Chapter 7

RESULTS

7.1 SECURITY ASSURANCE

Two standards were obtained which provide guidelines for the management of information security: The ISO 13335 [17] and the ISO 17799 [18]. A flow diagram showing the security management as implemented by these standards is shown in figure 7.1.

The methodology followed in these guidelines can be summarized as follows:

1. Establishment of a review boundary:
   Prior to asset identification and valuation, the boundaries of the review should be defined. A careful definition of boundaries at this stage avoids unnecessary work and improves the quality of the risk analysis. The boundary description should clearly define the system and any assumptions made. See section 3.1.

2. Risk analysis:
   An initial high level risk analysis is performed for the system assets, in each case concentrating on the business values and the serious risks to which the asset is exposed. For all other system components a baseline approach should be chosen to provide general security services. See section 3.2.

   - Identification of assets:
     As asset is a component or part of a total system to which an organization directly assigns value and hence for which the organization requires protection. See section 3.2.1.
   - Valuation of assets and establishment of dependencies:
     After listing all assets of the system under review, values should be assigned to these assets. Dependencies of assets on other assets should also be identified, since this might influence the values of the assets and the appropriate level of protection. See section 3.2.2.
   - Threat assessment:
     Both accidental or deliberate threat sources should be identified. It is essential that no relevant threat is overlooked, since this could result in failure or weaknesses in system security. At the completion of the threat assessment, there will be a list of threats identified, the assets or groups of assets they would affect. See section 3.2.3.

Figure 7.1:
Management of IT security

- Vulnerability assessment:
  This assessment includes identifying weaknesses that may be exploited by a threat source to cause harm to the assets or disrupt the system requirements they support. See section 3.2.3.
- Assessment of risks:
  The objective of this step is to identity and assess the risk to which the IT system and its assets are exposed. Risks are a function of the values of the assets at risk and the likelihood of threats occurring to cause potential adverse business impacts. See section 3.2.3.
- Identification of existing/planned safeguard:
  Possible security services and mechanisms that can safeguard the system are identified. See section 2.2.3.

3. Selection of safeguards:
   Appropriate safeguards must be selected to reduce the assessed risks to an acceptable level. The security and system architecture, and constraints of various types must be taken into account to allow for a proper selection. See chapter 4.

4. Implementation of security policy:
   Details must be given given of selected safeguards and how they must be used to ensure security. A security plan should be suggested that defines the actions that must be taken to implement the required safeguards in the system. See chapter 5.

5. Risk Acceptance:
   After evaluating the performance if the security policies residual risks are identified. No system is entirely secure and any implementation will have trade-offs between performance and security assurance. The system managers must review potential adverse effects of these risks and decide whether they are acceptable. This will determine which policy is best to implemented. See section 8.2.1.

The design methodology used in this dissertation is shown to cover the same areas as those specified in accepted standards. Therefore it can be concluded that the methodology used satisfy criteria 1 as specified in section 6.1.

In order to show that criteria 2 and 3 are satisfied all the identified threats and functional requirements are mapped to the security services that addresses them. Mechanisms used

to implement these services are well documented and based on proven algorithms. Therefore assurance is given that the implementation is secure and mitigates risk from the defined threats. Table 7.1 shows the implemented security services and the respective threats and functional requirements that they cover.

Table 7.1:
Threat/Functional Requirement vs Service mapping

S1	S2	S3	S4	S5	S6
F8, F9	F5, F6, F7, F8, F9	F4, F11	F10	F12	F1, F2, F3
N6, N7	N2, N4, N5, N6, N7	N3	N2	N8	N1
FAN1	FAN1, FAN2, FAN5	FAN4	FAN2, FAN3		
		PN3, PN4	PN2		PN1
G2, G3, G6,	G2, G3, G4, G5	G6	G6		G1
O3, O4	O2, O3, O4	O5	O6	O7	O1

7.2 PERFORMANCE OF SECURITY MECHANISMS

Performance measures were obtained from literature [58], calculations and measurements from the test system. Time taken to perform operations common to all mechanisms, e.g. key selection, has been ignored and only operations unique to the specific mechanisms, e.g. time taken to perform hash, were taken into account. The other operations common to all mechanism, e.g. selection of key, were ignored. These are not important in our analysis, as we are not interested in the detailed performances of the node or the smart card. Measurements and calculation must only provide a means whereby the relative speeds of the different implementation can be compared.

