通信情報保護學會誌
第1卷, 第3號, 1991. 12

개방형 시스템 보안 기술(1)

崔 陽 熙*

1. 배 경

컴퓨터 시스템 및 정보통신 시스템의 원활한 동작을 위하여 보안(Security) 기술이 어느때보다도 절실히 요구되고 있다. 많은 사고 및 범죄가 저질러졌으며, 이에 의한 피해는 앞으로 급증할 전망이므로 개방형 시스템(Open System)의 구축시에는 보안기능의 확보가 필수적이라고 하겠다. 보안기술에 관한 국제적 기술표준화(Standardization) 활동을 살펴봄으로서 개방형 시스템의 확산에 도움이 되고자 한다. 본고는 필자가 참여하고 있는 ISO/IEC JTC1/SC21/WG1의 보안 그룹이 작성하고 있는 보안관련 기술문서의 요약이다.

SC21/WG1은 유명한 OSI(Open systems Interconnection)의 기본 참조모델을 작성한 그룹이며, 요즘의 주요활동은 보안에 관한 기술표준화, 적합성 시험 등이다. SC21은 보안에 관한 일관성 있고 모든 분야를 포함하는 기술을 확립하여 필요한 시기에 개방형 시스템에 필요한 보안표준이 제공될 수 있도록 하는데 촛점을 두고 있다.

본고는 따라서 개방형 시스템에 관련된 보안 활동을 정리하고 체계화하는 목적으로 작성되었다. SC21의 보안에 관련된 가장 기초적인 문서는 ISO 7498-2 (개방형 시스템 상호접속 표준-보안 아키텍쳐)으로서 1989년에 발간되었다. 이는 보안 서비스와 메카니즘을 정의하고 있으며, 구현에 관련된 사항을 배제하고 있다. 따라서 보안 모델, 보안 골격 등의 구체적인 보안표준이 더 필요하게 되었으며, 이들 중에서 모든 통신 프로토콜에 공통적인 사항을 모아서 SC21에서 표준화를 현재 진행시키고 있다. 그림 1은 개방형 시스템에 필요한 각종 보안 요소의 상호관계를 정리하여 나타낸 그림이다.

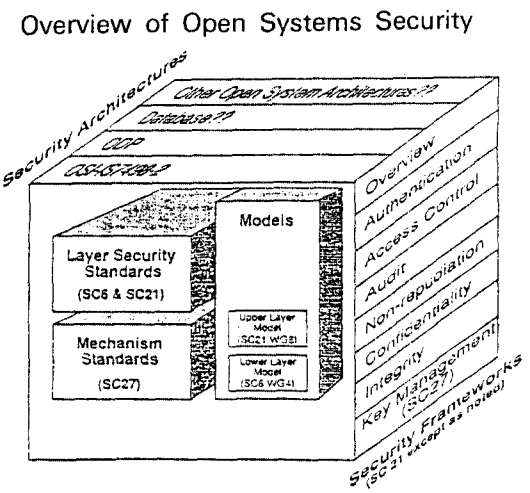

그림 1. 개방형 시스템 보안의 개관

* 서울대학교 컴퓨터공학과

2. 보안 아키텍쳐(Security Architecture)

보안 아키텍쳐란 개방형 시스템 구조내에서 필요한 기본적인 보안서비스, 메카니즘, 관리기능 등을 묘사하는 일관성 있는 기준을 의미한다. ISO 7498-2는 일반적인 시스템에서 일반적인 보안 및 보호가 요구될 때 적용될 수 있는 보안 아키텍쳐로서 OSI 기본 참조모델과 부합하고 이 모델내에 어떻게 보안서비스를 위치시킬 것인가를 정의하고 있다. 7498-2는 Authentication(peer entity와 data origin), access control, non-repudiation(origin과 delivery), integrity(connectionless, selective field connectionless, connection oriented with recovery, connection oriented without recovery, selective field connection oriented), confidentiality(traffic flow, connectionless, connection oriented, selective field) 등 통신관련 보안서비스를 묘사하고 있다. 그리고 이들을 7498(기본참조모델)내에 어디에 두는 것이 좋은 가를 권고하고 있다.

