Japan’s Smartcard PP and EU-Japan co-operations

29/03/2001

Yoshikazu Yorimoto

ICCS/ECSEC

ICCS

- ICCS: Research and Development Council for IC Card Commerce System

- This organization consists of 47 companies who are main smartcard vendor, card user, system integrator in Japan.

- This private organization was the base of establishing ECSEC.

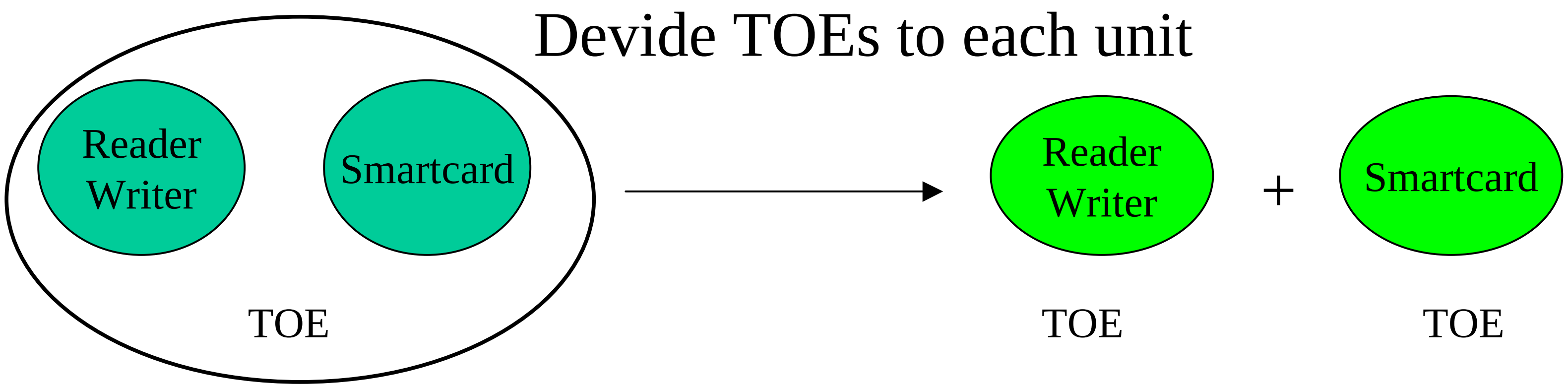
Process of creating ICCS-PP

- 1998: creation of protection profile in the field of IC cards under the supplementary budget of the Government.

- 2000.1.7 Delivery of PP in Japanese language, to the Japanese Government.

- Spring 2000 Translated into English .

