



*Chambres de Métiers  
et de l'Artisanat*

**APCM**


**CERTIFICATION POLICY**

**CERTIMETIERSARTISANAT**

Identification (OID)	1.2.250.1.191.1.1.1.2	Version	1.3
Creation date	28/05/2008	Updated on	20/01/2012

This document contains 76 pages


Document status	Official
Drafted by	APCM
Verified by	APCM
Approved by	APCM Management Committee (see. I.5.3)

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

## MODIFICATIONS


Date	Status	Version	Comments
02/12/2008	Official	1.0	
19/12/2008	Official	1.1	
25/11/2010	Official	1.2	
20/01/2012	Official	1.3	Correction following audit on 24/11/2011. Deviation forms n°3 (see with APCM), 4 (§XI and XII), 5 (§VIII.2), 10 (§I.3.2), 12 (§III.1.2 and III.1.5), 13 (§ IV.9.3.1), 14 (§ IV.9.7), 15 (§ IV.9.3.1).

## REFERENCED DOCUMENTS


	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

## CONTENTS


<b>MODIFICATIONS</b> .....	<b>2</b>
<b>REFERENCED DOCUMENTS</b> .....	<b>2</b>
<b>CONTENTS</b> .....	<b>3</b>
<b>I. INTRODUCTION</b> .....	<b>11</b>
I.1. OVERVIEW .....	11
I.2. DOCUMENT IDENTIFICATION .....	11
I.3. PKI PARTICIPANTS .....	12
I.3.1. <i>Certification Authorities</i> .....	12
I.3.2. <i>Registration Authorities</i> .....	13
I.3.3. <i>Certificate Bearers</i> .....	13
I.3.4. <i>The certificate users</i> .....	14
I.3.5. <i>Other participants</i> .....	14
I.3.5.1. PKI components .....	14
I.3.5.2. Certification Agent .....	14
I.3.5.3. Certification Operator.....	15
I.4. USE OF CERTIFICATES .....	15
I.4.1. <i>Areas of application</i> .....	15
I.4.1.1. Key pairs and bearer certificates .....	15
I.4.1.2. Key pairs and certificates of the CA and its components .....	15
I.4.2. <i>Prohibited certificate uses</i> .....	16
I.5. CP ADMINISTRATION .....	16
I.5.1. <i>Entity administering the CP</i> .....	16
I.5.1.1. Responsible entity .....	16
I.5.1.2. Natural person responsible for the CP .....	17
I.5.2. <i>Point of contact</i> .....	17
I.5.3. <i>Entity determining the compliance of the CPS with the CP</i> .....	17
I.5.4. <i>Procedures for approving the compliance of the CPS</i> .....	17
I.6. DEFINITIONS AND ACRONYMS .....	17
I.6.1. <i>Terms common to the PRIS</i> .....	18
I.6.2. <i>Terms specific to or supplemented/adapted for this CP</i> .....	19
I.6.3. <i>Terms common to the AFNOR AC Z74-400</i> .....	21
<b>II. PUBLICATION RESPONSIBILITIES</b> .....	<b>22</b>
II.1. ENTITIES RESPONSIBLE FOR THE PROVISION OF INFORMATION .....	22
II.2. MANDATORY PUBLICATION OF INFORMATION .....	22
II.3. PUBLICATION TIMETABLES AND FREQUENCY .....	23
II.4. CONTROL OF ACCESS TO PUBLISHED INFORMATION .....	23
<b>III. IDENTIFICATION AND AUTHENTICATION</b> .....	<b>24</b>

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012


III.1.	NAMING.....	24
III.1.1.	<i>Types of names .....</i>	24
III.1.2.	<i>Need for names to be meaningful .....</i>	24
III.1.3.	<i>Anonymity or pseudonymity of bearers .....</i>	25
III.1.4.	<i>Rules for interpreting various name forms.....</i>	25
III.1.5.	<i>Uniqueness of names .....</i>	25
III.1.6.	<i>Identification, authentication and the role of trademarks.....</i>	25
III.2.	INITIAL IDENTITY VALIDATION.....	26
III.2.1.	<i>Method for proving the possession of the private key.....</i>	26
III.2.2.	<i>Validation of the identity of an organisation .....</i>	26
III.2.3.	<i>Validation of the identity of an individual .....</i>	26
III.2.3.1.	<i>Registration of a Bearer without a CTA .....</i>	26
III.2.3.2.	<i>Registration of a Certification Agent .....</i>	27
III.2.3.3.	<i>Registration of a Bearer via a previously registered CTA .....</i>	27
III.2.4.	<i>Non-verified bearer information.....</i>	28
III.2.5.	<i>Validation of the authority of the applicant.....</i>	28
III.2.6.	<i>Criteria for CA inter-operation .....</i>	28
III.3.	IDENTIFICATION AND VALIDATION FOR RE-KEY REQUESTS .....	29
III.3.1.	<i>Identification and validation for the re-key of a current certificate .....</i>	29
III.3.2.	<i>Identification and validation for a re-key following a revocation .....</i>	29
III.4.	IDENTIFICATION AND VALIDATION OF A REVOCATION REQUEST .....	29
<b>IV.</b>	<b>CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS .....</b>	<b>30</b>
IV.1.	REQUEST FOR A CERTIFICATE .....	30
IV.1.1.	<i>Origin of the request .....</i>	30
IV.1.2.	<i>Processes and responsibilities for establishing a request for a certificate .....</i>	30
IV.2.	CERTIFICATE APPLICATION PROCESSING .....	30
IV.2.1.	<i>Execution of the identification and validation process for the request.....</i>	30
IV.2.2.	<i>Approval or rejection of the request .....</i>	31
IV.2.3.	<i>Time to generate the certificate.....</i>	31
IV.3.	DELIVERY OF THE CERTIFICATE.....	31
IV.3.1.	<i>Actions to be taken by the CA regarding the delivery of the certificate .....</i>	31
IV.3.2.	<i>Notification by the CA of the delivery of the certificate to the Bearer .....</i>	31
IV.4.	CERTIFICATE ACCEPTANCE.....	31
IV.4.1.	<i>Conduct constituting acceptance of the certificate.....</i>	31
IV.4.2.	<i>Publication of the certificate .....</i>	32
IV.4.3.	<i>Notification of certificate issuance by the CA to other entities.....</i>	32
IV.5.	KEY PAIR AND CERTIFICATE USAGE .....	32
IV.5.1.	<i>Bearer private key and certificate usage .....</i>	32
IV.5.2.	<i>The use of the public key and of the certificate by the certificate user.....</i>	32
IV.6.	CERTIFICATE RENEWAL.....	32
IV.6.1.	<i>Possible grounds for renewal of a certificate .....</i>	33
IV.6.2.	<i>Origin of a request for renewal.....</i>	33
IV.6.3.	<i>Procedure for processing a request for renewal.....</i>	33

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012


IV.6.4.	<i>Notifying the Bearer of the issue of a new certificate</i>	33
IV.6.5.	<i>Procedure for accepting a new certificate</i>	33
IV.6.6.	<i>Publication of a new certificate</i>	33
IV.6.7.	<i>Notification of other entities by the CA of the issue of the new certificate</i>	33
IV.7.	DELIVERY OF A NEW CERTIFICATE FOLLOWING A CHANGE TO THE KEY PAIR	33
IV.7.1.	<i>Possible grounds for changes to a key pair</i>	33
IV.7.2.	<i>Origin of a request for a new certificate</i>	33
IV.7.3.	<i>Procedure for processing a request for a new certificate</i>	34
IV.7.4.	<i>Notifying the Bearer of the generation of a new certificate</i>	34
IV.7.5.	<i>Procedure for accepting a new certificate</i>	34
IV.7.6.	<i>Publication of a new certificate</i>	34
IV.7.7.	<i>Notification of other entities by the CA of the issuance of the new certificate</i>	34
IV.8.	MODIFICATION OF THE CERTIFICATE	34
IV.8.1.	<i>Potential grounds for modifying a certificate</i>	34
IV.8.2.	<i>Origin of a request to modify a certificate</i>	34
IV.8.3.	<i>Procedure for processing a request to modify a certificate</i>	34
IV.8.4.	<i>Notifying the Bearer of the creation of a modified certificate</i>	34
IV.8.5.	<i>Procedure for acceptance of the modified certificate</i>	34
IV.8.6.	<i>Publication of the modified certificate</i>	34
IV.8.7.	<i>Notification of other entities by the CA of the delivery of the modified certificate</i>	35
IV.9.	REVOCATION AND SUSPENSION OF THE CERTIFICATE	35
IV.9.1.	<i>Possible grounds for a revocation</i>	35
IV.9.1.1.	<i>Bearer certificates</i>	35
IV.9.1.2.	<i>PKI component certificates</i>	35
IV.9.2.	<i>Origin of a request to revoke a bearer certificate</i>	35
IV.9.2.1.	<i>Bearer certificates</i>	35
IV.9.2.2.	<i>PKI component certificates</i>	36
IV.9.3.	<i>Procedure for processing a revocation request</i>	36
IV.9.3.1.	<i>Revocation of a Bearer certificate</i>	36
IV.9.3.2.	<i>Revocation of certificate issued by a PKI component</i>	37
IV.9.4.	<i>Revocation request grace period</i>	37
IV.9.5.	<i>Time within which the CA must process a revocation request</i>	37
IV.9.5.1.	<i>Revocation of a bearer certificate</i>	37
IV.9.5.2.	<i>Revocation of certificate issued by a PKI component</i>	37
IV.9.6.	<i>Verification requirements for revocations by certificate users</i>	38
IV.9.7.	<i>CRL issuance frequency</i>	38
IV.9.8.	<i>Maximum time limit for publishing a CRL</i>	38
IV.9.9.	<i>Availability of an online system for verifying revocations and the status of certificates</i>	38
IV.9.10.	<i>Requirements for the online verification of certificate revocations by certificate users</i>	38
IV.9.11.	<i>Other available means of obtaining information regarding revocations</i>	38
IV.9.12.	<i>Specific requirements for revocations due to compromised private keys</i>	38
IV.9.13.	<i>Possible grounds for a suspension</i>	38