개방형 시스템의 여러 분야 중 통신 이외의 분야에 대한 보안 아키텍쳐는 별로 집중적으로 연구되지 않았다. 현재 개방형 분산처리 (Open Distributed Processing), 데이타베이스, 전자우편 등에서 각각 추가적인 보안 아키텍쳐를 연구하고 있다.

3. 보안골격(Security framework)

보안 골격의 목적은 Authentication이나 Access Control과 같이 특정의 기능분야에 대해 종합적이며 일관성 있는 기준을 제공하는데 있다. 보안 골격은 보안서비스를 개방형 시스템 환경에 적용할때 관련되는데 이때 개방형 시스템이란 데이타베이스, 분산응용, 개방형 분산처리, 개방시스템 상호접속 등을 모두 포함할 수 있다. 보안골격은 데이타 요소와 동작(Operation)의 순서에 관련되며 시스템, 시스템간 접속, 데이타 등에 대하여 기술한다.

보안골격은 7가지로 세분화되며 이들을 authentication framework, access control framework, non-repudiation framework, integrity framework, confidentiality framework, audit framework, key management framework이다.

Authentication Framework

이 골격은 Authentication의 기본 개념을 정의하고, 메카니즘의 Class를 확인하며 서비스를 정의하고 있다. 또한 프로토콜을 위한 기능 요구사항을 제시하고 Authentication에서의 일반적인 관리 요구사항도 담고 있다. 이 골격은 관련 표준화의 맨 위에 위치하여 모든 개념, 용어, 분류등을 다루고 있다. 바로 밑으로는 ISO 9798(엔티티 Authentication 메카니즘) 등의 표준으로 구체적인 사항이 제시된다. 그리고 맨 아래에는 ISO 9594-8(디렉토리 Authentication 골격)과 같이 이를 특정 응용에 적용한 것이 놓이게 된다.

Access control Framework

여기에서는 사용자-프로세스, 사용자-데이타, 프로세스-프로세스, 프로세스-데이타등의 Access Control에 관한 모든 사항이 다루어진다.

Non-Repudiation Framework

ISO 7498-2 또는 CCITT X. 880 등에서 정의한 non-repudiation 보안 서비스의 개념을 확장시키고 있다. 이 골격은 암호 기술을 이용한 non-repudiation을 제시하고 있다.

Integrity Framework

데이타 retrieval, transfer, management 등에 관한 integrity를 다루며 기본개념, 메카니즘, 서비스, 관리 등을 다룬다. 이 골격은 특정 암호 알고리즘에 의존하고 있지 않으며, Integrity를 깨뜨린 것의 검출을 다루는 부분과 이의 정정을 다루는 부분으로 나뉜다.

Confidentiality Framework

다른 골격과 마찬가지로 개념, 서비스 등을 정의한다. 앞과 마찬가지로 골격은 특정 알고리즘에 의존하지 않도록 정의되고 있다.

Security Audit framework

여기에서는 Audit의 개념정의, Audit Record의 생성을 야기시킬 Event Class의 식별, 정보관리 기능 정의, Security Recovery의 소재 등이 다루어진다. 이 모든것의 제공은 물론 채택된 Security Policy의 환경 아래에서 동작하도록 설계되고 있다. 누가 Security Audit를 하는가는 표준화 대상이 아니므로 제외되었다.

Key Management Framework

SC27에 의해 현재 개발중인 이 골격은 암호화가 적절한 메카니즘으로 쓰일 수 있는 때에 이에 필요한 암호 Key 관리를 다루고 있다.

4. 보안 모델

보안 모델의 목적은 보안골격에 수록된 보안 개념을 개방형 시스템 아키텍쳐에 적용시키는 데 있다. 여기에서는 OSI 기본 참조 모델에 관련된 사항을 다루고자 한다.