From our experience



Devide TOEs to each unit

Reader Writer

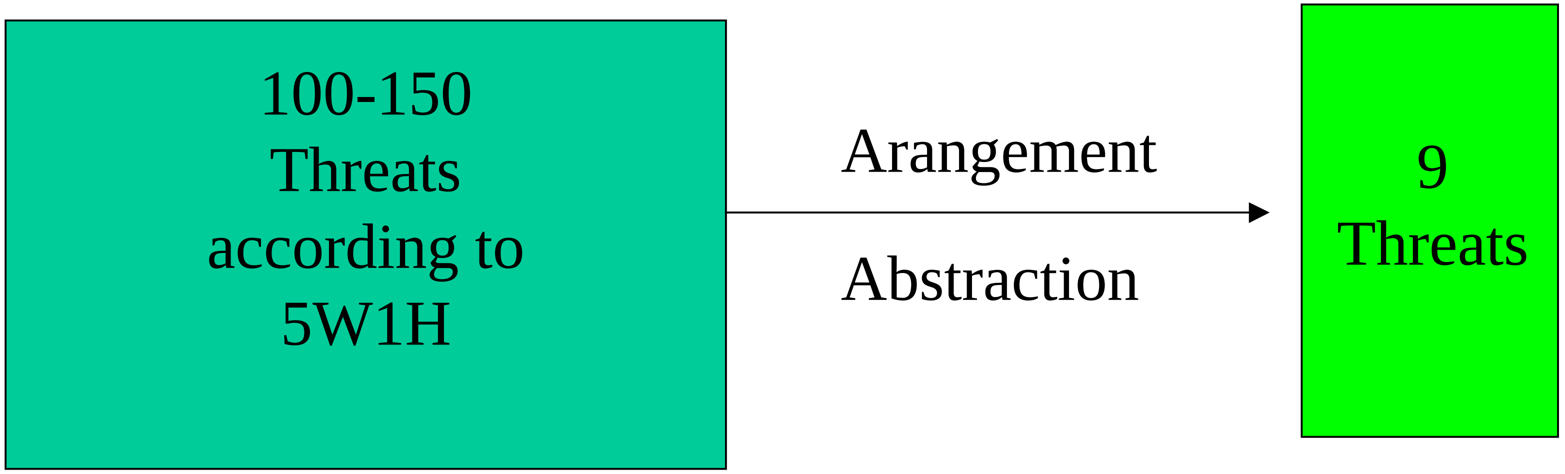
Smartcard

TOE

Reader Writer + Smartcard

TOE

TOE



100-150 Threats according to 5W1H

Arangement

Abstraction

9 Threats

ICCS-PP, EUROSMART-PP ,SCSUG-PP,
Comparative list

	Card Type	Life Cycle	Application Program Loading	File Delete & Creation in usage
ICCS-PP	ISO/IEC7816 And Contactless	usage	No	Yes
Eurosmart 9806/1919	ISO/IEC7816 And Contactless	Development to Personalization	No	No
Eurosmart 0001	ISO/IEC7816 And Contactless	Usage	Yes	
SCSUG-PP	ISO/IEC7816 And Contactless	usage	yes	yes

Japan-EU Project1

- 1999/Spring: Japanese MITI Minister and the EU Commissioner have agreed to the cooperation between the two parties.
- Joint creation of smart card PP is one of the themes of cooperation activity.
- On European side Eurosmart has been the private organization in charge.
- On Japanese side, ICCS has been in charge via New Media Development Association (extra-departmental body).