7.2.1 Confidentiality

The DES algorithm was implemented. The results obtained are shown in figure 7.2. DES is a block cipher with block size equal to 8 bytes. This can also be seen from the measurements as the time increase in steps at multiples of 8. Performance measures given by manufacturers are sometimes misleading as some only list the actual processing time. Unfortunatly the 9600 bps communication adds additional time as the data must first be transferred and then received back. The smart card might take only $17\mu s$ to encrypt/decrypt a 64 bit block but needs $13.3\mu s$ to transfer the data. In the encryption graph the effect of the data transfer is seen be the skew steps as n increases. Encryption has flat top steps because n is always a multiple of 8.

7.2.2 Digital Signatures

The RSA signatures and the MAC suggested were implemented. The results obtained are shown in figure 7.3. As expected the MAC was faster than the RSA public key signatures. The RSA algorithm however provides better non-repudiation as the MAC can be generated by two parties. It must also be remembered that the MAC is only 196 bits long while the RSA signatures are 512, 768 and 1024 bits respectively. This makes a difference when the signature is sent over a low-bandwidth network with small data packets and high overhead. This also increases the time taken to transfer data to the smart card. Due to the nature of RSA verification takes less time than signing. The MAC has taken the same time for signing and verification.

7.2.3 Authentication: PKI

The three-way authentication procedure was chosen because it does not need time stamps. A synchronized clock is difficult to implement in a distributed system and therefore freshness of messages must be ensured using a nonce. This authentication scheme can easily be performed by the owner and the gateway in a matter of milliseconds. It is therefore only needed to determine whether the nodes can perform this scheme and how long it would take them. Therefore the performance measurements are given for a node to node authentication.