OSI 상위계층 보안 모델

이 모델은 상위계층(5, 6, 7 계층)에 있어서 응용과 무관한 보안서비스와 프로토콜의 개발을 위한 아키텍쳐 모델을 제공하고 있다. 여기에 따른 서비스와 프로토콜을 사용하면 응용 서비스요소(ASE)는 내부적으로 따로 보안서비스를 갖지 않아도 된다. 이 모델은 세션, 표현, 응용계층에서 보안서비스의 상호 관련성을 따지며 이들을 어디에 놓을가도 논하고 있다.

OSI 하위계층 보안 모델

이는 하위계층(1, 2, 3, 4)에 있어서 OSI 기본 참조 모델과 관련하여 보안과 관련된 프로토콜을 개발하는 데 쓰이는 모델이다. 현재 SC6에서 작업중이며 지침서가 발간될 예정으로 있다.

5. 데이타 관리(Data Management) 보안

데이타 관리의 참조모델(ISO DIS 10032)은 Access Control을 Privilege로 묘사하고 있으며, Access Control에 대한 아키텍쳐 모델을 제공한다. 여기에서는 다른것 보다 Access control만을 보안서비스로 다루고 있다.

ISO 10027은 Information resource Dictionary Systems(IRDS) 골격이며, 어느 조직의 정보자원을 수록, 제어하는 데 필요하다. 특히 Information Resource Dicitionary (IRD)에 있는 Data를 Access하는 것을 제한하거나 제공하는 등의 내용을 기술하고 있다. IRDS의 서비스 인터페이스는 CD 10728에 수록되며 약간 Access Control과 관련된 사항을 담고 있다.

Remote Database Access(RDA) 서비스는 ISO 9579-1에서 정의되며 터미날로 부터 원격 데이타베이스에 대한 인터 액티브 Access를 허용하고 있다. 원격 데이타 자원을 Open 하려면 사용자는 자원에 대한 Access를 할 능력을 부여 받아야 한다. RDA는 Request/Indication 서비스 프리미티브에 User Identity와 Authorization Identity를 수용하고 있으므로 이를 통한 보안제어가 가능하다.

데이타베이스 언어 SQL(ISO 9075)는 SQL 데이타베이스에서의 기본 동작과 논리구조를 정의한다. SQL 내부에서 SQL 데이타의 사용자는 〈User Authorization Identifier〉로 식별된다. 사용자나 카탈로그 이외의 모든 SQL 엔티티는 SQL 사용자에 의해 생성되고 소유되며, 생성될 때 이에 대한 Access는 제한적으로 된다.

6. OSI 관리의 보안

OSI 관리 표준에서의 보안관련 사항을 알아보기로 하자. OSI 보안관리 개요 문서는 보안관리

기능에 대하여 개요를 싣고 있으며, 이들이 OSI 기본참조모델 및 Audit 골격과 어떤 관계에 있는가를 설명하고 있다(ISO 10164)

ISO DIS 10164-7은 ISO 10164-5의 경보보고 기능을 이용한 보안경보 Event를 제기하는데 CMIS를 사용하는 응용에 의한 시스템 관리기능을 규정하고 있다. "Event Forwarding Discriminator"의 생성, 제거, 수정을 통하여 보안경보 보고에 대한 통제가 가능하다.

ISO DIS 10164-8은 Audit Trail Log로 보내지는 Event 보고에 관한 시스템 관리 기능을 묘사하고 있다. 이는 ISO 10164-5, 6, CMIS 등을 사용한다. 또한 10164-9는 Target 종단시스템에서의 관리 오브젝트에 대한 Access Control의 제공을 모델링하고 있다. 이는 Access Control 서비스를 제공하기 위한 기능을 갖는 관리 오브젝트를 규격화 함으로써 가능해진다.

ISO 9595(Common Management Information Service 정의)의 수정인 9595/PDAM 4는 Access Control 파마미터에 대하여 일부 수정하고 있다. 이는 각종 보안에 관련된 파라미터의 목적을 기술할뿐, 아직 구체적인 양식이 정해지지 않고 있다. ISO 9594-8은 Certificate라고 불리우는 Data Origin Authentication 보안서비스와 Integrity에 의해 보호되는 Security Token을 기술하고 있다. 이는 공개키암호 시스템의 사용에서의 보호기능을 제공하는데 사용된다.

