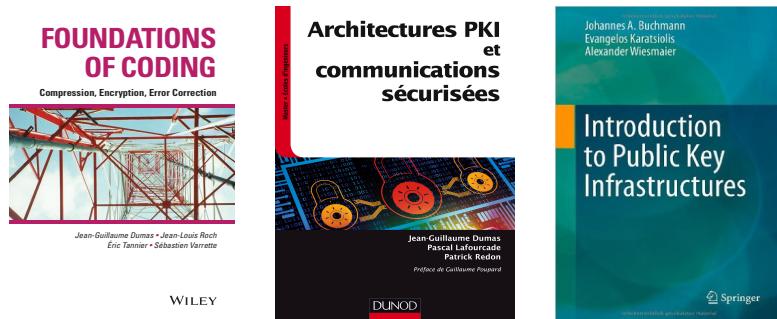
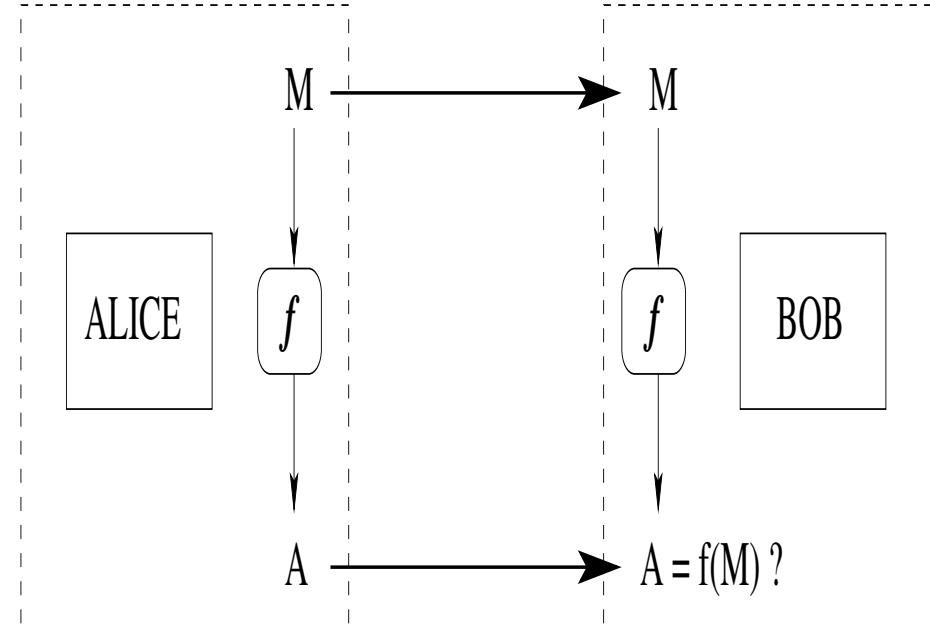
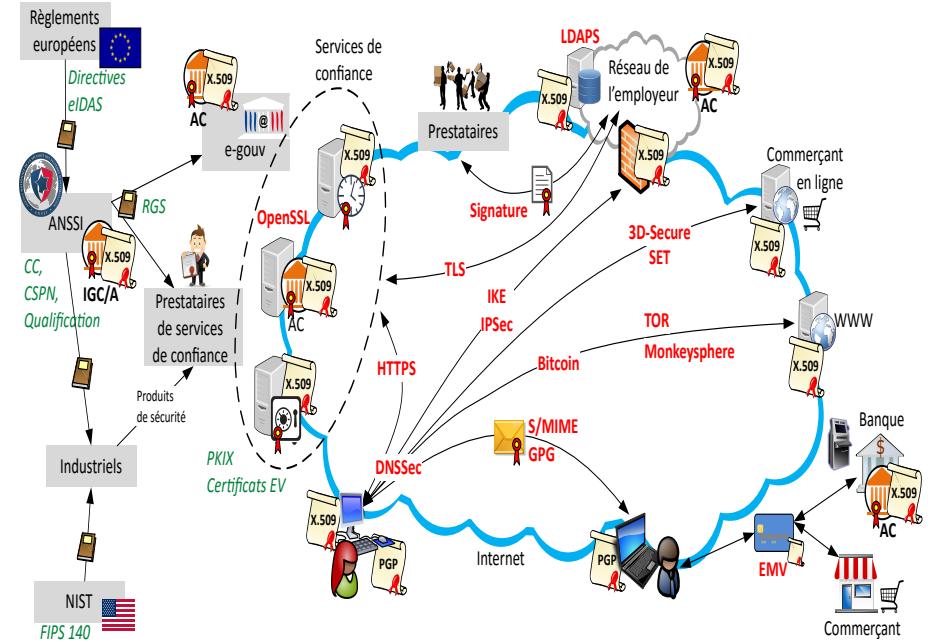
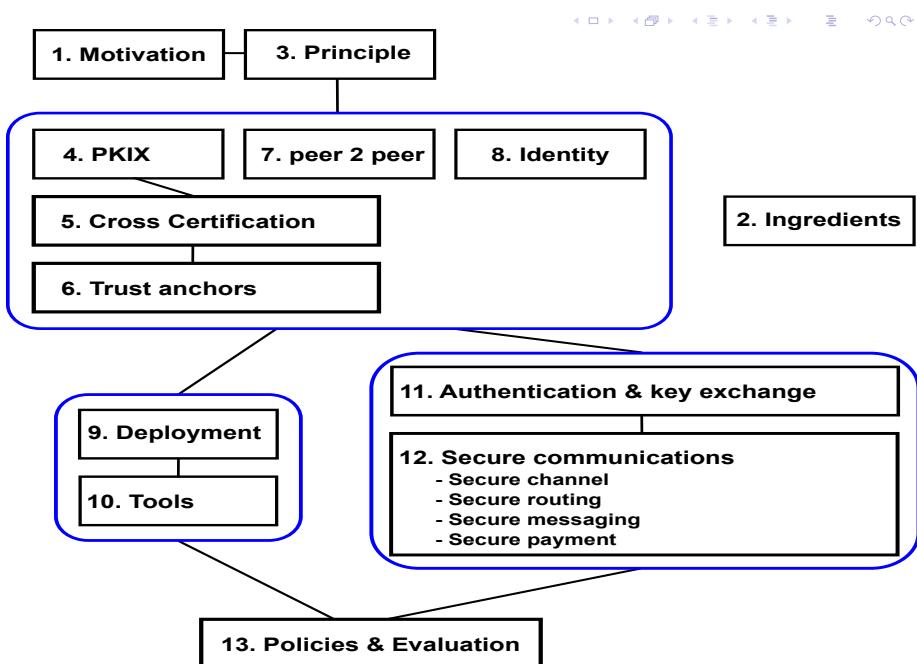
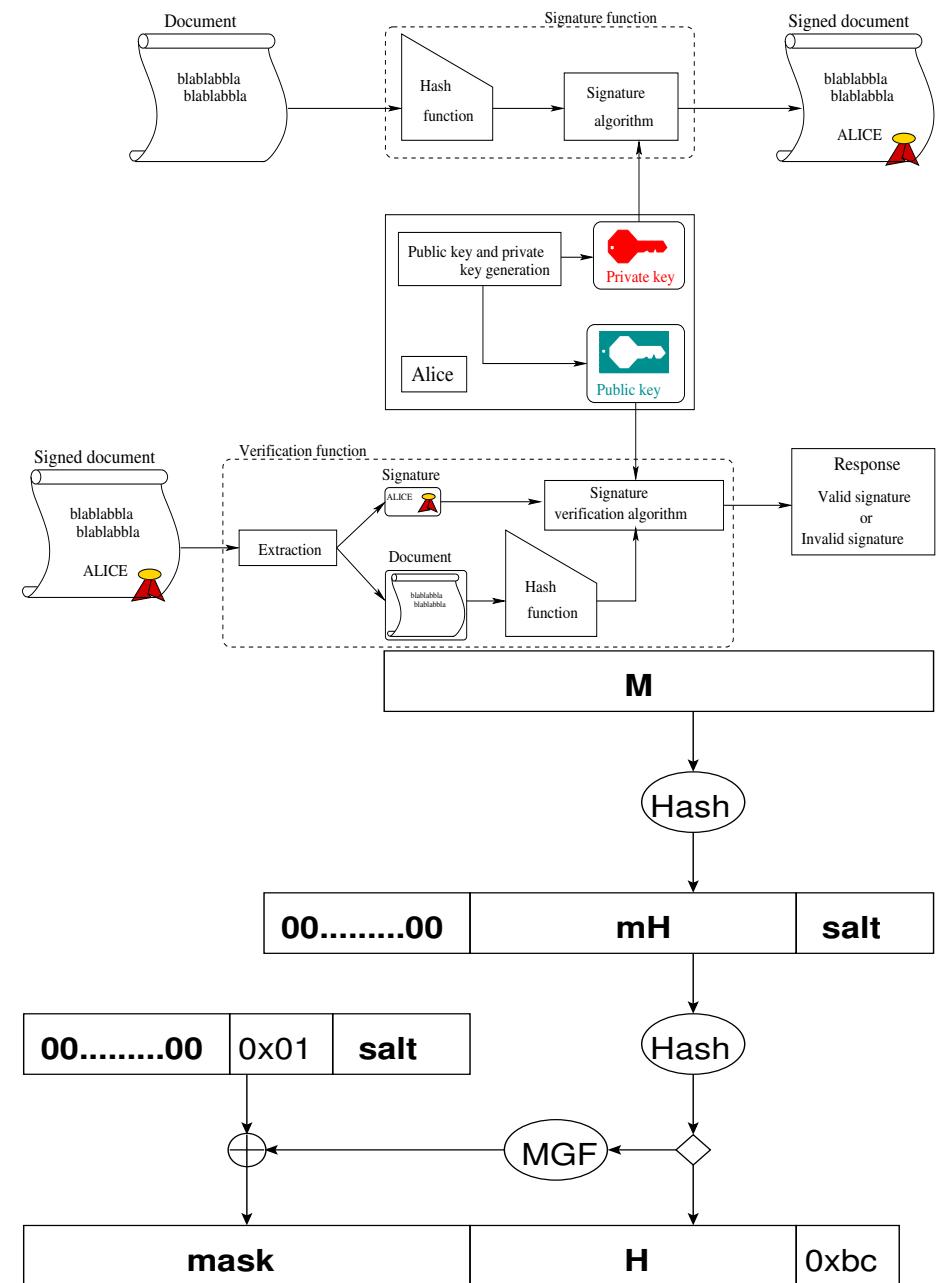
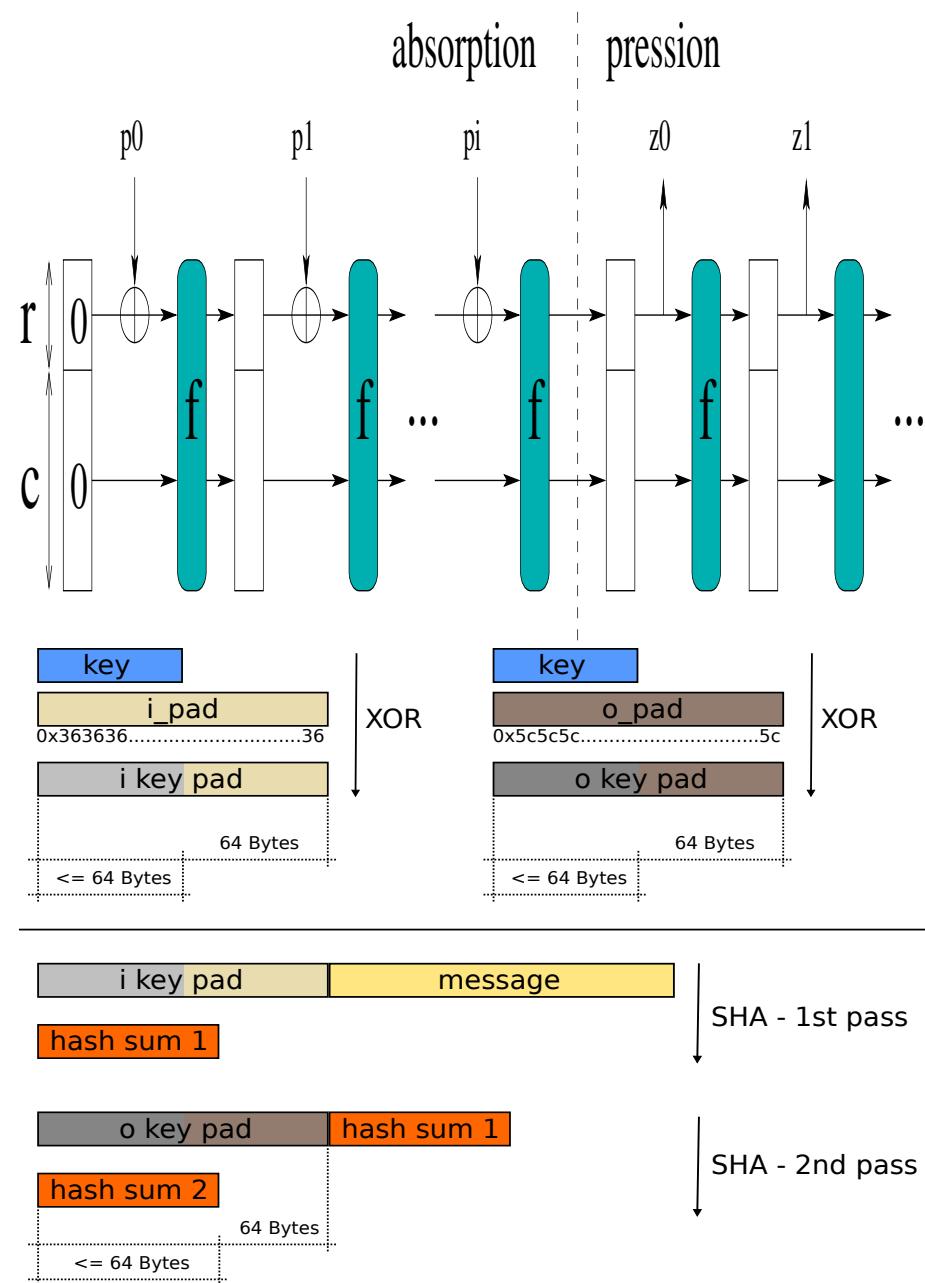


