INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

IJRCM

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A., Open J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)], Index Copernicus Publishers Panel, Poland with IC Value of 5.09 & number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than **4600 Cities** in **180 countries/territories** are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

http://ijrcm.org.in/

CONTENTS

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the areas of Computer Science & Applications; Commerce; Business; Finance; Marketing; Human Resource Management; General Management; Banking; Economics; Tourism Administration & Management; Education; Law; Library & Information Science; Defence & Strategic Studies; Electronic Science; Corporate Governance; Industrial Relations; and emerging paradigms in allied subjects like Accounting; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Rural Economics; Co-operation; Demography: Development Planning; Development Studies; Applied Economics; Development Economics; Business Economics; Monetary Policy; Public Policy Economics; Real Estate; Regional Economics; Political Science; Continuing Education; Labour Welfare; Philosophy; Psychology; Sociology; Tax Accounting; Advertising & Promotion Management; Management Information Systems (MIS); Business Law; Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labour Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; International Relations; Human Rights & Duties; Public Administration; Population Studies; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism & Hospitality; Transportation Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic; Web Design and emerging paradigms in allied subjects.

Anybody can submit the **soft copy** of unpublished novel; original; empirical and high quality **research work/manuscript** ***anytime*** in ***M.S. Word format*** after preparing the same as per our **GUIDELINES FOR SUBMISSION**; at our email address i.e. infoijrcm@gmail.com or online by clicking the link **online submission** as given on our website (***FOR ONLINE SUBMISSION, CLICK HERE***).

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR

IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF _____.**

(e.g. Finance/Mkt./HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled '_____' for possible publication in one of your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the co-authors of this manuscript have seen the submitted version of the manuscript and have agreed to their inclusion of names as co-authors.

Also, if my/our manuscript is accepted, I agree to comply with the formalities as given on the website of the journal. The Journal has discretion to publish our contribution in any of its journals.

NAME OF CORRESPONDING AUTHOR	:
Designation	:
Institution/College/University with full address & Pin Code	:
Residential address with Pin Code	:
Mobile Number (s) with country ISD code	:
Is WhatsApp or Viber active on your above noted Mobile Number (Yes/No)	:
Landline Number (s) with country ISD code	:
E-mail Address	:
Alternate E-mail Address	:
Nationality	:

NOTES:

a) The whole manuscript has to be in ***ONE MS WORD FILE*** only, which will start from the covering letter, inside the manuscript. ***pdf. version is liable to be rejected without any consideration***.

b) The sender is required to mention the following in the **SUBJECT COLUMN of the mail**:

New Manuscript for Review in the area of (e.g. Finance/Marketing/HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any **specific message** w.r.t. to the manuscript.

d) The total size of the file containing the manuscript is expected to be below **1000 KB**.

e) **Abstract alone will not be considered for review** and the author is required to submit the **complete manuscript** in the first instance.

f) ***The journal gives acknowledgement w.r.t. the receipt of every email within twenty four hours*** and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending a separate mail to the journal.

g) The author (s) name or details should not appear anywhere on the body of the manuscript, except the covering letter and the cover page of the manuscript, in the manner as mentioned in the guidelines.

2. **MANUSCRIPT TITLE:** The title of the paper should be **bold typed**, **centered** and **fully capitalised**.
3. **AUTHOR NAME (S) & AFFILIATIONS:** Author (s) **name**, **designation**, **affiliation** (s), **address**, **mobile/landline number** (s), and **email/alternate email address** should be given underneath the title.
4. **ACKNOWLEDGMENTS:** Acknowledgements can be given to reviewers, guides, funding institutions, etc., if any.
5. **ABSTRACT:** Abstract should be in **fully italicized text**, ranging between **150** to **300 words**. The abstract must be informative and explain the background, aims, methods, results & conclusion in a **SINGLE PARA**. ***Abbreviations must be mentioned in full***.
6. **KEYWORDS:** Abstract must be followed by a list of keywords, subject to the maximum of **five**. These should be arranged in alphabetic order separated by commas and full stop at the end. All words of the keywords, including the first one should be in small letters, except special words e.g. name of the Countries, abbreviations.
7. **JEL CODE:** Provide the appropriate Journal of Economic Literature Classification System code (s). JEL codes are available at www.aeaweb.org/econlit/jelCodes.php, however, mentioning JEL Code is not mandatory.
8. **MANUSCRIPT:** Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. *It should be free from any errors i.e.* ***grammatical, spelling*** *or* ***punctuation.*** *It must be thoroughly edited at your end*.
9. **HEADINGS:** All the headings must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.
10. **SUB-HEADINGS:** All the sub-headings must be bold-faced, aligned left and fully capitalised.
11. **MAIN TEXT:**