Directory Access Control에 관여하서는 ISO 9594-1, 2, 3, 8의 PDAM들에 나와 있으며, Access Control, Scheme 등을 정의하고 있다.

7. OSI 응용의 보안

화일전송(FTAM)은 ISO 8571로 정의되는데 이에 대한 Authentication과 Access Control을 다루기 위한 새로운 작업이 시작되었다. 트랜스액션 처리(TP)에서의 보안 문제는 Authentication, Access Control, Confidentiality, lategrity, Non-Repudiation, auditing, Access Right Revocation, Replay Protection, Denial of Service의 방지, Reliability, Traffic Flow Confidentiality 등으로 매우 광범위하다.

ISO CD 10184-1에서 다루는 Terminal Management에서의 보안문제는 아직 다루어지지 않고 있다. 그러나 JTM(ISO 8831)은 Authentication, Access Control, Accounting, Audit Trace 등에 대한 간단한 메카니즘을 갖고 있다.

현재 검토중인 Security Exchange ASE(Application Service Element) 서비스 및 프로토콜은 ASE 사이에서 보안에 관한 정보를 교환, 전송하는데 필요한 기능을 모아 놓은 것이다. 이는 응용계층에 위치하며 상위계층 보안 모델의 일환으로 규격화 되고 있다.

ACSE(Association control Service Element)의 Authentication 서비스는 8649/AMI에서 정의한다. 이는 A-Associate Request/Confirmation에서 Authentication 정보를 담을 수 있는 필드를 제공하고 있다. 또한 표현계층에서의 Confidentiality와 Integrity는 현재 개정작업이 진행중이다.

표현계층의 Cryptographic Technique은 Connection-Oriented 보안서비스를 제공하며, Peer Entity Authentication, Connection Confidentiality, Selective Field Confidentiality, Connection Integrity, Selective Field Connection Integrity 등과 이를 표현계층에 담기 위한 표현계층 프로토콜도 묘사하고 있다.

개방형 분산처리(Open Distributed Processing)에서의 보안은 OSI에서의 보안과 매우 밀접하다. ODP는 보안을 분산처리 시스템이 가져야 하는 여섯가지 Aspect의 하나로 간주하여 매우 중요하게 다루고 있으며, ODP 참조모델의 Part II에 설명이 들어 있다. Part III에는 분산시스템 보안을 위한 특정 기능에 대한 요구사항이 삽입될 것이다. Part I에서는 Tutorial 내용이 포함되어 있다.

8. 결 론

간단히 ISO/IEC ITC1/SC21/WG1에서 취급하는 Security 관련 표준화 활동을 나열하여 보았다. 개방형 시스템으로 점차 각종 정보기기가 진보하는 요즈음에 각종 기기 사이의 신뢰성 있는 안전한 통신의 보장 문제가 더욱 중요한 Issue로 떠오르고 있다. 보안에 관한 기술적 해결방법으로 지금까지 여러가지 알고리즘과 메카니즘이 제시 되었으나, 이들을 체계적으로 모델화하여 적절히 사용하지 않으면 오히려 비용의 증가, 처리속도의 저하 등의 부작용을 낳을 수 있다. 따라서 각종 시스템과 서비스에 보안기능을 추가하려고 할때는 먼저 종합적인 요구사항을 검토한 후, 이에 관한 각종 표준, 규격을 선택하는 순서로 작업이 진행되어야 할 것이다.

여러 기간전산망, VAN, PC통신, DB 산업의 성장이 활발한 이때에 많은 전문가들이 전산망 보안에 관한 연구하기를 바라며 보안표준에 대해 향후 자세한 기술 내용을 소개할 기회가 있었으면 한다.

참 고 문 헌

1. ISO/IEC SC21/N 6167, Guide to Open Systems Security, June 1991.
2. SC21 N6168, Access ControlFramework, June 1991.
3. SC21 N6163, Integrity Framework, June 1991.
4. SC21 N6164, Confidentiality Framework, June 1991.
5. SC21 N6165, Non-Repudiation Framework, June 1991.
6. SC21 N6166, Framework Overview, June 1991.
7. SC21 N6169, Audit Framework, June 1991.
8. "정보통신 보호 입문," 정보통신 표준연구센터, 한국전자통신연구소, 1991. 10.