## PKI architectures: references

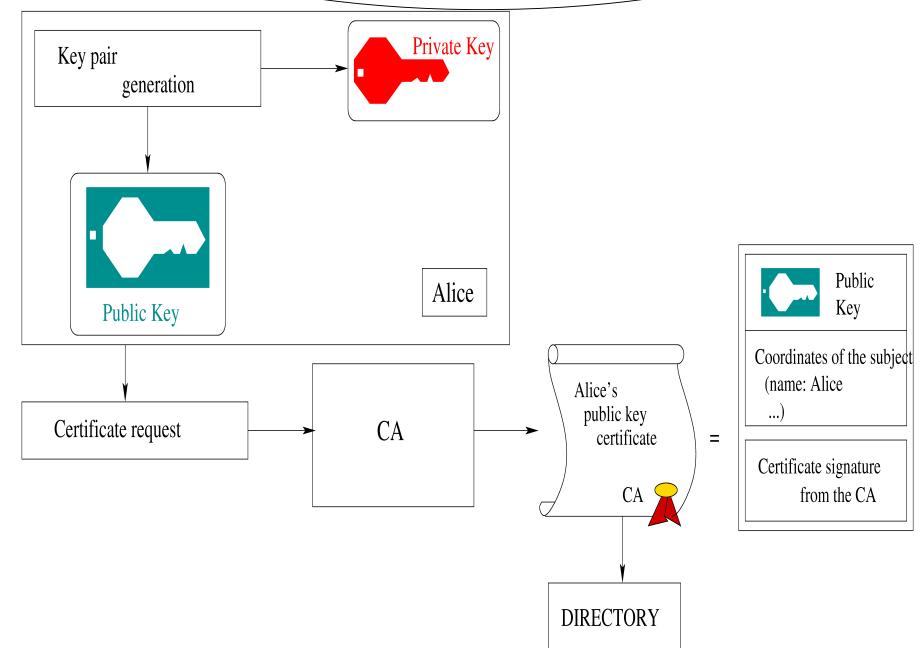
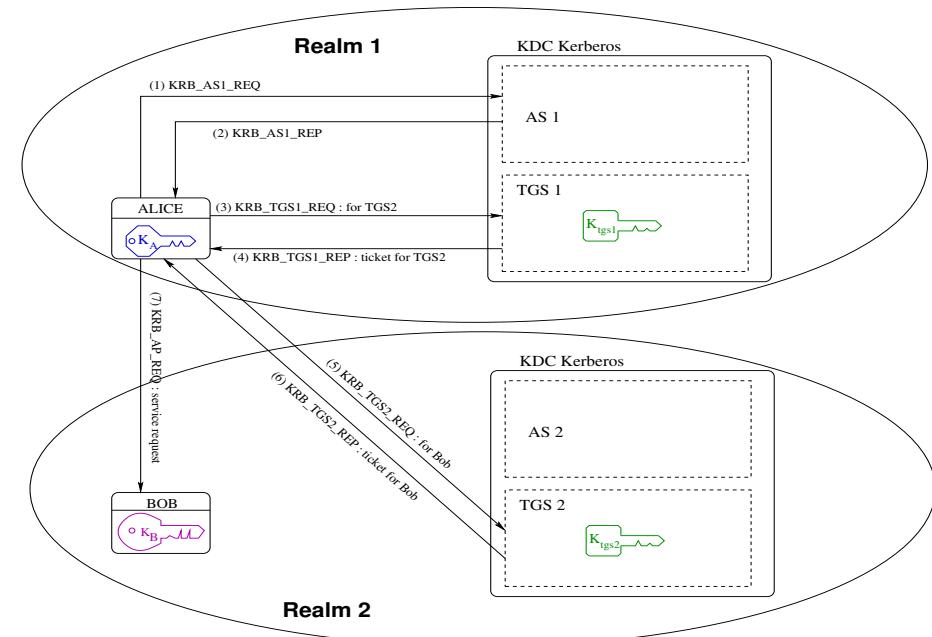
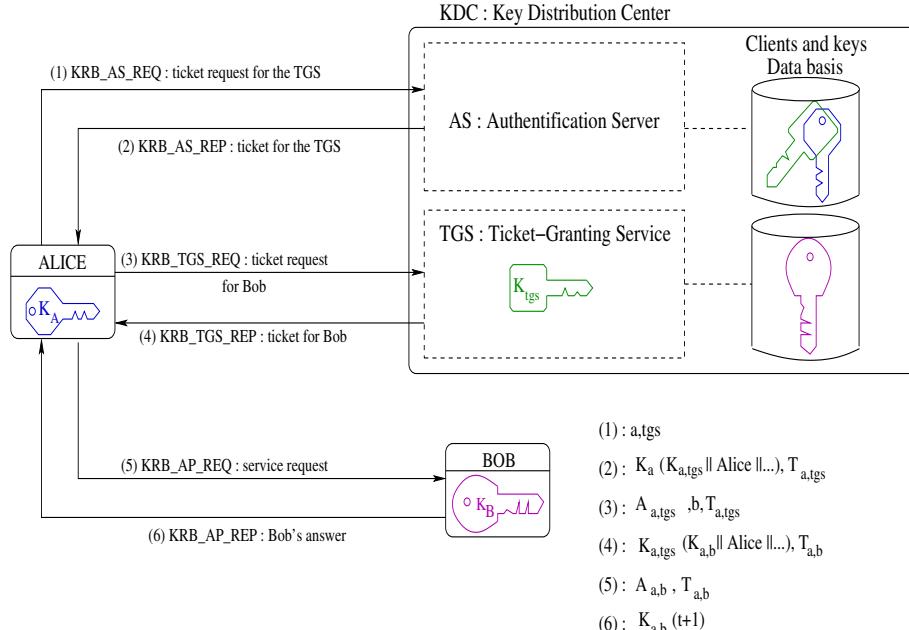


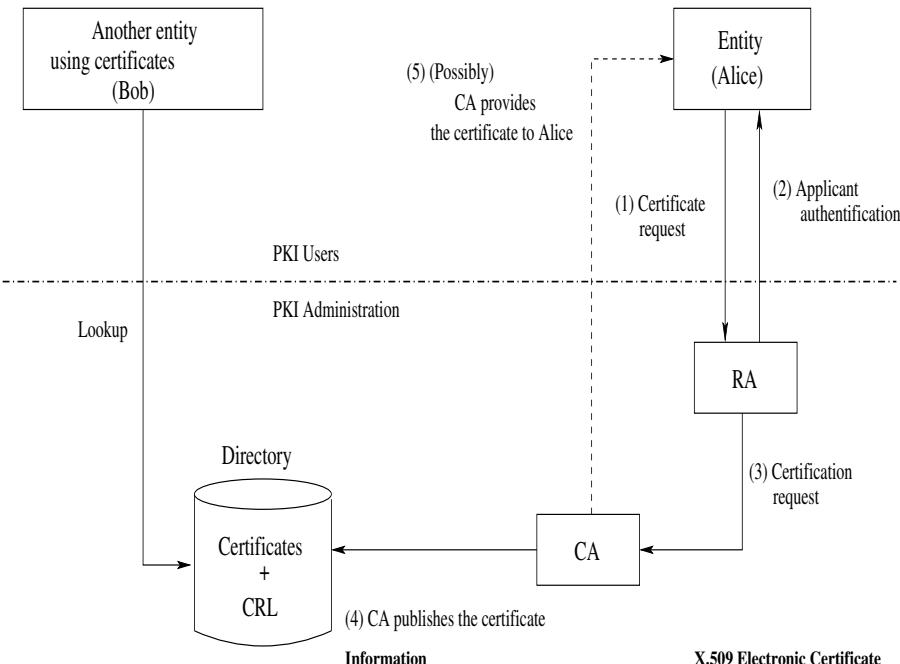
[ljk.imag.fr/membres/Jean-Guillaume.Dumas/Enseignements/PKI](http://ljk.imag.fr/membres/Jean-Guillaume.Dumas/Enseignements/PKI)





PKCS Standards Summary, From Wikipedia		
Version	Name	Comments
PKCS #1	2.1 RSA Cryptography Standard <sup>[1]</sup>	See RFC 3447. Defines the mathematical properties and format of RSA public and private keys (ASN.1-encoded in clear-text), and the basic algorithms and encoding/padding schemes for performing RSA encryption, decryption, and producing and verifying signatures.
PKCS #2	- Withdrawn	No longer active as of 2010. Covered RSA encryption of message digests; subsequently merged into PKCS #1.
PKCS #3	1.4 Diffie-Hellman Key Agreement Standard <sup>[2]</sup>	A cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.
PKCS #4	- Withdrawn	No longer active as of 2010. Covered RSA key syntax; subsequently merged into PKCS #1.
PKCS #5	2.0 Password-based Encryption Standard <sup>[3]</sup>	See RFC 2898 and PBKDF2.
PKCS #6	1.5 Extended-Certificate Syntax Standard <sup>[4]</sup>	Defines extensions to the old v1 X.509 certificate specification. Obsoleted by v3 of the same.
PKCS #7	1.5 Cryptographic Message Syntax Standard <sup>[5]</sup>	See RFC 2315. Used to sign and/or encrypt messages under a PKI. Used also for certificate dissemination (for instance as a response to a PKCS#10 message). Formed the basis for S/MIME, which is as of 2010 based on RFC 5652, an updated Cryptographic Message Syntax Standard (CMS). Often used for single-sign-on.
PKCS #8	1.2 Private-Key Information Syntax Standard <sup>[6]</sup>	See RFC 3208. Used to carry private certificate keypairs (encrypted or unencrypted).
PKCS #9	2.0 Selected Attribute Types <sup>[7]</sup>	See RFC 2985. Defines selected attribute types for use in PKCS #6 extended certificates, PKCS #7 digitally signed messages, PKCS #8 private-key information, and PKCS #10 certificate-signing requests.
PKCS #10	1.7 Certification Request Standard <sup>[8]</sup>	See RFC 2986. Format of messages sent to a certification authority to request certification of a public key. See certificate signing request.
PKCS #11	2.20 Cryptographic Token Interface <sup>[9]</sup>	Also known as "Cryptoki". An API defining a generic interface to cryptographic tokens (see also Hardware Security Module). Often used in single sign-on. Public-key cryptography and disk encryption <sup>[10]</sup> systems.
PKCS #12	1.0 Personal Information Exchange Syntax Standard <sup>[11]</sup>	Defines a file format commonly used to store private keys with accompanying public key certificates, protected with a password-based symmetric key. PFX is a predecessor to PKCS#12.
PKCS #13	- Elliptic Curve Cryptography Standard <sup>[12]</sup>	(Under development as of 2012). <sup>[13]</sup>
PKCS #14	- Pseudo-random Number Generation	(Under development as of 2012). <sup>[13]</sup>
PKCS #15	1.1 Cryptographic Token Information Format Standard <sup>[14]</sup>	Defines a standard allowing users of cryptographic tokens to identify themselves to applications, independent of the application's Cryptoki implementation (PKCS #11) or other API. RSA has relinquished IC-card-related parts of this standard to ISO/IEC 7816-15. <sup>[15]</sup>





C (country) : France  
 L (Locality) : Grenoble  
 ST : (State or Province) : Isère  
 O (Organization) : UdG  
 SO (Organizational Unit) : icluster  
 CN (Common Name) : Icluster\_CA  
 STREET (Adress) : 50 av Jean Kuntzmann  
 E (Email) : ca@udg.fr

C (country) : France  
 L (Locality) : Grenoble  
 ST : (State or Province) : Isère  
 O (Organization) : UdG  
 SO (Organizational Unit) : LJK  
 CN (Common Name) : Jean-Guillaume Dumas  
 STREET (Adress) : 51, av des Mathématiques  
 E (Email) : Jean-Guillaume.Dumas@imag.fr



Version	v3 (0x2)
Serial Number	14 (0xE)
Signature Algorithm ID	md5WithRSAEncryption
Issuer Name	
Validity Period	Not Before : Jun 8 14:52:40 2003 GMT Not After : Jun 7 14:52:40 2004 GMT
Subject Name	
Subjet Public Key Info :	Public Key Algorithm : rsaEncryption RSA Public Key (1024bit) Modulus (1024 bits) : 00:b3:e4:f..... Exponent : 65537 (0x10001)
Issuer Unique ID	
Subject Unique ID	
Extension	

X.509 Electronic Certificate	
Version	
Serial Number	
Signature Algorithm ID	
Issuer Name	
Validity Périod	
Subject Name	
Subjet Public Key Info :	
Issuer Unique ID	
Subject Unique ID	
Extension	
Signature	- Algorithm ID - Signature Value

Version :	Version du format de certificat X.509
Numéro de série :	Numéro de série du certificat(propre à chaque AC)
Algorithme de signature (OID) :	Identifiant des types d'algorithmes utilisés pour la signature du certificat
Nom de l'émetteur :	Distinguished Name (DN) de l'AC émettrice du certificat
Période de validité :	Période de validité du certificat
Nom du sujet :	Distinguished Name (DN) du détenteur de la clef publique
Clef publique du sujet :	Informations sur la clef publique du certificat
Issuer Unique ID :	Identifiant unique de l'émetteur du certificat
Subject Unique ID :	Identifiant unique du détenteur de la clef publique
Extensions :	Extensions génériques optionnelles
Signature :	Signature numérique par l'AC sur les champs précédents
Version :	X.509 format version number
Serial number :	certificate serial number (unique for each CA)
Signature Algo. (OID) :	Identifier of the used algorithm for the certificate signature
Issuer name :	Distinguished Name (DN) of the CA who created the certificate
Validity period :	The certificate lifetime
Subject name :	Distinguished Name (DN) of the owner of the certificate
Subject pub. key info. :	Data for the public key of the certificate
Issuer Unique ID :	Unique identifier for the CA issuing the certificate
Subject Unique ID :	unique identifier for the owner of the certificate
Extensions :	Optional generic extenstions
Signature :	Electronic signature by the CA of all the previous fields