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

IV.9.14.	<i>Origin of a request for a suspension .....</i>	38
IV.9.15.	<i>Procedure for processing a request to suspend a certificate .....</i>	38
IV.9.16.	<i>Limitations to the suspension period for a certificate .....</i>	39
IV.10.	CERTIFICATE STATUS INFORMATION SERVICE .....	39
IV.10.1.	<i>Operational characteristics.....</i>	39
IV.10.2.	<i>Service availability .....</i>	39
IV.10.3.	<i>Optional procedures.....</i>	39
IV.11.	TERMINATION OF THE RELATIONSHIP WITH THE BEARER.....	39
IV.12.	KEY ESCROW AND RECOVERY.....	39
IV.12.1.	<i>Policy and practices for recovery through key escrow.....</i>	39
IV.12.2.	<i>Policy and practices for recovery through session key encapsulation .....</i>	39
<b>V.</b>	<b>NON-TECHNICAL SECURITY MEASURES .....</b>	<b>40</b>
V.1.	PHYSICAL SECURITY MEASURES .....	40
V.1.1.	<i>Geographic location and site construction.....</i>	40
V.1.2.	<i>Physical access .....</i>	40
V.1.3.	<i>Electrical systems and air conditioning.....</i>	40
V.1.4.	<i>Vulnerability to flood damage .....</i>	40
V.1.5.	<i>Fire prevention and protection.....</i>	40
V.1.6.	<i>Media storage .....</i>	40
V.1.7.	<i>Decommissioning media .....</i>	40
V.1.8.	<i>Offsite data backup .....</i>	41
V.2.	PROCEDURAL SECURITY MEASURES .....	41
V.2.1.	<i>Positions of trust .....</i>	41
V.2.2.	<i>Number of persons required per task .....</i>	41
V.2.3.	<i>Identification and authentication for each role .....</i>	41
V.2.4.	<i>Roles requiring separation of duties .....</i>	42
V.3.	SECURITY MEASURES WITH RESPECT TO PERSONNEL.....	42
V.3.1.	<i>Required qualifications, skills and abilities.....</i>	42
V.3.2.	<i>Background check procedures.....</i>	42
V.3.3.	<i>Initial training requirements .....</i>	43
V.3.4.	<i>Requirements and frequency with regard to further training .....</i>	43
V.3.5.	<i>Job rotation frequency and sequence.....</i>	43
V.3.6.	<i>Sanctions for unauthorised actions .....</i>	43
V.3.7.	<i>Independent contractor requirements.....</i>	43
V.3.8.	<i>Documentation supplied to personnel .....</i>	43
V.4.	AUDIT LOGGING PROCEDURES.....	44
V.4.1.	<i>Types of events recorded.....</i>	44
V.4.2.	<i>Audit log processing frequency .....</i>	45
V.4.3.	<i>Audit log retention period .....</i>	45
V.4.4.	<i>Audit log protection .....</i>	45
V.4.5.	<i>Backup procedure for audit logs.....</i>	45
V.4.6.	<i>Audit log collection system .....</i>	46
V.4.7.	<i>Notification of event recording provided to the individual responsible for the event.....</i>	46


	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

V.4.8.	<i>Vulnerability assessment</i> .....	46
V.5.	RECORDS ARCHIVAL .....	46
V.5.1.	<i>Types of records to be archived</i> .....	46
V.5.2.	<i>Archive retention period</i> .....	46
V.5.3.	<i>Archive protection</i> .....	47
V.5.4.	<i>Backup procedures for archives</i> .....	47
V.5.5.	<i>Requirements for time stamping of records</i> .....	47
V.5.6.	<i>Archive collection system</i> .....	47
V.5.7.	<i>Archive retrieval and audit procedures</i> .....	47
V.6.	CA KEY CHANGEOVER .....	48
V.7.	COMPROMISE AND DISASTER RECOVERY .....	48
V.7.1.	<i>Incident and compromise handling procedures</i> .....	48
V.7.2.	<i>Recovery procedures in the event of corruption of IT resources (hardware, software and / or data)</i> .....	48
V.7.3.	<i>Recovery procedures in the event of compromise of a component's private key...</i>	48
V.7.4.	<i>Business continuity capabilities following a disaster</i> .....	49
V.8.	PKI TERMINATION.....	50
<b>VI.</b>	<b>TECHNICAL SECURITY CONTROLS .....</b>	<b>52</b>
VI.1.	KEY PAIR GENERATION AND INSTALLATION.....	52
VI.1.1.	<i>Key pair generation</i> .....	52
VI.1.1.1.	CA keys .....	52
VI.1.1.2.	Bearer keys generated by the CA.....	52
VI.1.1.3.	Bearer keys generated by the Bearer .....	52
VI.1.2.	<i>Delivery of the private key to its owner</i> .....	52
VI.1.3.	<i>Delivery of the public key to its owner</i> .....	52
VI.1.4.	<i>Delivery of the CA's public key to the certificate users.</i> .....	53
VI.1.5.	<i>Key size</i> .....	53
VI.1.6.	<i>Key pair parameter generation and quality verification</i> .....	53
VI.1.7.	<i>Key usage purposes</i> .....	53
VI.2.	SECURITY MEASURES FOR THE PROTECTION OF PRIVATE KEYS AND CRYPTOGRAPHIC MODULES .....	53
VI.2.1.	<i>Security measures and standards for cryptographic modules</i> .....	53
VI.2.1.1.	The CA's cryptographic modules .....	53
VI.2.1.2.	Bearer authentication and signature devices .....	53
VI.2.2.	<i>Control of the private key by more than one person</i> .....	54
VI.2.3.	<i>Escrow of the private key</i> .....	54
VI.2.4.	<i>Private key backup</i> .....	54
VI.2.5.	<i>Private key archival</i> .....	54
VI.2.6.	<i>Transfer of the private key into/from the encryption module</i> .....	54
VI.2.7.	<i>Private key storage on cryptographic modules</i> .....	54
VI.2.8.	<i>Private key activation method</i> .....	55
VI.2.8.1.	Private CA Keys.....	55
VI.2.8.2.	Private bearer keys.....	55
VI.2.9.	<i>Method for deactivating the private key</i> .....	55
VI.2.9.1.	Private CA keys .....	55


