificates and Kerberos tickets to SOAP messages. On the IBM/Microsoft roadmap for WS-Security, the following six specifications were projected, as shown in the following table 9.

WS-Security Stack		Overview of Stack Layer
Federation	WS-Secure Conversation	Defines a general method for managing and authenticating message exchanges between parties and establishing and deriving session keys.
	WS-Federation	Defines how Web services manage and broker trust relationships, authorization data and policies in a heterogeneous federated environment, including support for federated identities.
	WS-Authorization	Describes how to manage authorization data and Authorization policies.
Policy	WS-Policy	Describes how to express the capabilities and constraints of the security policies on intermediaries and endpoints, includes required security tokens, supported encryption algorithms, privacy rules.
	WS-Trust	A framework for trust models that enables Web services to securely interoperate by Defining the brokered trust relationships a Web services environment.
	WS-Privacy	Defines a model for how Web services and requesters state and implement privacy preferences and organizational privacy practice statements.

Table 9. The WS-Security Stack

Developments. Of particular interest here is the intersection of WS-Security and SAML and how they will work together. SAML defines a standard, XML-based approach for passing security tokens defining authentication and authorisation rights. SAML was started as a way to achieve single distributed sign-on before shifting its focus to Web services.

WS-Security defines how you insert information into a SOAP envelope. SAML defines what the security information is. WS-Security is an extension to the SOAP envelope header for attaching security tokens such as digital signatures to SOAP. WS-Security is the messaging language and SAML is the security language. SAML has adopted WS-Security as the appropriate method for binding SAML assertions into SOAP messages. And there are plans to add support for SAML tokens into WS-Security.

Microsoft plans to release specifications and implementations for other Web Services security related requirements, including WS-Trust, WS-Privacy, WS-Policy, WS-SecureConversation, WS-Federation and WS-Authorization over calendar year 2002 - 2004. The approach is to be security protocol independent, allowing users and companies to select the security protocol they want, i.e, choice between passport, Kerberos, name/password, X509 or SAML.

6.3.2.3 OGSA (Open Grid Services Architecture)

Looking further down the road, we see Grid Computing maturing and converging with Web Services. The convergence is taking place in the OGSA specification. OGSA builds on concepts and technologies from the Grid and Web services communities. It is an architectural plan that defines a uniform exposed Grid service, as well as standard mechanisms for creation, naming, and discovery. It incorporates Grid functionality into a Web services framework, and creates an open architecture to be applied within commercial computing as a basis for distributed system integration, within and across organisational domains.

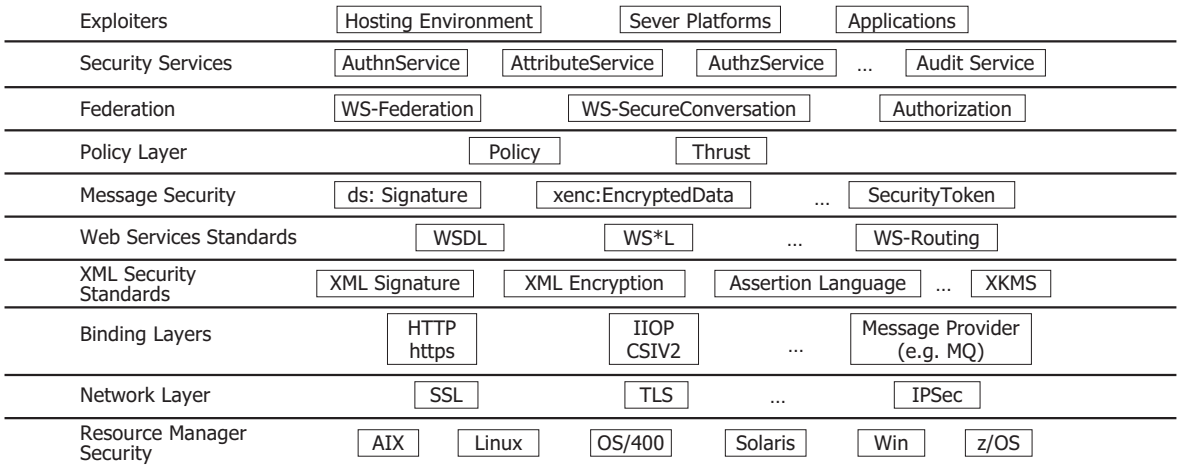


Figure 15. Grid Security Infrastructure
(Source: Global Grid Forum)

Who is Driving This. The Security architecture for Open Grid Services is a proposed specification meant to provide security to the bigger OGSA architecture. Two specifications, the Security Architecture for Open Grid Services and the OGSA Security RoadMap have been submitted to the Global Grid Forum. IBM, Virgina and Argonne are leading this effort.

About This Specification. The Security Architecture for Open Grid Services is a strategy that defines a comprehensive Grid security architecture that supports, integrates and unifies popular

security models, mechanisms, protocols, platforms and technologies in a way that enables a variety of systems to interoperate securely. This security architecture is intended to be consistent with the security model that is currently being defined for the Web services framework.

Developments. This has two implications to end-to-end security as outlined in the earlier section. Firstly, it extends the security architecture that is under discussion between the various web services proponents such as IBM, Microsoft. Secondly, it extends the access and delivery of security as a service, in a similar pattern to XKMS, with the vision of utility-like access.

6.4 Future Developments and Outlook

This section highlights the key security issues on the road ahead as well as predicted scenarios of the impact of XML-based web services on e-commerce environment.

6.4.1 End-To-End Security

According to a 2002 survey from Evans Data Corporation, developers feel that the most significant barrier to Web services implementation is the lack of end-to-end security. End-to-end security is a key requirement for web services application environment. There are several aspects to this.

The first issue is the security implications in the SOAP model itself. SOAP inherently provides a distributed processing model that might involve a SOAP message passing through multiple SOAP nodes. SOAP intermediaries are by definition men-in-the-middle, and represent an opportunity for man-in-the-middle attacks. Security breaches on SOAP intermediaries can result in serious security and privacy problems. A compromised or poorly protected SOAP intermediary might be used in the commission of a wide range of potential attacks. This deals with security vulnerabilities that occur in all the hops between participating SOAP nodes.

The second issue is that the second web service stack extends the Internet as we know it. Currently, security technologies such as SSL/TLS and IPSec provide satisfactory security at the network and session level. Web Services application model requires additional support at communication, message, community and composite level.

Security Levels in Web Service Stack. Web-service security should be provided at different levels, to construct a comprehensive and deep defence, attempting to prevent or deter the possible problems at every level. The table below lists the layers involved in a web services application model and provides an overview of the corresponding security requirements.