□ 著者紹介

최 양 희

1971－75 서울대학교 공과대학 전자공학과(학사)
1975－77 한국과학원 전기 및 전자공학과(석사)
1980－84 프랑스 국립 전기통신대학 전산과(공학박사)
1977－79 한국전기통신연구소
1981－84 프랑스 국립 전기통신연구소
1988－89 IBM Thomas J. Watson Research Center 방문연구원
1984－91 한국전자통신연구소
데이타통신 연구실장, 망기술 연구실장, 프로토콜 연구실장
정보통신 표준연구센터장 역임
1991－현재 서울대학교 컴퓨터공학과 조교수
서울대학교 중앙교육연구전산원 교육전산망부장

부 록
보안표준화 활동 목록

Summary of Security Standards Activity.

Part 1 - By Organization.

International Organization for Standardization (ISO).

Project/Work item	Status	Documents	Ref. No.
Joint Technical Committee 1 (JTC1) - Information Technology.			
SWG on Security Objectives	Ongoing	JTC1N531	a1
Catalogue of Security Related Projects	WD	JTC1N996	a2
JTC1/SC6 - Telecommunications and Information Exchange between Systems.			
Architectural Documents			
Lower Layer Security Guidelines	2nd WD	SC6N6569 Rev by N6884	b5
OSI Lower Layer Security Model	WD	SC6N5333	b2
WG3 - Network Layer			
Network Layer Security	NWI proposal	JTC1N666	b1
WG 4 - Transport Layer			
Transport Layer Security Protocol	DIS	DIS 10736	b3
Network Layer Security Protocol	CD	SC6N6585Rev	b4
JTC1/SC18 - Text and Office Systems.			
WG1 - User Requirements and Management Support.			
User Requirements for Security in TOS	WD	SC18N2233	c1
Proposed Draft Addendum to ISO 8613 for Security	DAD4	ISO 8613 DAD/4	c2
JTC1/SC17 - Identification and Credit Cards.			
WG4 - Integrated Circuit Card.			
Identification cards - IC cards with contacts:			
Part 1 Physical Characteristics	DIS	DIS 7816-1	d1
Part 2 Number and Position of Contacts	DIS	DIS 7816-2	d2
Part 3 Electronic Signals and Exchange Protocols	DIS	DIS 7816-3	d3
JTC1/SC22 - Programming Languages.			
WG15 - POSIX			
Security Interface for POSIX	WD	SC22WG15N46R1	

JTC1/SC21 - Information Retrieval, Transfer, and Management for Open Systems Interconnection.

WG1 - OSI Architecture

SC21 Security Coordination	Ongoing	SC21N2540	h1
Guide to Open System Security	WD	SC21N6167	h2
OSI Security Architecture	IS	ISO 7498-2	h3
Authentication Framework	DIS	DIS10181-2	h4
Access Control Framework	CD10181-3	SC21N6168	h5
WG1 - OSI Architecture ctd.	WD	SC21N6165	h6
Non-Repudiation Framework			
Integrity Framework	WD	SC21N6163	h7
Confidentiality Framework	WD	SC21N6264	h8
Framework Overview	WD	SC21N6166	h9
Framework for Security Audit Trail	CD10181-7	SC21N6169	J6

WG4 - OSI Management.

OSI Security Management - 7th draft	Mature WD	SC21N4091	j1
OSI Systems Management - Part 8: Security Audit Trail Function	CD	CD10164-8	j2
OSI Systems Management - Part 7: Security Alarm Reporting Function	CD	CD10164-7	j3
Objects and Attributes for Access Control	CD	CD10164-9	j5
Directory Authentication	IS	9594-8	j7
Directory Access Control (5 parts)	PDAM 1.2 9594 part 1	SC21N5942	j8
	PDAM 1.3 9594 part 2	SC21N5952	
	PDAM 1.3 9594 part 3	SC21N5953	
	PADM 1.3 9594 part 4	SC21N5954	
	PDAM 1.2 9594 part 8	SC21N5955	

WG6 - OSI Session, Presentation and Common Application Services.