Japan-EU Project2

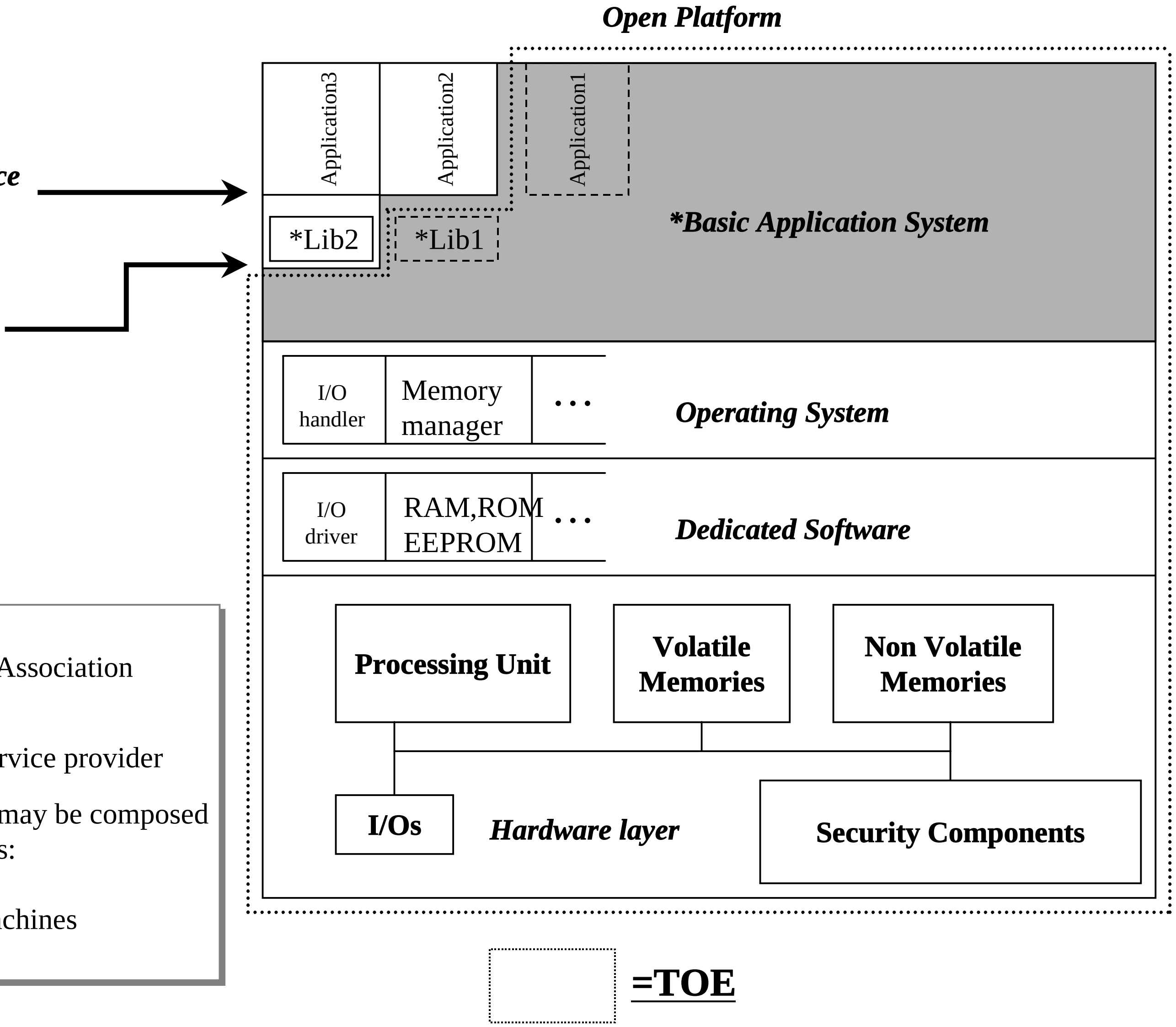
- Agreement on joint creation of smart card PP with application program loading functions.
- The basis of discussion is agreed to be Eurosmart PP9911,9806
- 2000/02 EU – Japan Workshop was held in Tokyo
- Eurosmart published PPnc0001
- 2000/06 EU – Japan Workshop was held in Marseilles
- 2000/08 Japanese proposal to meet the next PP Eurosmart is preparing.
- 2001/03 Joint Security Conference will be held in Tokyo

ECSEC proposal to Eurosmart PPs

TOE

Application System Interface
(Interpreter)

Service Provider Interface
(not native interface)
*Under study on *NMDA*



Open Platform

Application3

Application2

Application1

*Lib2

*Lib1

****Basic Application System***

I/O handler

Memory manager

. . .

Operating System

I/O driver

RAM,ROM EEPROM

. . .