Web Service Stack Level	Security Requirements
Composite Level	
Definition	This is the level where atomic, distributed web services are aggregated together to form a set of service. Examples include workflow, orchestration, composite web.
Issues	Security is required for ebXML, Rosettanet, Biztalk.
Activities	XACML, SAML.
Community Level	
Definition	This level is concerned with the cataloguing and description of web services. Examples include industry specific directories, ontologies based on UDDI, ADS, DISCO.
Issues	Security is required for UDDI and ebXML registries. Authentication is required to identify the ownership of content as well as for identifying what "privileges" an entity can be assigned to with respect to the objects in the registry. The integrity of the registry content is of great importance to those who refer to and use it for mission-critical business applications. Capabilities for organizations to publish information, which are seen only by their partners.
Activities	XACML, SAML.
Message Level	
Definition	This is the expansion of security to the XML message level. Data secured this way will stay secure even if it is being routed between different Web services and intermediaries.
Issues	Standards from bodies such as OASIS, W3C and IETF are emerging for XML security such as XML encryption, XML Signature and XKMS.
Activities	XML Encryption for confidentiality of message. PKI for authetication. XKMS to integrate PKI and digital certificates. SAML Assertions included in message header or payload.
Communications Level	
Definition	This is the level where the protocol SOAP works in. Other communication protocols such as Jini, XML-RPC, XPL exist, but are not reviewed in this report.
Issues	SOAP itself has not security. Security is comes from WS-Security and SOAP security extensions.
Activities	WS-Security to add security to SOAP.
Session Level	
Definition	Encryption of packets of information for transmission between two entities, ensuring that no third party can eavesdrop or tamper with the information.
Issues	SSL commonly used for session level security, also known as hop-to-hop security. The SSL protocol can also be used to fguard communication between Web services. But SSL offers only point to point security.
Activities	SSL appliances for cryptographic acceleration are emerging.
Network Level	
Definition	This is at the port level. Network level security is traditionally provided by firewalls.
Issues	Open firewall ports for http and https.
Technologies	SSL/TLS offers several security features including authentication, data integrity, and data confidentiality and enables point-to-point secure sessions. IPSec is another network layer standard for transport security that may become important for Web services. In summary, security at the network and session may be sufficiently met by current technologies.

Table 10. End-to-End Security Issues in Web Services

Technology Landscape for End to End Security. The above table outlined the layers of the web services stack and provided an overview of the issues involved. Below is a mapping of the security technologies discussed to the corresponding requirements.

Web Service Stack Level	Security Requirements				
	Authorisation	**Authentication**	**Confidentiality**	**Integrity**	**Non-repudiation**
Composite level	SAML		WS-Security		
Community Level	UDDI Security	UDDI Security			
Message Level	SAML XACML	X.509 or Kerberos Certificates XKMS	XML Encyption	XML Signatures	XML Signatures
Communications Level	WS-Security				
Session Level		SSL with X.509 Certificates	SSL Encyption	SSL with MACs	
Network Level	SSL/TLS & IPSec				

Table 11. Technology Landscape For End-to-End Security

Future Issues. Beyond the web services stack, issues at the XML storage level will grow in importance. There is a need to integrate access control policies designed by the XML community with XML storage mechanisms designed by the database community. A finer level of granularity is required for access control. Issues exist for storing, retrieving and managing XML documents. A common method is to map XML data onto structures maintainable by traditional DBMS. This introduces additional layers between the logical data and its physical storage, causing performance issues. Developments will emerge to support XML documents at low architecture levels.

Issues in Reaching End to End Security. In assessing the impact of XML on end-to-end security, XML security is nothing new but a translation or transformation from existing proprietary security technology and implementation into using XML-based formats and Internet protocols. This process is likely to take time to mature just like the evolution of most security implementations. Even if we get the translation from security technnology into XML-based format, there is still a need for interoperability to gain widespread adoption. There is also the question of whether there is really a need to remap everything to XML, where edge-level interoperability may be sufficient (eg. S/MIME, SSL are so prevalent and proven; PKIX has evolved to be Internet friendly too).

There are many application templates for deploying web services, such as EAI, Portlets, business to business commerce models and service provisioning. Not all require end-to-end security. For those that do, not all require *complete* end-to-end security. Security implementation must be commensurate with the risks and liabilities involved in performing the communication event (whether it is to retrieve some info or to perform some financial transaction).

Though end-to-end security is highlighted here as an issue, several proponents of web services do not see the slow development of end-to-end security slowing down web service deployment. Deployment of web service for intranet users and trusted extranet users do not require widespread interoperable security implementation. One example is Sun who is doing their own web services with their partners. In their opinion, transactional capability and automated workflow are more important areas.

6.4.2 Identity Management

"On the Internet, no one knows that you're a dog." A Digital Identity is the representation of a human identity that is used in a distributed network interaction with other machines or people. The purpose of the Digital Identity is to enable the ease and security where we all know each other and interact face-to-face, to a machine environment where we are often meeting each other for the first time as we enter into transactions over vast distances.

About Identity Management. Identity management is the creation, management and use of online, or digital, identities. The three main approaches to identity management are Silo, Closed Community and Federated.

Silo
- *Unique relationships with its customers, employees and partners.*

Closed Community
- *This model uses a central hub to act as a broker to all member organizations in the community. Examples of this are Identrus, Bolero and VISA.*

Federated
- *In a federated model, each partner agrees to trust user identities issued or authenticated by other organizations, while maintaining control of the identity and preference information of its own users.*
- *The two major Internet federated models are Microsoft .NET Passport and the Liberty Alliance.*

The development in the technology landscape is moving towards the goal of federated identity.

Identity Management Initiatives. Federation refers to the technology and business arrangements necessary for the interconnecting of users, applications, and systems. This includes authentication, distributed processing and storage, data sharing, and more. The two main initiatives, Liberty Alliance and Microsoft, are discussed as follows.

The Liberty Alliance is a multi-industry effort that is collaboratively developing open standards for network identity. The Alliance is currently comprised of more than 40 members; founding members include American Express, AOL Time Warner, Bell Canada Enterprises, Citigroup, France Telecom, General Motors, Hewlett-Packard, Mastercard International, Nokia, NTT DoCoMo, Openwave, RSA Security, Sony Corporation, Sun Microsystems, United Airlines and Vodaphone.

The Liberty version 1.0 specifications do not involve the exchange of personal information. It is a format for exchanging authentication information between companies so as to not reveal the identity of the user. The user may maintain separate identities in different locations. The first set of products implementing the Liberty protocol have already been announced, such as SUN's SunONE Identity Server 6.0 which is in early access beta The Liberty Alliance has already begun developing its next set of specifications, which will leverage Liberty version 1.0 and expand to include features for permission-based attribute sharing. This will extend the simplified sign-on capabilities in version 1.0 and enable organizations to share certain personal information of users according to the permissions and preferences granted by the user. The Alliance also anticipates that the next set of specifications will enable organizations to link and extend their service offerings between various "circles of trust" or industries. The next specifications are to be released in early 2003.