	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

VI.2.9.2.	Private bearer keys.....	55
<b>VI.2.10.</b>	<b>Method for destroying private keys .....</b>	<b>55</b>
VI.2.10.1.	Private CA Keys.....	55
VI.2.10.2.	Private bearer keys.....	55
<b>VI.2.11.</b>	<b>Assessment of the level of security of the cryptographic module.....</b>	<b>55</b>
<b>VI.3.</b>	<b>OTHER ASPECTS OF KEY PAIR MANAGEMENT .....</b>	<b>56</b>
<b>VI.3.1.</b>	<b>Public key archival .....</b>	<b>56</b>
<b>VI.3.2.</b>	<b>Certificate operational periods and key pair usage periods .....</b>	<b>56</b>
<b>VI.4.</b>	<b>ACTIVATION DATA .....</b>	<b>56</b>
<b>VI.4.1.</b>	<b>Activation data generation and installation .....</b>	<b>56</b>
VI.4.1.1.	Activation data generation and installation for the CA private key .....	56
VI.4.1.2.	Activation data generation and installation for the Bearer private key .....	57
<b>VI.4.2.</b>	<b>Activation data protection.....</b>	<b>57</b>
VI.4.2.1.	Activation data protection for the CA private key .....	57
VI.4.2.2.	Activation data protection for the Bearer private keys.....	57
<b>VI.4.3.</b>	<b>Other aspects of activation data .....</b>	<b>57</b>
<b>VI.5.</b>	<b>COMPUTER SECURITY CONTROLS .....</b>	<b>57</b>
<b>VI.5.1.</b>	<b>Specific computer security technical requirements.....</b>	<b>57</b>
<b>VI.5.2.</b>	<b>Computer security rating.....</b>	<b>57</b>
<b>VI.6.</b>	<b>LIFE CYCLE TECHNICAL CONTROLS.....</b>	<b>58</b>
<b>VI.6.1.</b>	<b>System development controls .....</b>	<b>58</b>
<b>VI.6.2.</b>	<b>Security management controls.....</b>	<b>58</b>
<b>VI.6.3.</b>	<b>Life cycle security controls rating .....</b>	<b>58</b>
<b>VI.7.</b>	<b>NETWORK SECURITY CONTROLS .....</b>	<b>58</b>
<b>VI.8.</b>	<b>TIME STAMPING / DATING SYSTEM .....</b>	<b>58</b>
<b>VII.</b>	<b>CERTIFICATE AND CRL PROFILES.....</b>	<b>59</b>
<b>VII.1.</b>	<b>CERTIFICATES PROFILES .....</b>	<b>59</b>
<b>VII.2.</b>	<b>CRL PROFILE.....</b>	<b>61</b>
<b>VII.2.1.</b>	<b>CRL fields .....</b>	<b>61</b>
<b>VII.2.2.</b>	<b>CRL extensions .....</b>	<b>61</b>
<b>VII.3.</b>	<b>OCSP PROFILE.....</b>	<b>61</b>
<b>VII.3.1.</b>	<b>Version number .....</b>	<b>61</b>
<b>VII.3.2.</b>	<b>OCSP extensions.....</b>	<b>61</b>
<b>VIII.</b>	<b>COMPLIANCE AUDIT AND OTHER ASSESSMENTS.....</b>	<b>62</b>
<b>VIII.1.</b>	<b>FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT.....</b>	<b>62</b>
<b>VIII.2.</b>	<b>IDENTITY/QUALIFICATIONS OF THE ASSESSORS .....</b>	<b>62</b>
<b>VIII.3.</b>	<b>ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITIES .....</b>	<b>62</b>
<b>VIII.4.</b>	<b>TOPICS COVERED BY THE ASSESSMENTS .....</b>	<b>62</b>
<b>VIII.5.</b>	<b>ACTIONS TAKEN FOLLOWING THE CONCLUSION OF THE ASSESSMENTS .....</b>	<b>62</b>
<b>VIII.6.</b>	<b>COMMUNICATION OF RESULTS .....</b>	<b>63</b>
<b>IX.</b>	<b>OTHER BUSINESS AND LEGAL MATTERS .....</b>	<b>64</b>
<b>IX.1.</b>	<b>FEES.....</b>	<b>64</b>
<b>IX.1.1.</b>	<b>Certificate issuance or renewal fees.....</b>	<b>64</b>




	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

IX.1.2.	<i>Certificate access fees</i> .....	64
IX.1.3.	<i>Revocation or status information access fees</i> .....	64
IX.1.4.	<i>Fees for other services</i> .....	64
IX.1.5.	<i>Refund policy</i> .....	64
IX.2.	FINANCIAL RESPONSIBILITY .....	64
IX.2.1.	<i>Insurance coverage</i> .....	64
IX.2.2.	<i>Other assets</i> .....	64
IX.2.3.	<i>Extended warranty coverage</i> .....	64
IX.3.	CONFIDENTIALITY OF BUSINESS INFORMATION.....	64
IX.3.1.	<i>Scope of confidential information</i> .....	64
IX.3.2.	<i>Information not within the scope of confidential information</i> .....	65
IX.3.3.	<i>Responsibility to protect confidential information</i> .....	65
IX.4.	PROTECTION OF PERSONAL INFORMATION.....	65
IX.4.1.	<i>Policy for the protection of personal information</i> .....	65
IX.4.2.	<i>Personal information</i> .....	65
IX.4.3.	<i>Information not within the scope of personal information</i> .....	65
IX.4.4.	<i>Responsibility to protect personal information</i> .....	66
IX.4.5.	<i>Notice and consent to use personal information</i> .....	66
IX.4.6.	<i>Disclosure to judicial or administrative authorities</i> .....	66
IX.4.7.	<i>Other circumstances in which private information may be disclosed</i> .....	66
IX.5.	INTELLECTUAL PROPERTY RIGHTS.....	66
IX.6.	REPRESENTATIONS AND WARRANTIES.....	66
IX.6.1.	<i>Certification Authorities</i> .....	67
IX.6.2.	<i>Registration service</i> .....	68
<b>ONLY THE</b> .....		<b>68</b>
IX.6.3.	<i>Certificate bearers</i> .....	68
IX.6.4.	<i>Certificate users</i> .....	69
IX.6.5.	<i>Other participants</i> .....	69
IX.7.	DISCLAIMERS OF WARRANTIES.....	69
IX.8.	LIMITATIONS OF LIABILITY .....	69
IX.9.	INDEMNITIES.....	69
IX.10.	TERM AND TERMINATION.....	69
IX.10.1.	<i>Term</i> .....	69
IX.10.2.	<i>Termination</i> .....	69
IX.10.3.	<i>Effect of termination and survival</i> .....	69
IX.11.	INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS.....	70
IX.12.	AMENDMENTS TO THE CP .....	70
IX.12.1.	<i>Amendment procedures</i> .....	70
IX.12.2.	<i>Notification mechanism and period</i> .....	70
IX.12.3.	<i>Circumstances under which the OID must be changed</i> .....	70
IX.13.	DISPUTE RESOLUTION PROVISIONS .....	70
IX.14.	GOVERNING LAW .....	70
IX.15.	COMPLIANCE WITH APPLICABLE LAWS AND REGULATIONS.....	70

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

IX.16.	MISCELLANEOUS PROVISIONS.....	70
IX.16.1.	<i>Entire agreement</i> .....	70
IX.16.2.	<i>Assignment</i> .....	71
IX.16.3.	<i>Severability</i> .....	71
IX.16.4.	<i>Application and waiver</i> .....	71
IX.16.5.	<i>Force majeure</i> .....	71
IX.17.	OTHER PROVISIONS .....	71
<b>X.</b>	<b>ANNEX 1 – REFERENCE DOCUMENTS.....</b>	<b>72</b>
X.1.	REGULATIONS .....	72
X.2.	TECHNICAL DOCUMENTS .....	73
<b>XI.</b>	<b>ANNEX 2: SECURITY REQUIREMENTS FOR THE CA'S CRYPTOGRAPHIC MODULE .....</b>	<b>75</b>
XI.1.	REQUIREMENTS REGARDING SECURITY OBJECTIVES .....	75
XI.2.	CERTIFICATION REQUIREMENTS.....	75
<b>XII.</b>	<b>ANNEX 3: SECURITY REQUIREMENTS FOR THE AUTHENTICATION AND SIGNATURE DEVICE .....</b>	<b>76</b>
XII.1.	REQUIREMENTS REGARDING SECURITY OBJECTIVES .....	76
XII.2.	CERTIFICATION REQUIREMENTS.....	76

	<p><b>PUBLIC</b></p>	<p>Status: Official</p>
<p><b>CERTIMETIERSARTISANAT</b></p>	<p>Certification Policy</p>	<p>Last updated: 20/01/2012</p>

## I. INTRODUCTION

---

### I.1.OVERVIEW

A Certification Policy (CP) is identified by a unique name (OID\*). It consists of a set of rules describing the terms of admissibility for a Certificate for requests with common security needs.

A CP is defined independently of the implementation methodology for the Public Key Infrastructure (PKI) to which it applies. It describes the requirements with which the PKI must comply in order to register and validate requests for Certificates, as well as for Certificate management. The certification procedures are compiled in a document known as the Certification Practice Statement (CPS), which is separate from the CP and which describes how these requirements are met in practice.

This CP is associated with the CPS that relates to the CERTIMETIERSARTISANAT CA. Unlike the CP, a request to the Electronic Certification Service Provider (ECSP) providing specific grounds for the request is required in order to consult the CPS.

Certificate management covers all of the operations that may occur during life cycle of the certificate, from the time that it is issued until the end of the certificate's life cycle (expiry or revocation).

This document constitutes the Certification Policy of the CERTIMETIERSARTISANAT Certification Authority.

The commitments set out in this CP are drawn from a range of sources:


- The French Référentiel Global de Sécurité version 2.2 (RGS), and in particular the Authentication and Signature Certification Policy Template [RGS] drafted by the DGME and the DCSSI.
- The RFC3647 by the IETF [RFC3647].

### I.2.DOCUMENT IDENTIFICATION

This CP is identified by the OID1.2.250.1.191.1.1.1.2.

