

# **Seminar Report Guidelines**

**Department of CSE, School of Engineering  
Sir Padampat Singhania University, Udaipur**

Version 1.1  
Prepared by: Ajay Prasad  
Date: 20/12/2009

# Contents

**Paper size and margins**

**Text/Fonts**

**Diagrams/Images/tables**

**Submitted Copies**

**Report format**

**Mainpage format**

**Certificates**

**Guide format**

**Completion format**

**Acknowledgement format**

**Abstract**

**Contents format**

**Chapters format**

**Appendix format**

**References format**

Version 1.1

Prepared by: Ajay Prasad

Date: 20/12/2009

## **Paper size and margins**

Pages should be printed on one side only.

### **Paper size:**

The paper size should strictly be A4 i.e 8.27 X 11.69 inches.

### **Margins:**

Margins must be:      left: 1.25”  
                                    Right: 1”  
                                    Top: 1”  
                                    Bottom: 1”

### **Headers and footers:**

The report pages should contain header and footers only with the chapters

## **Texts/Fonts**

**Font:** All text in Times New Roman, aligned in justify.

The paragraph line spacing should be 1.5 lines

### **Style and Font sizes**

<b>place</b>	<b>Style</b>	<b>Size</b>
Main section heading	Bold	14pt
Sub section heading	Bold	12pt
Sub-sub section heading	Bold and italics	12pt
Figures and table titles	normal	10pt
Chapter Title	bold	16pt
Chapter contents	Bold + italics	14pt
In between text (for emphasizing)	Normal + italics	12pt
All other text	normal	12pt

## **Diagrams/Images/Tables**

1. All Diagrams/Images/Tables should be clear, electronically drawn and should be having good resolution.

Version 1.1

Prepared by: Ajay Prasad

Date: 20/12/2009

2. Single Diagrams/Images/Tables should not be more than the available page size (within margins).
3. Diagrams/Images/Tables should be aligned centrally to the page.
4. Diagrams/Images/Tables titles should be also aligned centrally to the page.

### **Submitted Copies**

1. 4 hard copies of report (1 Library, 1 Department, 1 Guide, 1 self) to be submitted in spiral bind form.
2. 1 soft copy of presentation and report to be submitted in a CD.

### **Report format**

The report should have following structure/sequence:

Main page  
Certificates  
Acknowledgement  
Abstract  
Contents  
Chapters  
Appendix  
References

**Main page format:** given as in appendix 1.

### **Certificates**

1. *Guide format:* to be certified by guide: given as in appendix 2
2. *Completion format:* to be certified by HOD and evaluator: given as in appendix 3

**Acknowledgement format:** As per student ( text and font guidelines to be followed)

### **Abstract format:**

1. Not more than 300 words.
2. Precise, concise and duly approved by the guide.
3. Text and font guidelines to be followed.

**Content's format:** (as shown in the appendix 4)

1. Chapter's title and its sub section title (no sub-sub sections or more) should be there.
2. All chapters must be numbered, All sections must be numbered.
3. Page numbers of each chapter and sub sections must be kept in contents.
4. Text and font guidelines to be followed.

**Chapter's format:** (as shown in the appendix 5)

Version 1.1

Prepared by: Ajay Prasad

Date: 20/12/2009

1. Every chapter must have a title, the sub-sections must be listed in the beginning of the chapter. every sub section must be numbered.
2. Every numbering should be in numeric. For example chapter 2, section 1 should be numbered as 2.1.
3. The first and last chapter of every seminar report must be *Introduction* and *Conclusion* respectively
4. Text and font guidelines to be followed.
5. Number of chapters should not exceed 6.

