# SECURITY MODEL OF CMP

## Message Authentication

Security of PKI Messages are based on Shared Secret Keys (with HMAC) or Asymmetric Keys

We are using RSA Key Pairs to sign PKIMessage. As long as Clients keep their private keys secret, PKI Message Signature will be used to verify Request Authentication for EKK. CA trusts Certificate of Key Pair which signs PKI Message and CA validates that certificate. And CA signs Response Messages so Clients can verify Responses. Nonce and TransactionIDs are used in Header also(to avoid various type of attacks, see security considerations in RFC 4210)

PKI Message

Header

Body

Consists of multiple Requests (x509, CVC etc)

Signature of Header+Body

## Request Security

Body may consists of various type of Requests(Certification, Revocation, Key Update, Key Recovery etc.) in EKK we use Certification Request Types.(See RFC 4211 for details). Normally Requests&Responses are encoded into PKIMessage directly.

* We do not use POP(proof of possession), since keys are generated in Server side.
* We use Protocol Encryption Keys to carry Private Keys between Server and Client.
* Client Side is responsible to keep Private Key of Protocol Encryption Key secure.
* Currently we support RSA key pairs as Protocol Encryption Key

CA Encrypts Private Key with AES256\_CBC method.(Using 16byte iv, 32 byte Symmetric Key). And CA encrypts(RSA\_PKCS1) AES256 Symmetric Key with Requestor Public Key. And CA creates Encrypted Content with “iv”, Encrypted Symmetric Key, Algorithm Identifier, Encrypted Value of Private Key. See RFC 4211 for more details on Encrypted Value.

CA(Server Side)

EE(Client Side)

Each Request in PKI Message carry Public Key of Protocol Encyption

CA Encrypts Private Key with AES256\_CBC method. And Encrypt Simetric Key RSA\_PKCS1 using Protocol Encryption Key.

Confirm- Last Confirm