Microsoft is also working on its own Federated Identity solutions. Launched in 1999, Microsoft .NET Passport, is a suite of Web-based services that provides users with single sign-on capability at a number of participating Web sites. .NET Passport employs encryption technologies such as Secure Sockets Layer (SSL) and the Triple Data Encryption Standard (3DES) algorithm. Microsoft stated that Passport, which is aimed primarily at authentication and authorisation for consumer Web services, will include federation support in 2003.

Passport is designed for day-to-day consumer-oriented services. Microsoft states that they currently do not position passport as a solution for corporate single sign-on, as that is a solution to be addressed by the upcoming Windows Trustbridge solution in 2003. Trustbridge is a product implementation available for windows, that allows Federation of security across the Internet across two or more organizations and Internet/external communication (outside the firewall). It will communicate with other federated sites using WS-Security Web Services standards. Internally, it will enable mapping to Active Directory accounts and Kerberos v5.0. Trustbridge will be based on the WS-Security standard.

With regard to the intersecting efforts in the identity management landscape, vendors such as RSA, Oblix and Netegrity have outlined plans this week to support a range of identity protocols. One example is OpenNetwork which supports both Passport and SAML in its DirectorySmart application, an enterprise Web identity and access-management platform.

6.4.3 XML Security Devices

Reprogrammable Hardware. Tarari, an Intel Corp. spin-off is using reprogrammable hardware to tackle the XML-processing and virus-detection markets, both of which require deep inspection of incoming packets. Tarari say that their hardware, which handles Layer 7 application level processing, is aimed at the more complex XML processing and virus detection.

XML firewalls vs traditional firewalls. Traditional firewalls examine header information of passing data to determine if it will be allowed to pass through. But such a cursory inspection won't be enough for XML traffic, all of which will slide through because it looks like general Web traffic.

XML firewalls are differentiated from traditional IP-level network firewalls. An XML firewall has to go beyond inspecting the packet or protocol level to examining the actual content of the transmission. Adding to the complication is that messages have to be decrypted or uncompressed. A SOAP message needs to be examined to make sure it is an authorized request. And this SOAP message may be encrypted. As a means of contrast, the view is that traditional security models deal with perimeter based security and scans incoming traffic at the network level, whereas XML firewalls work at the application level.

There are two kinds of XML firewalls, appliances and software firewalls. The firewall appliances offer more performance versus the software firewalls which are programs that can be installed on an application server and are more flexible in terms of where to install the firewall than a hardware appliance.

Forrester predicts that XML firewalls would not become mainstream until 2003 or 2004.

7 Singapore Landscape

With the pervasive adoption of Internet and all the infocomm infrastructures being interconnected globally, security for infocomm is essential. Maintaining the health of these infrastructures is what iSecurity is all about.

The following section presents several issues and developments in the local landscape for the respective security technologies.

7.1.1 Cryptographic Controls in Singapore

The use of cryptography is essential for the development of e-commerce as it allows the protection of electronic data and records from unauthorised access or modification. In line with the ongoing effort to promote Singapore as a trusted international e-commerce hub, IDA has lifted the control on the import of cryptographic products with effect from 21 Jan 2000. With this lifting of import restrictions, IDA believes it will help to promote confidence among companies to conduct e-commerce in Singapore.

With the relaxation of export controls for cryptographic products in EU countries and the US, and the lifting of Singapore's own import control on such products, businesses in Singapore are further encouraged to employ the use of cryptography to protect their IT assets and e-commerce activities, and further promote confidence to conduct e-commerce in Singapore.

To complement the broad range of foreign cryptography products and technologies (including those from Europe, the US and Israel) that are currently available in Singapore, a number of Singapore companies provide a variety of locally developed, standards-based security solutions as well as consultancy services in this area. These companies include CISCO Computer Security (www.cisco.com.sg), DigiSAFE (www.digisafe.com), NTS Consulting (www. ntsc.net), PrivyLink (www.privylink.com), and KeyTrend Technology (www.keytrend.com.sg)

7.1.2 Leading Smart Card Deployments And Applications

In the area of smart cards, there are promising efforts underway and initiatives planned. The leading card deployments and applications are outlined below.

NETS CashCard. In terms of e-purse schemes in Singapore, NETS (www.nets.com.sg) manages one of the world's most successful nationwide e-purse called CashCard. Together with Visa, NETS can in future provide a CEPS-compliant e-purse to the region providing multi-

currency support. In most organisations, CashCards are combined with other applications such as door access, special loyalty programmes and any other value-added application developed by the organisations.

Today, CashCards have moved from single-application cards to multi-application co-branded cards. Examples include bank ATM card, Public Sector Card, SAF Card, CashCard, VisaCash, and NTUC Link Card. CashCard accepting devices have also become more pervasive e.g. POS, ATM, kiosk, in-vehicle unit, payphone, photocopier, PC, car-park system, mobile phone, etc. In the arena of combi cards, NETS has started developing applications based on ISO and other global standards. Smart Cards, PKI and cryptographic technologies remain to be important building blocks to NETS.

NTUC LINK Card. Another large-scale successful smart card initiative launched in Singapore was the NTUC Link Card (www.ntuclink.com.sg) by NTUC Link Pte Ltd. The NTUC Link Card is a chip-based photo card that replaces all existing NTUC membership cards. The company aspires to be the leading smart card issuer in Singapore with its 500,000 strong NTUC Union and Co-operatives members. The card will support e-commerce applications, especially if it is injected with a digital certificate. The cardholder can continue to use the same card when he changes his job and joins another union, or is promoted to a higher level in the same company.

Public Sector Card. The Public Sector Card (PS Card) is also undergoing PKI upgrade from Netrust for about 65,000 civil servants. The technology used is a hybrid card consisting of MIFARE 8 Kbit EEPROM contactless (Type A) standard from Philips (Mikron) and a contact chip of 8 KB EEPROM with 4 KB reserved for the digital certificate. The contactless interface is used mainly for door access. The applications developed for contact chip include remote network access; secure email and government e business (GeBiz). The card supports the CashCard e-purse functionality. A second phase upgrade is planned to include an open standard and PKCS #11 compliance card.

ez-link Transportation Card. The Land Transport Authority (LTA) is currently migrating from the magnetic fare card to ez-link card, the contactless smart cards for the MRT, LRT and buses. Transit smart cards are known to have expanded their scope of services to non-core businesses such as e-purse for micro-payments such as in the case of Hong Kong's Octopus transit card used in micro-payment applications (7-Eleven, fast food chains, etc). There is possibility that these could one day expand their applications to e-commerce enabled terminals in Singapore, subject to monetary regulations among other possible factors.