- Iso(1)
  - member-body(2)
    - fr(250)
      - type-org(1)
        - APCM (191)
          - CA CERTIMETIERSARTISANAT (1)
            - CPCERTIMETIERSARTISANAT (1)
              - Major version (1)
                - Minor version (2)

The Certification Policy and the Certification Practice Statement are hereinafter referred to as the “CP” and the “CPS”.

	<p><b>PUBLIC</b></p>	<p>Status: Official</p>
<p><b>CERTIMETIERSARTISANAT</b></p>	<p>Certification Policy</p>	<p>Last updated: 20/01/2012</p>

## I.3. PKI PARTICIPANTS

The Public Key Infrastructure (PKI) is composed of a number of entities, which are described below.

### I.3.1. CERTIFICATION AUTHORITIES

The authority to which certification service users give their trust for the purpose of the creation and issuance of certificates is called the Certification Authority, and is listed in the CA document.


A CA is an Electronic Certification Service Provider (ECSP) that issues the certificates.

The CA is wholly responsible for providing the certification services described below:

- **Registration Authority (RA)** –this function verifies the credentials of future bearers via its registration service before sending the request to the certificate generation service. The Registration Authority may appoint a Delegated Registration Authority to carry out the services related to the registration and delivery of the authentication and signature device to the Bearer.
- **Delegated Registration Authority** –appointed by the RA, this function verifies the credentials of future bearers through its registration service before sending the request to the RA's certificate generation service. It is responsible for delivering the authentication and signature device to the Bearer.
- **Registration service** – verifies the identification data of the Bearer of a certificate during its initial registration or renewal.
- **Certificate generation service** – generates and signs the certificates based on the information transmitted by the registration service.
- **Publication and distribution service** – makes available to the parties concerned the general terms and conditions, the policies and practices published by the CA, the CA certificates and all other relevant information intended for the Bearers and/or the users of certificates, excluding information concerning the status of the certificates. Subject to the policy of the CA, it may also distribute the valid bearer certificates.
- **Service for delivering the device to the Bearer** – delivers an authentication and signature device containing the key pair and the Bearer's certificate to the Bearer.
- **Service for delivering the activation code to the Bearer** –this service delivers the activation code for the authentication and signature device to the Bearer.
- **Revocation management service** – processes revocation requests (including the identification and authentication of the applicant) and determines the actions to be taken. The results of this process are distributed via the certificate status information service. One component of this service is equipped to handle emergency revocations.
- **Certificate status information service** – provides information about the status of certificates (revoked, valid, etc.) to certificate users.
- **Bearer assistance service** – assists the Bearers and the users of certificates issued by the CA. This service is accessible by telephone or by email.

A certain number of entities / individuals external to the PKI interact with it. These include:

- **Bearer/Subject** – The natural person who is identified on the certificate and who is the holder of the private key corresponding to the public key listed on the certificate.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

- **Certification Agent (CTA)** – The Certification Agent is appointed by and is under the responsibility of the client entity. It is in direct contact with the RA. It provides the RA with a number of verifications regarding the identity and, if necessary, the attributes of the entity's bearers (in particular, conducts face-to-face meetings to identify the Bearers when this is required).
- **Certificate user** – The entity or natural person who receives a certificate and who places their trust in the certificate to verify the authenticity of the certificate bearer or to verify the electronic signature originating from the certificate bearer.
- **Authorised person** – This is a person other than the Bearer and the certification agent who is authorised under the CA's certification policy or by contract with the CA to carry out certain actions on behalf of the Bearer (request for revocation, renewal, etc.). Typically, in a company, this would be the Bearer's line manager or a human resources manager.

As part of its operational functions, which it may undertake directly or outsource to external entities, the CERTIMETIERSARTISANAT CA, as the head of the PKI, has conducted a risk analysis to determine the specific security objectives needed to cover the business risks of the whole of the PKI. The ad hoc security measures have been implemented.

### I.3.2. REGISTRATION AUTHORITIES

The APCM serves as the Registration Authority (RA) and is responsible for the following services, as set out in §I.3.1:

- the registration service,
- the service for delivering the device to the Bearer,
- the revocation management service.

The APCM, in its capacity as the Registration Authority, delegates the verification of the certificate request file and the delivery of the device to the Bearer or to his or her agent at the *Chambres de métiers et de l'artisanat* (the French Chambers of Trades and Crafts). These Chambers act as the Delegated Registration Authority.


### I.3.3. CERTIFICATE BEARERS

With respect to this CP, certificates are issued to natural persons who are affiliated with an entity. It is therefore necessary to distinguish between the subscriber who signs the contract with the CA and the Bearer or subject to whom the certificate applies.

The Bearer uses his or her private key and the corresponding certificate as part of his or her activities in connection with the entity identified in the certificate and with which he or she has a contractual / hierarchical / regulatory relationship.

The Bearer and the subscriber must comply with the terms that are applicable to them as stipulated in the CP.

The subscriber is ultimately responsible for the use of the private key associated with the public key certificate, but the Bearer is the individual authenticated by his or her private key.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

### I.3.4. THE CERTIFICATE USERS

Certificate users, also known as third party users, rely on the certificates issued by the CA and/or on the digital signatures verified through the use of the certificate. Users may include:

A government service that can be accessed electronically by users (application, web server, database, etc.), under the responsibility of a natural or legal person who uses a certificate and an authentication verification device to validate an access request made by the Bearer of the certificate in the context of controlling access in order to authenticate either the origin of a message or the data transmitted by the Bearer of the certificate. The application must comply with the policy and security practices determined by the application manager.

An agent of an administrative authority (natural person) who is the recipient of a message or data and who uses a certificate and an authentication verification device to authenticate the origin of this message or data transmitted by the Bearer of the certificate. The agent must comply with the policy and the security practices determined by the manager of his or her entity.

A user who receives a message or data from an agent of an administrative authority and who uses a certificate and an authentication verification device to authenticate the origin of this message or data transmitted by the Bearer of the certificate.

Certificate users may also be public market platforms or any application authorised by the CA. A list of these users can be found on <http://www.artisanat.fr>.

### I.3.5. OTHER PARTICIPANTS

#### I.3.5.1. PKI components

The breakdown of the services provided by the CA is given above. The components of the PKI that execute these services are presented in the CA's Certification Practice Statement (CPS).

#### I.3.5.2. Certification Agent

An entity is not obliged to appoint a certification agent (CTA). An entity may appoint one or more CTAs.


In the event that the entity chooses to appoint a CTA, the CTA is formally appointed by a legal representative of the entity concerned. The CTA is in direct contact with the RA of the PKI.

The CTA's commitments in regard to the CA are specified in a written contract with the relevant entity of the CTA. In particular, this contract stipulates that the CTA will:

- properly and independently verify the identity of the future bearers of the entity for which it is the CTA;
- comply with the sections of the CP and of the DCP that apply to it.
- In addition, the entity will notify the CA, if possible in advance but in any event without delay, of the departure of the CTA and, where relevant, will notify the CA of any successor.

Under no circumstances will the CTA have access to any means that would permit him or her to activate and use the private key associated with the public key contained in the certificate delivered to the Bearer.

*Note: Under no circumstances will the CTA possess the activation codes for the certificate bearers' authentication and signature devices. These will be sent directly to the Bearer in all cases.*

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

### I.3.5.3. Certification Operator

The Certification Operator (CO) is a component of the ECSP that is responsible for the following services, as stipulated in §I.3.1:

- the certification generation service,
- the publication and distribution service,
- the service for delivering the activation code to the Bearer,
- the emergency revocation management service,
- the certificate status information service,
- the Bearer assistance service.

The CO must comply with the sections of the CA's CP and CPS that apply to it.

## I.4. USE OF CERTIFICATES

### I.4.1. AREAS OF APPLICATION

#### I.4.1.1. Key pairs and bearer certificates


This CP concerns the key pairs and the certificates intended for the categories of bearers identified in section I.3.3 above, so that these bearers are able to authenticate themselves and/or to electronically sign data (documents, messages) in the context of digitised exchanges with the categories of users identified in section I.3.4 below.