X.509 Electronic Certificate

```

Certificate ::= SEQUENCE {
    tbsCertificate   TBSCertificate,
    signatureAlgorithm  AlgorithmIdentifier,
    signatureValue     BIT STRING }

TBSCertificate ::= SEQUENCE {
    version      [0] IMPLICIT Version DEFAULT v1,
    subject      CertificateSerialNumber,
    issuer       AlgorithmIdentifier,
    validityPeriod  Validity,
    subjectName   Name,
    subjectPublicKeyInfo SubjectPublicKeyInfo,
    issuerUniqueId [1] IMPLICIT UniqueIdentifier OPTIONAL,
                    -- If present, version MUST be v2 or v3
    subjectUniqueId [2] IMPLICIT UniqueIdentifier OPTIONAL,
                    -- If present, version MUST be v2 or v3
    extensions    [3] EXPLICIT Extensions OPTIONAL,
                    -- If present, version MUST be v3
}

Version ::= INTEGER ( v1(0), v2(1), v3(2) )

CertificateSerialNumber ::= INTEGER

AlgorithmIdentifier ::= SEQUENCE(
    algorithm OBJECT IDENTIFIER,
    parameters  ANY DEFINED BY algorithm OPTIONAL)

Validity ::= SEQUENCE {
    notBefore Time,
    notAfter  Time }

Time ::= CHOICE {
    utctime    UTCTime,
    generalTime GeneralizedTime }

UniqueIdentifier ::= BIT STRING

SubjectPublicKeyInfo ::= SEQUENCE {
    algorithm AlgorithmIdentifier,
    subjectPublicKey BIT STRING }

Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension

Extension ::= SEQUENCE {
    extnID OBJECT IDENTIFIER,
    critical BOOLEAN DEFAULT FALSE,
    extnValue OCTET STRING }

Name ::= CHOICE {
    rdnSequence RDNSequence }

RDNSequence ::= SEQUENCE OF RelativeDistinguishedName

RelativeDistinguishedName ::= SET SIZE (1..MAX) OF AttributeTypeAndValue

AttributeTypeAndValue ::= SEQUENCE {
    type AttributeType,
    valueAttributeValue }

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY DEFINED BY AttributeType
  
```

Monday September 26, 2011

1/71

```

-----BEGIN X509 CRL-----  

version v3  

serialNumber 1234567890,  

signature  

{  

    algorithm ( 1 2 840 113549 1 1 5 ), -- SHA1RSA  

parameters RSAParams : NULL  

} issuer rdnSequence :  

{ ( type ( 2 5 4 6 ),  

    value PrintableString : "DE" ) ,  

( type ( 2 5 4 10 ),  

    value UTF8String : "GMD - Forschungszentrum Informationstechnik GmbH" )  

}  

validity  

{ notBefore utcTime : "000501100000Z",  

notAfter utcTime : "001101100000Z" }  

subject rdnSequence :  

{ ( type ( 2 5 4 6 ),  

    value PrintableString : "DE" ) ,  

( type ( 2 5 4 10 ),  

    value UTF8String : "Barzin" ) ,  

( type ( 2 5 4 4 ),  

    value UTF8String : "Petra" ) }  

subjectPublicKeyInfo  

{ algorithm  

{ algorithm ( 1 2 840 113549 1 1 1 ), -- RSA  

parameters RSAParams : NULL  

subjectPublicKey '00110000 10000001 10000111 00000010 1000 ...'B  

extensions  

{  

extnid { 2 5 29 9 }, -- subjectDirectoryAttributes  

extnValue '302B301006082B06010505070904310413024445300FO ...'H ),  

extnid { 2 5 29 15 }, -- keyUsage  

critical TRUE,  

extnValue '03020640'H ),  

extnid { 2 5 29 32 }, -- certificatePolicies  

extnValue '3009300706052B24080101'H ),  

extnid { 2 5 29 35 }, -- authorityKeyIdentifier  

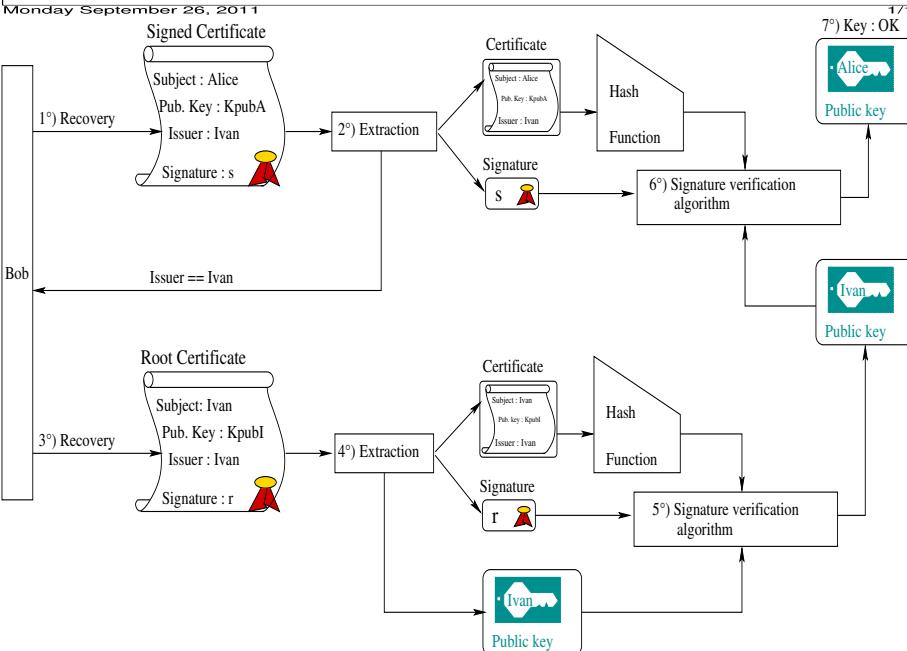
extnValue '3016801406010203040506070809A0B0C0D0E0F0FEDCBA98'H ),  

extnid { 1 3 6 1 5 5 7 1 3 }, -- qcStatements  

extnValue '302B302906082B06010505070B01301D301B81196D756 ...'H ) }  

}
-----END X509 CRL-----

```

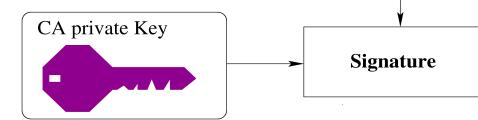


### Information

Version (v1=0;v2=1)
Signature Algorithm ID
Issuer Name
This Update Date/Time
Next Update Date/Time
CRL :
Certificate Serial Number
Revocation Date
Certificate Serial Number
Revocation Date
⋮
Certificate Serial Number
Revocation Date
CRL Extensions

### CRL

Version (v1=0;v2=1)
Signature Algorithm ID
Issuer Name
This Update Date/Time
Next Update Date/Time
CRL :
Certificate Serial Number
Revocation Date
Certificate Serial Number
Revocation Date
⋮
Certificate Serial Number
Revocation Date
CRL Extensions
Signature
Algorithm ID
Signature Value

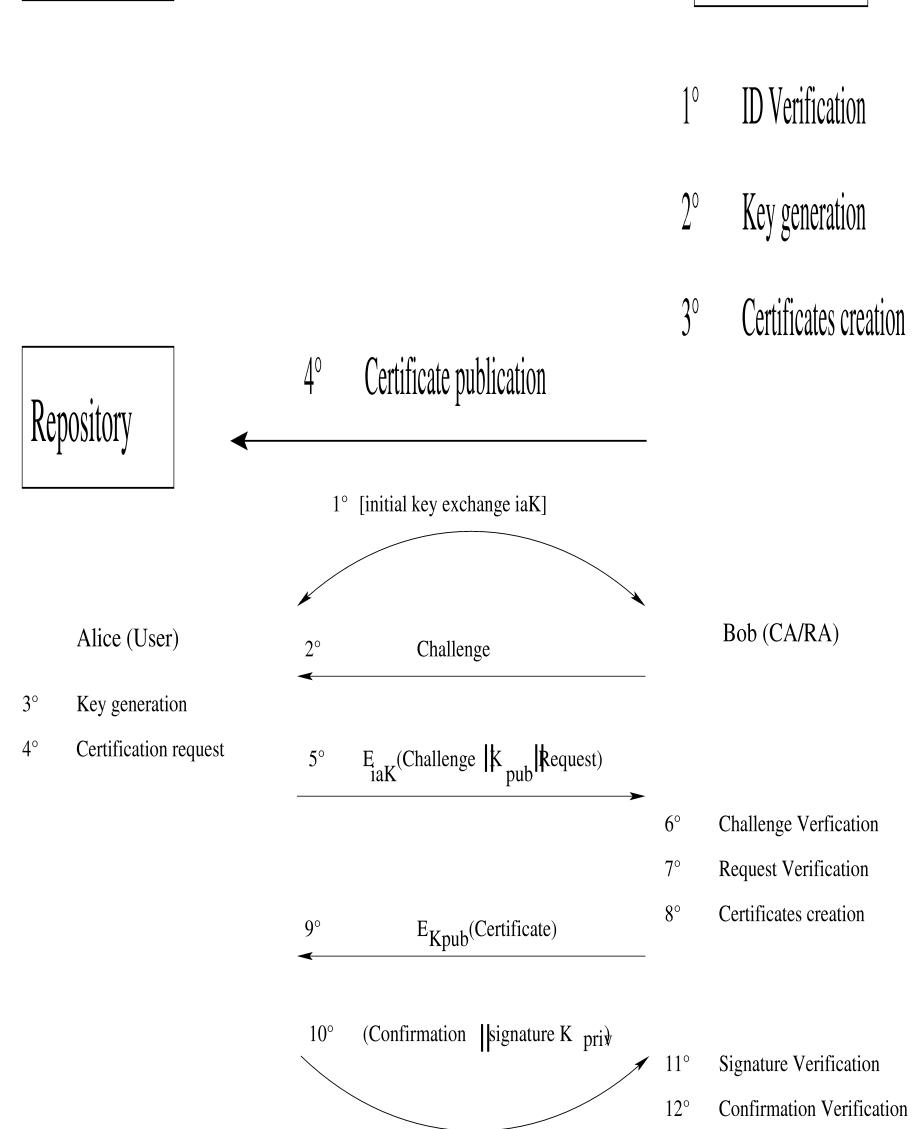
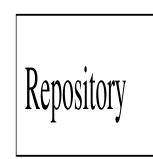
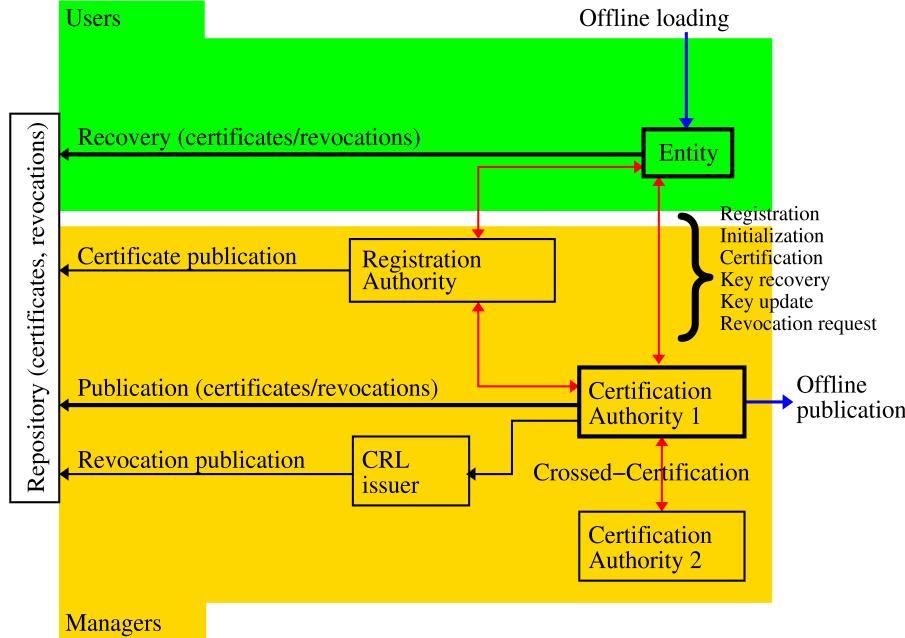


## Reasons to revoke a certificate [\[RFC 5280\]](#)

- unspecified (0)
- keyCompromise (1)
- CACompromise (2)
- affiliationChanged (3)
- superseded (4)
- cessationOfOperation (5)
- certificateHold (6)
- removeFromCRL (8)
- privilegeWithdrawn (9)
- AACompromise (10)

Obs.: Value 7 is not used.