Healthcare via Internet. In future, Singaporeans could access their own medical records that are stored electronically in government hospitals, polyclinics and specialist centres. Patient records will also be shared electronically among hospitals and authorised health-care

professionals. Two groups of medical institutions set up by the Ministry of Health (MOH) – National Healthcare Group (NHG) in the west and Singapore Health Services (Sing-Health) in the east are participating in the project to share their records. MOH has also set up a committee to look into data standards, privacy and security.

Bank Cards. In Singapore, it seems that the migration to EMV-compliant ATM cards would be slow due to the high costs of upgrading the banks' infrastructure and the complexity to migrate to smart cards. We do not see many implementations worldwide currently. Banks will need to justify the costs against the potential benefits in reducing or eliminating frauds.

Recently, MAS has promulgated security guidelines on electronic and Internet banking for the banking industry. Banks are required to assess the risks relating to their online banking products and adopt appropriate security control measures to address and mitigate the risks involved. They are directly responsible for the safety and soundness of the services and systems they provide to their customers. With the increasing concern of online fraud, we foresee banks moving toward a more secure mean of access(i.e EMV compliance smart card) than just the traditional magnetic stripe card and user id and pins.

Some local banks also pointed out that the current challenge is that the so-called generic readers available are not able to accept all existing and future services. As such, card readers would have to be changed when we modify or add to the existing set of applications. This is not practical for mass deployment. Technology can make a difference by enabling the new smart cards to become interoperable and enabling the flexibility to add-on new services. Technology can help in the standardisation of the basic smart cards and readers framework to allow the deployment of common infrastructure which different businesses can rely upon to build or add his services with time. For instance, with a common card framework, a consumer can change bank service to another rival bank but still using the same card and reader. With new services offered by the bank, consumers can also add these into the smart card without the need for major upgrades. This can help justify the initial cost of infrastructure deployment of cards and readers. The solution must be upgradeable and interoperable.

7.1.3 Biometrics Adoption Issues

Promoting Biometrics. The industry in Singapore has expressed a concern for the high cost of biometrics implementation and its limitation to niche markets. Research and development in some biometric technologies is still at an early stage to be widely affordable. As such, Nanyang Technological University (NTU) and LIT are spearheading a consortium in partnership with industry stakeholders and supported by IDA to develop enabling technologies and infrastructure to allow for low-cost biometrics and security for mobile commerce. Other major

concerns are public acceptance, security and privacy issues. Unlike PIN and password, biometric cannot be easily replaced once there is identity fraud where the biometric information is compromised. Users would also want to have control over their biometric information rather leave them at the hand of corporations.

BEAM. In the local community, the Biometrics Enabled Mobile Commerce (BEAM) consortium, was set up to jointly conduct research and develop solutions for biometrics-enabled mobile commerce. Research areas of interest include low-cost fingerprint sensor and recognition system, integration of biometrics and PKI, integrated solution for biometrics verification on smart cards, e-security and payment modes, new mobile devices with integrated fingerprint recognition capability, and mobile broadband services and applications that can support future biometrics mobile commerce.

Immigration Automated Clearance System. In the area of applications, biometric based physical access control system is getting popular as the cost is becoming affordable. Biometrics has been implemented to control access to restricted areas at companies, condominiums and at schools. The use of biometrics for time and attendance is also becoming popular among companies and being trial tested in selected schools in Singapore. Since 1997, the Singapore Immigration & Registration (SIR) introduced the Immigration Automated Clearance System (IACS) for fast immigration clearance among frequent travellers. IACS uses biometrics and smart card technology to authenticate the identity of travellers. Presently, the IACS is available at Changi International Airport and the bus passenger halls of the Woodlands and Tuas Checkpoints. SIR has not stopped at this but has ventured to experiment other innovative means to serve the travellers better. Currently, SIR is conducting a trial using iris recognition technology for identification of motorcyclists at Woodlands and Tuas Checkpoints. Applications of biometrics in Singapore schools are also getting popular as a means of access control and for time and attendance.

Local Biometrics Innovators. In Singapore, the Biometrics Standardisation Working Group under the IT Standards Committee (ITSC) is responsible for standards work in biometrics. Besides the two local universities – National University of Singapore (NUS) and Nanyang Technological University (NTU), The Laboratories for Information Technology (LIT) is also actively researching in biometrics.

The biometrics processing research team at LIT, formerly of Centre for Signal Processing (CSP), emerged top in speed and runner-up in accuracy in the fingerprint algorithm processing at FVC 2000[6], an international fingerprint verification competition. This has been extended into

6 FVC 2000 was the first fingerprint verification competition organised by the University of Bologna (Italy), the US National Biometric Test Center and the Michigan State University (US). Details are available at http://bias.csr.unibo.it/fvc2000/.

novel areas such as improving the false rejection and false acceptance rate achievable from a small fingerprint sensor by synthesizing the fingerprint templates derived from various portions of a finger to form a single template and incorporation of codeword into fingerprint recognition. They have also developed a fast fingerprint matching on smart card and Java card and an algorithm to improve and update the fingerprint template through series of positively identified templates. Other areas of active research include complete fingerprint processing on card, quantitative fingerprint image quality analysis and deformation measure, and fingerprint image enhancement.

Besides fingerprint, LIT also does work on voice biometrics, face recognition, hand geometry, facial thermogram, ECG as well as optimal multi-modal fusion of biometrics. LIT has developed a text-dependent speaker verification system with recent research focus on developing robust speech enhancement algorithms and innovative microphone array structures which will ensure a high-quality capture of speech signals in noisy environments. This will allow voice biometrics to be used in various environments. For face recognition, an interesting aspect is the work on face synthesis that generates various face templates in different poses and lighting conditions. This is shown to provide greater accuracy under real world conditions with varied lighting and different facial poses. The face synthesizer can be seamlessly integrated into any existing face recognition system to meet the most challenging of facial scanning requirements. .

"Novel Biometric Digital Signatures For Internet Based Applications" is a research project underway in School of Electrical and Electronic Engineering, NTU. This research project examines the notion of a Biometric Signature: a new approach to integrate biometrics with public key infrastructure, PKI using biometric based digital signature generation which is secure, efficacious, fast, convenient, non-invasive and correctly identifies the maker of a transaction. It also suggests two schemes for biometric signature using two existing and widely used digital signature algorithms, RSA and DSA and discusses the problems associated with them individually.

