

PD02-0740-023



2002. 10. 5.



ETRI
한국전자통신연구원

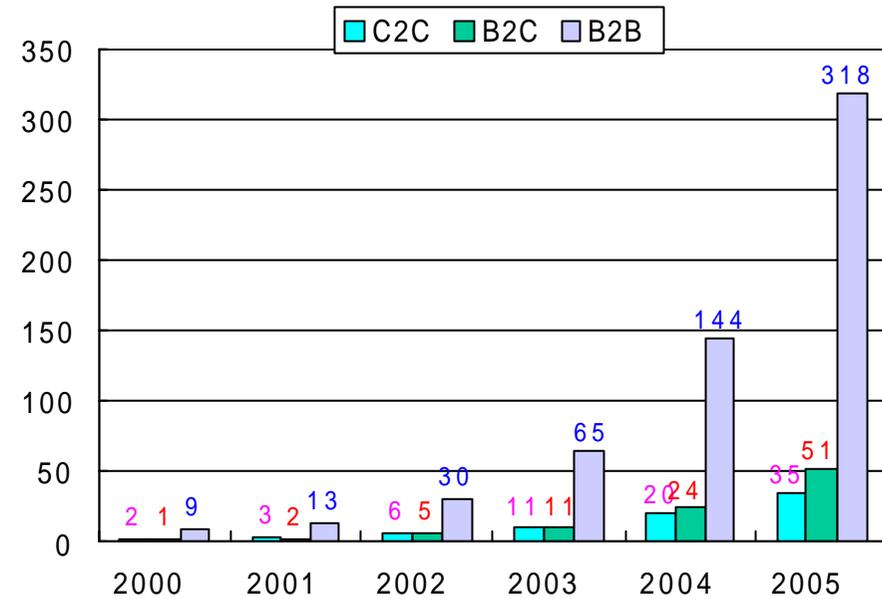
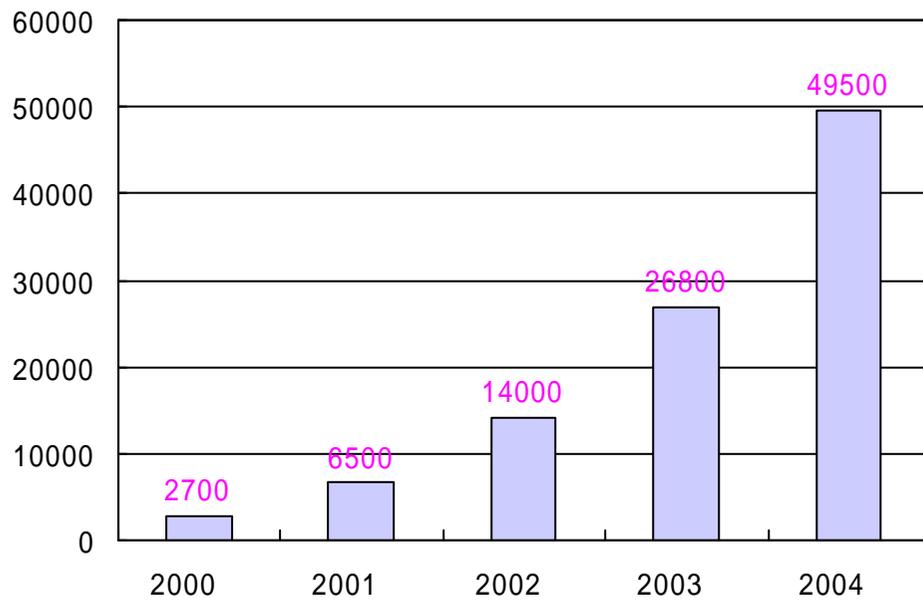
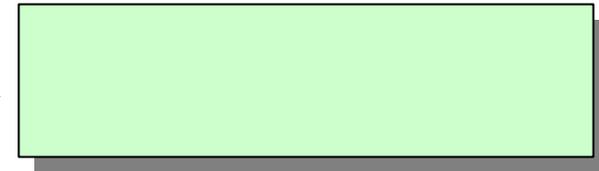
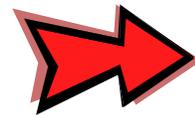
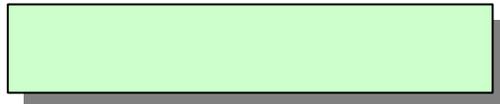
.

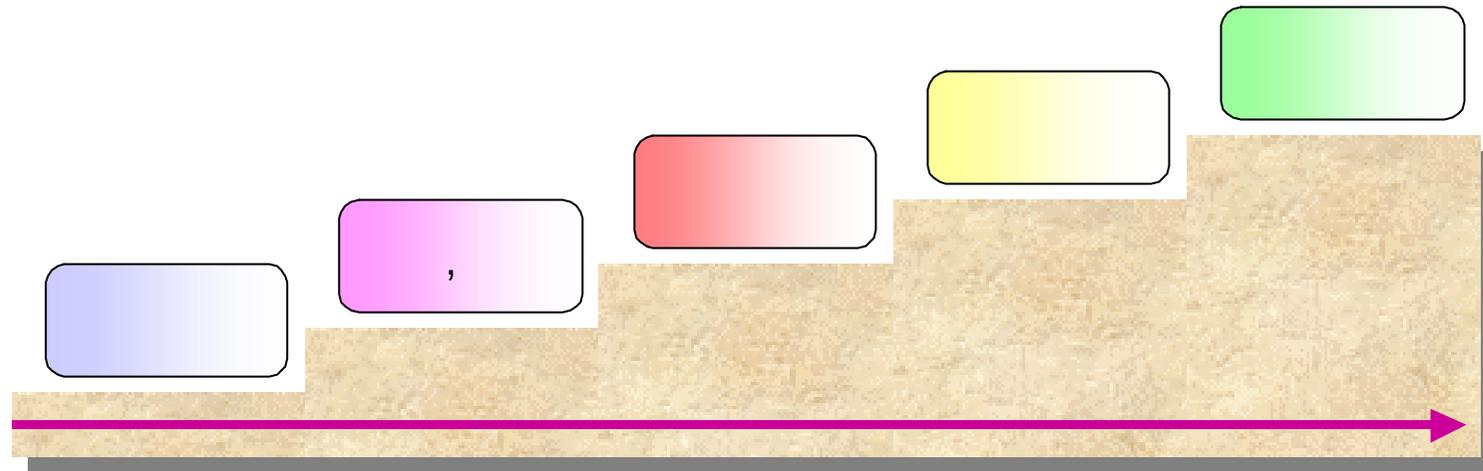
SAM

: IC



IT +





> (,)
>
>

>
>
>

가 /

가 가

가 , IC



, ,

가

,

가

가

가

,

가

,

가 가

가

.

가 : /
- : 가
- :
: / / /
: (\$5 ~)/ (\$0.01 ~ \$10)
, : / /
: /

						IC	
		X	X	O	O	X	O
가		(가)	()	()	O		O
		O	X	O/X	X	O	O
		O	X	X	X	O	O
	가	O	-			O	O
가		X	-	-	X	O	O

가 => / 가

,

가

: , , tamper resistant ,
: 가 , , ,
: ,

(Independence)

가 ,

, 가 (Security)
,
가 ,
/ ,

(Privacy, Untraceability : , 가)
가 가
: /
가 , ,

(Off - line)

,

(Transferability)

가

가

가 (Divisibility)

,

,

,

가



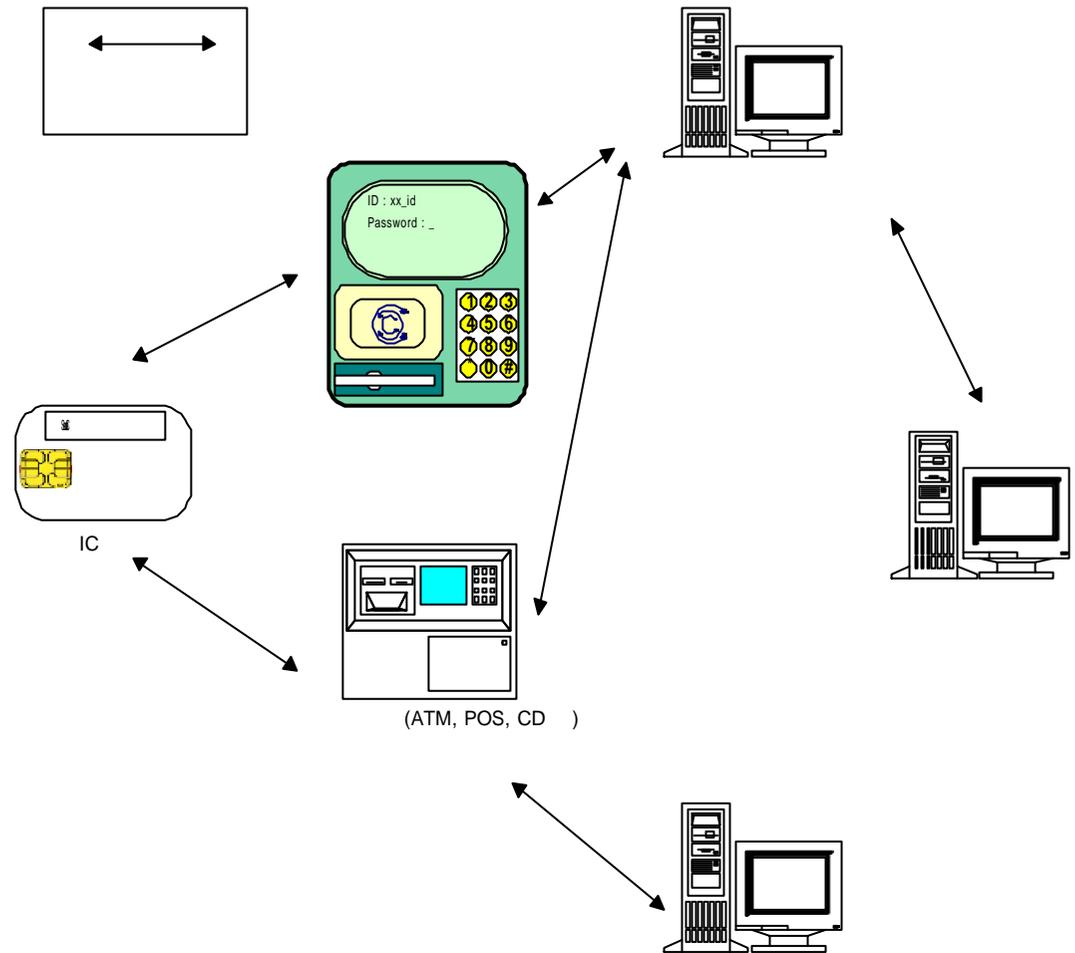
ETRI
한국전자통신연구원

De facto
 CEPS (Common Electronic
 Purse Specification)
 EMV (Europay, Master, Visa)

IC

IC
 (Read-writer)
 (ATM)

Host Computer (,)
 ,)



IC

5

K-Cash

- , 가 , SEED
- : 2 - -

V-Cash

- , , VISA , NETS
- RSA, 3-DES

Mondex card

- Mondex Korea
- 80 , COEX,

Mybi

-
-

A-Cash

-
-

* NETS : Network For Electronic Transfers Singapore Private Limited

K - Cash(www.kftc.or.kr)

가
가

- 20 가 7 가
- 가 가
- CD, ATM
(SEED)
가

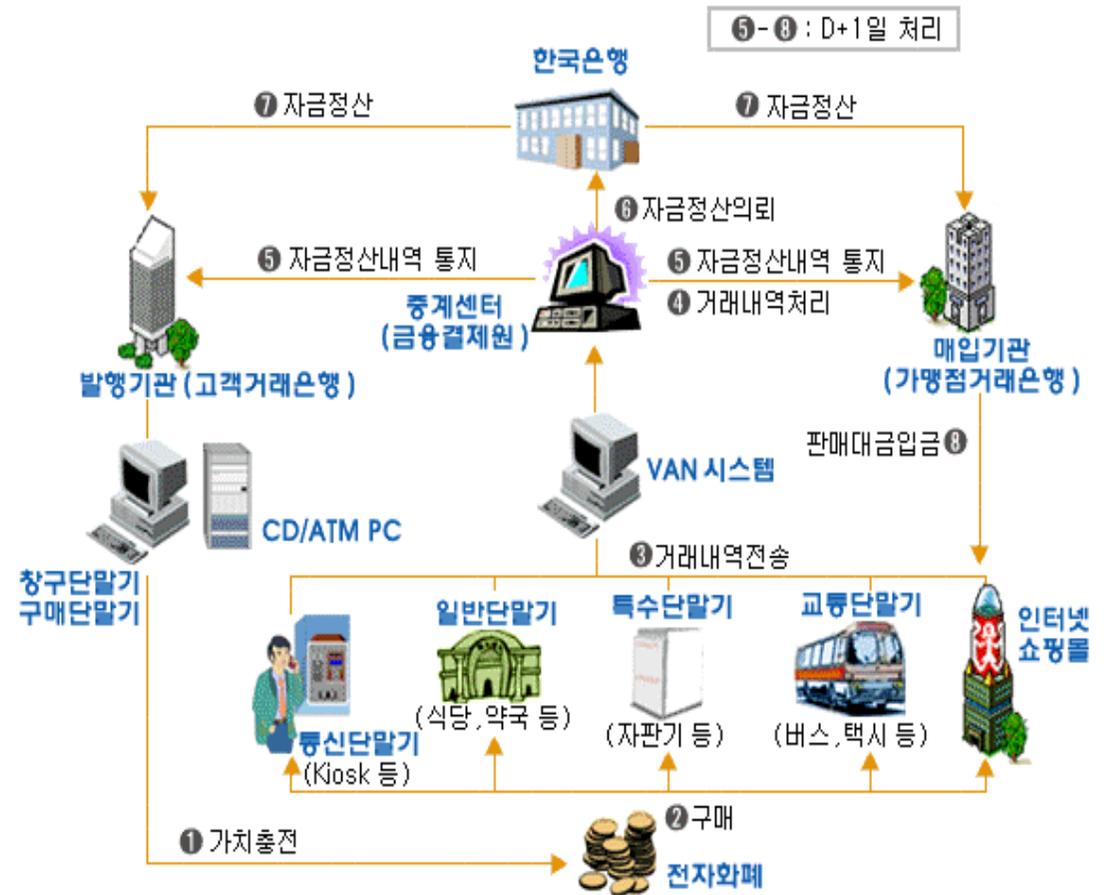
“ IC ” CEPS

K - Cash

가 ()
 가 , ()
 가 ()
 가 ()
 가 가 (~)

CD/ATM

PC



V-cash (www.visacash.co.kr)

, SK, Visa 18 ()가

Singapore NETS ,

CEPS(Common Electronic Purse Specification)

, ,
가
가
가

RSA, 3-DES

Mondex (www.mondexkorea.com)

COEX , , , Gemplus, 10
5
가
RSA, 3-DES 가 (*ITSEC E6)

A - Cash (www.a-cash.co.kr)

	, LG,	가	가	가	IC	Multi Application
	(COS)	IC				
- IC		IC	가	가	.	
-	,		2-3		가	
-	,	,				A - CASH
-	,	,		,		A - CASH
-						



SAM



ETRI
한국전자통신연구원

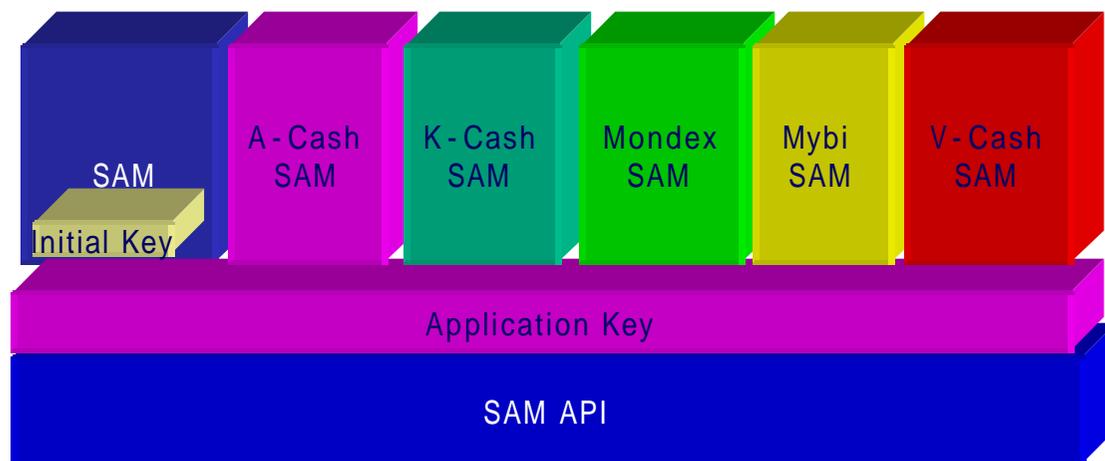
(' 99. 8.)

: INTEC, C&C()
: INTEC
: INTEC, A - Cash
: K - Cash
: A - Cash
: A - Cash
:
, : Mybi
: K - Cash
: , Mybi
: INTEC

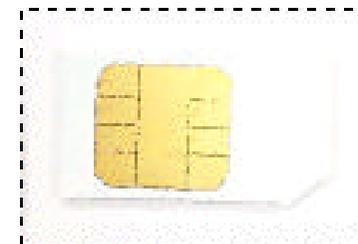
SAM

SAM : source
SAM :

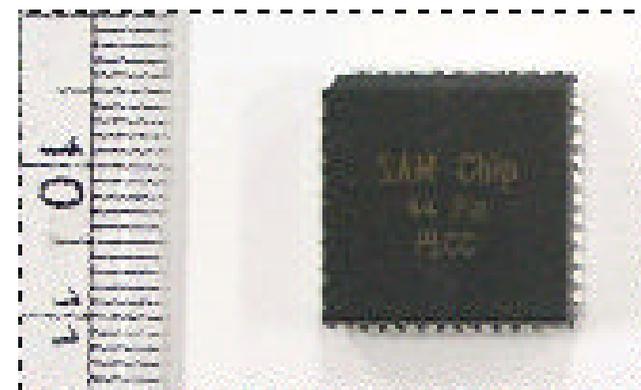
SAM



SIM-Type



PLCC-Type





: IC



IC (Smart Card)

IC

- H/W : , , I/O
- S/W : COS(Card OS), API, VM

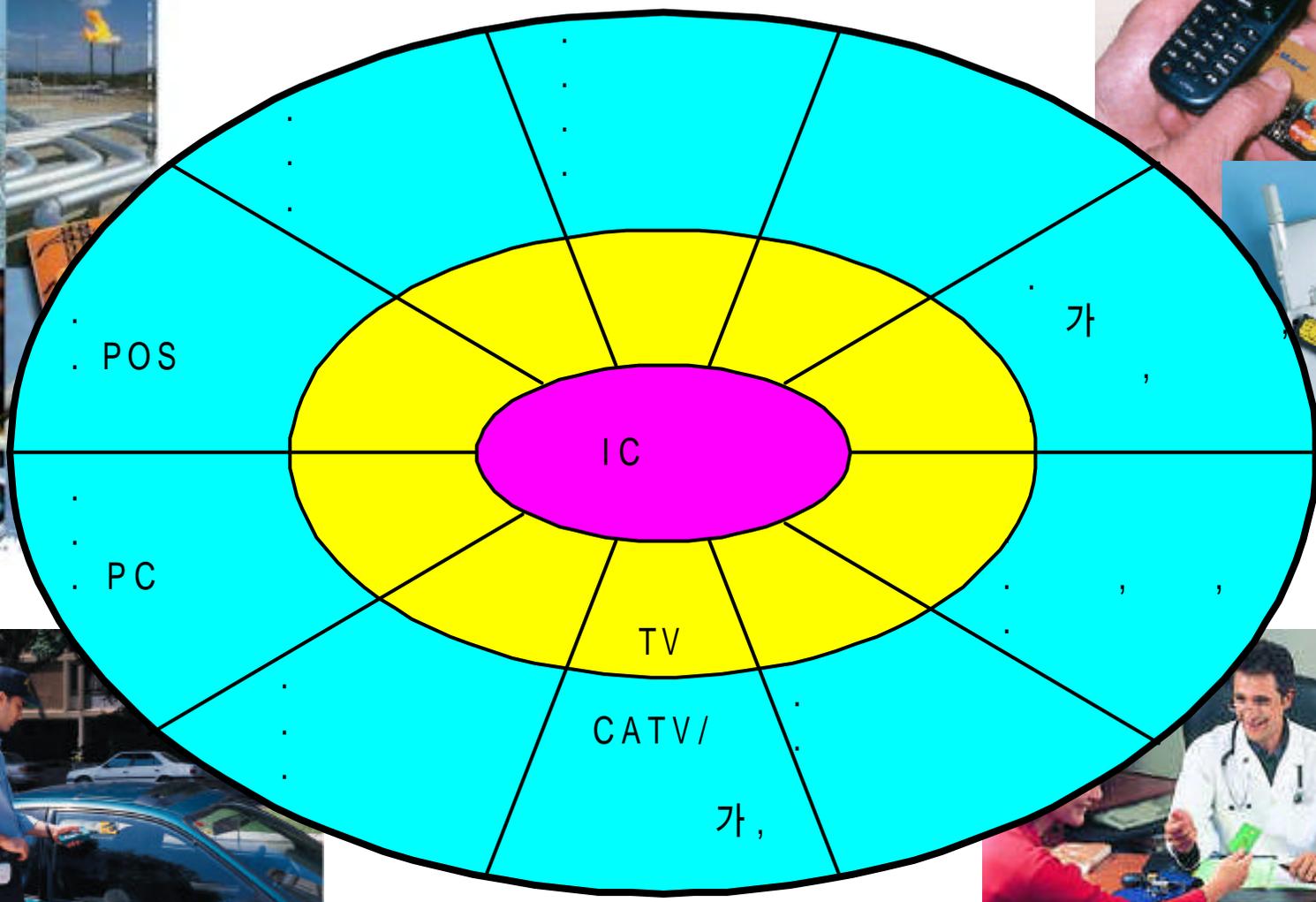
: IC ,

- (8)
- : , ,

IC

- : IC IC
- (Combi) : IC

IC



IC

(1)

(:)	2000	2001	2002	2003	2004	2005	2006	
Public Telecoms	1,030	1,134	1,261	1,390	1,495	1,545	1,570	7%
Wireless	353	512	663	794	901	977	1,045	21%
Financial Services	120	153	224	310	416	546	692	34%
Healthcare	70	110	136	167	200	231	265	26%
Pay-TV	33	51	71	91	113	137	161	31%
Transport/eTicketing	44	65	87	108	126	141	153	24%
Security/Access	15	21	32	46	61	79	97	37%
Retail/Royalty	30	38	47	54	61	67	72	16%
University	5	6	8	12	17	24	33	37%
Government	4	6	8	11	16	22	28	36%
Total	1,704	2,096	2,537	2,983	3,406	3,769	4,116	16%

Source : Datamonitor

- IC (Datamonitor)
 - 1) 2001 , IC 21
 - 2) 2006 : 41 IC 가
 - 3) 2000 ~2006 IC 16%

IC

(2)

(:)	2000	2001	2002	2003	2004	2005	2006	
Public Telecoms	206	251	319	395	437	427	377	11%
Wireless	1,482	2,149	2,785	3,335	3,784	4,103	4,389	20%
Financial Services	276	352	515	713	957	1,256	1,592	34%
Healthcare	105	196	251	319	394	461	536	31%
Pay-TV	108	171	239	307	383	464	546	31%
Transport/eTicketing	21	57	96	132	162	184	199	45%
Security/Access	28	38	64	97	134	179	224	41%
Retail/Royalty	8	15	22	27	32	35	38	30%
University	13	17	22	33	47	68	94	39%
Government	8	10	14	21	34	47	61	39%
Total	2,255	3,256	4,327	5,379	6,364	7,224	8,056	24%

Source : Datamonitor

- IC (Datamonitor)
 - 1) 2000 , Wireless가 66% , 2006 , 54%
 - 2) 2006 : Wireless, Financial Service, Pay-TV, Healthcare가

IC

32 bit

-

MMU

-

MMU

Coprocessor
RSA

-

IC

가

가

, , ,

가

IC

IC

IC 가 IC 가

: ISO/IEC 7816, 14443

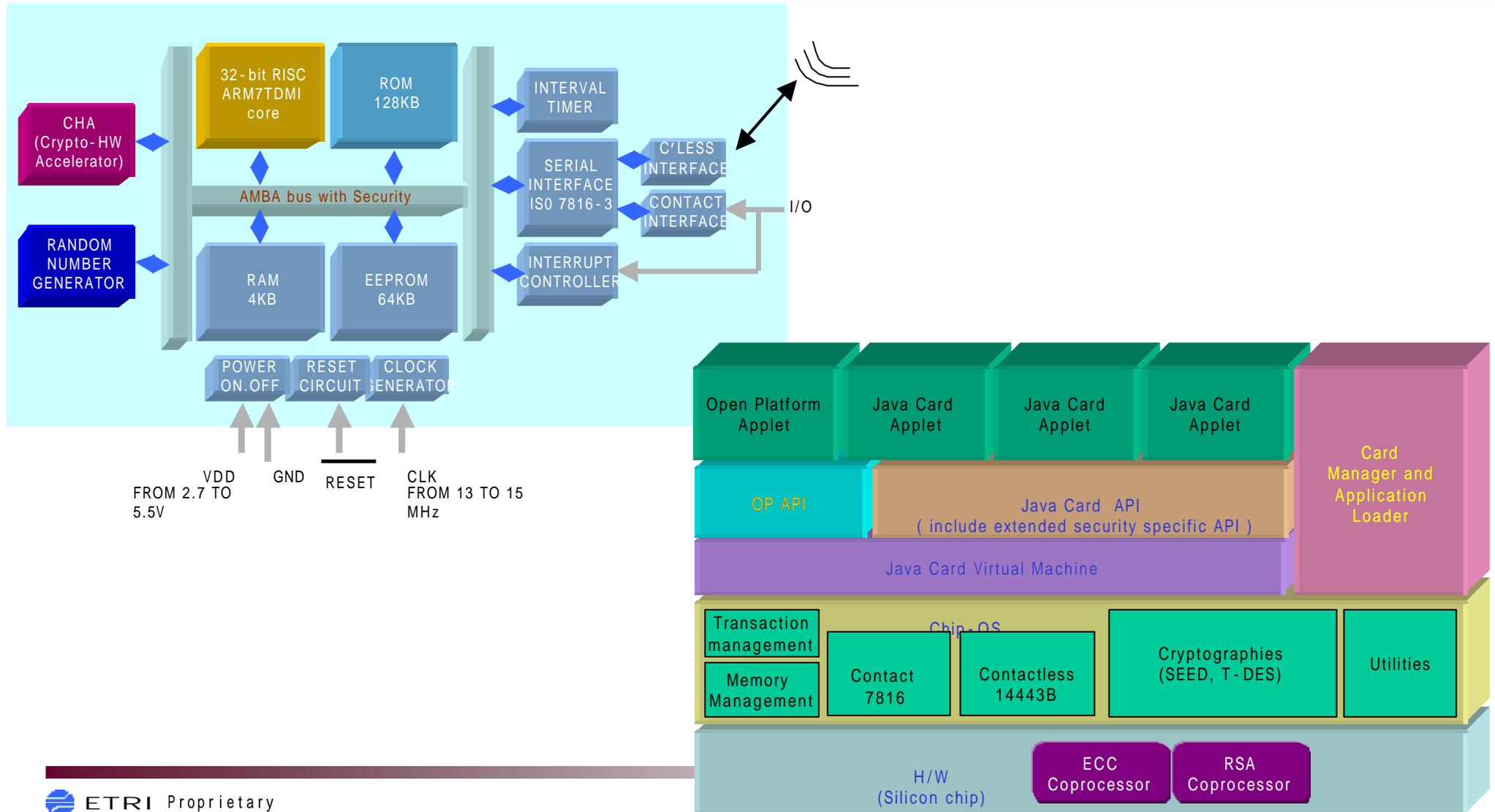
CPU : 32bit ARM processor

: RSA, ECC, SEED, DES

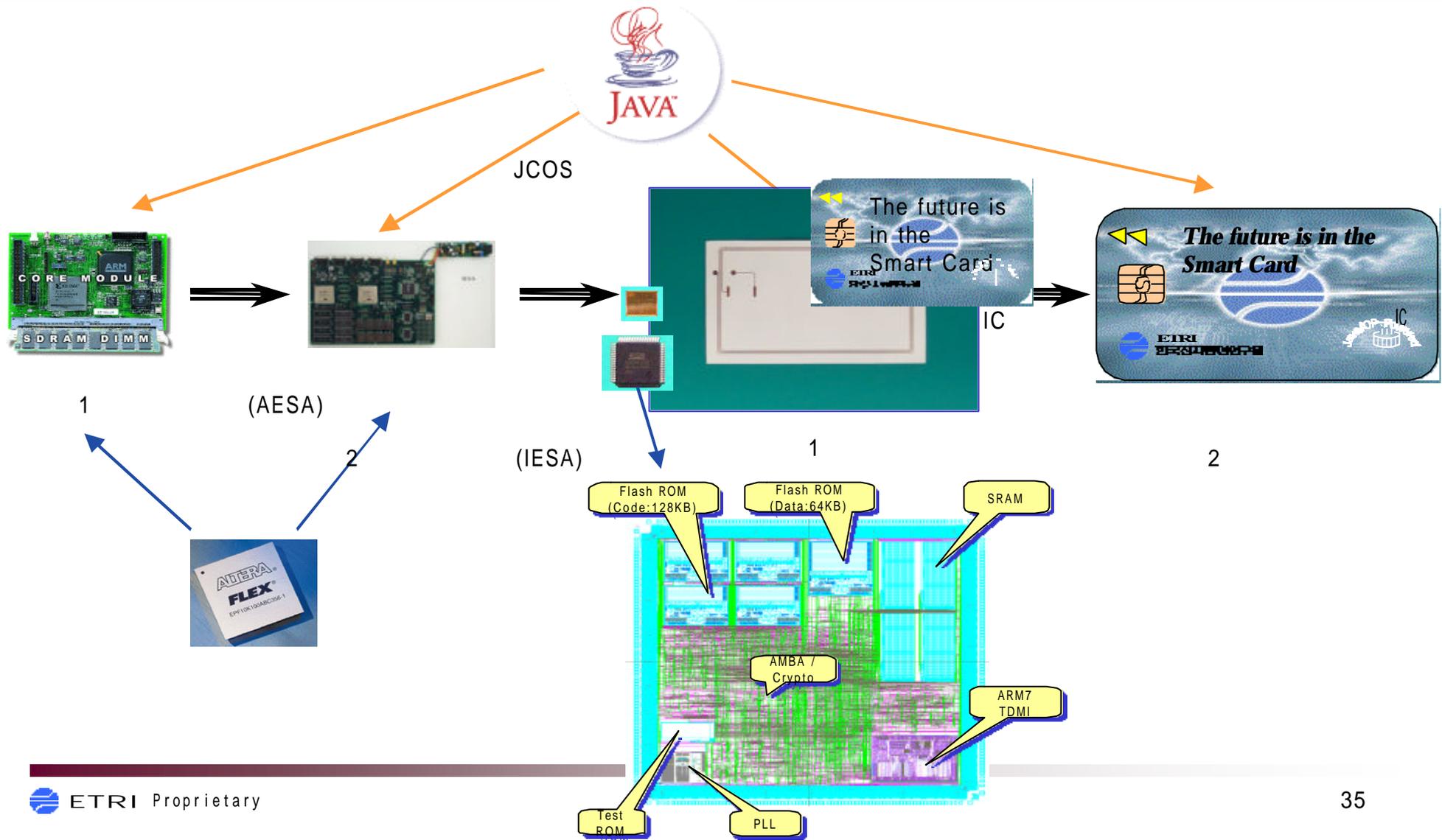
COS : Javacard 2.1

RF Interface : ISO/IEC 14443 Type B

IC



IC





∴ , , ,
∴ , ,
∴ , , ,

IC

- ,

-

- ()

- IC

- 가

-

가

—
가
,
가
,
— IC , ,