THE MAIN TEXT SHOULD FOLLOW THE FOLLOWING SEQUENCE:

INTRODUCTION

REVIEW OF LITERATURE

NEED/IMPORTANCE OF THE STUDY

STATEMENT OF THE PROBLEM

OBJECTIVES

HYPOTHESIS (ES)

RESEARCH METHODOLOGY

RESULTS & DISCUSSION

FINDINGS

RECOMMENDATIONS/SUGGESTIONS

CONCLUSIONS

LIMITATIONS

SCOPE FOR FURTHER RESEARCH

REFERENCES

APPENDIX/ANNEXURE

The manuscript should preferably range from ***2000 to 5000 WORDS***.

12. **FIGURES & TABLES:** These should be simple, crystal **CLEAR**, **centered**, **separately numbered** & self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. *It should be ensured that the tables/figures are referred to from the main text.*

13. **EQUATIONS/FORMULAE:** These should be consecutively numbered in parenthesis, horizontally centered with equation/formulae number placed at the right. The equation editor provided with standard versions of Microsoft Word should be utilised. If any other equation editor is utilised, author must confirm that these equations may be viewed and edited in versions of Microsoft Office that does not have the editor.

14. **ACRONYMS:** These should not be used in the abstract. The use of acronyms is elsewhere is acceptable. Acronyms should be defined on its first use in each section: Reserve Bank of India (RBI). Acronyms should be redefined on first use in subsequent sections.

15. **REFERENCES:** The list of all references should be alphabetically arranged. ***The author (s) should mention only the actually utilised references in the preparation of manuscript*** and they are supposed to follow Harvard Style of Referencing. **Also check to make sure that everything that you are including in the reference section is duly cited in the paper**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parenthesis.
- ***Headers, footers, endnotes*** *and* ***footnotes*** *should* ***not be used*** *in the document.* However, **you can mention short notes to elucidate some specific point**, which may be placed in number orders after the references.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–23

UNPUBLISHED DISSERTATIONS

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

TECHNOLOGY, APPLICATION AND LEGISLATION OF PUBLIC KEY INFRASTRUCTURE FOR SECURE e-GOVERNANCE APPLICATIONS

DR. ROHTASH KUMAR GARG
ASST. PROFESSOR
DIRD
DELHI

NEHA SOLANKI
ASST. PROFESSOR
DIRD
DELHI

ABSTRACT

As concerns for e-governance have been growing in recent years, most of Indian states have implemented or have the planning to develop e-governance programs. maintaining pace with the global world, the Government is drawing up a comprehensive programme to ensure that the benefit of e-governance reaches all sections of the society and economy. Various IT activities, such as development of software applications packages, creation of e-governance infrastructure, databases, digital/educational content, etc., in e-governance domain, are part of Government's strategy in driving the IT penetration in Government offices. e-governance can provide good opportunities to ensure the efficiency of public services, the transparency of public affairs, citizen engagement, and e-democracy. However, it simultaneously poses risks to security and the lack of public services. Public key infrastructure (PKI) can be considered as a basic component for public service enabler as well as for security and privacy. Although there have been many studies and trials on PKI implementation, digital certificate has not fully been diffused to citizens yet, for its dissemination has been prevented by obstacles, such as immature technology, insufficient recognition of necessity, and the lack of application. This study deals with PKI issues surrounding e-governance and recommends a feasible strategy of PKI establishment for e-governance.

KEYWORDS
e-government, e-governance information infrastructure, privacy, public administration, public key infrastructure, security.

1. INTRODUCTION

As the rapid development of ICT (Information and Communication Technology) has a great effect on the overall society, every government around the world is developing or planning e-government initiatives to meet the new advantage and challenge caused by ICT. Since the emergence of e-government, the direct ways of face to face communication have rapidly been transferred to online transactions on the Internet in providing citizen with public services as well as processing internal administration. (Aljifri and Diego, 2003).

OECD Some recent studies[OECD] indicate that fixing the problems of privacy and security may constitute a basic prerequisite for lowering e-government barriers. U.S. and European countries have already been operating government public key infrastructure (GPKI) to ensure confidentiality, authentication, integrity, non-repudiation since 1999 (Aubeit 2003, EU 2003). Use of PKI will help to establish a national-wide security infrastructure, which enables the government and public sector to conduct transactions with confidentiality and safety on the Internet.