Dedicated Software

Processing Unit

Volatile Memories

Non Volatile Memories

I/Os

Hardware layer

Security Components

=TOE

*NMDA:
New Media Development Association

*Lib1: Common library
*Lib2: Library loaded by service provider

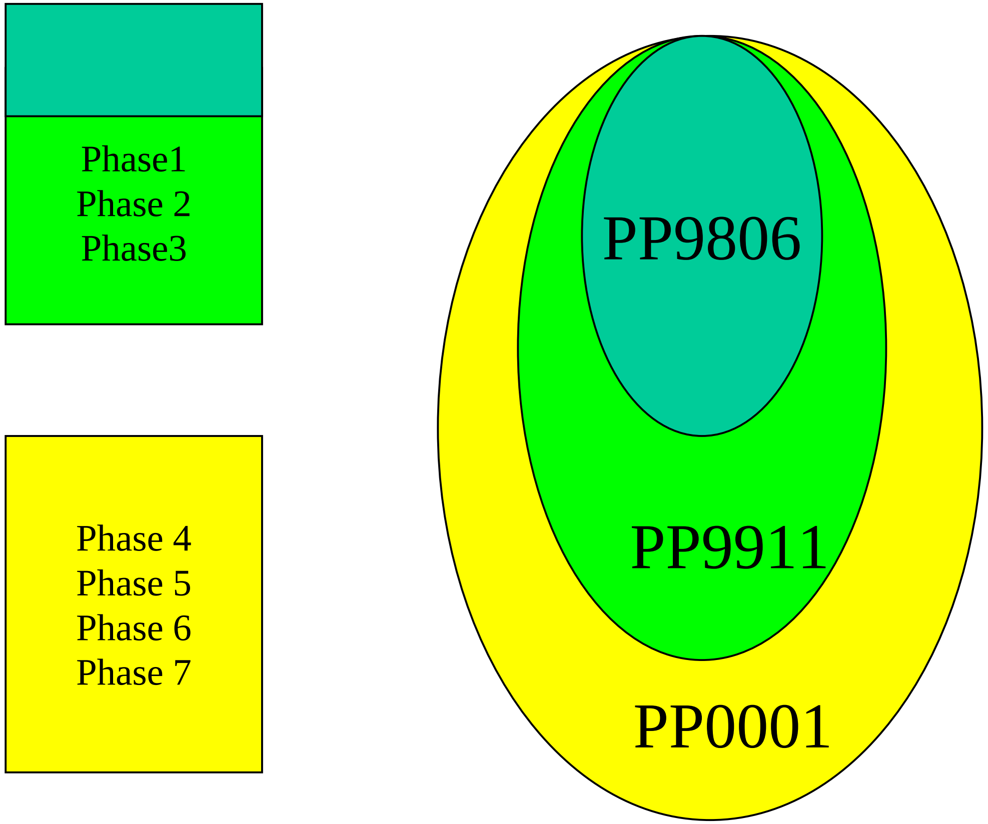
*Basic Application System may be composed of the following components:
-The Loader
-One or several Virtual Machines
-Card Manager

Eurosmart requires in PPnc0001 to use PP9806/PP9911, which have already been certified and registered in France.

This means PP9806/PP9911 are parts of PPnc0001 or, series of three PPs act as one PP.

This is the most significant feature of Eurosmart PPs.

Smartcard IC
database construction
IC Photomask
Fabrication
IC Manufacturing
IC Testing and
Prepersonalisation
IC Packaging
Testing
Smartcard product
Finishing process
Testing
Personalisation
Testing
Smartcard product
End-Usage
End of life process



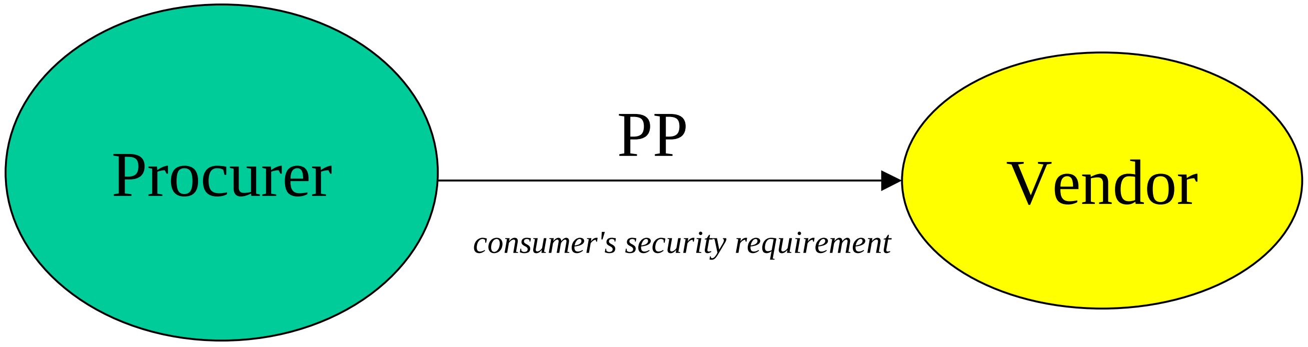
The ideal process

As the PP is primary for consumer's security requirement in procurement, the process below should be ideal.