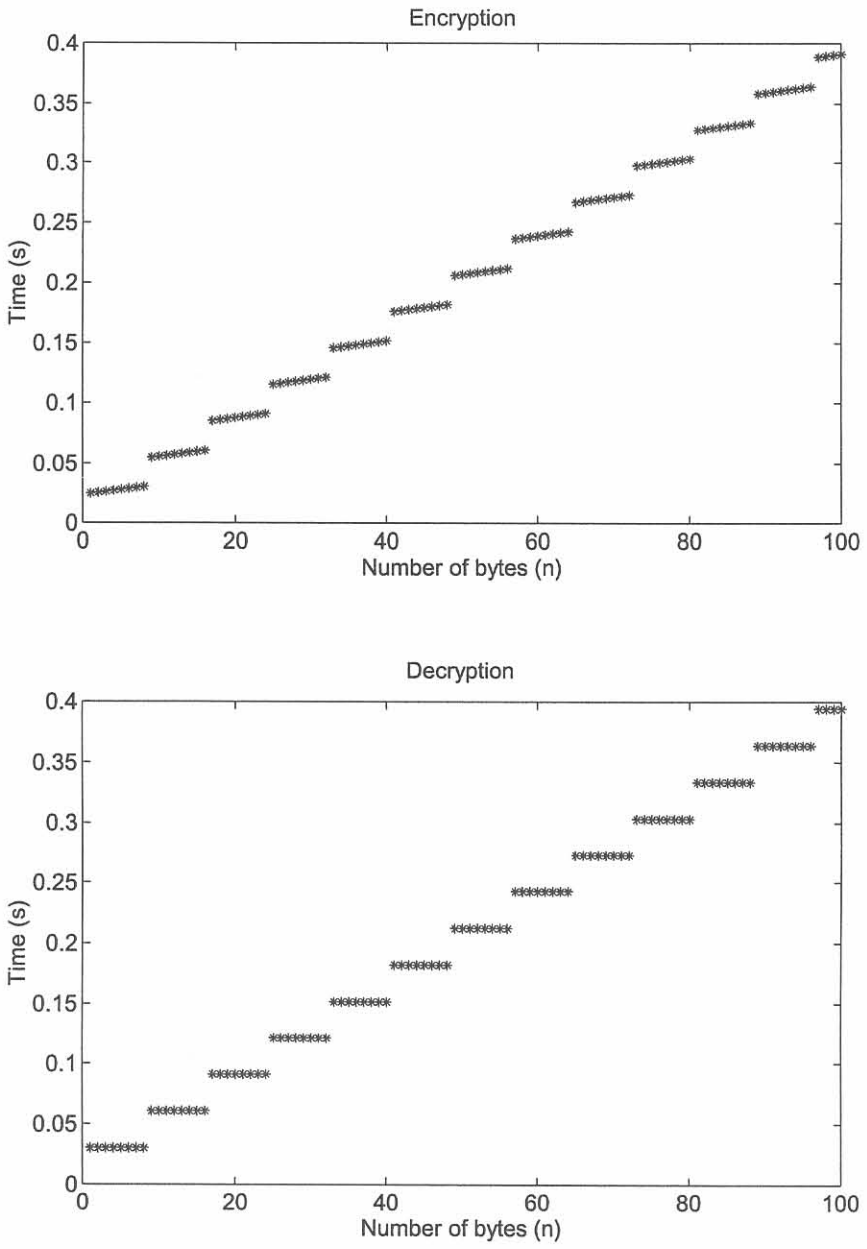

Figure 7.2:
Performance of DES encryption and decryption

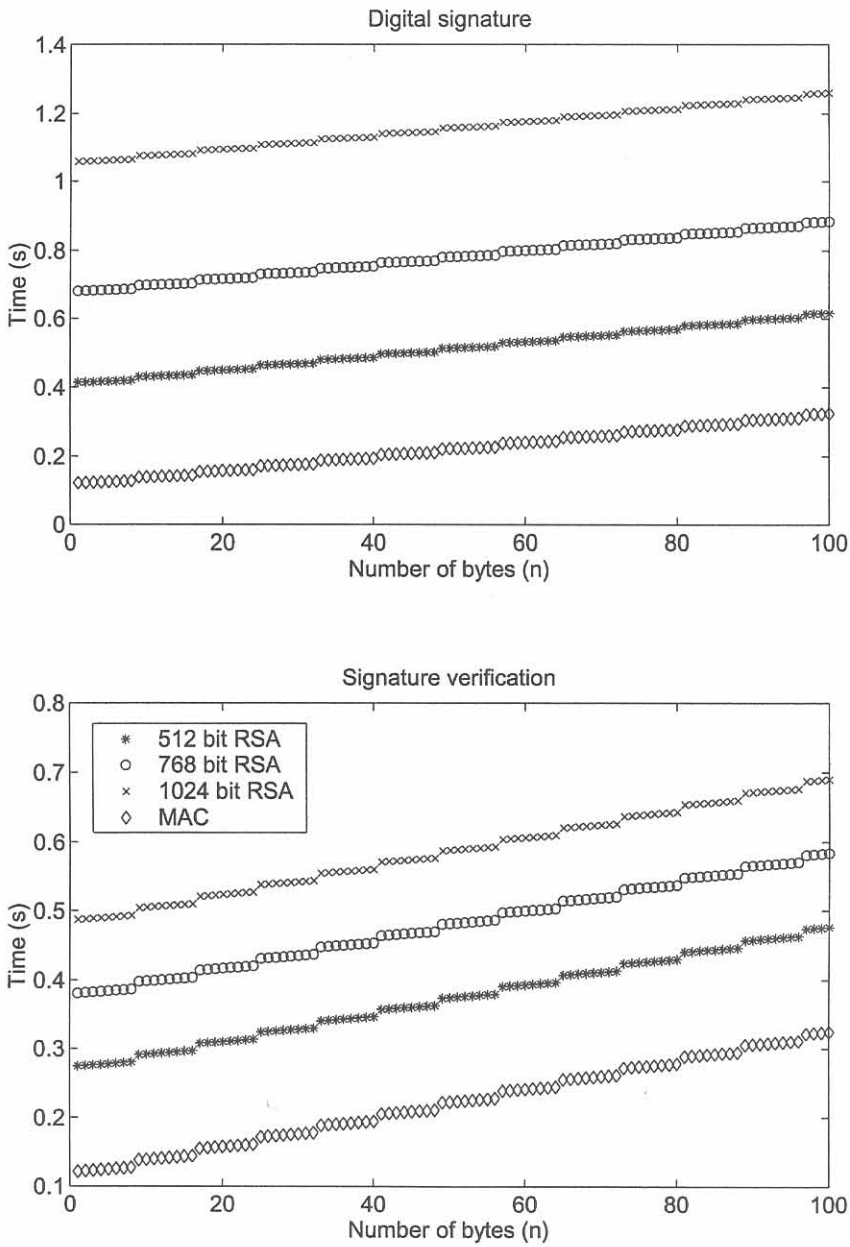

Figure 7.3:
Performance of proposed digital signature mechanisms

Calculations are shown using the RSA - 512 bit algoritm:

1. 1st Step: A to B
   - Two random numbers for K_{AB} and r_A: $110ms$
   - Encryption K_{AB}: $270ms$
   - Signature: $587ms$
   - Transmission: $126ms$
   - Verification: $393ms$
   - Decryption: K_{AB}: $456ms$
   - TOTAL: $1.942s$
2. 2nd Step: B to A
   - One random numbers for r_A: $55ms$
   - Encryption K_{AB}: $270ms$
   - Signature: $587ms$
   - Transmission: $126ms$
   - Verification: $393ms$
   - Decryption K_{AB}: $456ms$
   - TOTAL: $1.887s$
3. 3rd Step: A to B
   - Signature: $456ms$
   - Transmission: $54ms$
   - TOTAL: $510ms$
4. TOTAL (Steps 1 to 3): $4.339ms$

Given the previous performance measurements of RSA signatures with 768 bit and 1024 bit keys it can be estimated that (with the extra bits needed to be transferred to the smart card and the other node) authentication with the larger keys sizes might take respectively up to $1.5s$ and $3s$ longer.

7.2.4 Authentication: Symmetric

This authentication scheme can easily be performed by the owner and the gateway in a matter of μ's. The owner and the gateway would probably only use PKI when authenticating each other. It is therefore only needed to determine whether the nodes can perform this scheme and how long it would take them. Therefore the performance measurements are given for a node to node authentication.

$A \Rightarrow B\ A(r_A, ID_A, ID_B)$

$B \Rightarrow A\ B(K_{AB}[ID_A, ID_B, r_A, r_B, DerivedKeyInfo])$

$A \Rightarrow B\ A(K_{AB}[ID_B, r_B, DerivedKeyInfo])$

1. 1st Step: A to B
   - Random number generation: $55ms$
   - Signature: $124ms$
   - Transmission: $23ms$
   - Verification: $124ms$
   - TOTAL: $326ms$
2. 2nd Step: B to A
   - Random number generation: $55ms$
   - Encryption: $28ms$
   - Signature: $128ms$
   - Transmission: $27ms$
   - Decryption: $30ms$
   - Verification: $128ms$
   - TOTAL: $396ms$
3. 3rd Step: A to B
   - Encryption: $27ms$
   - Signature: $128ms$
   - Transmission: $27ms$
   - Decryption: $30ms$

- Verification: $128ms$
- TOTAL: $340ms$

4. TOTAL (Steps 1 to 3): $1.06s$

As expected this system is much faster and the session key does not need to be explicitly updated as many smart cards support build in functionality using derived keys.

7.2.5 Messages

The required message formats are:

1. Message format for Node A to gateway:
   $NodeA(K_{GA}[SeqNo, Instruction]NodeA(K_{OA}[Data]))$
2. Message format for gateway to owner:
   $Gateway(K_{GO}[NodeA(K_{OA}[Data]))$
3. Message format for owner to gateway:
   $Owner(K_{GO}[Owner(K_{OA}[Data]))$
4. Message format for gateway to Node A:
   $Gateway(K_{GA}[SeqNo, Instruction]Owner(K_{OA}[Data]))$
5. Message format for Node A to Node B:
   $NodeA(K_{AB}[SeqNo, Instruction, Data])$

Message 1 requires 2 symmetric encryptions and two signatures. Based on previous results it would be an advantage if symmetric signatures were used. Message 2 requires 1 symmetric encryption and 1 signature. The gateway and owner can implement public key signature easily and effectively and therefore RSA must be used to sign this message. RSA will also give better non-repudiation and integrity protection seen as this message must traverse the public network. Message 3 requires 2 symmetric encryptions and two signatures. Based on previous results it would be an advantage if symmetric signatures were used when signing the payload (taken that the node will have to verify it). The complete message can be signed using RSA and will be verified by the gateway. Message 4 requires 1 symmetric encryption and 1 signature. The node must verify the signature and there a symmetric signature would speed up the communication process. Message 5 requires 1 symmetric encryption and 1 signature. Communication between nodes is not feasible using RSA. The previous messages all had one or more entity that could do public key cryptography efficiently. If both entities are hampered communication is drastically slowed down. Therefore a symmetric integrity and signing mechanism must be used.