Alg.	Hash.	OID	Identifier
3DES-CBC		1.2.840.113549.3.7	DES-EDE3-CBC
RSA		1.2.840.113549.1.1.1	RSAEncryption
RSA	MD5	1.2.840.113549.1.1.4	md5withRSAEncryption
RSA	SHA-1	1.2.840.113549.1.1.5	sha1withRSAEncryption
DSA		1.2.840.10040.4.1	id-dsa
DSA	SHA-1	1.2.840.10040.4.3	id-dsawithSha1
DSA	SHA-1.320	1.3.14.3.2	id-dsawithSha1.320
ECDSA	SHA-1	1.2.840.10045.1	ecdsawithSha1



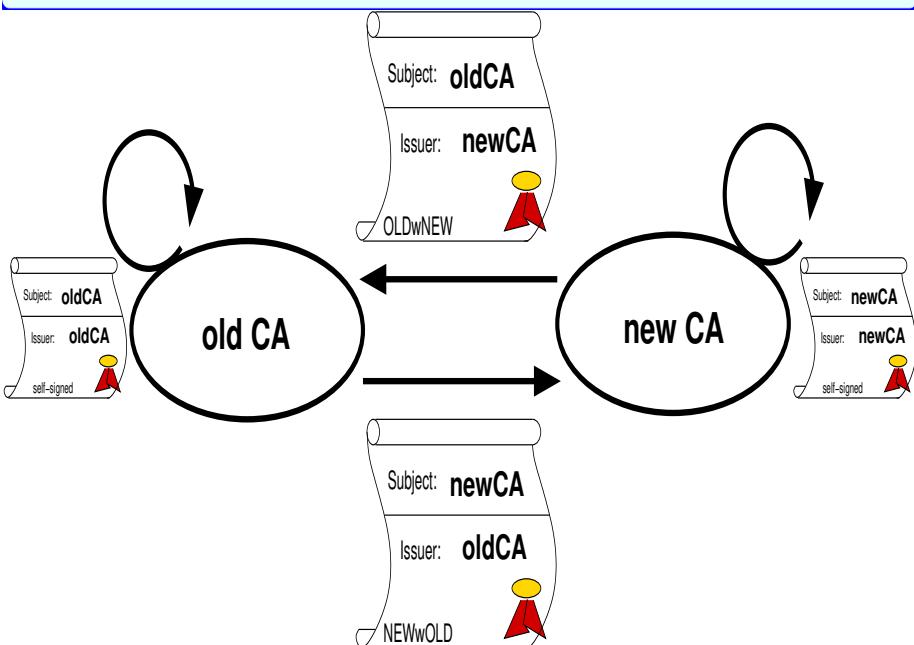
```

CertReqMsg ::= SEQUENCE {
    certReq CertRequest,
    signature SIGNED{ certReq } OPTIONAL,
}

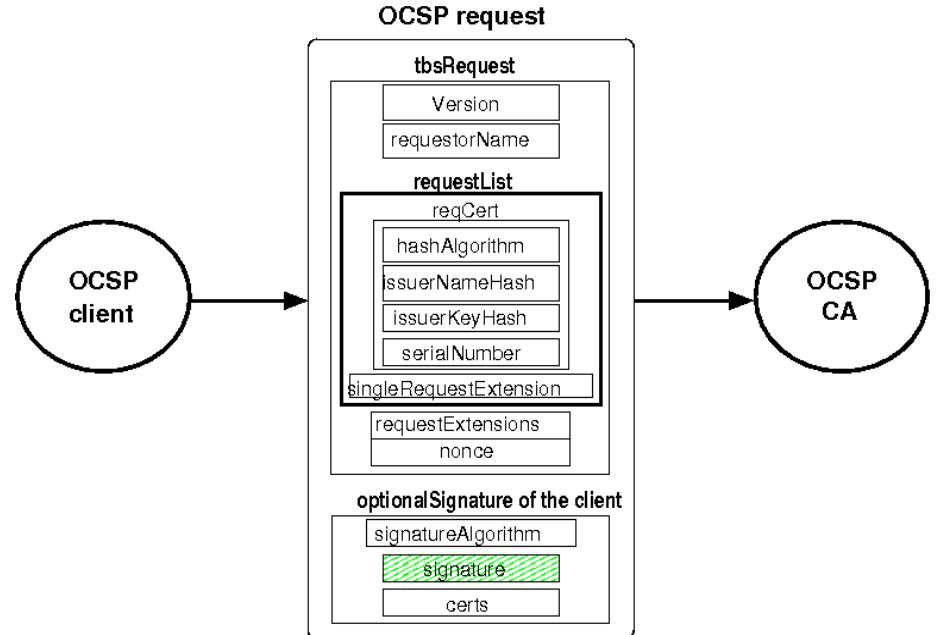
CertRequest ::= SEQUENCE {
    certReqId INTEGER, -- ID for matching request and reply
    certTemplate CertTemplate, -- Selected fields of cert to be issued
}

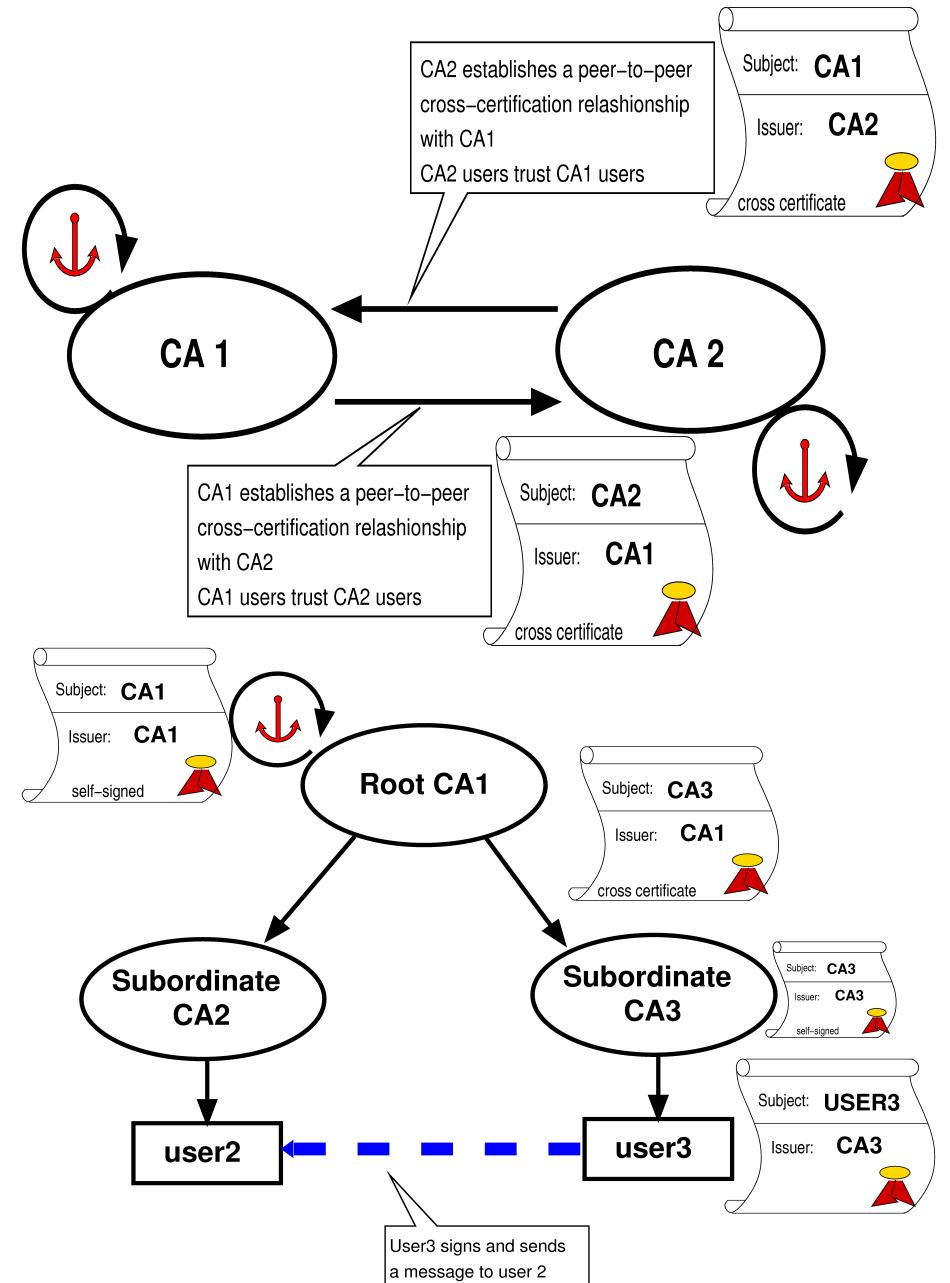
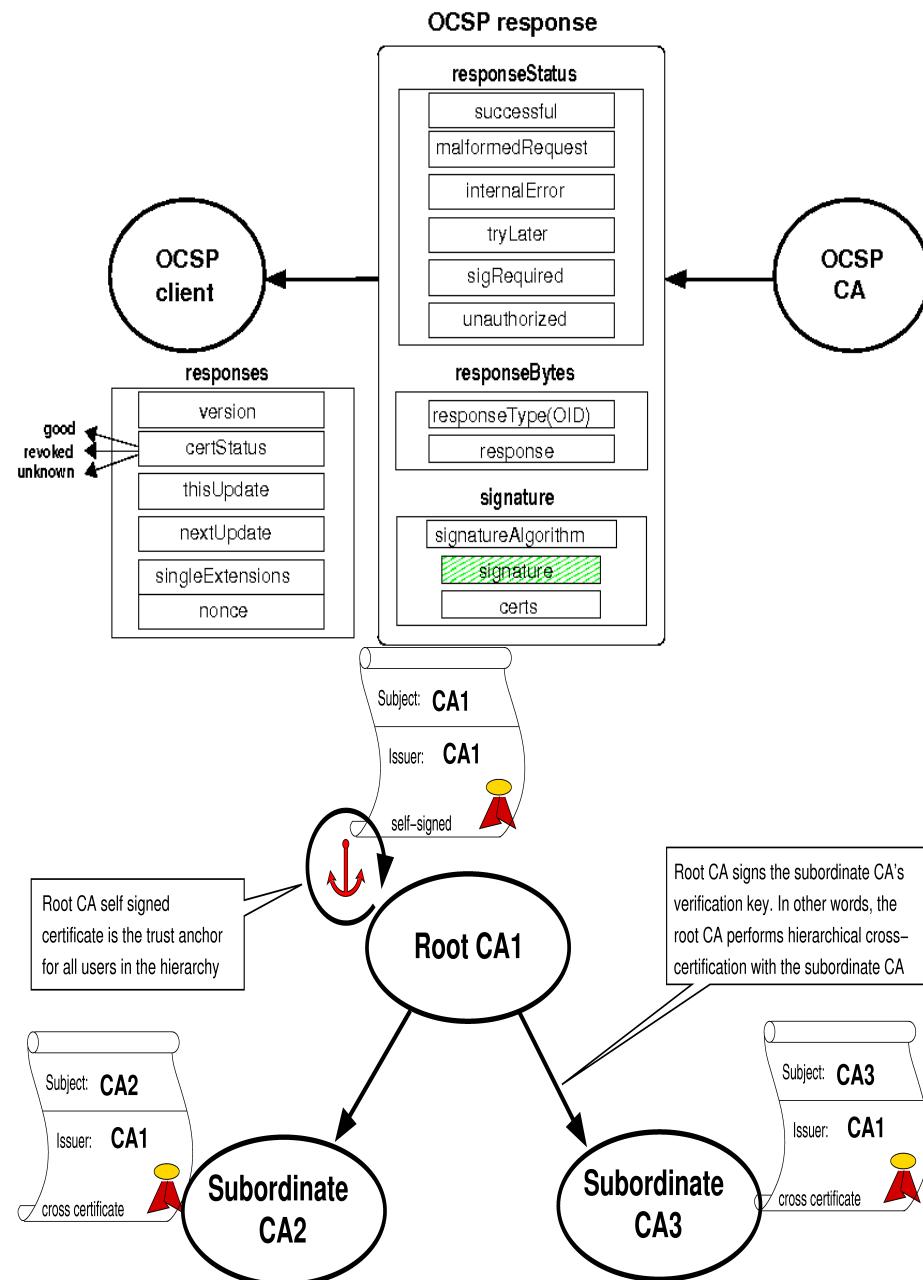
CertResponse ::= SEQUENCE {
    certReqId INTEGER,
    status PKIStatusInfo,
    certificate Certificate OPTIONAL,
    rspInfo OCTET STRING OPTIONAL
}

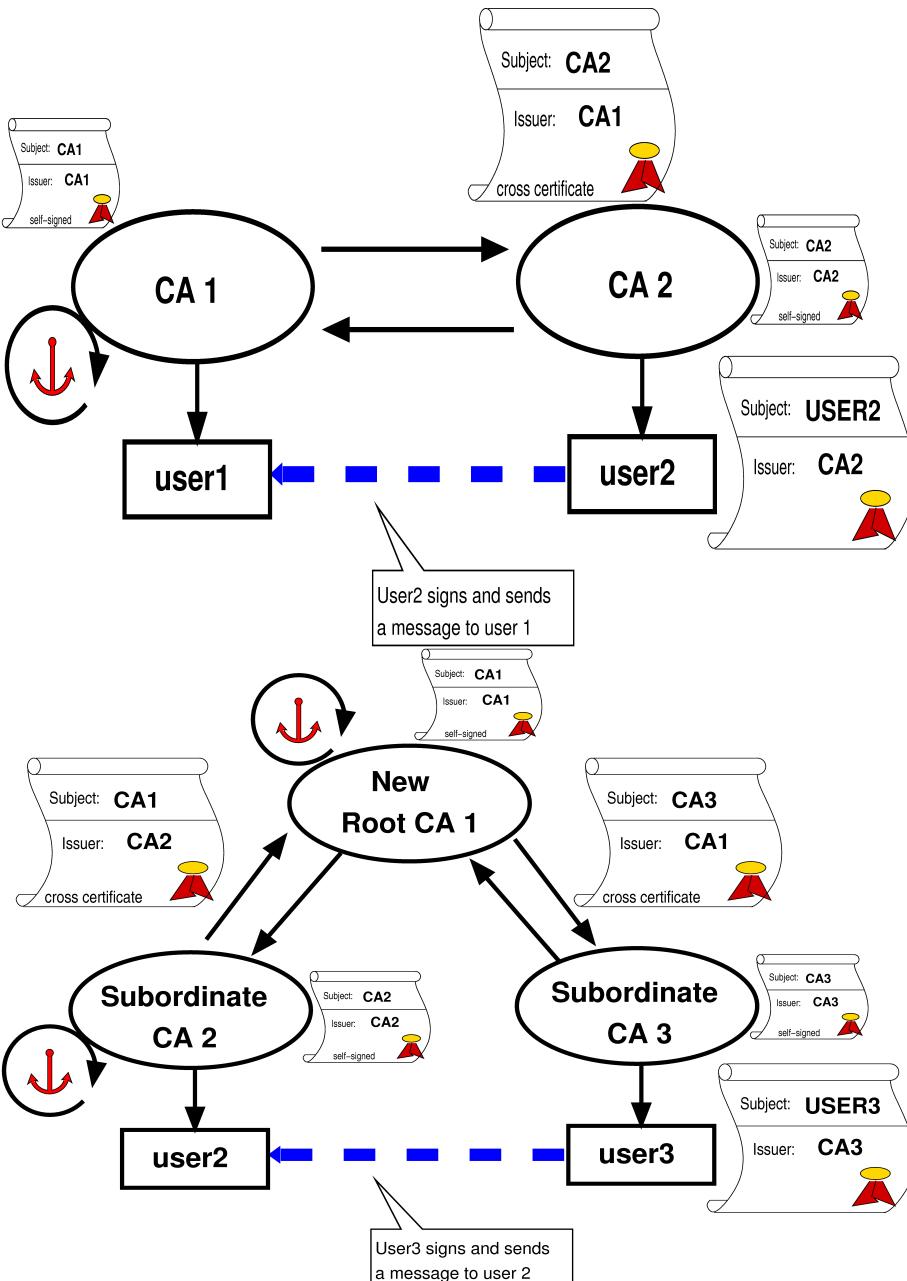
```