7.1.4 PKI for Trust

Electronic Transactions Act. Singapore has a vision of becoming a trusted international e-commerce hub, where e-commerce transactions that are carried out around the world are processed. We therefore consider PKI and the range of security services that it offers to be the key foundation for secure e-commerce of the 21st century. A number of efforts are being carried out by the Government and the industry towards this end. The first is legislation which is outlined below. This is followed by an overview of the activities and associations in PKI, as well as a look at an academia research project exploring trust issues for e-commerce.

In order to achieve Singapore's e-commerce hub vision, a conducive and comprehensive legal and policy framework for building trust and confidence is required for e-commerce to flourish. Singapore's Electronic Transactions Act (ETA) was enacted in 1998 to provide a legal framework for electronic transactions and secure e-commerce in Singapore. The ETA

- removes the uncertainty surrounding the legality of contracts that are formed electronically, and accords legal recognition to electronic records and signatures;
- exempts the network service providers who merely carry third party traffic from criminal and civil liability;
- establishes the voluntary licensing of certification authorities as trusted third parties
- and enables Government agencies to accept the filing of documents and to issue licences, permits and approvals electronically, without the need to amend their own parent Acts.

A subsidiary legislation, the *Electronic Transactions (Certification Authority) Regulations* came into effect in 1999 and stipulate the requirements for a certification authority to obtain a licence in Singapore.

Voluntary CA Licensing Scheme. With the enactment of the ETA (1998) and the associated Electronic Transactions (CA) Regulations, Singapore put in place a voluntary licensing scheme for CAs. In addition to laying down the administrative framework for licensing by the CCA, the Regulations also stipulate the criteria for a CA in Singapore to be licensed, and the continuing operational requirements after obtaining a licence. The criteria that CAs will be evaluated against include their financial standing, operational policies and procedures, and track record. The voluntary licensing programme aims to promote high-integrity CAs that can be trusted. A CA wishing to get licensed will have to meet stringent licensing criteria in various aspects, including financial soundness, personnel integrity, strict security controls and procedures. Only CAs that meet the high integrity and security standards set up by the CCA will be licensed. Currently, there is one licensed CA in Singapore, Netrust Pte Ltd.

More information on the ETA, the Regulations and the CA licensing scheme, including the Security Guidelines for CAs, is available at the CCA website at www.cca.gov.sg.

e-ASEAN. The e-ASEAN Task Force is an advisory body to ASEAN, composed of representatives from the public and the private sector from ASEAN member countries such as Brunei, Malaysia, the Philippines, Singapore, and Thailand. Multinational corporations include General Motors, IBM and Sun Microsystems; and educational institutions such as Thailand's Assumption University and the National Library Board of Singapore.

The Certification Authority Forum and the Legal Infrastructure Meeting were both set up under the auspices of e-ASEAN. The Certification Authority Forum studies how policy and legal harmonisation can take place in order to facilitate the recognition of digital signatures amongst the member countries of ASEAN, as well as the business and technical aspects of PKI. The Legal Infrastructure Meeting is working on a legal infrastructure reference framework for the ASEAN countries.

A Novel Trust Service Provider for Internet Based Commerce Applications. We would also like to highlight this research project to the technology innovators in the local infocomm industry. This project is directed at constructing a framework for enhancing trust in Internet Commerce. Experience shows that efficient cryptographic protocols are not enough to guarantee peoples' confidence in Internet Commerce; the transacting parties must also trust each other. Hence, the main ingredient missing in today's E-Commerce infrastructures is modeling and implementing Trust. Several attempts have been made to provide secure and trusted protocols but few have seen any practical use. This paper shows how trust can be provided through a network of Trust Service Providers (TSp). It identifies a set of services that should be offered by a TSp, and also presents a distributed object-oriented implementation of trust services using CORBA, JAVA and XML.

7.1.5 XML Adoption Issues

ICPAS XML-Based Electronic Filing. The adoption of XML in Singapore is growing in strength. One example is the effort by the Institute of Certified Public Accountants of Singapore (ICPAS) to adopt a framework for electronic filing and reporting of business financial information to the public and other mandated disclosure and filing to government agencies. This framework is based on XML as a core technology for web based financial reporting.

XML Industrial Project. Contributing to its momentum are efforts from the local infocomm community to promote and grow XML adoption. For example, the XML Working Group under the Information Exchange Technical Committee launched an XML Industrial Project at the beginning of this year to help SMEs jumpstart using XML. It was co-funded by ITSC, to produce a starter-kit for local organisations, especially SMEs, to help them get up to speed with the practical applications of XML. Another example is the Pilot and Trial Hotspots (PATH) prgram, an IDA initiative, seeks to accelerate the development of innovative infocomm infrastructure, applications, and products by supporting the pilot and trial of emerging infocomm technologies and best-of-breed services. This will include among others, XML web services.

Industry Initiatives. At the industry level, we see active developments. Sun, a member of OASIS, is involved in crafting several JCP initiatives to define standard Java application

programming interfaces in the area of XML security (such as JSR 104, JSR 105, JSR 106). An initiative is a SUN and IDA joint effort in forming a competency centre for smart web services called Java Smart Services Lab (JSSL), which is helping local players as well as international companies to develop web services competencies in manufacturing sector and other areas. Other activites include Microsoft who launched the XML Web Services Centre, SCS and Microsoft who jointly established the Regional RosettaNet XML Services Centre and Software AG who launched the XML Academy.

Scalable XML Access Control System. Technology innovators may be interested in this research project from the Department of Computer Science at NUS called "A Scalable XML Access Control System". This project addresses the design of a scalable XML access control system. The approach is to integrate access control policies designed by the XML community with XML storage mechanisms designed by the database community. The system has the following features. First, it can regulate access control at a fine granularity (e.g., at the tag level). Second, it stores XML documents as tables in relational databases. Third, it is efficient compared to existing systems as it only examines the relevant data. Fourth, it is scalable as it can handle very large XML documents that may not fit into the main memory. Finally, it provides very fast initial response time.

8 Conclusion

In this report, we have focussed on five significant infocomm security technologies that enable e-commerce in the next five years. These technologies are cryptography, smart cards, biometrics, public key infrastructure and XML security. We have outlined our findings pertaining to these technologies in the preceding chapters of this report.

It is equally important, if not more important, to look at market forces, legal support, payment regulations, consumer acceptance and understanding, as well as many other non-technological factors that would ultimately determine the whole success of e-commerce. However, many non-technological factors are difficult to roadmap and could be purely business and consumer decisions that could either accelerate or impede on technology adoption. The best secure technology might not be widely implemented if there is a lack of multiple suppliers, a scarcity of developers, or simply because it is too costly and user-unfriendly. These are moderating factors that would shape the technology roadmap into various branching scenarios, and that we have tried to take into consideration explicitly or implicitly in writing this report. It would be effective for you and your business to also take into account your specific environment and interpret the information in the context of your country of operation.