### **Appendix format:**

Appendix should not be numbered as chapters. Appendix should be numbered only in Roman. The title of appendix should be appropriate and the contents must be specific. The necessity of the appendix must be explained to the respective guide. Every appendix must have proper explanations of usage and should contain the source from where its derived. (text and font guidelines to be followed)

### **References:**

1. References should be cited clearly in the text wherever required with square brackets containing reference number. (For example[12] says that the preceding text has relevance with support from the cite mentioned in reference number 12).
2. Not more than 12 and not less than 5 references are allowed. In case of any deference from the stipulated range one must get the approval of concerned guide and HOD.
3. Website and web pages reference format:  
Title, full url  
Example: 1. Grid security infrastructure  
<http://www.globus.org/security/overview.html>
4. Books reference  
Author(s), Title, Publication, Edition, Year  
Example: 2. Stallings W., Data and Computer Communications, Prentice-Hall of India, 5th Ed., 2003.
5. Research paper reference.  
Author(s), title, journal/ workshop etc, (*volume( issue):pages*), month year  
Example: 3. K. M. Chandy and L. Lamport. Distributed snapshots: Determining global states of distributed systems. ACM Transactions on Computer Systems, (3/1):63–75), Feb. 1985.  
All other references must be approved by the concerned guide.

Version 1.1

Prepared by: Ajay Prasad

Date: 20/12/2009

**APPENDIX-1: Main page format**

A  
Seminar Report  
On  
“Title of Seminar”

Submitted in partial fulfillment of the requirement  
For the award of the  
Degree of  
Bachelor of Technology  
In  
Computer Science  
(Sir Padampat Singhania University)

Under the supervision of  
**Name of Guide**

Submitted by  
**Student Name**



Department of Computer Science and Engineering  
**SIR PADAMPAT SINGHANIA UNIVERSITY**  
**UDAIPUR**

## APPENDIX-2: Certificate from Guide



Department of Computer Science and Engineering  
**SIR PADAMPAT SINGHANIA UNIVERSITY**  
UDAIPUR

---

### CERTIFICATE

This is to certify that Mr/Ms.  
.....a student of  
B.Tech.(Computer Science and Engineering) ..... semester has  
submitted His/her Seminar entitled  
“.....” under my/our  
guidance.

**Guide**

## APPENDIX-3: Certificate of Completion



Department of Computer Science and Engineering  
**SIR PADAMPAT SINGHANIA UNIVERSITY**  
UDAIPUR

---

### CERTIFICATE OF COMPLETION

This is to certify that Mr/Ms.  
.....a student of  
B.Tech.(Computer Science and Engineering) ..... semester has  
Presented and have successfully completed His/her Seminar  
entitled “.....” in presence  
of the undersigned dignitaries.

**HOD**

**External Evaluator(s)**

# APPENDIX-4: Contents

## Contents

<b>1. Introduction</b>	<b>1</b>
1.1 Basic Concepts of security	1
1.2 E-Commerce and Electronic Transactions	2
1.3 Security requirements in Electronic transactions.	3
<b>2. Technologies Used</b>	<b>4</b>
2.1 DES-symmetric key cryptography	4
2.2 Hashing	5
2.3 MD5	5
2.4 HMAC.	6
2.5 Public Key Cryptography and message authentication.	7
2.6 RSA	8
2.7 Digital Signatures.	9
2.8 Digital Certificates.	12
2.9 X.509v3 Authentication and Certificate Authority.	12
<b>3. SET protocol</b>	<b>14</b>
3.1 SET protocol.	14
3.2 Dual Signature.	15
3.3 SET supported transactions.	16
3.4 Where does SET stand?	17
<b>4. Implementation</b>	<b>18</b>
4.1 Issues	18
4.2 Major Modules	19
4.3 Client server actions.	20
4.3.1 Transactions	21
4.3.2 Registration	22
<b>5. Inputs output</b>	<b>23</b>
<b>6. Conclusion</b>	<b>25</b>

### INTRODUCTION

Basic Concepts of security E-Commerce and Electronic Transactions Security requirements in Electronic transactions.
---

#### 1.1 Basic Concepts of Security

The Security is becoming the most important issue in today's scene of day to day computing. With the advent of internet every aspect of human day to day activities are getting into online frameworks. The issue of mass approval and acceptance of the online activities are mostly dependent on security aspects. Sooner or later fool proof security features have to be put forward so as to convince the users.