	Certificate signed with $NEW_{priv}$	Certificate signed with $OLD_{priv}$
Repository contains OLD and NEW		
$NEW_{pub}$ within PSE	DIRECT verification	Recover $OLDwNEW$ Verify $OLDwNEW$ with $NEW_{pub}$ Verify certificate with $OLD_{pub}$
$OLD_{pub}$ within PSE	Recover $NEWwOLD$ Verify $NEWwOLD$ with $OLD_{pub}$ Verify certificate with $NEW_{pub}$	DIRECT verification
Repository contains only OLD		
$NEW_{pub}$ within PSE	DIRECT verification (without the Repository)	FAILURE (Repository's fault)
$OLD_{pub}$ within PSE	FAILURE (Repository's fault)	DIRECT verification







Printed by U-CycloneJgdt

cross-certif.asn1

Oct 17, 07 15:20

```

pkiCA OBJECT-CLASS ::= {
    SUBCLASS OF { top }
    KIND auxiliary
    MAY CONTAIN {cACertificate | certificateRevocationList | authorityRevocationList | crossCertificatePair }
    ID joint-iso-ccitt(2) ds(5) objectClass(6) pkiCA(22)}

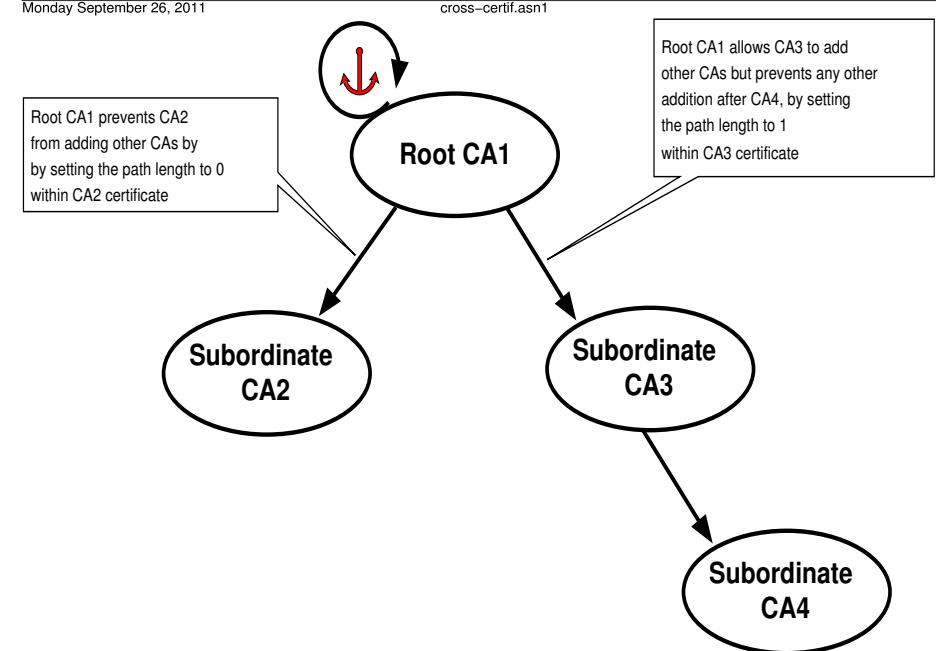
cACertificate ATTRIBUTE ::= {
    WITH SYNTAX Certificate
    EQUALITY MATCHING RULE certificateExactMatch
    ID joint-iso-ccitt(2) ds(5) attributeType(4) cACertificate(37)}

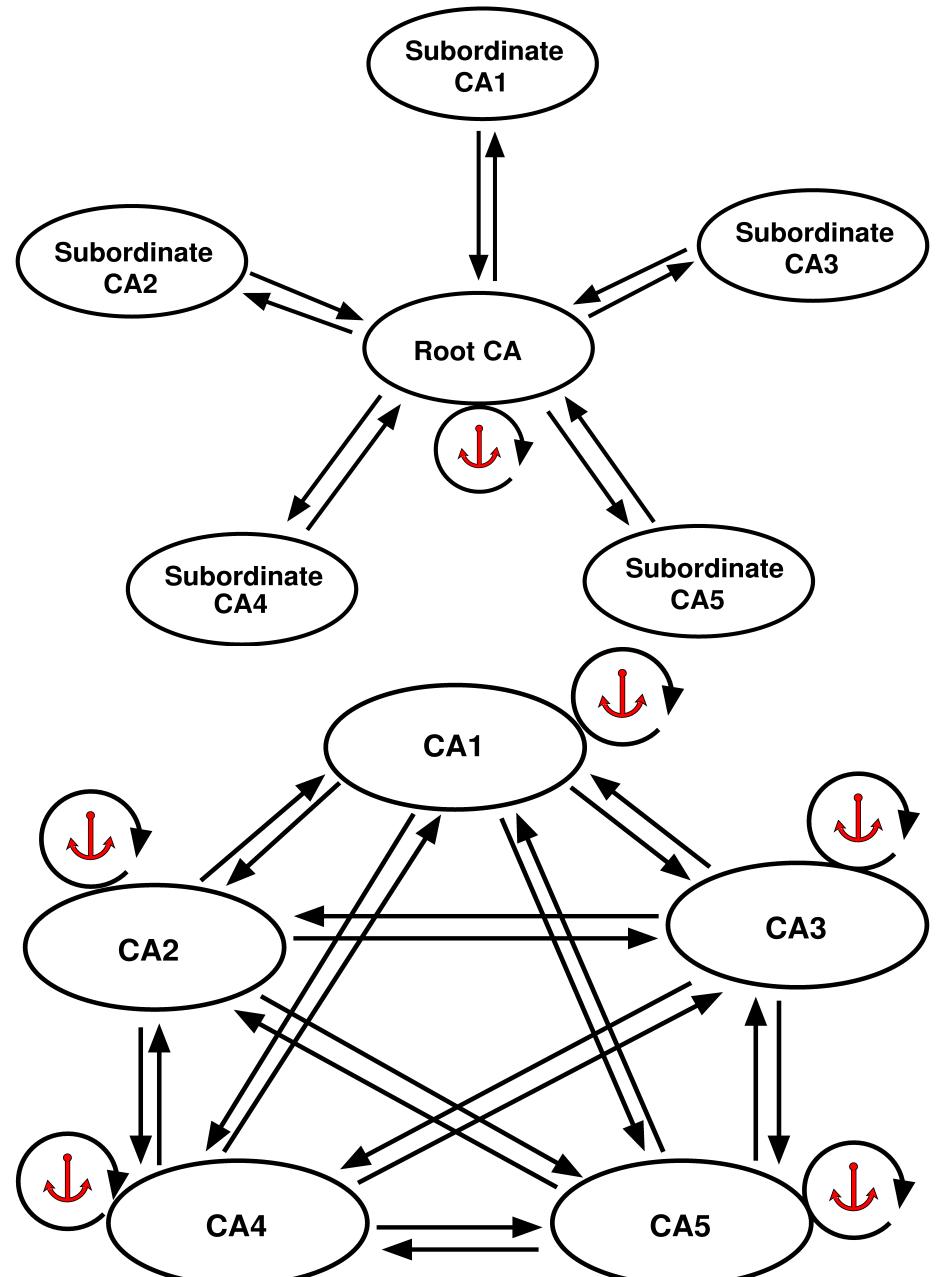
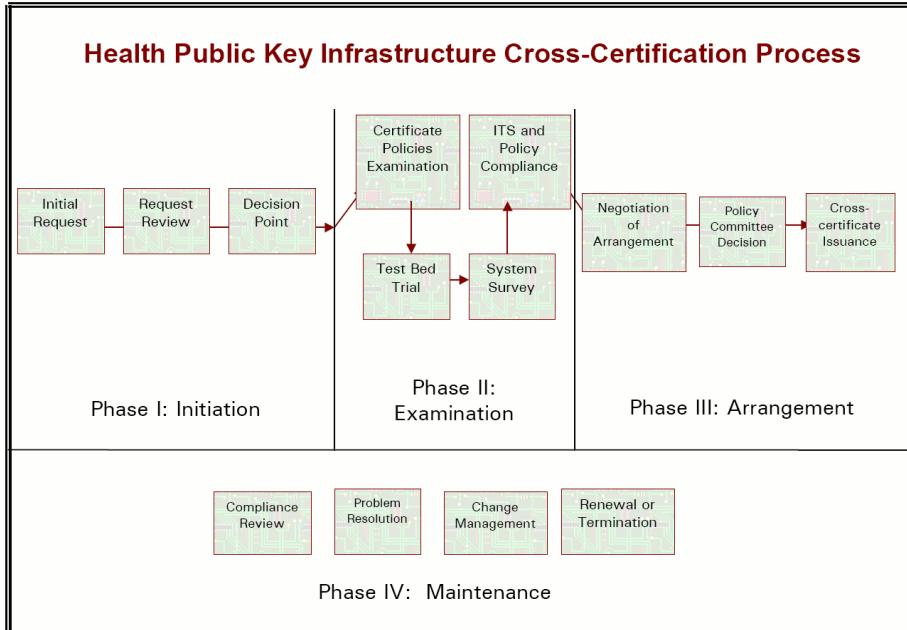
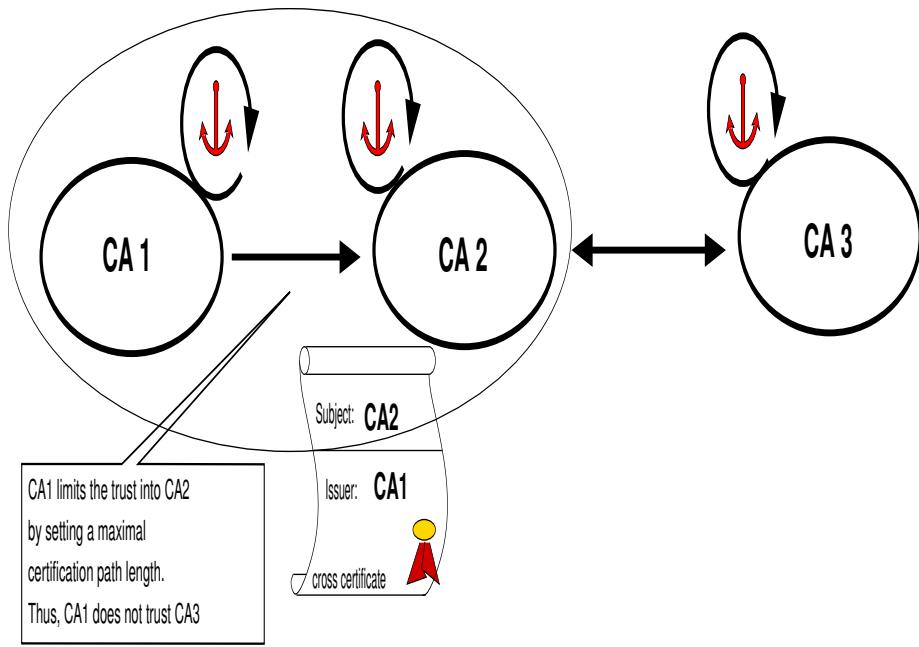
crossCertificatePairATTRIBUTE:={ 
    WITH SYNTAX CertificatePair
    EQUALITY MATCHING RULE certificatePairExactMatch
    ID joint-iso-ccitt(2) ds(5) attributeType(4) crossCertificatePair(40)}

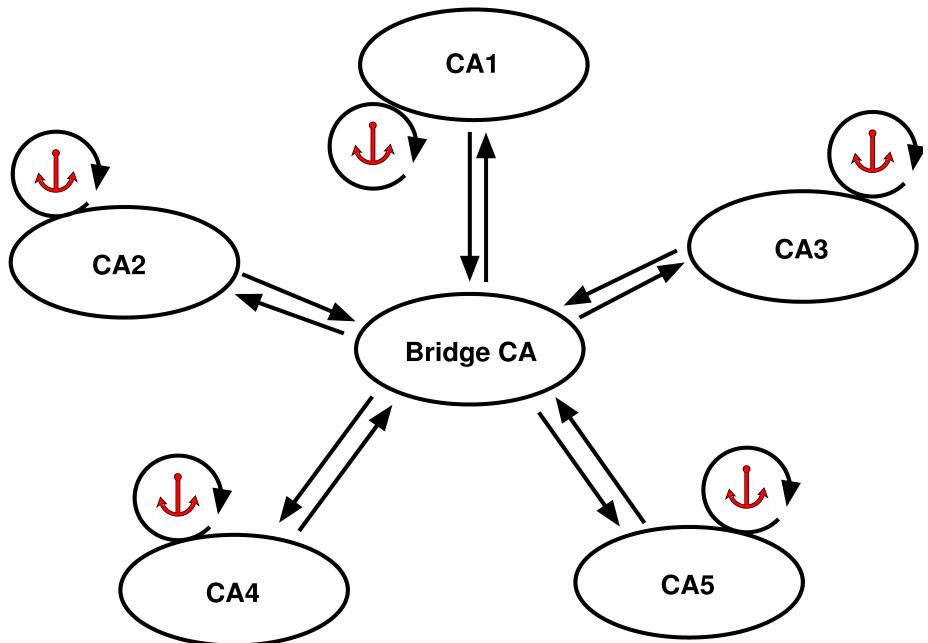
-----
CertificatePair ::= SEQUENCE {
    forward [0] Certificate OPTIONAL,
    reverse [1] Certificate OPTIONAL,
    -- at least one of the pair shall be present -- }

Monday September 26, 2011

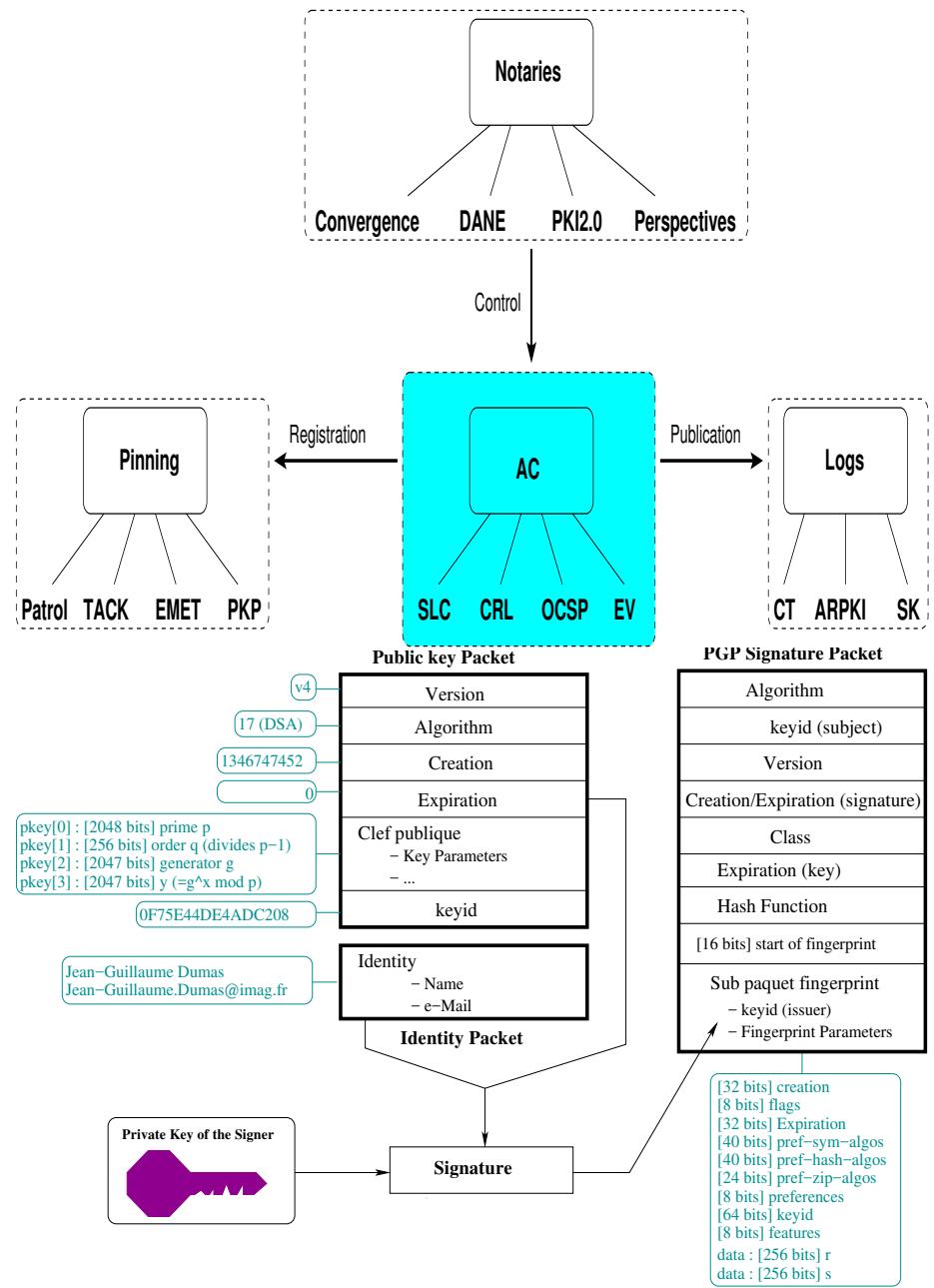
```