ACSE Authentication Service and Protocol	IS addendum	IS 8649	k1
OSI Upper Layers Security Model	CD10745	SC21N6095	k2
Security Exchange ASE	Mature WD	SC21N6096	

JTC1/SC27 - Security Techniques.

(Note: this SC has assumed most of the work items of SC20. This summary captures the proposed redistribution of the SC20 work items.)

Register of Encipherment Algorithms	DIS	DIS 9979	e5

WG1 - Generic Security Requirements

Glossary of IT Security Definitions	Standing Document	N270	
Entity Authentication Mechanisms - General Model	DIS	DIS 9798/1	f1
Cryptographic mechanisms for key management - Overview	Approved NWI		e6
Key Management Framework	WD	27N233	f6
Security Information Objects	NWI proposal	27N225	e7
Guidelines for Management of IT Security	NWI proposal	27N111	e8

WG2 - Security Techniques and Mechanisms

Modes of operation for 64-bit block cipher algorithm	complete	ISO 8372	e1
Modes of operation for n-bit block cipher algorithm	DIS	DIS 10116	e2
Data Integrity mechanism using a cryptographic check function employing an n-bit algorithm with truncation	IS	IS 9797	e3
Entity Authentication Mechanisms - Part 2 Entity		DIS 9798/2	e4

Authentication using symmetric techniques	DIS		
Entity Authentication Mechanisms - Part 3 Entity Authentication using a public key algorithm	CD	CD9798-3	f2
Authentication with three-way handshake using zero-knowledge techniques	WD		f3
Digital Signature scheme with message recovery	DIS	DIS 9796	f4
Hash Functions	Study Period	27N223 & 224	f5
Zero Knowledge Techniques:			
Part 1 General Model	NWI proposal	27N177	f8
Part 2 Mechanisms based on Identity and Factorization		27N178	
WG2 - Security Techniques and Mechanisms ctd			
Key Management			
Part 1 Framework (see WG1 above)			
Part 2 Mechanisms using Symmetric Techniques	NWI proposal	27N179	f7
Part 3 Mechanisms using Asymmetric Techniques			
WG3 Security Guidelines.			
Evaluation Criteria for IT Security			
Part 1 Introduction and Model	NWI Proposal	27N235	f9
Part 2 Functionality of IT Systems			
Part 3 Assurance of Systems			
Collection and Analysis of of Requirements for IT Security Evaluation Criteria	NWI Proposal	27N234	f10
note: the SC20 work items listed below have been reassigned to SC6 and SC21 of JTC1)			
SC20 work items assigned to SC6:			
Data Encipherment - Physical layer interoperability requirements	complete	ISO 9160	g1
Transport layer cryptographic techniques	WD	SC20/3 N101	g2
Network layer cryptographic techniques	WD	SC20/3 N100	g5
SC20 work items assigned to SC21:			
Presentation layer cryptographic techniques	WD	SC20/3 N102	g3
Practical conditions for ACSE Authentication	WD		g4
Technical Committee 68 (TC68) - Banking and Related Financial Services.			
TC68/SC2 - Operations and Procedures.			
Requirements for Message Authentication	complete	ISO 8730	m1
Approved Algorithms for Message Authentication - Part 1 DEA-1 algorithm (Same as ANSI X9.9 - 1982)	complete	ISO 8731/1	m2
Approved Algorithms for Message Authentication - Part 2 Message Authentication Algorithm	complete	ISO 8731/2	m3
Approved Algorithms for Message Authentication - Part 3 FEAL - MAC	proposed	ISO 8732	m4
Key Management (see also ANSI X9.17)	complete		m5
Procedures for Message Encipherment - Part 1 General Principles; Part 2 Algorithms (same as ANSI X9.23)	complete	ISO 10126	m6
Sign-on Authentication (Ref ANSI X9.26)	CD	CD 11131	m7
Banking-Key Management - Multiple Centre Environment (Ref ANSI X9.28)	propsed WI		m8
Data Security Framework for Financial Applications	WD	SC2 WG2N227	
Key Management by Means of Asymetric Algorithms	CD	CD 11166	m9

TC68/SC6 - Financial Transaction Cards, Related Media and Operations.