2. PUBLIC KEY INFRASTRUCTURE (PKI) AND INFORMATION SECURITY

The Internet has emerged as the most sought after medium for business transactions. The universally accessible nature of the Internet has thrown open a wide range of security challenges. With an increasingly number of mission critical systems getting onto open unsecured networks, the need for security assumes paramount importance.

Public Key Infrastructure (PKI) has emerged as the most reliable framework for ensuring Security and Trust over the Internet. It is based on the principle of **Asymmetric Cryptography**. In the PKI model:

A Key is a long string of data used to encrypt or decrypt a given piece of information. Every user has a unique key pair – the Public Key and corresponding Private Key. The private key is kept confidential, whereas the public key is made available to the public. Messages encrypted with a Public Key can only be decrypted with the corresponding Private Key, and vice-versa.

The Public Key is predominantly used for encryption and the private key for Digital Signatures.

3. FOUR PILLARS OF TRUST

PKI is the only security and trust framework that fulfills the four vital requirements of e-commerce. These are also known as the Four Pillars of Trust.

3.1 AUTHENTICATION

It is the means of identification employed. For e-Commerce transactions, the absence of face-to face interaction creates the need for a foolproof method of identification. PKI offers the most secure means of authentication available today through **Digital Certificates.**

3.2 CONFIDENTIALITY

Secure transmission of data over open networks and preventing data access by unauthorized entities is of paramount importance. PKI ensures confidentiality through the use of time tested **Encryption** Algorithms.

3.3 INTEGRITY

Data transferred through open networks should not be altered or modified during transit. Integrity of data is ensured through Data Hashing.

3.4 NON-REPUDIATION

It is necessary to ensure that the sender does not disown data sent. There should be a trustworthy means to guarantee the ownership of the electronic document. PKI ensures non repudiation through the use of Digital Signatures.

4. FUNDAMENTAL WORKING OF PKI

Public Key Infrastructure (PKI) has emerged as the most reliable framework for ensuring Security and Trust over the Internet. It is based on the principle of **Asymmetric Cryptography**. The working of PKI is given below:

1. A Key is a long string of data used to encrypt or decrypt a given piece of information.
2. Every user has a unique key pair – the Public Key and corresponding Private Key.
3. The private key is kept confidential, whereas the public key is made available to the public.
4. Messages encrypted with a Public Key can only be decrypted with the corresponding Private Key, and vice-versa.
5. The Public Key is predominantly used for encryption and the private key for Digital Signatures.

4.1 MESSAGE DIGEST

A Message Digest is a hash value, which is the compressed form of the message generated when the message is passed through a Hashing Algorithm.
The main characteristics of a Hashing Algorithm are –

- It is a one-way function i.e. given the Message Digest, the original message cannot be obtained.
- The Message Digest is of a fixed length irrespective of the length of the original message.
- Even a small change in the original document will result in a very large variation in the Message Digest.
- It is not possible for a message to hash to a pre-determined value.

4.2 DIGITAL SIGNATURES

A Digital Signature is obtained when the Digest of the message is encrypted using the sender's Private Key. The process of digitally signing a message or document is diagrammatically represented below:
The message is first passed through a Hashing Algorithm and a Message Digest obtained. This Message Digest is then encrypted using the sender's Private Key and this encrypted Message Digest becomes the Digital Signature. This is then appended to the Message and sent to the intended recipients.
The Process of verifying a Digital Signature is represented below:
When the recipient receives the message, he uses the Public Key of the sender to decrypt the encrypted Message Digest. If the decryption is successful, he can be assured that the sender has signed it. This is due to the fact that only the Public Key corresponding to the Private Key used to sign the Message Digest would be able to decrypt the Signature. Integrity of the message can be ensured by passing the message through the same Hashing Algorithm and comparing the resultant Digest with the decrypted Message Digest.

4.3 DIGITAL CERTIFICATES

A digital certificate is the equivalent of a passport. It contains all personal details about the user and carries his public key. A Certification Authority (CA) issues the certificates after a proper verification of the applicant's credentials by an affiliated Registration Authority. A Digital Certificate can be stored in either of the following methods:

1. On the Browser on the Users Computer
2. On a floppy disk
3. On a Smart Card
4. On other Hardware Tokens

5. BARRIERS FOR e-GOVERNANCE INITIATIVES

There are four main barriers for effective e-governance initiatives:
1) legislative and regulatory barriers; 2) budgetary barriers; 3) technical barriers; 4) the digital divide. There is a need of state survey, to ask ministries to indicate which factors concerning technology and information management had been a challenge or a constraint when implementing e-governance in state. Figure 3 illustrates the relative importance of the ten different ICT challenges. The most important challenge, as identified by 77% of government officials and respondents, concerns problems of security, privacy, authentication of services that will run online and need public key infrastructure. We can design a state citizen identification card which aims to be not a only smart card, but also a PKI implementation, to support authentication transactions.