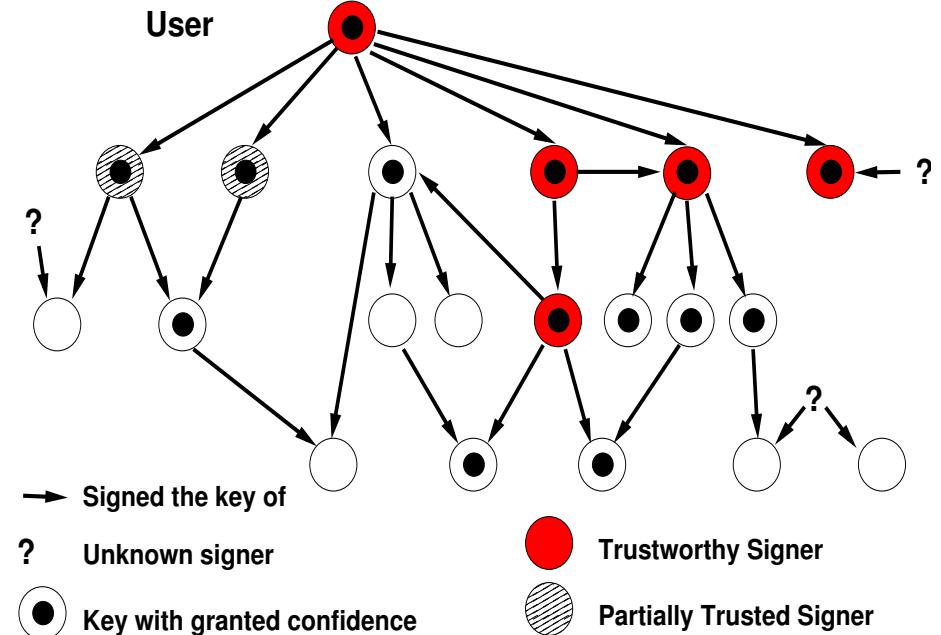
System	Trust Anchor Stores
Debian 7	/etc/ssl/certs/ca-certificates.crt
Windows 10	C:\Windows\System32\certmgr.msc
Mac OS X	Applications>Utilities>Keychain Access
Android 4	Settings>Security>Credential Storage>Trusted Credentials>Display Trusted CA certificates
Iceweasel 31	/usr/share/ca-certificates/mozilla/*.crt
Firefox 36	Preferences>Privacy&Security>Certificates>Manage Certificates
Chrome 40	Settings>Advanced settings>Manage certificates (using certmgr.msc or Keychain)
Safari 5	using Keychain
IE 11	Internet Options>Content>Certificates (using certmgr.msc)



- 0     – Reserved - a packet tag MUST NOT have this value  
 1     – Public-Key Encrypted Session Key Packet  
 2     – Signature Packet  
 3     – Symmetric-Key Encrypted Session Key Packet  
 4     – One-Pass Signature Packet  
 5     – Secret-Key Packet  
 6     – Public-Key Packet  
 7     – Secret-Subkey Packet  
 8     – Compressed Data Packet  
 9     – Symmetrically Encrypted Data Packet  
 10    – Marker Packet  
 11    – Literal Data Packet  
 12    – Trust Packet  
 13    – User ID Packet  
 14    – Public-Subkey Packet  
 17    – User Attribute Packet  
 18    – Sym. Encrypted and Integrity Protected Data Packet  
 19    – Modification Detection Code Packet  
 60 to 63 – Private or Experimental Values

0x00	Signature of a binary document
0x01	Signature of a canonical text document
0x02	Standalone signature
0x10	Generic certification of a User ID and Public-Key packet
0x11	Persona certification of a User ID and Public-Key packet
0x12	Casual certification of a User ID and Public-Key packet
0x13	Positive certification of a User ID and Public-Key packet
0x18	Subkey Binding Signature
0x19	Primary Key Binding Signature
0x1F	Signature directly on a key
0x20	Key revocation signature
0x28	Subkey revocation signature
0x30	Certification revocation signature
0x40	Timestamp signature
0x50	Third-Party Confirmation signature

field	byte	content
a.1	1	0x99
a.2	1	most-significant bits of the size of fields (b) to (e)
a.3	1	least-significant bits of the size of fields (b) to (e)
b	1	version number = 4
c	4	key creation date
d	1	signature algorithm, (e.g., 17 for DSA)
e		specific to the algorithm, e.g., for DSA :
e.1	256	prime number (e.g., $p$ on 2048 bits)
e.2	32	group order (e.g., $q$ on 256 bits)
e.3	256	group generator (e.g., $g$ on 2048 bits)
e.4	256	public key value (e.g., $y$ on 2048 bits)



keyid	public key	ciphered private key	timestamp	user
...	...	...	...	...
...	...	...	...	...
0x70096AD1	$KU_i$	$E_{H(P_i)}(KR_i)$	$Time_i$	$User_i$
...	...	...	...	...
...	...	...	...	...
keyid	public key	ciphered private key	timestamp	user
key				trust
...	...	...	...	...
...	...	...	...	...
...	...	...	...	...
0x70096AD1	$KU_i$	$E_{H(P_i)}(KR_i)$	$Time_i$	$User_i$
...	...	...	...	$trust_i$
...	...	...	...	$sign_i$
...	...	...	...	...

## Search results for '0x0f75e44de4adc208'

Type bits/keyID cr. time exp time key expir

---

pub 2048D/[E4ADC208](#) 2012-09-04

uid Jean-Guillaume Dumas <jgdumas@imag.fr>

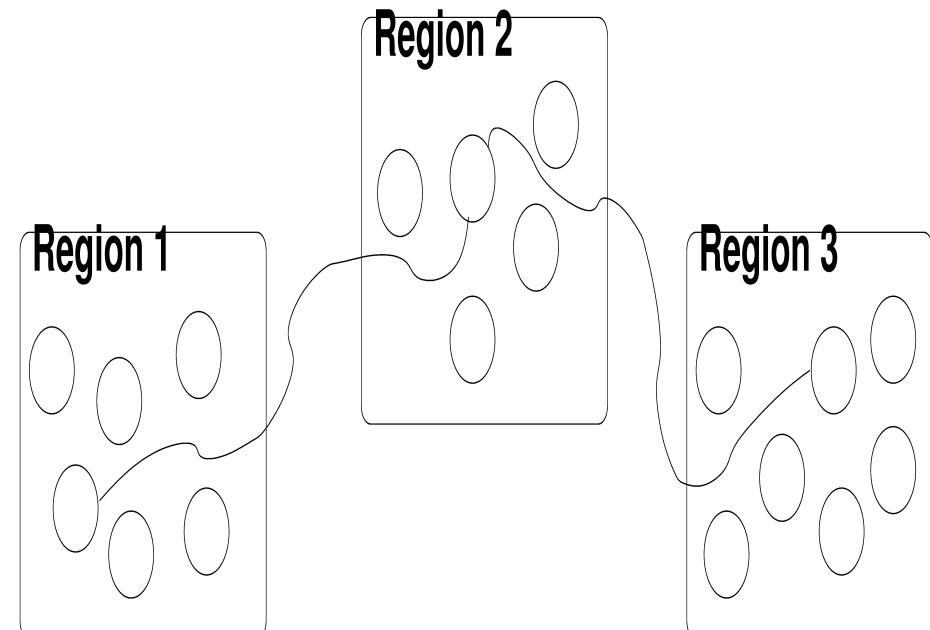
sig sig3 [E4ADC208](#) 2012-09-04 \_\_\_\_\_ 2016-09-03 [selfsig]