WG6 - Security in Retail Banking.

Retail Message Authentication	DIS	DIS 9807	n1
Pin Management and Security			
Pt 1 PIN Protection Principles and Techniques	DIS	DIS 9564-1	n2
Pt 2 Approved Algorithms for PIN Encipherment	DIS	DIS 9564-2	n2
Retail Key Management Standard -			n3
Financial Transaction Cards:			
Part 1 - Introduction to Key Management	CD	CD11568-1	n4
Part 2 - Physical Security Requirements	WD	WD11568-2	n5
Part 3 - Key Management Techniques for Symmetric Ciphers	CD	CD11568-3	n6
Part 4 - Key Life Cycle for Symmetric Ciphers	CD	CD11568-4	n7
Part 5 - Key Management Techniques for Asymmetric Ciphers	Proposed		n8
Part 6 - Key Life Cycle for Asymmetric Ciphers	Proposed		n9
Part 7 - Key Management Schemes	Proposed		n10
Part 8 - Security-Related Control Information Data Element (SRCIDE)	Proposed		n11

WG7 - Security Architecture of Banking Systems using the Integrated Circuit Card.

Financial Transaction Cards:			
Part 0 - System Overview	CD	CD 10202-0	p0
Part 1 - Card Life Cycle	IS	IS 10202-1	p1
Part 2 - Transaction Process	DP	DP 10202-2	p2
Part 3 - Cryptographic Key Relationships	CD	CD 10202-3	p3
Part 4 - Security Application Modules	WD	WD 10202-4	p4
Part 5 - Use of Algorithms	WD	WD 10202-5	p5
Part 6 - Cardholder Verification	CD	WD 10202-6	p6
Part 7 - Key Management	CD	CD 10202-7	p7

Comité Consultatif International Télégraphique et Téléphonique (CCITT)

SG VII Q18 - Message Handling Systems

Message Handling Systems Framework	complete	X.400 series	q1
EDI Security	Draft Recommendation	X.435	q2

SG VII Q19 - Framework for Support of Distributed Applications

OSI Security Architecture	Approved Rec.	X.800	r1
OSI Security Frameworks	Joint ISO work item	see h4 - h9	r2
Upper Layer Security Model	Joint ISO work item	see k2	r3
Security Model for Distributed Applications	Joint ISO work item	see JTC1N544	r4

SG VII Q20 - Directory Systems.

Authentication	Complete	X.509	s1
Access Control	Current work item	see also j8	s2

SG VIII Q28 - Security in Telematic Services.

Proposed Security Framework for Telematic Services	Current work item	see ISO SC18	t1

European Computer Manufacturers Association (ECMA).

TC29/TG5 - Security Aspects of Documents

Security Extensions to ODA	WD	see c2	x1

TC32/TG2 - Distributed Interactive Processing

TC32/TG6 - Private Switching Networks

Integrating Cryptography in ISDN			u1

TC32/TG9 - Security in Open Systems.

Security Framework	complete	TR46	v1
Data Elements and Service Definitions	complete	ECMA Std-138	v2
Authentication and Security Attribute Service Definition	WD	TG9/90/24	v3
Secure Association Service and Management	WD	TG9/90/43	v4

European Telecommunications Standards Institute (ETSI).

TC - Special Mobile Services Group (GSM)

GSM1 Services and Facilities

Security Aspects	ETS	GSM 02.09
Subscriber Identity Modules, Functional Charateristics	ETS	GSM 02.17
Specification of the Internal Logical Organization of the Subscriber Identity Module (SIM) and its Interfaces	ETS	GSM 11.11

GSM3 Network Aspects

Security Related Network Functions	ETS	GSM 03.20

Terminal Equipment (TE)

STC TE9 - Card and Card Terminals.

Specification of Intelligent Cards and Terminals for Telecommunications	work item

American National Standards Institute and Federal Information Processing Standards.