Collective Trends in the Security Landscape. E-Commerce Security is like a Chinese puzzle formed from an assembly of interlocking parts that need to be looked at both individually and as a whole. We need to be aware of the developments in each constituent security technology as well as have a strategic top-level view of the whole. Thus, we examined the trends and developments and drew out the following encompassing future trends.

End to End Security. Taking a strategic view of security, we see streams of security technologies converging to create standards-based end-to-end security for the emerging global, distributed and heterogeneous networks, such as the Next Generation Internet, mobile, home networks). Today end-to-end is only achievable via proprietary technology in closed environments.

Security Delivered as a Service. Regardless of the issues of privacy and trust raised by corporate customers, several players in the security eco-system are moving towards a service oriented model, be it (technology) certificate verification, (manpower) management and operational services or (expertise) consulting and professional services. Security professional services firms are combining managed security services with incident response planning, vulnerability assessment and forensics consulting. We see the opportunity for Managed Security Service providers to have high growth in this space.

On the technical front, XKMS (W3C XML Key Management Specification) which is based on Web Services standards WSDL and SOAP, is designed to be implemented as a Web service. In Grid Computing, specifications for exposing existing security solutions as services, as well as building new required security functions as services to achieve a level of abstraction that helps provide an integrated, secure Grid environment are being developed (Grid Security Infrastructure). Security services under exploration include authentication services, identity mapping services, virtual organisation policy services, credential conversion services and audit services.

Co-ordination, Convergence and Consolidation. We see this undercurrent in the security landscape, manifested in the emergence of single consoles for the management of security systems and unified security management across distributed and heterogeneous environments.

On the standards front, IETF has released a draft of the protocol called Common Open Policy Service (COPS). A recent article from Information Security magazine envisions COPS as the standard that could allow any management console to talk to any security server or client regardless of device type, brand, OS, application or location, allowing co-ordination across a heterogeneous and distributed security infrastructure.

One architecture from the industry is the Intel's Common Data Security Architecture (CDSA), a security middleware specification that is open source, cross-platform, interoperable, and extensible. CDSA enables "matchmaking" between a variety of different applications and security services allowing co-ordination and transparent plug and play security.

Also emerging is resource provisioning, a key tool in managing behind-the-firewall security that centralizes and manages the process of giving access to distributed web services environments. Gartner predicts that advanced provisioning will develop as authorization, authentication, privilege and identity management tools overlap in 2002 through 2004, and will converge in products and customized solutions for large enterprises in 2004 through 2006.

Specialised Appliances and Devices. As the scope of security expands and as it gains importance, we see an increase in dedicated security devices targeted at specific areas of security. One example is the security appliance. These appliances are standalone specialised devicessuch as SSL appliances and XML firewall appliances. Appliances are usually more secure as it runs its own software as well as faster as it is dedicated to a specific task. SSL Appliances are dedicated devices servicing multiple servers for SSL session establishment and XML appliance firewalls are dedicated devices which go beyond the cursory inspection of traditional firewalls.

Secure public-key–processing devices, also known as hardware security modules (HSMs) are another emerging dedicated device. HSMs are designed to protect the creation, storage, and management of private keys. The speciality of a HSM would be the provision of a safe and trusted environment for cryptographic operations and the protection of cryptographic keys.

Singapore as a World Class Secure E-Commerce Hub. With the help and synergy of the many players and stakeholders in Singapore, and with the support of consumers and businesses, we hope to make Singapore a world class secure e-commerce hub. We hope the highlighted trends and developments will prove useful to the technology innovators in the local Infocomm industry.

3G	Third Generation' Mobile Communications Systems
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
APEC	Asia-Pacific Economic Cooperation
API	Application Programming Interface
APSCA	Asia Pacific Smart Card Association
ASEAN	Association of Southeast Asian Nations
B2B	Business-to-business
B2C	Business-to-consumer
BAPI	Biometric Application Programming Interface (I/O Software)
BioAPI	Biometric Application Programming Interface (BioAPI Consortium)
BXA	Bureau of Export Administration (US)
CA	Certification Authority
CBEFF	Common Biometric Exchange File Format
CCA	Controller of Certification Authorities (Singapore)
CCD	Charge-Coupled Device
CDSA	Common Data Security Architecture
CDSA/HRS	Common Data Security Architecture/Human Recognition Services
CEC	Chip Electronic Commerce
CEPS	Common Electronic Purse Specification
CMOS	Complementary Metal Oxide Semiconductor
CP	Certificate Policy
CPS	Certification Practice Statement
CPU	Central Processing Unit
CRL	Certificate Revocation List
CRT	Certificate Revocation Tree
CSP	Centre for Signal Processing (Singapore)
DARPA	Defense Advanced Research Projects Agency (US)
DES	Data Encryption Standard
DRM	Digital Rights Management
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
eESC	eEurope Smart Cards
EBX	Electronic Book Exchange
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read-Only Memory
EESSI	European Electronic Signature Standardisation Initiative
EMMS	Electronic Media Management System (IBM)
EMV	Europay/MasterCard/Visa

ETA	Electronic Transactions Act (Singapore)
ETSI	European Telecommunications Standards Institute
EU	European Union
FIPS	Federal Information Processing Standard (US)
GGF	Global Grid Forum
GMCIG	Global Mobile Commerce Interoperability Group
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GTA	Global Trust Authority
HA-API	Human Authentication Application Programming Interface
HEPKI-TAG	Higher Education PKI Technical Activities Group
HKMIF	Hong Kong Mobile Certificate Implementation Forum
HSMs	hardware security modules
IDA	Infocomm Development Authority (Singapore)
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPR	Intellectual Property Rights
IPSec	Internet Protocol Security
ISAKMP	Internet Security Association Key Management Protocol
ISO	International Standards Organisation
ITSC	Information Technology Standards Committee (Singapore)
ITSEC	Information Technology Security Evaluation Criteria
ITU	International Telecommunication Union
JINI	Java Intelligent Network Infrastructure
KRDL	Kent Ridge Digital Laboratory (Singapore)
LDAP	Lightweight Directory Access Protocol
MAS	The Monetary Authority of Singapore
MEL	MULTOS Executable Language
MISPC	Minimum Interoperability Specification for PKI Components
MSS	Managed Security Services
MULTOS	Multi-Application Operating System for Smart Cards
NETS	Network for Electronic Transfers (Singapore)
NIST	National Institute of Standards and Technology (US)
OCF	OpenCard Framework
OCSP	Online Certificate Status Protocol
OEBF	Open eBook Forum
OECD	Organisation for Economic Cooperation and Development
OEM	Original Equipment Manufacturer