Security is seen on the perspective of security goals. confidentiality: confirms that no part of the message or online activity is revealed in any case. Integrity: confirms error free delivery with assurance. Availability: Assures user of getting what they deserve to get. One more issue which is only possible when all the three are present that is Authenticity.

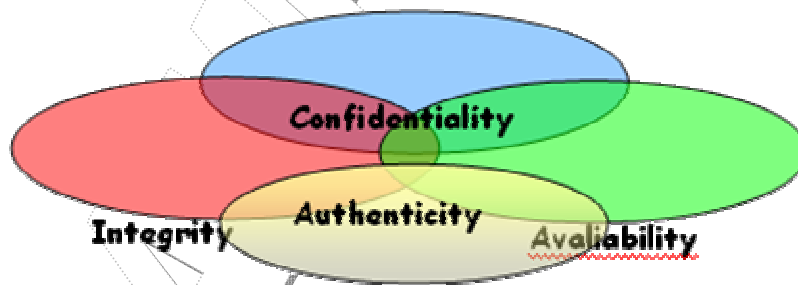


Figure1: Security Goals

To get clean on the security goals one must need to understand in what ways and at what places we need to ponder into for security. Study of security attacks tells us where and what to ponder.

#### Security Attacks

Version 1.1

Prepared by: Ajay Prasad

Date: 20/12/2009

## APPENDIX-5: Sample Chapter

1. **Interruption:** This is an attack on availability
2. **Interception:** This is an attack on confidentiality
3. **Modification:** This is an attack on integrity
4. **Fabrication:** This is an attack on authenticity

Once we have seen where to go we can now demand some security services from our providers.

### Security Services

1. Confidentiality (privacy)
2. Authentication (who created or sent the data)
3. Integrity (has not been altered)
4. Non-repudiation (the order is final)
5. Access control (prevent misuse of resources)
6. Availability (permanence, non-erasure)

The technical aspects as to how we can achieve the services are discussed in the preceding section. But in short, the technologies and science in security mostly revolves around

1. Cryptography.
2. Digital Signatures.

### 1.2 E-Commerce and Electronic Transactions

Electronic Commerce (e-commerce) can be highly beneficial in reducing business costs and in creating opportunities for new, simple and improved customer services. Attempting to define e-commerce we can suppose that is the operation of maintaining business transactions (exchange of value) with the use of telecommunication networks Reference [6] divide e-commerce into three classes:

1. Electronic Fund Transfer (EFT): the methods or the systems of paying electronically, transferring money or funds electronically and exchange digital information by means of electronic payments.

Version 1.1

Prepared by: Ajay Prasad

Date: 20/12/2009

## **APPENDIX-5: Sample Chapter**

2. Electronic Commercial Information Transfer System: the system that exchange commercial information digitally.
3. Electronic Marketplace: the domains on the Internet where the expectant buyer can seek and purchase goods and services.

E-commerce can be differentiated in:

1. Business-to-business transactions
2. Consumer-to-business transactions.

The transaction of e-commerce process can be visualized as a cycle of four phases:

1. Negotiation (conditions of satisfaction)
2. Request (request of providence)
3. Performance (fulfilment and notification of realization process)
4. Settlement (acceptation and payment)

### **Electronic Payment**

“Electronic payment” or “e-payment” is the transfer of electronic means of payment from the payer to the payee through the use of an electronic payment instrument. An “electronic mean of payment” would be defined as a mean of payment that is represented and

Next, the time when the monetary value is actually taken from the payer attributes e-payments into

1. Pre-paid systems – customer’s account debited before payment
2. Pay-now systems – customer’s account debited at the time of payment
3. Post-pay systems – merchant’s account credited before customer’s account is debited transferable in electronic form.