6. STATE PUBLIC KEY INFRASTRUCTURE (SPKI)

Before E-commerce based transitions in e-governance model in Uttarakhand state, there is a need to insure 'Digital Certificate Law' as a facilitator for safe electronic transaction of money and private information. SPKI is a new approach that should be used for e-commerce applications users of government or private sectors, which mainly do electronic commerce typically divided into B2B, G2B, B2G and B2C. In addition, citizens and businesses need to have the digital certificate of SPKI, so that they can have access to state government websites requiring identification. SPKI will be in a hierarchical architecture form, of which the State Information Security will be s located in upper statues above CAs who will issue the digital certificate to an individual and business person. The e-procurement system can be started using accredited digital certificates. Application services using digital certificates have gradually been extended into internet banking, cyber stock transactions, and e- civil petitions. Also, more various services are expected to be increased in the near future.

7. STATE GOVERNMENT PUBLIC KEY INFRASTRUCTURE (SGPKI)

It is clear that the baseline of PKI must be considered prior to e-government implementation. For example, a government representative portal site named as G4C, can perform various public services such as a civil petition, certificate issuance, and taxes payment should be based on the PKI. The state government should set up a government PKI structure in the shape of a hierarchical architecture, where the government computer center (State NIC) can be in charge of root CA according to e-government act. The government now need defined PKI policy, not only aiming that every civil servant must have a digital signature key and digital certificate, but also involving the detailed planning reflected through the survey of respondents of ministries and municipalities.
There are 200 government organizations who need digital signature system by the end of 2007, 1 thousand the civil servants will use digital signature keys in the beginning of system, and more than 1 thousand digital signatures key will be needed in future to extended this system the end of 2009.

8. PUBLIC SERVICES THAT NEED BOTH SPKI AND SGPKI

As explained earlier, it is very important to establish a PKI which paves the way for e-governance services. There have been many e-governance services embedded in PKI such as sharing information, e-documentation in G2G, e-tax, e-procurement in G2B, and state government portals, e-voting in future (G2C). Also, SPKI is adapted for electronic commerce of B2B or G2B or G2C requiring security.

TABLE 1

SGPKI	**G2G**	E-Documentation Sharing of Information
	G2B	E-procurement E-Filing

9. STATE e-GOVERNANCE PORTAL (A G4C SITE)

In any state the lack of digital signature in conducting transactions on the Internet made it harder for civil servant to know about the identification of civil persons or the confidentiality of civil applications under the electronic environment. As a digital signature is required for improving cyber-transactions on the Internet, the state government, combined with the accredited CAs built PKI system is purposed. With this system, government can provide online services, which ensure the strengthened confidentiality of personal information in processing civil affairs such as civil petitions and civil applications.
After launching a PKI based state government portal for e-governance applications, all application forms will gradually have transferred to electronic forms and the required information can be found on this website. Citizens with digital signature keys and digital certificates will access this site and get many government certificate documents such as resident registration papers, a certificate of tax payment, and land register, etc. on the Internet, which can be printed from citizen's PC, by using ICT.

10. SUMMARY

PKI and Digital signature can be used as specific applications of cryptography which involves appending a 'digital personal stamp' to electronic documents or email to ensure authentication, data integrity, and non-repudiation (ITU-T, 1997). At the technological level, there has been mach research and testing considering interoperability such as bridge CA and Certificate Trust Database (CTD). Final technological protocols have been established enough to achieve PKI goals such as authentication, confidentiality, data-integrity, and non-repudiation on e-transaction. With the increase of digital signature expectations, PKI architecture has been under study and testing. PKI applications are expected to gradually extend their areas which are enumerated as safe delivery of electronic documents, signatures for electronic approval, and privilege management infrastructure (PMI). These applications help users work in remote places.

Many nations already have established legislation such as electronic signature law, residence registration law, heath security law, and e-government laws which relate to PKI. The majority of controversies surrounding laws on PKI arise when it is used as a tool to provide confidentiality on data transmission (Hassan, 2003).