OGSA	Open Grid Services Architecture
OpenPGP	Open Specification for Pretty Good Privacy
OS	Operating System
PDA	Personal Digital Assistant
PDF	Portable Document Format (Adobe)
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RAM	Random Access Memory
ROM	Read-Only Memory
RSA	Rivest-Shamir-Adleman
SAML	Security Assertion Markup Language
S/MIME	Secure Multipurpose Internet Mail Extensions
SCOS	Smart Card Operating Systems
SCTC	Smart Card Technical Committee (Singapore)
SDMI	Secure Digital Music Initiative
SECG	Standards for Efficient Cryptography Group
SET	Secure Electronic Transaction
SIM	Subscriber Identification Module (GSM)
SMS	Short Message Service (GSM)
SPKI	Simple Public Key Infrastructure
SSL	Secure Socket Layer
SSTC	Security Standards Technical Committee (Singapore)
SVAPI	Speaker Verification Application Programming Interface
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TCPA	Trusted Computing Platform Alliance
TESPAR	Time Encoded Signal Processing and Recognition
TLS	Transport Layer Security
TRIPS	Trade-Related Aspects of Intellectual Property Rights
UMTS	Universal Mobile Telecommunications System
UNCITRAL	United Nations Commission on International Trade Law
USIM	Universal Subscriber Identity Module
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WAP	Wireless Application Protocol
WfSC	Windows for Smart Cards (Microsoft)
WIM	WAP Identity Module

WMF	Windows Media Format (Microsoft)
WML	Wireless Markup Language (WAP)
WTLS	Wireless Transport Layer Security (WAP)
XACML	eXtensible Access Control Markup Language
XENC	W3C XML Encryption Specification
XKMS	XML Key Management Specification
XML	eXtensible Mark-up Language
X-KISS	XML Key Information Service Specification
X-KRSS	XML Key Registration Service Specification
XrML	eXtensible rights Mark-up Language

IDA Technology Roadmap November 2002

Infocomm Security Technologies in E-Commerce

With active contribution from the industry and research community, IDA has launched the *Infocomm Technology Roadmap Release November 2002*. You have either attended the Roadmap Symposium or downloaded a copy of the Technology Roadmap document from our website. Your feedback is valuable to us to better our future services for you. We appreciate if you could spare a few minutes to fill up the following survey.

Please return the completed questionnaire to IDA:
via Fax: **+(65) 6211 2211 (Attention to Ms Saliza Mohd)**
or via Mail to the address on the previous page.

Company Name : _____

Your Name : _____

Designation/
Area of Expertise : _____

Email Address : _____

Contact Number : _____

Q1. With regards to the Roadmap Report Release November 2002 on "Infocomm Security Technologies in E-Commerce", please rate the following on a scale of 1 to 6.

Factors	Excellent					Poor
Usefulness of the roadmap	6	5	4	3	2	1
Completeness of coverage and contents	6	5	4	3	2	1
Ease of understanding	6	5	4	3	2	1
Usefulness of the Roadmap Chart 2002-2007	6	5	4	3	2	1
Relevance to you or to your business strategy/planning	6	5	4	3	2	1

Comments (if any):

_____

_____

_____

Q2. Please indicate the accuracy (in terms of trend & development) of each chapter in the Technology Roadmap Report. Please rate them on a scale of 1 to 6.

Chapter	Accurate			Inaccurate		
Crytography	6	5	4	3	2	1
Smart Card	6	5	4	3	2	1
Biometrics	6	5	4	3	2	1
PKI	6	5	4	3	2	1
XML Security	6	5	4	3	2	1
Singapore Landscape	6	5	4	3	2	1
Roadmap Chart 2002-2007	6	5	4	3	2	1

Comments (if any):

_____

_____

_____

Q3. Do you have any suggestions for improvement on the Technology Roadmap?

_____

_____

_____

Q4. Would you like to be informed of our future Infocomm Technology Roadmap Seminars/Reports?Yes / No

…. Thank You ….

INFOCOMM SECURITY TECHNOLOGIES IN E-COMMERCE ROADMAP 2002 to 2007

		2002		2003	2004	2005	2006	2007
Cryptography	**AES to gain dominance over Triple-DES Standardisation efforts for ECC**	• As 56-bit DES protected messages have already been broken, DES is currently permitted only on legacy systems • New system implementation should at least use the 168-bit Triple-DES algorithm • The US Secretary of Commerce has approved the use of AES as an official govt standard, effective from May 2002 • AES incorporated into FIPS 197 by US government to protect sensitive but unclassified information	**ECC incorporated into following standards:** • ANSI X9.62 – ECDSA • ANSI X9.63 – ECIES, ECDH, ECMQV • FIPS186-2 - ECDSA • IEEE P1363-ECDSA, ECDH, ECMQV • IEEE P1363A - ECIES • IPSEC – ECDSA, ECDH • ISO 14888-3 – ECDSA • ISO 15946 – ECDSA, ECDH, ECMQV	• DES will be phased out from the financial industry group due to advances in computing • AES will not likely replace more than 30% of DES operations before 2004 • ECC will see some application in mobile devices due to its reduced key size than a comparable RSA public key system • Due to advances in computing power, the minimum public key size for RSA should be increased from 1024 to 2048 • With the increase in the key size, it would require a hardware co-cryptoprocessor for comparable performance. Hence, it may not be implementable in some mobile devices due to its hardware constraint	• Secure b2b e-commerce gets increasingly demanding, will further drive DES to end of lifecycle • AES like will not replace more than 50% of all crypto operation while the rest is mainly dominated by Triple-DES • With better algorithm implementation, ECC likely will not replace more than 20% of all encryption uses in mobile devices such as mobile phone, PDA, etc • RSA 768-bit key is expected to be secure until at least year 2004	• AES which is faster and much secure than Triple-DES, likely will not replace more than 50% of most of the crypto-systems • ECC likely will not replace more than 40% of all encryption uses in mobile devices	• ECC expected to be significant in m-commerce security	• DES would be phased out. However, NIST anticipates that the stronger Triple-DES, which utilises 168-bit keys, will still be around till 2007 • NIST will formally re-evaluate AES's role in FIPS
Smart Cards	**Progress to a Single Multi-Application Card a reality as technical capabilities develop**	• Dual Interface for both Contact/contacless cards • Integration with USB Interface • Support DES/3DES/RSA • Support ECC in Java SIM	• Smart card chip memory 64MB • SIM card chip memory 512 32KB • Data link speed 480Mbps • EU releases Global Interoperability Framework for Identification, Authentication and Electronic Signature with Smart Cards	• Support 128/192 bit AES • Support Java SIM 2.2 • The development of flash chips is rapid and SONY announced that its proprietary memory sticks will be available in 512MB and 1GB versions by 2003	• Support 256 bit AES • Support BioAPI • Smart card chip memory 224MB • SIM card chip memory 512 64KB • Data link speed USB2.0 480Mbps	• For High-density high-speed smart cards, a conservative forecast would be that an application could shuttle 1GB of data between different appliances in 17 seconds at a rate of 60Mbps	• Smart card containing biometrics data grow from 12 million issued in 2001 to 260 million cards by 2006. [Frost and Sullivan]	• Services from different industry sectors converge, resulting in one card (e.g. for transit) Smart card chip memory 512MB • SIM card chip memory 128MB
	EMV Migration-Standards for e-payment will boost e-commerce	• UK as World's first EMV migration project • 30 million EMV cards, 300 thousand terminals and 20 thousand ATMs worldwide		• Most ATMs in Europe would be EMV compliant • All new acquiring bank-owned smart card terminals are required to be compliant with industry-wide EMV specifications effective on Jan 2003	• Major EMV migration to be completed for France, Spain, Germany and Italy. With planning underway in Greece and Sweden • Critical mass achieved by end 2004	• The EMV deadline in 2005 will convert Europe into a chip card society		• Visa's goal is to migrate 90% of existing payment cards in Asia Pacific to the EMV global chip standard by 2008