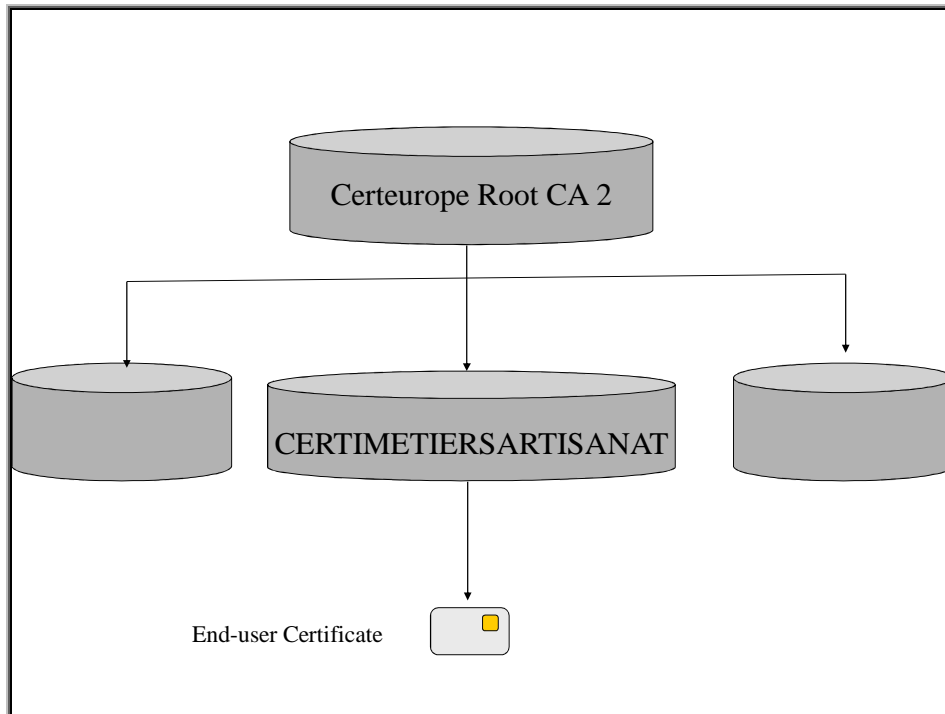
With respect to the **authentication** function, this may relate to authentication in the context of controlling access to a server or an application, or to authenticating the origin of data in the context of an electronic message.

With respect to the **signature** function, this provides, apart from demonstrating the authenticity and integrity of the signed data, the consent of the signatory with respect to the content of these data.

#### I.4.1.2. Key pairs and certificates of the CA and its components

The CA possesses a single key pair and the corresponding certificate forms part of a certification authority. The confidence model is the following:

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012



In accordance with [CWA14167-1], the PKI's various internal keys can be divided into the following categories:

- the CA's signature key is used to sign the certificates generated by the CA as well as information concerning the status of the certificates (CRLs and, if relevant, OCSP responses);
- the infrastructure keys, used by systems contributing to the PKI for authentication, audit log signature, the encryption of data transferred or stored within the PKI, etc.;
- control keys, assigned to PKI personnel in order to self-authenticate vis-à-vis the various systems, to sign and/or encrypt transferred messages or data, etc. For example, keys used by RA personnel who authenticate and sign certificate requests.

#### **I.4.2. PROHIBITED CERTIFICATE USES**

Restrictions on the use of key pairs and certificates are stipulated in section IV.5 below. The CA must comply with these restrictions and ensure the compliance of the Bearers and users of the certificates.

### **I.5.CP ADMINISTRATION**


#### **I.5.1. ENTITY ADMINISTERING THE CP**

##### **I.5.1.1. Responsible entity**

The company APCM is responsible for this CP.

**APCM**  
12 Avenue Marceau  
75008 FRANCE



	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

#### **I.5.1.2. Natural person responsible for the CP**

Monsieur Alain Griset  
 President  
 12 Avenue Marceau  
 75008 FRANCE

#### **I.5.2. POINT OF CONTACT**

All users of certificates issued by this CA may contact APCM:

- By post, at the following address:
- 12 Avenue Marceau, 75008 France
- By email, at the following address:  
[info@apcm.fr](mailto:info@apcm.fr)
- By telephone, at the following number: +33.1.44.43.10.00

#### **I.5.3. ENTITY DETERMINING THE COMPLIANCE OF THE CPS WITH THE CP**


**APCM**, via its Management Committee, determines the compliance of the CP.

#### **I.5.4. PROCEDURES FOR APPROVING THE COMPLIANCE OF THE CPS**

The compliance of the CPS with the CP is approved by the APCM Management Committee, composed of all of its directors.

### **I.6. DEFINITIONS AND ACRONYMS**

CA	Certification Authority
RA	Registration Authority
DRA	Delegated Registration Authority
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information – the French Central Administration for Information Systems Security
PA	Policy Authority
C	Country
ECS	European Committee for Standardization
CISSI	French Interministerial Commission for the Security of Information Systems
CN	Common Name
SF	Subscription File
DGME/SDAE	Directorate General for the Modernisation of the State / Service for the Development of Electronic Administration
DN	Distinguished Name
CPS	Certification Practice Statement
DSA	Digital Signature Algorithm
EAR	Entité d'Audit et de Référencement (French Auditing and Listing Agency)

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012


ETSI	European Telecommunications Standards Institute
PKI	Public Key Infrastructure
CCRL	CA Certificate Revocation List
CRL	Certificate Revocation List
LDAP	Light Directory Access Protocol
CTA	Certification Agent
MD5	Message Digest n°5
MINEFI	Ministry of the Economy, Finance and Industry
O	Organisation
CO	Certification Operator
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organisation Unit
CP	Certification Policy
PDS	PKI Disclosure Statement
PP	Protection Profile
ECSP	Electronic Certification Service Provider
RSA	Rivest Shamir Adelman algorithm
S/MIME	Secure/Multipurpose Internet Mail Extensions
SN	Serial Number
SSCD	Secure Signature Creation Device
SHA-1	Secure Hash Algorithm One
SP	Publication Service
ISS	Information Systems Security
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator

### I.6.1. TERMS COMMON TO THE PRIS

**Applications using the certificates** – Application services using the certificates issued by the Certification Authority for purposes of authentication, encryption or signature of the certificate bearer.

**Administrative Authorities** – This generic term refers to government departments, local authorities, public administrative entities, entities administering social welfare systems and other entities responsible for managing a public administration service.

**Time stamping authority** – Authority responsible for the management of a time stamping service (see the PRIS model time stamping policy).

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

**Public Key Infrastructure (PKI)** – The entirety of the components, services and procedures used to administer the encryption keys and certificates used by Trusted Third Party services. A PKI may consist of a certification authority, a certification operator, a central and/or local registration authority, certification agents, an archiving entity, a publication entity, etc.

**Security product** – A mechanism or device, such as software and/or hardware, the use of which is required in order to implement the security functions necessary to secure digital information (in the course of the transfer, processing and/or storage of such information). This generic term covers devices such as those for digital signatures, authentication and for protecting confidentiality.

**Application promoter** – The manager of a service in the public domain accessible by electronic means.

**Qualification of security products** – An act by which the DCSSI attests to the level of security of a security product, based on the French procedure for evaluating and certifying the security of information technology products and systems. This procedure is described in the [CERTIF] decree.

## I.6.2. TERMS SPECIFIC TO OR SUPPLEMENTED/ADAPTED FOR THIS CP

**Certification Authority (CA)** – Within the ECSP, a Certification Authority is responsible, on behalf of and under the responsibility of the ECSP, for the request of at least one certification policy and is identified as such, being listed as the issuer on certificates issued under this certification policy. In the context of this CP, the term “ECSP” is not used other than in this section and in section I, and the term CA is the only term used herein. This designates the CA responsible for the request of the certification policy, in accordance with the requirements of this CP.


**Registration Authority** – See section I.3.2

**Electronic certificate** – An electronic file attesting that key pair belongs to the natural or legal person or to the hardware or software component identified, directly or indirectly (pseudonym), in the certificate. It is issued by the Certification Authority. In signing this certificate, the CA validates the link between the identity of the natural or legal person or the hardware or software component and the key pair. The certificate is valid for the period of time specified on the certificate. In the context of this CP template, the term “electronic certificate” refers exclusively to a certificate issued to a natural person and bound to authentication and signature key pair, unless explicitly stated otherwise (CA certificate, certificate issued by a component, etc.).

**PIN code** – A code delivered to the Bearer via the postal service after having been randomly and automatically generated by the CA. This code enables the activation of the Bearer’s authentication and signature device. The Bearer must preserve the secrecy of the PIN code under all circumstances, as the use of this code will be deemed to conclusively demonstrate that the Bearer is indeed the initiator of the action (non-repudiation).

**Certificate revocation code** – A code known only by the Bearer and used to apply to for a revocation of the certificate.

**Component** – A platform operated by an entity consisting of at least one computer workstation, a request and, where appropriate, a means of encryption and which plays a specified role in the operational

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

implementation of at least one function or service of the PKI. The entity may be the ECSP itself or an external entity related to the ECSP by a contractual, regulatory or hierarchical link.

**Common Name (CN)** – Real name or pseudonym of the Bearer\* (example: CN = Jean Dupont).

**Community** – A group of people bound together either by contract (for example, a company and its suppliers, a company and its employees, etc.) or by their quality (members of an order, etc.).

**Compromised** – A key is said to be compromised when it is known by individuals other than those authorised to use it.

**Subscription File (SF)** – All supporting documents to be provided to the RA to enable it to verify the information requested by the CA in order to issue a certificate. These supporting documents are described in this CP.