## **APPENDIX-5: Sample Chapter**

### **1.3 Security requirements in Electronic transactions.**

In the world of e-commerce, electronic payment most commonly refers to the use of a credit or debit card by a consumer to purchase a product or service online. For online merchants to accept credit or debit card numbers as payment, they must use online credit card processing technology that processes payments via online platforms such as the World Wide Web. To alleviate consumer concerns regarding the risk involved in using credit and debit cards online, most online sites use secure electronic transaction specifications that help to protect personal information like credit card numbers.

Like traditional merchants, online businesses also must work in conjunction with an acquiring bank in order to process transactions and obtain cash from credit card purchases. For example, once a consumer at a music e-tailer like [CDNOW.com](http://CDNOW.com) inputs his or her credit card information as payment, the online merchant uses real-time online processing software to send the information to the acquiring bank. Once the acquiring bank receives the request, it seeks credit card authorization from an acquiring processor, which handles credit card processing, billing, reporting, and settlement services. The acquiring processor transmits the request to the card-issuing bank—the bank that issued the credit card to the consumer—which either responds with an approval or denial code. The acquiring processor then sends the code to the merchant. Despite its complexity, this entire process typically is completed in less than 15 seconds.

During the late 1990s, a phenomenon known as electronic bill presentment and payment (EBPP) began to grow in popularity. EBPP is a process that allows businesses to bill clients and secure payment via the Internet. Invoices typically are transmitted by an e-mail message that includes a link to an online payment service provider's Web page, which houses more detailed billing information and allows payees to make an electronic payment with a single click. The most popular online payment service provider is CheckFree Corp., which makes money by charging transaction fees to the billing companies. International Data Corp. predicted that by 2004, EBPP will produce revenues in excess of \$1 billion as consumers become more comfortable with security issues and as business-to-business enterprises increase their use of such technology.

## **APPENDIX-5: Sample Chapter**

### **Transaction Issues - Accommodating Customers, Technical Aspects**

As companies embraced electronic commerce and worked to devise winning online business strategies they faced a number of key challenges. Among these, perhaps none were more pressing or problematic in the late 1990s and early 2000s than the issues related to online transactions. With problems ranging from implementing effective online ordering systems to securing electronic payments and customer information, from devising quick and efficient delivery and return operations to integrating transaction applications into the technological infrastructure, transaction issues were at the heart of the movement to electronic commerce.

Before the Electronic Age, paper-based documents validated and sealed with a written signature were the overwhelmingly dominant means of conducting commercial transactions for nearly a thousand years. The onset of electronic transactions disrupted established models for nearly every area of commerce, and businesses, facing tough competitive pressures, scrambled to find new models to adjust to a changed commercial environment. How does one validate an electronic document? At what point in an electronic transaction is it considered legally sent and received? What kind of infrastructure is required to record and store electronic transactions? What measures are required to protect sensitive information, such as credit-card numbers or company secrets?

E-COMMERCE partners (customers, merchants and financial organizations) are no longer interacting by direct physical experience. Instead their experience is mediated through multidimensional interactive environments. Consequently, it is an uppermost issue for the transaction process of exchange of information over open heterogeneous environments (as the Internet) to create trust. The formal procurator, the WorldWide Web can be thought as an untrusted environment with no trust affiliations. In contradistinction, a desired trusted environment is the one that the entities constitute it, are unique, unquestionably identifiable and ruled by a set of priorities and conditions.

Version 1.1

Prepared by: Ajay Prasad

Date: 20/12/2009

## **APPENDIX-5: Sample Chapter**

### **Main requirements**

1. Confidentiality of payment and ordering information
2. Integrity of all transmitted data
3. Authentication of cardholder
4. Authentication of merchant
5. The above requirements are the heart of the usage aspect of SET.