0.1.1 According to the PP as consumer's security requirement in procurement, final manufacturer prepares the Security Target and all evidences of TOE.

0.1.2 If the vendor who is responsible to the final product or system, could do prepare all evidences of TOE, that manufacturer shall prepare another PP for proceeding manufacturers (manufacturers for proceeding process) and request their system or product to be evaluated.

0.1.3 It is ideal to generate PPs from the consumer to upper stream.

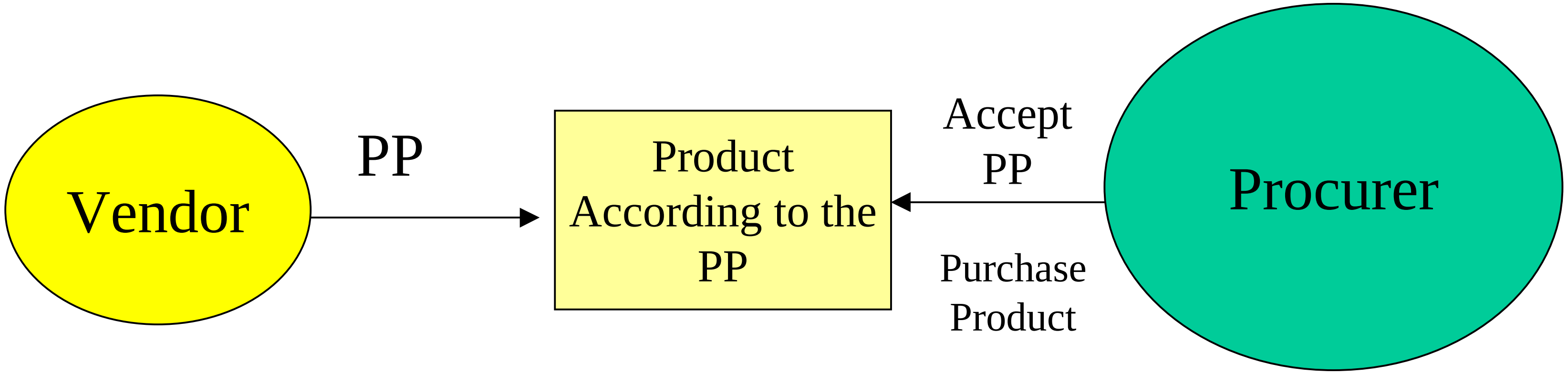


But this approach is not practical

But this approach is not acceptable to whom developing parts of products.

For example, some venders are developing IC chips before the negotiat from the smart card manufacturers.

For these manufacturers, it seems to be practical to generate PPs from upper stream to downstream, such like Eurosmart's approach.