**Certification Practice Statement (CPS)** – A CPS identifies the practices (organisation, operational procedures, technical and human means) that the CA applies in the context of providing its electronic certification services to users in compliance with the certification policy or policies with which it has undertaken to comply.

**Entity** – Designates an administrative authority or business in the broadest sense; in other words, it may also include legal persons under private law, such as associations.

**Certification Agent** – See section I.3.1.


**Authorised person** – See section I.3.1.

**Certification Policy (CP)** – A set of rules, identified by a name (OID), which defines the requirements with which a CA must comply in establishing and providing its services and indicating the applicability of a certificate to a particular community and/or to a class of requests with common security requirements. A CP may also, if necessary, identify the obligations and requirements that apply to other stakeholders, including, among others, certificate bearers and users.

**Bearer** – See section I.3.1

**Electronic Certification Service Provider (ECSP)** – Any person or entity that is responsible for the administration of electronic certificates throughout the life cycle of the certificates, with respect to the Bearers and users of these certificates. An ECSP may provide different categories of certificates designed for different purposes and/or different security levels. An ECSP contains at least one CA, but may contain several CAs depending on the needs of its organisation. The various CAs contained in an ECSP may be independent from each other and/or linked by hierarchical or other relationships (Parent/Child CAs). An ECSP is identified on a certificate for which it is responsible through its CA that issued the certificate, and which is itself directly identified in the “issuer” field of the certificate.

**Listing** – An operation that consists, for the Administration, of maintaining and updating the list of electronic certification offers provided by ECSPs which meet the requirements specified in the PRIS. Only certificates of listed offers can be used by the Administration for its digitised exchanges. An offer listed

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

with respect to a particular PRIS service and a given level of security may be used in any digitised data transfer application that requires this service and this level of security or any lower level of security. For users, listing enables users to understand which offers of electronic certificates they can use for a given digitised transfer.

**Registration service** – See section I.3.1

**Certificate generation service** – See section I.3.1

**Publication and distribution service** – See section I.3.1

**Service for delivering the device to the Bearer** – See section I.3.1

**Service for delivering the activation code to the Bearer** – See section I.3.1

**Revocation management service** – See section I.3.1

**Certificate status information service** – See section I.3.1

**Bearer assistance service** – See section I.3.1

**User** – A natural person acting on his or her own behalf or on behalf of a legal person in his or her relations with a government department.

*Note* – An agent for an administrative authority that is contact with another administrative authority is, from the perspective of the latter, a user.

**Certificate user** – See section I.3.1

### I.6.3. TERMS COMMON TO THE AFNOR AC Z74-400


**Secure Signature Creation Device** – device

**Advanced electronic signature** – electronic signature that meets the following requirements:

- a) Uniquely linked to the signatory;
- b) Enables the identification of the signatory;
- c) Created using a method that ensures that the signatory is able to keep it under his or her exclusive control; and
- d) Linked to the data to which it relates, in such a way that any subsequent modification of the data is detectable (see Directive 1999/93/CE).

**Subscriber** – see section I.3.3

**Subject** – see Bearer

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

## II. PUBLICATION RESPONSIBILITIES

### II.1. ENTITIES RESPONSIBLE FOR THE PROVISION OF INFORMATION

The CO is responsible for the following publication services:

- the publication and distribution service,
- the certificate status information service.

The CO uses a number of channels for disseminating information based on availability requirements.

The channels used are:

- copy 1 (original): ldap://lcr1.certimetiersartisanat.fr/CN=CERTIMETIERSARTISANAT, OU=0002 187500046, O=APCM, C=FR?certificateRevocationList;
- copy 2: ldap://lcr2.certimetiersartisanat.fr/CN=CERTIMETIERSARTISANAT, OU=0002 187500046, O=APCM, C=FR?certificateRevocationList;
- copy 3: http://lcr.certimetiersartisanat.fr/reference/certimetiersartisanat.crl.

### II.2. MANDATORY PUBLICATION OF INFORMATION


On behalf of the CERTIMETIERSARTISANAT CA, the CO publicly distributes:

- the current CERTIMETIERSARTISANAT Certification Policy (CP);
- the Certificate Revocation List (CRL);
- the CA's currently valid certificates;
- information that enables users to verify the origin and status of the CA's certificates;
- the application forms for registering, revoking and renewing a certificate;
- the general terms of sale;
- the digital fingerprint for published data (for example, hash files for the CP).

The recommended format for publishing documents is PDF, to ensure ease of reading for users.

On behalf of the CERTIMETIERSARTISANAT CA, the CO undertakes to publicly distribute:

- the current CERTIMETIERSARTISANAT Certification Policy (CP), available at suivante [http://pc.certimetiersartisanat.fr/reference/pc-certimetiersartisanat\\_v1.3\\_en.pdf](http://pc.certimetiersartisanat.fr/reference/pc-certimetiersartisanat_v1.3_en.pdf);
- the Certificate Revocation List (CRL);
- the certificate of the currently valid Certeuropa Root CA 2, to which the CERTIMETIERSARTISANAT CA's key is subordinated. This certificate is available on the APCM website at [http://pc.certimetiersartisanat.fr/reference/certeuropa\\_root\\_ca\\_2.cer](http://pc.certimetiersartisanat.fr/reference/certeuropa_root_ca_2.cer). The digital fingerprint of the certificate is also available to ensure its integrity;
- the CERTIMETIERSARTISANAT CA's current certificate and its digital fingerprint. This certificate is available on the APCM website at <http://pc.certimetiersartisanat.fr/reference/certimetiersartisanat.crt>. The digital fingerprint of the certificate is also available to ensure its integrity;
- the general terms and conditions of use: "PKI Disclosure Statement";

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

- the general and specific terms and conditions of use of the certificates;
- The form for requesting a certificate;
- The form for revoking a certificate.

The complete certification application file is available at:

[http://www.artisanat.fr/portals/0/services/certimetiersartisanat/Craftsman\\_subscription\\_contract.pdf](http://www.artisanat.fr/portals/0/services/certimetiersartisanat/Craftsman_subscription_contract.pdf).

As the CERTIMETIERSARTISANAT CA is not cross-certified with any other CA, publication of the list of CAs with which it is cross-certified is not applicable.

### II.3. PUBLICATION TIMETABLES AND FREQUENCY

The timetables and frequency of publication depend on the information concerned:

- For information related to the PKI (new version of the CP, forms, etc.), the information is published as soon as is necessary in order to ensure that the published information and the CA's commitments, mechanisms and personnel procedures are consistent at all times.
- For CA certificates, the information must be released prior to any distribution of bearer certificates and/or the corresponding CRLs, within a 24 hour period.
- For information regarding the status of the certificates, see §IV.9.

The availability requirements for the systems that publish this information depend on the information concerned:


- For information related to the PKI (new version of the CP, forms, etc.), the systems are available during hours, with a maximum period of non-availability due to service interruptions (breakdowns or maintenance) of 8 hours (working days) and a total maximum duration of non-availability per month of 32 hours (working days), except in cases of force majeure.
- For CA certificates, the systems are available 24 hours a day, 7 days a week with a maximum period of non-availability due to service interruptions (breakdowns or maintenance) of 2 hours and a total maximum duration of non-availability per month of 8 hours, except in cases of force majeure.
- For information on the status of certificates.

### II.4. CONTROL OF ACCESS TO PUBLISHED INFORMATION

All information published for the benefit of certificate users is accessible on a read-only basis.

Write access to certificate status information publication systems (adding, deleting or modifying published information) is strictly limited to authorised internal functions of the PKI, with strong access control (based on a two-factor authentication procedure).

Write access to other information publication systems is strictly limited to authorised internal functions of the PKI, with password-restricted access control based on a strict password management policy.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

### III. IDENTIFICATION AND AUTHENTICATION

---

#### III.1. NAMING

##### III.1.1. TYPES OF NAMES

The names used comply with the specifications of the X.500 standard.

In each X509v3 certificate, the CERTIMETIERSARTISANATCA (issuer) and the Bearer (subject) are identified by a X.501 “Distinguished Name” (DN) in accordance with the requirements stipulated in the document [[PROFILS].


##### III.1.2. NEED FOR NAMES TO BE MEANINGFUL

The names selected to designate the Bearers of the certificates must be meaningful.

The information contained in the “Subject” field of the Certificate is explicitly described below according to the different X509v3 fields:

- in the “**CountryName**” field: the characters FR;
- in the “**OrganizationalName**” field:
  - The full official name of the entity, as it appears on the company’s K-Bis (company registration certificate) or in its SIRENE (French business register) notice;
- in the “**OrganizationUnitName**” field:
  - This field contains the company’s SIREN number, which is listed on the company’s K-Bis or on its SIRENE notice. The number is preceded by the number string “0002” and a space.
  - If the “**OrganizationUnitName**” attribute is present in other instances, these entries must not begin with a 4-number string.
- in the “**CommonName**” field:
  - This field contains the first given name of the Bearer’s full legal name (if the identity document presented for the registration lists additional given names, there is no requirement to list these additional names on the certificate. However, if these additional names are listed, they must be listed in the same order as on the identity document and separated by a comma, with no space either before or after the comma), followed by a space, followed by either the Bearer’s full legal surname, or by his or her customary surname as listed on his or her identity document. This choice is at the discretion of the Bearer. Following the full legal surname, and depending on the needs of the CA, other information may be included in this attribute (separated by spaces), such as information that will enable the CA to process the information in the event of names with similar spelling within the CA’s domain. However, if the “**SerialNumber**” attribute is included on the certificates, this is the attribute that must be used to process the information in the event of names with similar spelling (see [RFC3739]).
- in the “**SerialNumber**” field:
  - This field is used to ensure the uniqueness of the DN through the use of a HASH (SHA-1) generated from the Bearer’s personal information contained in the identity document (national identity card or passport or residence permit). This makes it possible to resolve instances of similar spelling (see [RFC3739]).
- in the “**Description**” field:



	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

- This field contains the registration number of the trades register. This number is used for information purposes. It is listed in the trades register kept by the chambers of trades and crafts.
- in the **“BusinessCategory”** field:  
This field contains the APE code, which categorises the primary business activity of the applicant.
- in the field **“1.2.250.1.191.20.1”**:

This field contains the code of the Registration Authority that generated the certificate.

This field is defined according to the following naming convention:

- Iso(1)
  - member-body(2)
    - fr(250)
      - type-org(1)
        - APCM (191)
          - Field specific to the management of the RAs (20)
            - Version (1)

For example: DN = {C=FR, O=APCM, OU= 0002 432159752, CN=Jean-Claude DUPONT, SN=5e4be36a5566813d7b0ee92c4e01189a9abcd6ad, Description=01234567891, 2.5.4.15=10.71C, [Email=jean-claude.dupont@apcm.fr](mailto:jean-claude.dupont@apcm.fr), 1.2.250.1.191.20.1=APCM}

### III.1.3. ANONYMITY OR PSEUDONYMITY OF BEARERS

The use of pseudonyms is not permitted.

Under no circumstances may certificates that are subject to the CERTIMETIERSARTISANAT CA be anonymous.

### III.1.4. RULES FOR INTERPRETING VARIOUS NAME FORMS

No particular interpretation is required for information contained in the **“Subject”** field of the certificates.

This information is determined by the RA and relies primarily on the following rules:

- all characters are in the *printableString* or *UTF8String* format, i.e. using neither accents nor characters that are specific to the French language and that comply with the X.501 standard;
- compound (double-barrelled) given names and surnames are separated with a hyphen: “-”.

### III.1.5. UNIQUENESS OF NAMES


The uniqueness of the DN is ensured by the uniqueness of the information used to create the DN. The DN is composed of the SIREN number to differentiate between two companies, the name and surname of the Bearer and the HASH of the number in his or her identity document.

### III.1.6. IDENTIFICATION, AUTHENTICATION AND THE ROLE OF TRADEMARKS

The right to use a name that is a trademark, business name or service mark or other distinctive mark (trade name, logo, company name) as defined in Articles L.711-1 et seq. of the Intellectual Property Code (codified by Law No. 92-957 of 1<sup>st</sup> July 1992 and subsequent amendments) belongs to the rightful owner of that trademark, business name, service mark or other distinctive mark, or its licensees or assignees.

The RA restricts its verifications on the right to use a name to the verification of the information contained in the identification documents, any mandates, the K-bis and the SIRENE notice.

APCM disclaims all liability for unauthorised use by customers and subscribers of trademarks, well-known brands and distinctive symbols, as well as domain names.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

The CA is committed to ensuring the uniqueness of the names of its Bearers, in accordance with section III.1.5, and makes procedures available for the amicable resolution of disputes.

## III.2. INITIAL IDENTITY VALIDATION

The registration of a Bearer may be executed either directly with an RA, or through a Certification Agent. In the latter case, the CTA is previously registered by the RA.

The initial validation of the identity of an entity or of a natural person is therefore obtained, in the following cases, by:

- Registration of a Bearer without a CTA: validation by the RA of the identity of the “legal person” that is the entity with which the Bearer is associated, and of the identity of the “natural person” who is the future bearer.
- Registration of a CTA: validation of the identity of the “legal person” that is the entity on behalf of which the CTA is acting, and of the identity of the “natural person” who is the future CTA.
- Registration of a Bearer via a CTA that has already been registered: validation by the CTA of the identity of the “natural person” who is the future bearer.

For simplicity of presentation, these different cases are grouped together in section III.2.3.

### III.2.1. METHOD FOR PROVING THE POSSESSION OF THE PRIVATE KEY

Not applicable. The Bearer does not generate his or her private key.

### III.2.2. VALIDATION OF THE IDENTITY OF AN ORGANISATION

See §III.2.3.


### III.2.3. VALIDATION OF THE IDENTITY OF AN INDIVIDUAL

#### III.2.3.1. Registration of a Bearer without a CTA

For the distribution of certificates by the RA, a face-to-face meeting is mandatory. This face-to-face meeting may take place directly between the Bearer and the RA. In this case, the RA will verify the original of the Bearer’s official identification document containing the Bearer’s photograph and signature, and will take a copy of this identity document.

The registration document submitted directly to the RA must include, at a minimum:

- A request for a certificate
  - a written request, on letterhead bearing the SIREN number of the company, signed by the company’s legal representative and dated no earlier than 3 months prior to the request date. A template is available on [www.artisanat.fr](http://www.artisanat.fr);
  - a declaration by the Bearer accepting the Bearer commitments;
  - the Bearer’s professional postal address;
  - the surname of the Subscriber to be listed on the certificate;
  - the applicant’s email address;

	<p><b>PUBLIC</b></p>	<p>Status: Official</p>
<p><b>CERTIMETIERSARTISANAT</b></p>	<p>Certification Policy</p>	<p>Last updated: 20/01/2012</p>

The supporting documents proving the identity of the Bearer:

- a photocopy of an identity document containing a photograph of the Bearer (national identity card, passport or residence permit). This document must indicate the Bearer's date and place of birth.

The supporting documents proving the identity of the entity (Company):

- a photocopy of an identity document of the company's legal representative containing a photograph of the legal representative (national identity card, passport or residence permit). This document must indicate the legal representative's date and place of birth;
- an extract of the certificate of registration with the trades register.

*Note: The Bearer must be informed that his or her personal identity information may be used as part of the authentication process in the event of a revocation request.*

### III.2.3.2. Registration of a Certification Agent

An RA may choose to create a registration file for a Certification Agent (CTA) to meet the following needs:

- To use the CTA's file as a reference for the entity identification data for all of the Bearers presented by the CTA.
- If necessary, to provide a certificate to the CTA so that it may electronically sign the registration files for the Bearers of the entities that it represents.

The registration of a CTA must include:


- A written request, dated less than 3 months prior to the submission of the registration file, signed by a legal representative of the entity,
- a mandate, dated less than 3 months prior to the submission of the registration file, signed by a legal representative of the entity that is designating the CTA as its agent. This mandate is signed by the CTA to document its acceptance of the mandate,
- a commitment on the company letterhead or seal dated less than 3 months prior to the submission date, signed by the CTA, undertaking to respect and enforce all contractual provisions and procedures in accordance with the electronic signature service subscription contract,
- an undertaking, dated less than 3 months prior to the submission of the registration file, signed by the CTA, notifying the RA of its departure from the entity,
- a document, valid as of the date of registration, bearing the company's SIREN number (K-bis extract or certificate of identification from the Répertoire National des Entreprises et de leurs Etablissements (the French National Registry of Companies) or, if neither of these documents is available, an alternative document proving the unique identity of the company that will be listed on the certificate;
- a valid official identity document for the CTA containing an identity photograph (such as a national identity card, passport or residence permit). This document will be presented to the RA, which will retain a copy,

*Note: The CTA must be informed that his or her personal identity information may be used as part of the authentication process in the event of a revocation request.*

*Note: A face-to-face meeting must be held between the CTA and the RA.*

### III.2.3.3. Registration of a Bearer via a previously registered CTA

For the distribution of certificates by the RA, a face-to-face meeting is mandatory. This face-to-face meeting may take place directly between the Bearer and the CTA. In this case, the CTA will verify the

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

original of the Bearer's official identification document containing the Bearer's photograph and signature, and will take a copy of this identity document.