Topic	FIPS	ANSI	Ref. No
Data Encryption Algorithm/Standard (DES)	FIPS 46-1	X3.92-1981	w1
DES Guidelines	FIPS 74	none	w2
DES Modes of Operation (ISO 8372)	FIPS 81	X3.106	w3
DES in Physical and Data Link (ISO 9160)	FIPS 139/ FS1026	X3.105-1983	w4
PIN Management and Security	none	X9.8-1982	w5
Computer Data Authentication/ Retail Message Authentication	FIPS 113	X9.19-1985	w6
Retail Key Management	none	X9.24	w7
Wholesale Message Authentication (ISO 8730 and 8731)	FIPS 113	X9.9-1986	w8
Wholesale Key Management/Option set for government use.	(restricted X9.17)	X9.17-1985	w9
Wholesale Message Encryption (ISO 10126-1 and -2)	none	X9.23	w10
Wholesale Sign-on Authentication	proposed Work item	X9.26	w11
DES Equipment Security Requirements	FIPS 140	none	w12
DES for Group 3 FAX	FIPS 141/FS1028	none	w13
Password usage	FIPS 112	none	w14
EDI Security Structures	none	X12.58	w15
Wholesale Multiple Center Key Management	none	X9.28	w16
EDI Security - Crypto Message Transaction set		X12.42	w17

Part 2 - By Topic

Topic	Reference
Organization of work	a1,a2,h1,h2
Access Control	h5,j5,j8,s2
Alarm Reporting	j3,
Architectural documents	b2,b5,c2,h3,h4-h9,k2,m8,r1-r4,t1,v1-v4,w15,x1
Audit	j2,j6
Authentication	e4,f1,f2,f3,g5,h4,j7,k1,m1,m2,m3,n1,s1,w6,w8,w11
Confidentiality	h8
Digital Signature	f4,
EDI	c2,q2,w15,w17,x1
Encipherment/ Cryptographic Techniques	e1-e7,f1-f7,g1-g5,m5,m6,p5,u1,w1-w4,w10,w12,w13,w17
Evaluation Criteria	f9,f10
Hash Functions	f5
Integrity	e3,h7
Key Management	e6,e7,e8,f6,f7,m4,n3-11,w7,w9,w16
Message Handling	q1
Network Layer Security	b1,g5
Non-Repudiation	h6
Network Layer Security	b4
Presentation Layer Security	g3
Security Management	j1, e8
Security Information Objects	e7
Threats	y1
Transport Layer Security	b3,g2
User Requirements	c1
Zero Knowledge Techniques	f8

Annex A. Other Relevant Security Documents and Activities.

The following activities/documents, while not included in the main body of the report, are identified here because they are potentially candidates for future submission to the international IT security standards work.

a. Activities

IEEE 802.10 - Standard for Interoperable LAN Security (SILS).
IFIP 11.3 - Secure Database Management Systems.

b. Documents

Canadian Trusted Computer Product Criteria - Communications Security Establishment.
Information Security Evaluation Criteria - France, Germany, Nederlands & UK joint initiative.
Secure Data Networking System (SDNS) - US Dept. of Defense National Computer Security Center:

SDN/201		Overview
SDN/301	15 May, '89	Secure Protocol 3
SDN/401	2 May, '89	Secure Protocol 4
SDN/601	11 Aug. '89	Key Management Profile
SDN/701	1 Aug. '89	Message Security Protocol
SDN/801	26 July, '89	Access Control Concept Document
SDN/801/1	26 July, '89	Access Control Information Specification Addendum 1
SDN/902	1 Aug. '89	Key Management Protocol - Definition of Service
SDN/903	1 Aug. '89	Key Management Protocol - Specs. for Protocol

Trusted Computer Systems Evaluation Criteria - Orange Book (Computer Security)
- Yellow Book (Implementation Guidelines)
Trusted Network Systems Evaluation Criteria - Red Book (Network Interpretation)
Green Book - Authentication/Password Management.
Grey Book - Trusted Database Evaluation Criteria (still classified)