Vendor

PP

Product According to the PP

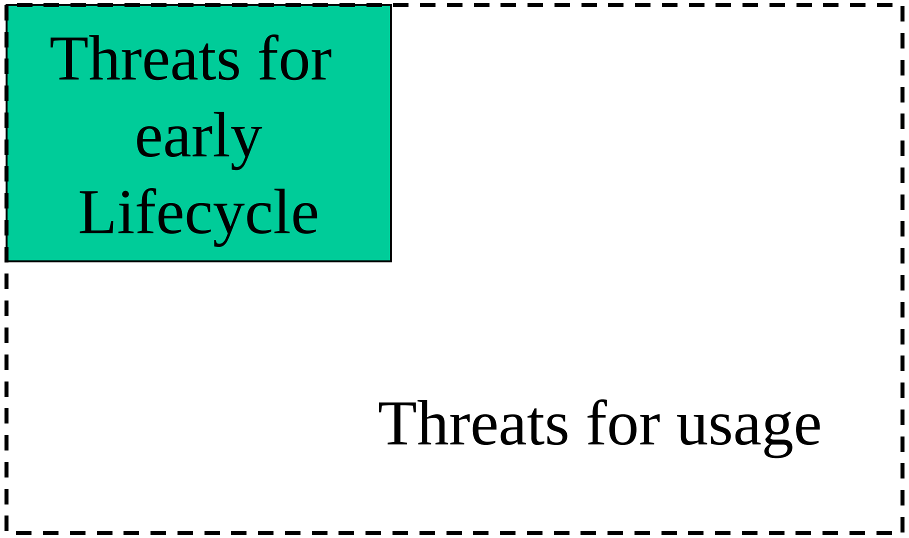
Accept PP

Purchase Product

Procurer

Problem on Eurosmart PP approach

There is a problem on the approach generating PP from upper stream to down like Eurosmart. PPs in upper stream cannot define threats in usage of the fin product clearly.



Threats for early Lifecycle

Threats for usage

Our proposal to Eurosmart

We think, in the case of approach like Eurosmart, at least, PP in usag shall show all threats in usage clearly, even threats are in the scope o upper PPs. This is in order not to lead ST generators and evaluators t misunderstanding.

Thus, we propose to add an application note PP in usage, to show al threats in usage (phase 6/7) and explain relationship with security requirements, in order not to lead ST generators and evaluators t misunderstanding.

Security Objectives for the Environment (Mapping from Threat and Assumptions)

		9806																		9911				0001
Threats	Objectives	DESIGN _ACS	DEV_DIS	DEV_ TOOLS	DLV_ AUDIT	DLV_ PROTECT	DLV_ RESP	DSOFT_ ACS	IC_DLV	MASK_ FAB	MECH_ ACS	SOFT_ ACS	SOFT_ DLV	SOFT_ MECH	TEST_ OPERATE	TI_ACS	TOE_ PRT	USE_ DIAG	USE_ SYS	DEV_ DIS_ES	DLV_ DATA	INIT_ ACS	SAMPLE _ACS	APPLI_ DEV
9806	T.CLON	2	1	1				2	3	2	2	2	1	1		2	3			1		1	1	▨
	T.DIS_DEL			1									1							1		1		▨
	T.DIS_DESIGN	2									2					2	3							▨
	T.DIS_DSOFT							2									3							▨
	T.DIS_INFO		1																	1				▨
	T.DIS_PHOTOMASK									2							3							▨
	T.DIS_SOFT											2					3							▨
	T.DIS_TEST																3							▨
	T.DIS_TOOLS	2															3							▨
	T.MOD_DEL												1							1		1		▨
	T.MOD_DESIGN	2									2					2	3							▨
	T.MOD_DSOFT							2									3							▨
	T.MOD_PHOTOMASK									2							3							▨
	T.MOD_SOFT											2					3							▨
	T.T_DEL												1											▨
	T.T_PHOTOMASK									2							3							▨
	T.T_PRODUCT								3								3							▨
	T.T_SAMPLE	2							3								3							▨
9911	T.DIS_DEL1																				1			▨
	T.DIS_DEL2														1									▨
	T.DIS_ES1			1																1		1		▨
	T.DIS_TEST_ES			1									1							1				▨
	T.MOD																			1		1		▨
	T.MOD_DEL.1																				1			▨
	T.MOD_DEL.2														1									▨
	T.T_SAMPLE2																						1	▨
	T.T_TOOLS			1																				▨
0001	T.APP_DISC	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	×
Assumptions																								
9806	A.DEV_ORG			1									1							1				▨
	A.DLV_AUDIT				4～7																			▨
	A.DLV_PROTECT					4～7																		▨
	A.DLV_RESP						4～7																	▨
	A.SOFT_ARCHI			1										1										▨
	A.USE_DIAG																	7						▨
	A.USE_PROD														4～6									▨
	A.USE_SYS																		7					▨
	A.USE_TEST														4～6									▨
0001	A.APPLI_CONT	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	4～7

Security Objectives for the TOE (Mapping from Threats)

		9806							9911		0001							
Threats	Objectives	CLON	DIS_ MECHANISM	DIS_ MEMORY	FLAW	MOD_ MEMORY	OPERATE	TAMPER	DIS_ MECHANISM2	TAMPER _ES	EFFECT _L	EFFECT _R	LOAD	REMOVE	RESOURCE	ROLLBACK	SECURITY	SEGREGATE
9806	T.CLON	4～7		4～7					4～7									
	T.DIS_DESIGN		4～7					4～7										
	T.DIS_DSOFT			4～7				4～7										
	T.DIS_SOFT			4～7				4～7										
	T.DIS_TEST			4～7				4～7										
	T.MOD_DESIGN				4～7		4～7	4～7										
	T.MOD_DSOFT				4～7	4～7	4～7	4～7										
	T.MOD_SOFT				4～7	4～7	4～7	4～7		4～7								
	T.T_PRODUCT						4～7											
	T.T_SAMPLE						4～7											
9911	T.DIS_ES2			4～7	4～7		4～7		4～7	4～7								
	T.MOD_EXE	4～7			4～7	4～7	4～7			4～7								
	T.MOD_LOAD	4～7			4～7	4～7	4～7			4～7								
	T.MOD_SHARE	4～7			4～7	4～7	4～7			4～7								
	T.T_CMD				4～7	4～7	4～7			4～7								
	T.T_ES				4～7	4～7	4～7			4～7								
0001	T.APP_CORR										4～7							
	T.APP_DISC																4～7	
	T.APP_MOD																	4～7
	T.APP_READ																	4～7
	T.APP_REMOVE													4～7				
	T.DEL_REMOVE											4～7						
	T.ERR_REMOVE													4～7				
	T.LOAD_APP										4～7		4～7					
	T.LOAD_MAN												4～7					
	T.LOAD_MOD																4～7	
	T.LOAD_OTHER										4～7							
	T.RESOURCES														4～7	4～7		

Security Functional Requirements (Mapping from Security Objectives)

			9806							9911		0001								カード名
		objective	CLON	DIS_ MECHANISM	DIS_ MEMORY	FLAW	MOD_ MEMORY	OPERATE	TAMPER	DIS_ MECHANISM2	TAMPER _ES	EFFECT _L	EFFECT _R	LOAD	REMOVE	RESOURCE	ROLLBACK	SECURITY	SEGREGATE	
9806	EAL4 requirements					X														
	FIA_UAU.2	User authentication before any action	P	X	X		X	X	X											
	FIA_UID.2	User identification before any action	P	X	X		X	X	X											
	FIA_ATD.1	User attribute definition	P	X	X		X	X	X											
	FPT_TST.1	TOE security functions testing					X	X												
	FDP_SDI.1	Stored data integrity monitoring					X													
	FMT_MOF.1	Management of security functions behaviour						X												
	FMT_MSA.1	Mnagement of security attributes						X										requirements		
	FMT_SMR.1	Security roles						X												
	FMT_MSA.3	Static attribute initialisation						X												
	FDP_ACC.2	Complete access control	P	X	X		X	X												
	FDP_ACF.1	Security attribute based access control	P	X	X		X	X												
	FDP_IFC.1	Subset information flow control	P	X	X		X	X												
	FDP_IFF.1	Simple security attributes	P	X	X		X	X												
	FAU_SAA.1	Potential violation analysis	P					X												
	FPR_UNO.1	Unobservability	P	X	X		X	X	X											
	FPT_PHP.2	Notification of physical attack	P	X	X		X	X	X											
	FPT_PHP.3	Resistance to physical attack	P	X	X		X	X	X											
9911	EAL4 requirements					X														
	FAU_SAA.1	Potential violation analysis			X		X	P		P	X									
	FCS_CKM.3	Cryptographic key access	P		P		P	P			X									
	FCS_CKM.4	Cryptographic key destruction	X		P		P	P			X									
	FCS_COP.1	Cryptographic operations	P		X						X									
	FDP_ACC.2	Complete access control	P		X		P	P		X	X									
	FDP_ACF.1	Security attribute based access control	P		X		P	P		X	X									
	FDP_DAU.1	Basic Data Authentication	P				X	P			X									
	FDP_ETC.1	Export of User Data without Security Attributes			X		P													
	FDP_ITC.1	Import of user data without security attributes			X															
	FDP_RIP.1	Subset residual information protection			P						X									
	FDP_SDI.2	Stored data integrity monitoring and action					X	P												
	FIA_AFL.1	Basic authentication failure handling	P				P	P			X									
	FIA_ATD.1	User attribute definition					P	P			X									
	FIA_UAU.1	Timing of authentication	P		X		X				X									
	FIA_UAU.3	Unforgeable authentication	P		X		X				X									
	FIA_UAU.4	Single-use Authentication Mechanisms	P		X		X				X									
	FIA_UID.1	Timing of identification	P		X		X				X									
	FIA_USB.1	User-subject binding	P		X		X				X									
	FMT_MOF.1	Management of security functions behavior	P		P		P	X		X	X									
	FMT_MSA.1	Management of security attributes	P		P		P	P		X	X									
	FMT_MSA.2	Secure security attributes	P		P		P	P		X	X									
	FMT_MSA.3	Static attribute initialisation	P		P		P	P		X	X									
	FMT_MTD.1	Management of TSF data	P		X		X													
	FMT_SMR.1	Security roles						X			X									
	FPR_UNO.1	Unobservability	X		X		X	P			X									
	FPT_FLS.1	Failure with preservation of secure state									X									
	FPT_PHP.3	Resistance to physical attack	X		X		X	X		X	X									
	FPT_SEP.1	TSF domain separation			X					X	X									
	FPT_TDC.1	Inter-TSF data consistency					X				X									
	FPT_TST.1	TSF testing					X	P												
0001	FAU_APP.1	Security alarms														X				
	FAU_SAA.1	Potential violation analysis														X				
	FCO_NRO.2	Enforced proof origin												X	X			X		
	FCS_CKM.4	Cryptographic key destruction												X	X			X		
	FCS_COP.1	Cryptographic operations												X	X			X		
	FDP_ACC.2	Complete access control												X	X				X	
	FDP_ACF.1	Security attribute based access control										X	X						X	
	FDP_IFF.1	Simple security attributes												X						
	FDP_ITC.1	Import of user data without security attributes																X		
	FDP_RIP.1	Subset residual information protection													X					
	FDP_ROL.1	Basic rollback															X			
	FIA_UID.1	Timing of identification												X	X					
	FMT_MSA.1	Management of security attributes												X	X					
	FMT_MSA.2	Secure security attributes												X	X					
	FMT_MSA.3	Static attribute initialisation												X	X					
	FMT_MTD.1	Management of TSF data																	X	
	FMT_MTD.2	Management of limits TSF data												X		X				
	FMT_REV.1	Revocation																	X	
	FMT_SMR.1	Security roles												X	X					
	FPT_FLS.1	Failure with preservation of secure state										X	X				X		X	
	FPT_RCV.4	Function recovery										X	X				X			
	FPT_RVM.1	Non-bypassability of the TSP												X	X				X	
	FPT_SEP.1	TSF domain separation																	X	
	FRU_RSA.1	Maximum quotas														X				

X: relevant P: partial

Proposal1:It will be more clear to explain the "partial" in detail. Why it is partial or the scope of the part.

Proposal2:It will be better to clarify the functinal requirments for TOE(figure1) adding * or something, to other functional requiremnets in three PPs. .

○: 問題なし
×: 問題有り
?: 調査中

Japan ’s Next Project

PP for the Japanese next generation smartcard

Will be issued until summer 2001
With application program loading function
Contactless or with contact
According to specification for Japanese e-government purchasing
Concerning JICSAP ver2.0 specification
« Threats Analysis » is already started March 2001