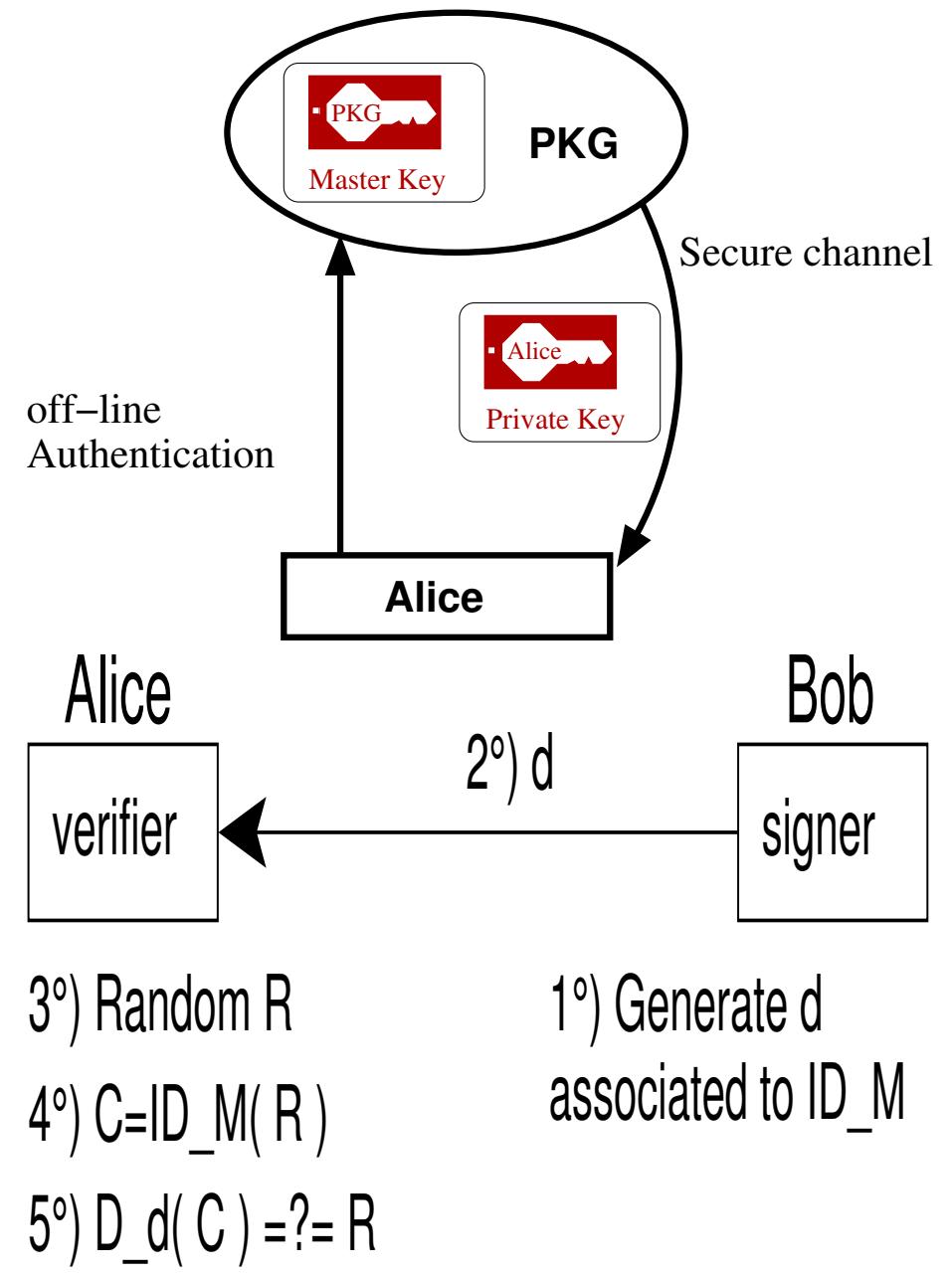
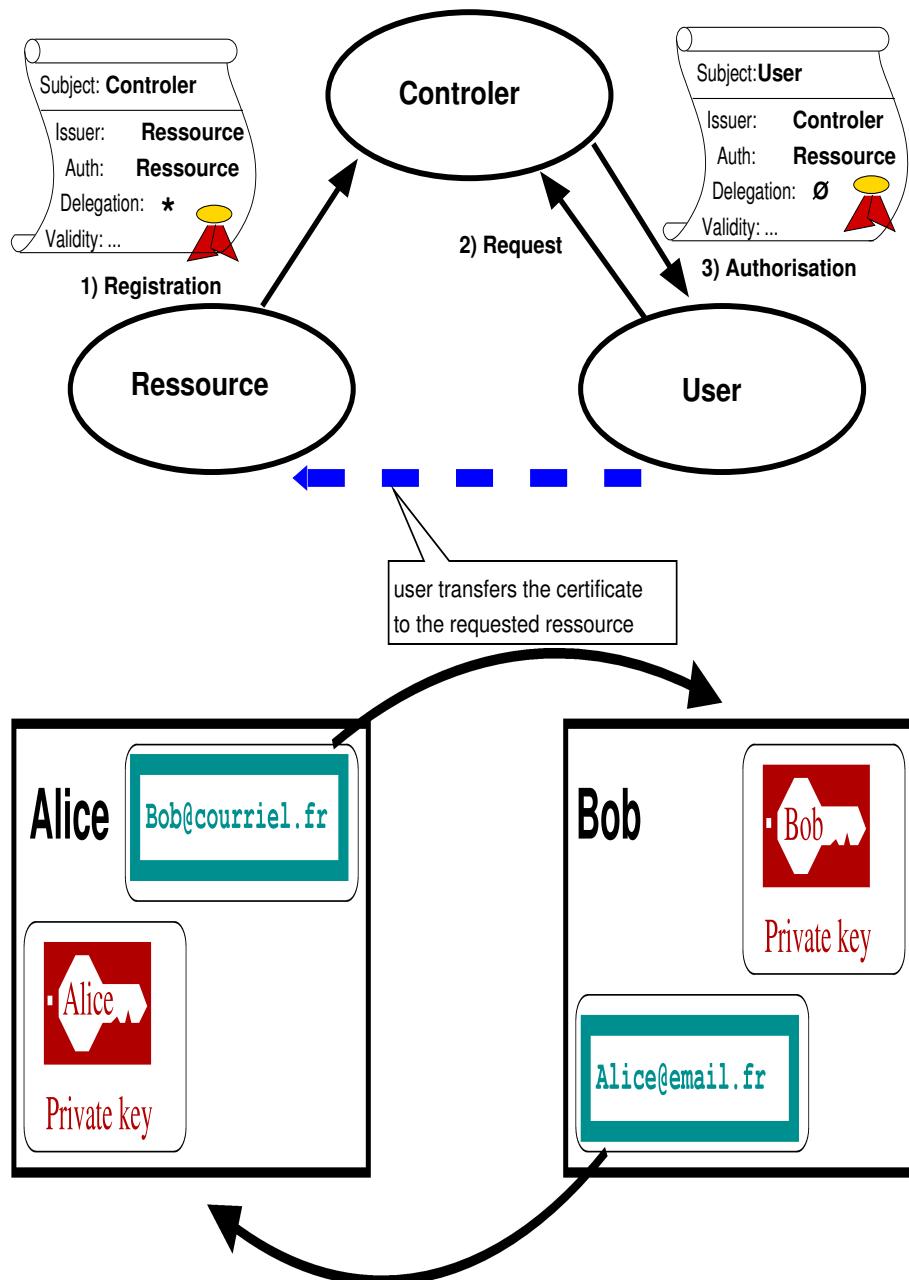
sig sig [1F829E58](#) 2012-12-07 \_\_\_\_\_ [ ]

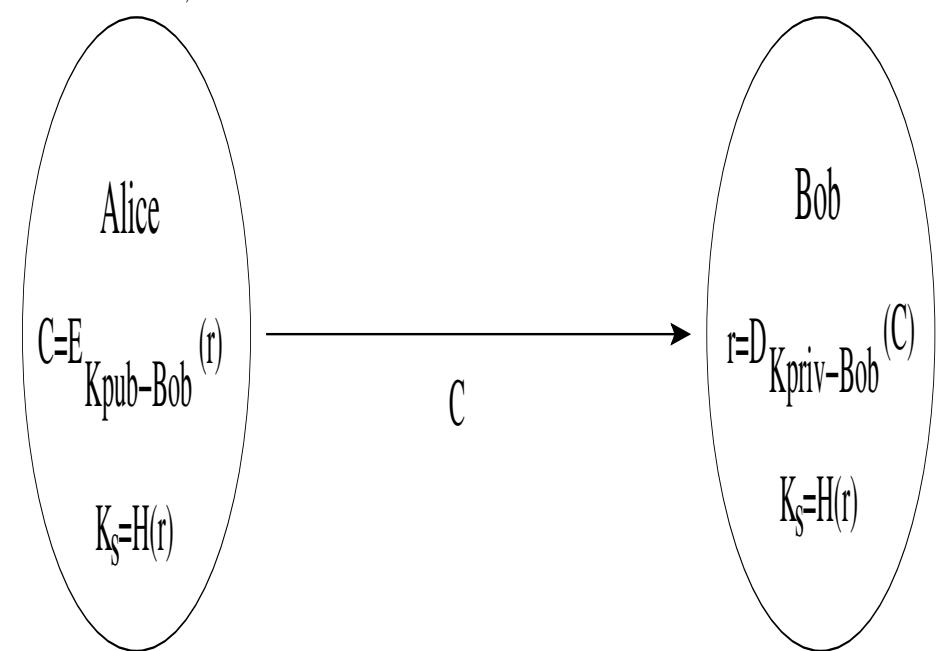
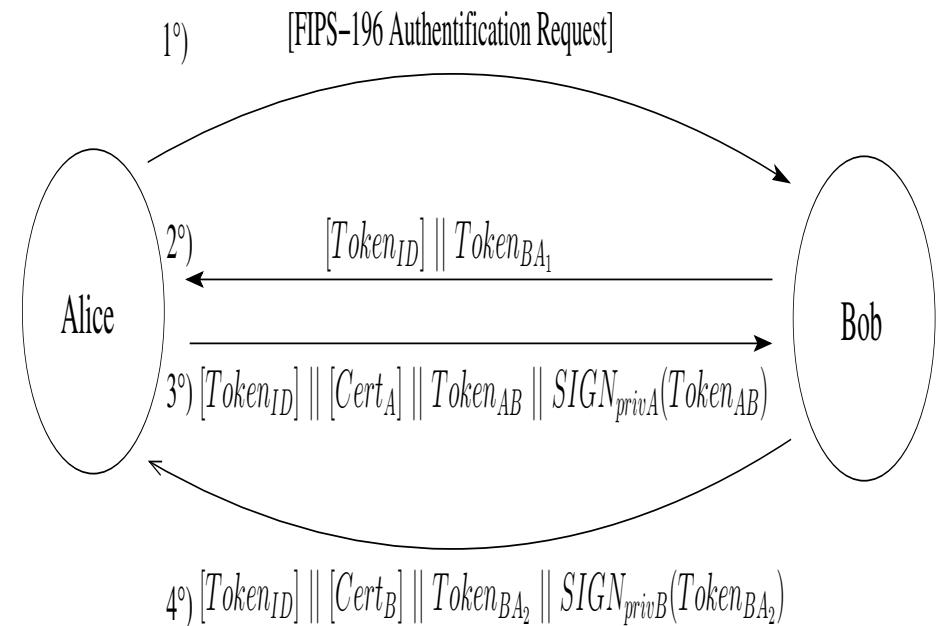
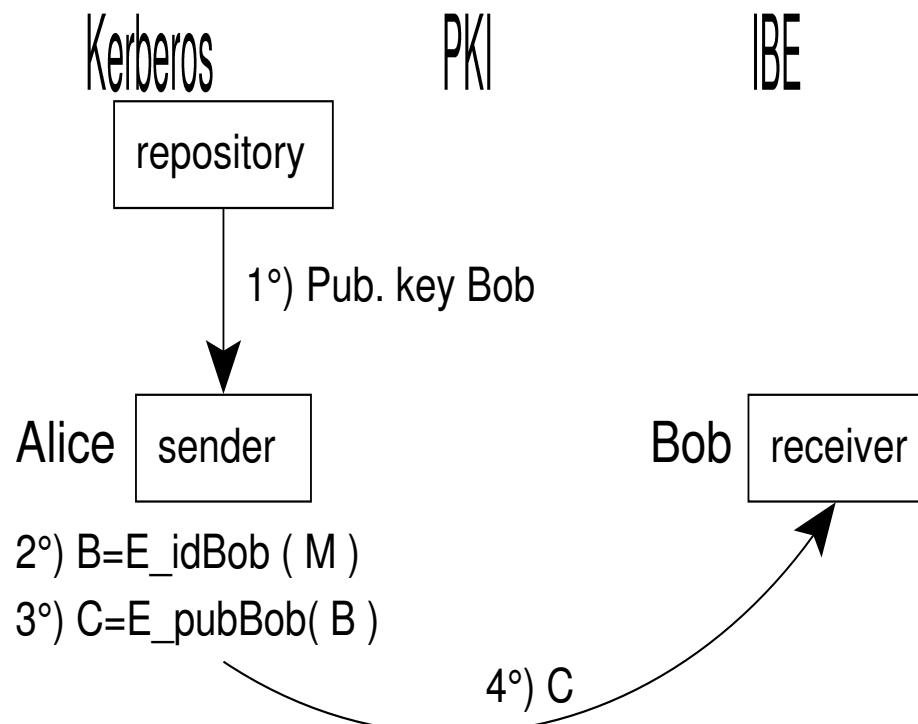
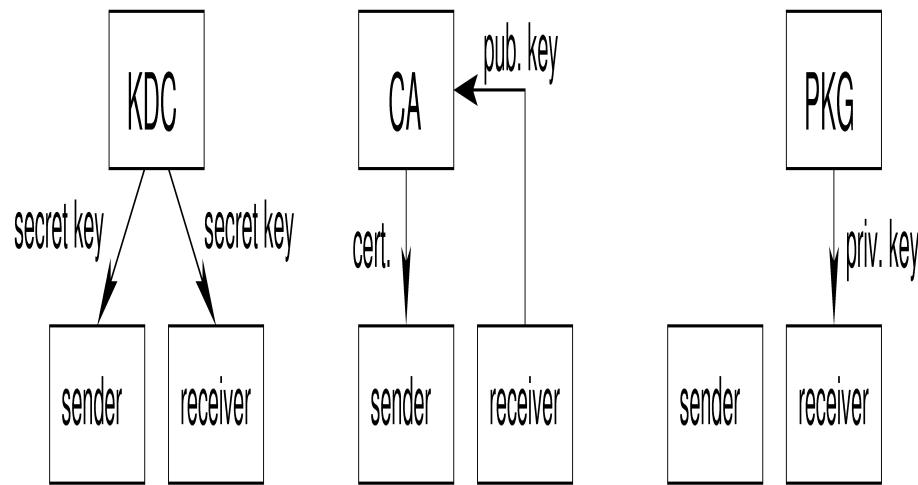
sig sig [7A6574F0](#) 2012-12-07 \_\_\_\_\_ [Dominique Duval \(pour safe pki\) <Dominique.Duval@imag.fr>](#)

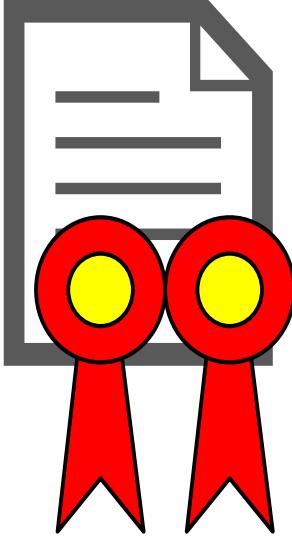
sub 2048g/322DC83F 2012-09-04

sig subind [E4ADC208](#) 2012-09-04 \_\_\_\_\_ 2016-09-03 [ ]









## Co-signature

**PDF  
Signature**

**« simple »  
Signature**

PDF



## Countersignature

**Binary  
Signature**

PKCS#7  
CMS

**XML  
Signature**

XML/DSig

**« advanced »  
Signature**

PAdES

CAdES

XAdES

Certificate policy	Certification practice statement	Terms and conditions
Certificates will be validated at each use to ensure that the certificate remains current. Validations returns will be made in nn minutes...	Certificates will be validated using an OCSP-based validation service held in a secure location and managed...	Each time you use your certificate we will check to make sure it is valid...
The registration of new users will be conducted by xyz registration authority and will require the presentation of two sets of IDs...	The RA will communicate with the CA via a secure link utilizing abc encryption techniques and each request will be signed...	On requesting a certificate you will be required to provide two items of proof of your name and address; this can be a utility bill, bank statement, driving licence...
Certificates will be valid for nn years	The CA will revoke and reissue certificates every nn years using the existing keys to roll over the certificate and automated notification to users of their new certificate...	We will issue you with an updated certificate every nn years...