INFOCOMM SECURITY TECHNOLOGIES IN E-COMMERCE ROADMAP 2002 to 2007 (cont'd)

		2002	2003	2004	2005	2006	2007
Biometrics	**Potential for Widespread bionetrics as it expands beyond the niche**	• Biometrics authentication remains niche • Biometrics Application Segmentation in 2002: Physical Access Control 51%, Logical Access Control 40%, Time Attendance 9%, Telecommunication – negligible, Automotive – negligible • On-chip processing integrated with fingerprint sensor emerged (e.g. Atmel) • USA Transportation Security Administration to use biometrics in smart card pilot projects for identification technology of 10 million to 15 million workers	• For price sensitivity, sensor and processing for fingerprint/voice/face biometrics performed by cell phone processor. A competing trend is self-contained biometrics for mobile equipment in next four years • There will be prototype development of low cost biometrics sensors and mobile devices with integrated biometrics capability. Major effort will be in fingerprint biometrics • Emergence of low cost biometrics sensors in mobile devices, majority base on fingerprint	• Fingerprint-based authentication for PC and portables will be largely limited to special cases, with fewer than 5% of new PC procurements requiring integrated biometrics readers through 2004 [Gartner] • Stand-alone biometrics system for physical access and time-and-attendance will be more widely adopted. Prototypes of biometrics for usage control and personalization of machine is expected • Release of ISO/IEC standards for biometrics API and identity verification in smart cards	• Atmel aims towards single chip integration including on-chip analogue to digital conversion and on-chip microprocessor processing for their fingerprint thermal sensor biometrics. Fingerprint technology should mature. • Expected surge in demand for biometrics products between 2000 and 2005 for PC peripherals, etc. [Frost and Sullivan] Services and applications supporting biometrics are expected to increase, especially in payment related e-commerce. • Release of ISO/IEC standards for biometrics in travel document • Availability of integrated smart card with fingerprint sensor	• Biometrics Application Segmentation in 2006: Physical Access Control 24%, Logical Access Control 11%, Time Attendance 5%, Telecommunication 56%, Automotive 4% [IBIA] • Sales of devices that authenticate identity based on physical characteristics are projected to climb from US$132m in 2002 to US$550m in 2006 [Yankee Group]	• Privacy issues arise against biometrics. Government legislation regarding identity protection likely. • Iris Recognition expected to be 2nd largest technology in terms of revenues (2007?) • Major biometrics for telecommunication would be fingerprint, face, voice and signature (2007?)
PKI	**Trust Services for e-commerce**	• Emerging trend of enterprise PKI service outsourcing • Growing deployment of Community Identity Management such as Identrus, TrustAct, SWIFT and bolero.net	• For PKI Software Products, slow growth in 2002, but the massive force of e-commerce will continue to push the market to US$586.3m by 2003 [Gartner] • By 2003, support for the creation and audited storage of digitally signed records, digital receipts for payment transactions and secure time stamping, will be enabled within applications. Dispute-resolution processes that enable businesses to examine the secure record store as required will be enacted [META Group]	• 50% of all large businesses to have major PKI projects for authentication beyond passwords and encryption [META Group] • Completion of XKMS specifications and emergence of XKMS interoperation solutions	• Trend of PKI outsourcing will drive the growth of managed services, with the market growing from US$720m in 2000 to an estimated US$2.2b by 2005 [IDC] • Deployment of wireless PKI following 3G networks rollout	• Global investment in PKI products and services is set to grow from US$436m in 2000 to US$3.4b by 2006. Shift to outsourced PKI services form 60% all revenues in 2006. Growth driven by demand for encryption and authentication services from mobile operators. Mobile services grow from 1% of all PKI revenues in 2000 to 43% by 2006 [Datamonitor]	
XML Security	**End to End Security for Web Services**	• WS-Security Specification released by IBM & Microsoft; Spec submitted to OASIS for approval as standard • Initial implementation of WS-Security Specification emerged (e.g. IBM WebSphere Application Server) • Initial implementation of Liberty Alliance Specification emerged (e.g. Sun Identity Server)	• WS-security interoperability with SAML • Written specifications expected for WS-Policy, WS-Trust, WS-Privacy, WS-Secure Conversation, WS-Federation, WS-Authorization • Advanced Federated capabilities such as trust brokering with external trust providers and corporate single sign-on appear in products (e.g. IBM Access Manager, Microsoft Trustbridge) • Liberty version 2.0 specifications released	• OASIS to drive development of a unified set of security standards for Web Services from the various overlapping standards • XML firewalls would not become mainstream until 2003 or 2004 [Forrester]	• Grid and autonomic computing generation of web services on a Grid Security Specification expected to appear in 2005 • MSSP (Managed Security Service Provider) market expected to grow from US$140m in 1999 to US$2.6b by 2005 [Yankee Group]	• Inconsistent and overlapping standards in web services and security expected to still be an issue in 2006	• By 2007, Web services core standards, UDDI, will be firmly entrenched, although large-scale, public UDDI registries will still be few, given continuing concerns about security and a dearth of commercially available Web services [Gartner]