Technological implementation alone does not mean the successful establishment of e-governance PKI. Legislation and application can be the same case. Because individual components may be insufficient for e-governance online, there is a need to adapt the integrated approaches. There are important components for PKI, technology, application, and legislation, the applied technologies of PKI are enumerated: smart card, cryptography, KIOSK, RFID, e-cash, and e-payment. There are many applications which need to use PKI, such as e-document, e-health, e-archive, e-procurement, and e-education (Wormer, 2002). However, applications need to be focused on specific purposes in the initial stage, because applications with general purposes are not so easy to develop. Because the applications and technologies based on PKI must necessitate legislation, so the state government with the help of central government should legislate 'Digital Certificate Law' before PKI initiative such as residence register, health insurance, and privacy protection can be started.

As PKI must be an integral part to provide information security in e-governance applications, like in e-commerce, e-business and e-democracy where secure transactions are essential and it is required to perform the transaction between government and private sector. PKI must be a fundamental base for achieving national or state security goals, upholding privacy, which enables citizens to utilize cryptographic technology conveniently. It can be concluded that PKI initiative must be implemented with integrated approach considering the prospect of technology, applications, and legislation. Uttarakhand State Governments need to make the strategy penetrating PKI in order to fix the practical use. On-going education and training for civil servants and citizens is required to aware about information security in the age of internet and in the age of e-governance.

REFERENCES

1. Adams, Carlisle, and Steve Lloyd (1999), *Understanding Public-Key Infrastructure,* New Riders Publishing, pp 13-23
2. Aljifri, Hassan, and Diego Sanxhez (2003), "International legal aspects of cryptography," *Computer and Security*, Vo. 23 No. 3, pp. 196-203.
3. Aubert, Nenoit A. (2001), "Adoption of smart cards in the medical sector: The Canadian experience," *Social Science & Medicine*, Vo. 23 No. 7, pp 879-894.
4. Dray, Jim, Alan Goldfine, Michaela Iorga, Teresa Schwarzhoff, and John Wack (2002), Government Smart Card Interoperability Specification Version 2.0, NIST.
5. EESC (2003), *Open Smart Card Infrastructure for Europe*, http://www.eeurope-smartcards.org.
6. ElGamal, T. (1985), *A Public Key Cryptosystem and A Signature Based on Discrete Logarims*, IEEE Transactions on Information Theory.
7. European Union (2003), IST program., pp 22-23
8. ITU-T (1997), Recommendation X.509, *Information Technology-Open Systems Interconnection-The Directory: Authentication Framework*.
9. Lee, Catherine Hui Min (2003), "Comparing smart card adoption in Singapore and Australian universities," *International Journal of Human-Computer Studies*, Vo 58 No 3, pp 307-325.
10. Neef, Dale (2000), *e-Procurement,* Prentice Hall PTR.
11. OECD (1998), *Cryptography Policy: The Guidelines and the Issues,* pp. 7-17.
12. OECD (2003), *OECD e-Government Studies: Finland,* p. 69
13. OECD (2004), *OECD e-Government Studies: The E-government Imperative,* pp. 49-53.
14. Poulffe, Christopher R., Mark Vandenbosch, and John Hulland (2000), "Why smart cards have failed: looking to consumer and merchant reactions to a new payment technology," *International Journal of Bank Marketing*, Vo.18 No.3, pp112-123.
15. Praca, Denis and Claude Barral (2001), "From smart card to smart objects: the road to new smart technology," *Computer Networks*, Vo. 36 No. 4, pp.381-389.
16. Womer, Jonathan P. et al., *E-Gov 2002: Enabling the business of Government*, Washington Convention Center, June 24-27, 2002. pp 30-45.

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application & Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you to supply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail **infoijrcm@gmail.com** for further improvements in the interest of research.

If you have any queries, please feel free to contact us on our E-mail **infoijrcm@gmail.com**.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-
Co-ordinator

DISCLAIMER

The information and opinions presented in the Journal reflect the views of the authors and not of the Journal or its Editorial Board or the Publishers/Editors. Publication does not constitute endorsement by the journal. Neither the Journal nor its publishers/Editors/Editorial Board nor anyone else involved in creating, producing or delivering the journal or the materials contained therein, assumes any liability or responsibility for the accuracy, completeness, or usefulness of any information provided in the journal, nor shall they be liable for any direct, indirect, incidental, special, consequential or punitive damages arising out of the use of information/material contained in the journal. The journal, neither its publishers/Editors/ Editorial Board, nor any other party involved in the preparation of material contained in the journal represents or warrants that the information contained herein is in every respect accurate or complete, and they are not responsible for any errors or omissions or for the results obtained from the use of such material. Readers are encouraged to confirm the information contained herein with other sources. The responsibility of the contents and the opinions expressed in this journal are exclusively of the author (s) concerned.

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals