

# KSignKMI WHITEPAPER

2002.6.24

1(KMI)

 **KSIGN** (주) 케이사인

# KSignKMI WHITEPAPER V1.0

1. KSIGNKMI	.....	3
2. KSIGNKMI	.....	5
2.1	(KEY ESCROW SERVICE) .....	5
2.2	(KEY RECOVERY SERVICE).....	6
2.3 PKI	(PKI ROAMING SERVICE) .....	6
2.4	.....	7
2.5	.....	7
3. KSIGNKMI	.....	7
4. KSIGNKMI	.....	7

## 1. KSignKMI

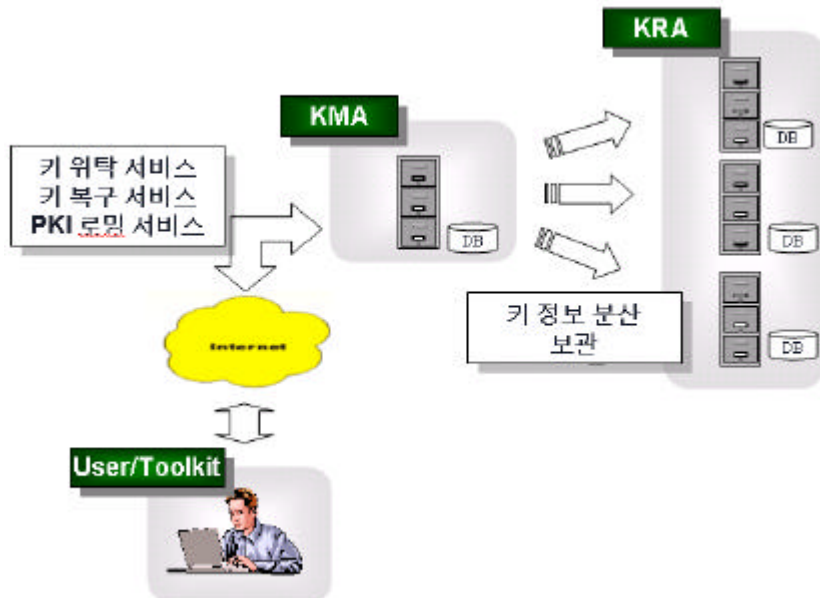
KSignKMI

PKI  
가,  
,  
가 가 ,  
가 가

. KSignKMI 가  
가  
KSignKMI E-Commerce

가

1-1 KSignKMI



1-1 KSignKMI

# KSignKMI WHITEPAPER V1.0

KSignKMI PKI

가

.

- 
- 
- PKI
- 
- 
- 
- KRA

Escrow

KSignKMI

가

.

## 2. KSignKMI

KSignKMI PKCS#7(Cryptographic Message  
Syntax Standard)

KSignKMI

### 2.1 (Key Escrow Service)

KSignKMI User/Toolkit  
KMA  
User/Toolkit (Hard Disk,  
Smart Card, Floppy Disk)

ActiveX  
PKCS#7(Cryptographic  
Message Syntax Standard)

KMA

RFC2459(Internet X.509 Public Key Infrastructure  
Certificate, and CRL Profile)

CRL(Certificate Revocation List)

가

(Self-sign)

CRL

. CRL

, CRL



# KSignKMI WHITEPAPER V1.0

## 2.4

KSignKMI

KRI

## 2.5

KSignKMI

KSIGN

KCASE

0-1KSignKMI

Cryptography

	RSA, KCDSA, DSS, ECC
	DES, DES-EDE SEED, AES, RC2/4/5, IDEA, CAST
	SHA-1, SHA, MD2/4/5, HAS160

## 3. KSignKMI

- 가 가
- 가
- , B2B, B2C

## 4. KSignKMI

KSignKMI KSIGN 가

. KMA,KRA KSignKMI

User/Toolkit x86 MS Windows 가

KSignKMI Toolkit Microsoft® Windows UNIX

DLL . ATL(Active Template Library)

# KSignKMI WHITEPAPER V1.0

가 ,  
 가 .  
 ! . KSignKMI

## KSignKMI KMA,KRA

<b>Platform</b>	SUN, IBM, HP, COMPAQ
<b>O/S</b>	32Bit O/S
<b>Database</b>	Oracle DBMS 8.0.5 (4User )
<b>SmartCard Reader</b>	ISO 10373 (RS-232C)

## KSignKMI Toolkit for C

	x86
( )	MS Windows 98/NT/2000/XP
<b>Application</b>	ATL/COM

0-1 KSignKMI