1. Introduction	9
1.1 Overview	9
1.2 Document name and identification	9
1.3 PKI participants	9
1.3.1 Certification authorities	9
1.3.2 Registration authorities	9
1.3.3 Subscribers	9
1.3.4 Relying parties	9
1.3.5 Other participants	10
1.4 Certificate usage	10
1.4.1 Appropriate certificate uses	10
1.4.2 Unappropriate certificate uses	10
1.5 Policy administration	10
1.5.1 Organization administering the document	10
1.5.2 Contact person	10
1.5.3 Person determining CPS suitability for the policy	10
1.5.4 CPS approval procedures	10
1.6 Definitions and acronyms	10
2. Publication and repository responsibilities	12
2.1 Publication of private key	12
2.2 Publication of certification information	12
2.3 Time or frequency of publication	12
2.4 Access controls on repositories	12
3. Identification and authentication	13
3.1 Naming	13
3.1.1 Types of names	13
3.1.2 Need for names to be meaningful	13
3.1.3 Uniqueness or pseudonymity of subscribers	13
3.1.4 Rules for interpreting various name forms	13
3.1.5 Uniqueness of names	13
3.1.6 Recognition, authentication, and role of trademarks	13
3.2 Initial identity validation	13
3.2.1 Method to prove possession of private key	13
3.2.2 Authentication of organization identity	14
3.2.3 Authentication of individual identity	14
3.2.4 Need for identity label information	14
3.2.5 Validation of authority	14
3.2.6 Criteria for interoperability	14
3.3 Identification and authentication for re-key requests	14
3.3.1 Identification and authentication for routine re-key	14
3.3.2 Identification and authentication for re-key after revocation	14
3.4 Identification and authentication for revocation request	15
4. Certificate life-cycle operational requirements	16
4.1 Certificate Application	16
4.1.1 Enrollment process for certificate application	16
4.1.2 Enrollment process and responsibilities	16
4.2 Certificate application processing	16
4.2.1 Performing identification and authentication functions	16
4.2.2 Approval or rejection of certificate applications	17
4.2.3 Time to process certificate applications	17
4.3 Certificate issuance	17
4.3.1 CA actions during certificate issuance	17

4.3.2	Notification to subscriber by the CA of issuance of certificate .....	17
4.4	Certificate acceptance .....	17
4.4.1	Conduct constituting certificate acceptance .....	17
4.4.2	Publication of the certificate by the CA .....	17
4.4.3	Notification of certificate issuance by the CA to other entities .....	17
4.5	Key pair and certificate usage .....	17
4.5.1	Key pair generation and distribution .....	17
4.5.2	Relying party public key and certificate usage .....	18
4.6	Certificate renewal .....	18
4.6.1	Circumstance for certificate renewal .....	18
4.6.2	Who may request certificate renewal .....	18
4.6.3	Processing certificate renewal requests .....	18
4.6.4	Notification of new certificate issuance to subscriber .....	18
4.6.5	Conduct constituting acceptance of a renewal certificate .....	18
4.6.6	Publication of the renewal certificate by the CA .....	18
4.6.7	Notification of certificate issuance by the CA to other entities .....	18
4.7	Certificate re-key .....	18
4.7.1	Circumstance for certificate re-key .....	18
4.7.2	Who may request certification of a new public key .....	18
4.7.3	Processing certificate re-keying requests .....	19
4.7.4	Notification of new certificate issuance to subscriber .....	19
4.7.5	Conduct constituting acceptance of a re-keyed certificate .....	19
4.7.6	Publication of the re-keyed certificate by the CA .....	19
4.7.7	Notification of certificate issuance by the CA to other entities .....	19
4.8	Certificate modification .....	19
4.8.1	Circumstance for certificate modification .....	19
4.8.2	Who may request certificate modification .....	19
4.8.3	Processing certificate modification requests .....	19
4.8.4	Notification of new certificate issuance to subscriber .....	19
4.8.5	Conduct constituting acceptance of modified certificate .....	19
4.8.6	Publication of the modified certificate by the CA .....	19
4.8.7	Notification of certificate issuance by the CA to other entities .....	19
4.9	Certificate revocation and suspension .....	19
4.9.1	Procedure initiated for revocation .....	20
4.9.2	Who can request revocation .....	20
4.9.3	Procedure for revocation request .....	20
4.9.4	Revocation request grace period .....	20
4.9.5	The time within which CA must process the revocation request .....	20
4.9.6	Revolocation tracking requirements for relying parties .....	20
4.9.7	CRL issuance frequency (if applicable) .....	20
4.9.8	Maximum latency for CRLs (if applicable) .....	20
4.9.9	On-line revocation/status checking availability .....	20
4.9.10	Off-line revocation/status checking requirements .....	20
4.9.11	Other forms of revocation advertisements available .....	20
4.9.12	Special requirements re-key compromise .....	21
4.9.13	Circumstances for suspension .....	21
4.9.14	Who can request suspension .....	21
4.9.15	Procedure initiated for suspension .....	21
4.9.16	Limits on suspension period .....	21
4.10	Certificate status services .....	21
4.10.1	Operational characteristics .....	21
4.10.2	Service availability .....	21
4.10.3	Optional features .....	21
4.11	End of subscription .....	21
4.12	Key escrow and recovery .....	21
4.12.1	Key escrow and recovery policy and practices .....	21
4.12.2	Session key encryption, isolation and recovery policy and practices .....	21
5	Facility, management and operational controls .....	22
5.1	Physical controls .....	22
5.1.1	Site location and construction .....	22
5.1.2	Physical access .....	22
5.1.3	Power and air conditioning .....	22
5.1.4	Water exposures .....	22
5.1.5	Fire prevention and protection .....	22
5.1.6	Media storage .....	22
5.1.7	Waste disposal .....	22
5.1.8	Off-site backup .....	22
5.2	Procedural controls .....	22
5.2.1	Trusted roles .....	22
5.2.2	Number of persons required per task .....	22
5.2.3	Identification and authentication for each role .....	22
5.2.4	Roles requiring separation of duties .....	22
5.3	Personnel controls .....	22
5.3.1	Qualifications, experience, and clearance requirements .....	22
5.3.2	Background check procedures .....	23
5.3.3	Training requirements .....	23
5.3.4	Retraining frequency and requirements .....	23
5.3.5	Job rotation frequency and sequence .....	23
5.3.6	Sanctions for unauthorized actions .....	23
5.3.7	Independent audit or review requirements .....	23
5.3.8	Documentation supplied to personnel .....	23
5.4	Audit logging procedures .....	23
5.4.1	Types of events recorded .....	23
5.4.2	Frequency of processing log .....	23
5.4.3	Retention period for audit log .....	23
5.4.4	Protection of audit log .....	23
5.4.5	Audit log backup procedures .....	23
5.4.6	Audit collection system (internal vs. external) .....	23
5.4.7	Number of audit log entries per subject .....	23
5.4.8	Vulnerability assessments .....	24
5.5	Records archival .....	24
5.5.1	Types of records archived .....	24
5.5.2	Retention period for archive .....	24
5.5.3	Protection of archive .....	24
5.5.4	Archive backup procedures .....	24
5.5.5	Requirements for time-stamping of records .....	24
5.5.6	Archive collection system (internal or external) .....	24
5.5.7	Procedures to obtain and verify archive information .....	24
5.6	Key changeover .....	24
5.7	Compromise and disaster recovery .....	24
5.7.1	Incident and compromise handling procedures .....	24
5.7.2	Compliance requirements for data when data are corrupted .....	25
5.7.3	Entity private key compromise procedures .....	25
5.7.4	Business continuity capabilities after a disaster .....	25
5.8	CA or RA termination .....	25
6	Technical security controls .....	26
6.1	Key pair generation and installation .....	26
6.1.1	Key pair generation .....	26
6.1.2	Private key delivery to subscriber .....	26
6.1.3	Public key delivery to certificate issuer .....	26
6.1.4	CA/public key delivery to relying parties .....	26
6.1.5	Key sizes .....	26
6.1.6	Public key parameters: generation and quality checking .....	26
6.1.7	Key usage purposes (as per X.509 v3 key usage field) .....	26
6.2	Private key protection .....	27
6.2.1	Cryptographic module standard and controls .....	27
6.2.2	Private key (in or out of m) multi-person control .....	27
6.2.3	Private key escrow .....	27
6.2.4	Private key backup .....	27
6.2.5	Private key archival .....	27
6.2.6	Private key transfer into or from a cryptographic module .....	27
6.2.7	Private key storage on cryptographic module .....	27
6.2.8	Method of activating private key .....	27
6.2.9	Method of deactivating private key .....	27
6.2.10	Method of destroying private key .....	27
6.2.11	Cryptographic Module Rating .....	27
6.3	Other aspects of key pair management .....	28
6.3.1	Public key archival .....	28
6.3.2	Certificate operational periods and key pair usage periods .....	28
6.4	Activation .....	28
6.4.1	Activation data generation and installation .....	28
6.4.2	Activation data protection .....	28
6.4.3	Other aspects of activation data .....	28
6.5	Computer security controls .....	28
6.5.1	Specific computer security technical requirements .....	28
6.5.2	Computer security rating .....	28
6.6	Life cycle technical controls .....	28
6.6.1	System development controls .....	28
6.6.2	Security management controls .....	28
6.6.3	Life cycle security controls .....	28
6.7	Network security controls .....	29
6.8	Time-stamping .....	29
7	Certification and OCSP profiles .....	30
7.1	Certificate profile .....	30
7.1.1	Version number(s) .....	30
7.1.2	Certificate extensions .....	30
7.1.3	Algorithm object identifiers .....	30
7.1.4	Name form .....	30
7.1.5	Name constraints .....	31
7.1.6	Certificate policy object identifier .....	31
7.1.7	Usage of Policy Constraints extension .....	31
7.1.8	Policy qualifiers .....	31
7.1.9	Processing semantics for the critical Certificate Policies extension .....	31
7.2	CRL profile .....	31
7.2.1	Version number(s) .....	31
7.2.2	CRL entry extensions .....	31
7.3	OCSP profile .....	31
7.3.1	Version number(s) .....	31
7.3.2	OCSP extensions .....	31
8	Compliance audit and other assessments .....	32
8.1	Freedom of information statement of assessment .....	32
8.2	Identity/qualifications of assessor .....	32
8.3	Assessor's relationship to assessed entity .....	32
8.4	Topics covered by assessment .....	32
8.5	Actions taken as a result of deficiency .....	32
8.6	Communication of results .....	32
9	Other business and legal matters .....	33
9.1	Fees .....	33
9.1.1	Certificate issuance or renewal fees .....	33
9.1.2	Certificate access fees .....	33
9.1.3	Revocation or status information access fees .....	33
9.1.4	Fees for other services .....	33
9.1.5	Refund policy .....	33
9.2	Financial responsibility .....	33
9.2.1	Insurance coverage .....	33
9.2.2	Other assets .....	33
9.2.3	Insurance or warranty coverage for end-entities .....	33
9.3	Confidentiality of business information .....	33
9.3.1	Scope of confidential information .....	33
9.3.2	Information not within the scope of confidential information .....	33
9.3.3	Responsibility to protect confidential information .....	33
9.4	Privacy of personal information .....	33
9.4.1	Privacy plan .....	33
9.4.2	Information treated as private .....	33
9.4.3	Information not deemed private .....	34
9.4.4	Responsibility to protect private information .....	34
9.4.5	Notice and consent to use private information .....	34
9.4.6	Disclosure pursuant to judicial or administrative process .....	34
9.4.7	Other information disclosure circumstances .....	34
9.5	Intellectual property rights .....	34
9.6	Representations and warranties .....	34
9.6.1	CA representations and warranties .....	34
9.6.2	RA representations and warranties .....	34
9.6.3	Subscriber representations and warranties .....	34
9.6.4	Relying party representations and warranties .....	34
9.6.5	Representations and warranties of other participants .....	34
9.7	Disclaimers of warranties .....	34
9.8	Limitations of liability .....	35
9.9	Indemnities .....	35
9.10	Term and termination .....	35
9.10.1	Term .....	35
9.10.2	Termination .....	35
9.10.3	Effect of termination and survival .....	35
9.11	Individual notices and communications with participants .....	35
9.12	Amendments .....	35
9.12.1	Procedure for amendment .....	35
9.12.2	Notification mechanism and period .....	35
9.12.3	Circumstances under which OID must be changed .....	35
9.13	Dispute resolution provisions .....	36
9.14	Governing law .....	36
9.15	Compliance with applicable law .....	36
9.16	Miscellaneous provisions .....	36
9.16.1	Entire agreement .....	36
9.16.2	Assignment .....	36
9.16.3	Severability .....	36
9.16.4	Enforcement (attorneys' fees and waiver of rights) .....	36
9.16.5	Force Majeure .....	36
9.17	Other provisions .....	36
	Bibliography .....	37

# Business Process - Legal - Technical

