

PKI

I. , PKI

가. PKI (Public Key Infrastructure)

- (CA) (Certificate)
- 3 , ,

. PKI

- CA 가
-
-

II. PKI

가. PKI



. PKI

(CA)	- Certificate Authority - , ,
	- - LDAP -
(RA)	- Registration Authority -
	-

, () 5 , (),

. PKI

CRL	- Certificate Revocation List - CA가 CRL
OCSP	- Online Certificate Status Protocol - CRL - OCSP - , - OCSP « »
SCVP	- Simple Certificate Validation Protocol - , CRL - SCVP « »

III. PKI

가. PKI

→ [+] (, , SSL)	
→ [+]	
(PKI)	
(, , B2B, B2C, PG, , ...)	

. PKI

Six e-security needs		e-security technologies	
Access Control()	→	PKI-KMI-PMI	→ PKI provides All
Confidentiality()	→		
Integrity()	→	/	
Authentication()	→		
Authorization()	→		
Non-repudiation()	→		

IV. PKI

