

# Security Services

## **1 Availability**

### **1.1 REDUNDANCY**

1.1.1 Functional

1.1.2 Data

### **1.2 FAULT TOLERANCE**

## **2 Non-repudiation**

### **2.1 DIGITAL SIGNATURES**

2.1.1 El Gamal

2.1.1.1 Digital Signature Standard (DSS)

## **3 Confidentiality**

### **3.1 CRYPTOGRAPHY**

3.1.1 Symmetric cryptography

3.1.1.1 DES

3.1.1.2 AES (Rijndael)

3.1.1.3 Triple DES

3.1.2 Public Key cryptography

3.1.2.1 RSA

3.1.2.2 Blowfish

## **4 Integrity**

### **4.1 HASHING ALGORITHMS**

4.1.1 MD4

4.1.2 MD5

4.1.3 SHA-1

### **4.2 CHECKSUMS**

4.2.1 CRC

### **4.3 CODES**

4.3.1 Hamming Code

## **4.4 AUDIT LOGS**

4.4.1 Application

4.4.2 Host

4.4.3 Network

## **5 Authentication**

### **5.1 ACCESS CONTROL**

5.1.1 Biometrics

5.1.1.1 Eye scanning

5.1.1.2 Hand geometry

5.1.1.3 Fingerprint

5.1.1.4 Voice

5.1.1.5 Physical behavior

5.1.1.5.1 Gait

5.1.2 Passwords

5.1.3 Public Key Infrastructure

5.1.4 Types

5.1.4.1 Mandatory access control

5.1.4.2 Discretionary access control

5.1.5 Smartcards and tokens

### **5.2 ATTRIBUTION**

5.2.1 Audit logs