The registration file, lodged with the RA via a CTA, will include:

- A request for a certificate
  - A written request, on letterhead containing the SIREN number of the company, signed by the legal representative or the CTA, dated no earlier than 3 months prior to the request date. A template is available at [http://www.artisanat.fr/portals/0/services/certimetiersartisanat/Craftsman\\_subscription\\_contract.pdf](http://www.artisanat.fr/portals/0/services/certimetiersartisanat/Craftsman_subscription_contract.pdf)
  - a declaration by the Bearer accepting the Bearer commitments;
  - the Bearer's professional postal address;
  - the surname of the Subscriber to be listed on the certificate;
  - the applicant's email address;
- The supporting documents proving the identity of the Bearer:
  - a photocopy of an identity document containing a photograph of the Bearer (national identity card, passport or residence permit). This document must indicate the Bearer's date and place of birth.
- The CTA's registration file if the CTA has not previously been registered (see III.2.3.2).

*Note: The CTA must be mandated by the legal representative of the Bearer's entity.*

- The supporting documents proving the identity of the entity (Company), if these are different from those of the CTA;
  - a photocopy of an identity document of the company's legal representative containing a photograph of the legal representative (national identity card, passport or residence permit). This document must indicate the legal representative's date and place of birth;
  - an extract of the certificate of registration with the trades register

*Note: The Bearer must be informed that his or her personal identity information may be used as part of the authentication process in the event of a revocation request.*

#### **III.2.4. NON-VERIFIED BEARER INFORMATION**


The Email, Description and BusinessCategory fields are for information purposes only and cannot be used for supplementary verification purposes.

#### **III.2.5. VALIDATION OF THE AUTHORITY OF THE APPLICANT**

This step is performed at the same time as the validation of the identity of the natural person (either directly by the RA or by the CTA).

#### **III.2.6. CRITERIA FOR CA INTER-OPERATION**

Not applicable. The CERTIMETIERSARTISANAT CA has no recognition agreement with any other CA.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

### **III.3. IDENTIFICATION AND VALIDATION FOR RE-KEY REQUESTS**

#### **III.3.1. IDENTIFICATION AND VALIDATION FOR THE RE-KEY OF A CURRENT CERTIFICATE**

The CERTIMETIERSARTISANAT Certification Authority does not permit re-keying in the sense used by the PRIS. For the purposes of the CERTIMETIERSARTISANAT CA, rekeying a certificate is broken down into two phases:

- revocation of the existing certificate; and
- generation of new keys and a new certificate.


#### **III.3.2. IDENTIFICATION AND VALIDATION FOR A RE-KEY FOLLOWING A REVOCATION**

Following definitive revocation of a certificate, regardless of cause, the procedure for identification and validation of the renewal application is identical to the initial registration procedure (see § III.2). However, when the revocation takes less than 6 (six) months after the issue date of a certificate, the procedure is limited to the application for the certificate only. The only check required is of the applicant's registration with the trades register.

### **III.4. IDENTIFICATION AND VALIDATION OF A REVOCATION REQUEST**

A request for revocation may be made:

- by post or by fax. It is signed by the applicant and the Revocation Management Service verifies the identity of the applicant (the signature must be checked against a previously recorded signature) and his or her authority with respect to the certificate to be revoked.
- by telephone or by email. The applicant will be formally authenticated: verification of the identity of the applicant and of his or her authority with respect to the certificate that is to be revoked. The identity of the applicant will be established through a series of 3 questions regarding information specific to the applicant, including a revocation code known only to the applicant.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

## IV. CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS

---

### IV.1. REQUEST FOR A CERTIFICATE

#### IV.1.1. ORIGIN OF THE REQUEST

A CERTIMETIERSARTISANAT certificate may be applied for by the future bearer, the legal representative of the entity or the duly authorised CTA for that entity. In all cases, the prior consent of the future bearer is mandatory.

#### IV.1.2. PROCESSES AND RESPONSIBILITIES FOR ESTABLISHING A REQUEST FOR A CERTIFICATE

The following information is part of the request for a certificate (see section III.2 above):

- the name of the Bearer to be listed on the certificate (real name or pseudonym);
- the Bearer's personal identification data;
- the identification data of the entity (except in cases where the registration is carried out by a CTA acting as an intermediary)

The request file may either be created directly by the future bearer, based on the elements provided to him or her by his or her entity, or created by the entity and signed by the future bearer. If the company has not appointed a CTA, the file is sent directly to the RA. If the company has appointed a CTA, the file is sent to that CTA.

### IV.2. CERTIFICATE APPLICATION PROCESSING

#### IV.2.1. EXECUTION OF THE IDENTIFICATION AND VALIDATION PROCESS FOR THE REQUEST

A request for a certificate may be lodged or sent by post to the RA's registration service.

When the registration file is received, the RA will execute the following operations:


- validate the identity of the future bearer;
- verify the consistency of the supporting documents provided;
- ensure that the future bearer is aware of the applicable terms and conditions for the use of the certificate.

*Note: If the file is not complete, the applicant is contacted in order to complete the file. Regardless of the outcome of the request, the applicant is informed.*

In the case of requests made via a CTA, the CTA will forward the file to the RA after carrying out the operations listed above. The RA will ensure that the request is consistent with the CTA's mandate.

Once these operations have been carried out, the RA issues the request to generate the certificate to the appropriate function of the PKI (see section I.3.1).

The RA retains the documents specified in the archiving procedure; in particular, it retains an original copy of the request signed by the future bearer and by the RA, or by the CTA where applicable, together with a photocopy of the identity document presented with the request.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

#### **IV.2.2. APPROVAL OR REJECTION OF THE REQUEST**

In the event that the request is rejected, the RTA will inform the Bearer, or the CTA where applicable, by letter explaining the reasons for the rejection of the request.

#### **IV.2.3. TIME TO GENERATE THE CERTIFICATE**

The time required to generate a certificate is three working days from the day on which the complete request is received. This does not take into account the time that may be required for the keys to be delivered via the postal service.

### **IV.3. DELIVERY OF THE CERTIFICATE**

#### **IV.3.1. ACTIONS TO BE TAKEN BY THE CA REGARDING THE DELIVERY OF THE CERTIFICATE**

When a request for a certificate has been approved by the RA's registration service, the RA will next issue a request for the certificate to be generated to the CA's certificate issuance service. When this request is made, the Bearer's keys will be generated on the authentication and signature device.

Following authentication of the origin of the request and verification of the integrity of the request originating from the RA, the CA will initiate the certificate generation procedure.

Once the certificate has been generated, the CA's code activation provision service (OSC) will send the PIN code to the Bearer, who is thus officially notified that the certificate has been issued.

*Note: The service for delivering the signature and authentication device activation code to the Bearer is necessarily independent of the APCM. This independence ensures that only the Bearer is in a position to use his or her authentication and signature device.*

The time required to generate a certificate is 3working days from the day on which the complete request is received. NB: this refers to the time required to generate the certificate (the time necessary for the RA to generate the key) and not the time required to deliver the certificate.

#### **IV.3.2. NOTIFICATION BY THE CA OF THE DELIVERY OF THE CERTIFICATE TO THE BEARER**


The Bearer is immediately notified by email as soon as the certificate is generated.

The RA's service for delivering the device to the Bearer delivers the signature and authentication device to the Bearer or to the CTA in a face-to-face meeting. During this face-to-face meeting, the RA verifies the identity of the Bearer or of the CTA by ensuring that the supporting documents submitted with the request correspond to the original documents presented during the meeting.

### **IV.4. CERTIFICATE ACCEPTANCE**

#### **IV.4.1. CONDUCT CONSTITUTING ACCEPTANCE OF THE CERTIFICATE.**

The acceptance of the cryptographic module from the RA constitutes the acceptance of the certificate.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

During the face-to-face meeting in which the SSCD is delivered, either the Bearer or the CTA signs a receipt certifying their acceptance of the certificate. This receipt is included in the Bearer file maintained by the RA.

#### **IV.4.2. PUBLICATION OF THE CERTIFICATE**

Bearer certificates are not published by the CA.

#### **IV.4.3. NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES**

When the new Certificate is generated:

- the RA is necessarily notified, as it is the RA who initiates the process and who ensures that the certificate that has been applied for is contained on the Bearer's authentication and signature device;
- the CO is aware of the request by the RA, as this organisation is responsible for the technical part of the CA and, in particular, for the signature of the certificate. In addition, all requests are tracked;
- the CA, in its role as the entity that manages the PKI as a whole, has a monitoring tool available to it that enables it to track certificate issuance;
- the Bearer is notified by email as soon as the certificate is issued;
- the applicant is contacted by the RA to collect his or her certificate.

### **IV.5. KEY PAIR AND CERTIFICATE USAGE**

#### **IV.5.1. BEARER PRIVATE KEY AND CERTIFICATE USAGE**

The use of the Bearer's private key and its associated certificate is strictly limited to authentication and signature. The Bearers must strictly observe the authorised uses of the key pairs and the certificates. If they fail to do so, they will be held liable.

The authorised use of the Bearer's key pair and the associated certificate is indicated on the certificate itself, through the extensions concerning the uses of the keys.

#### **IV.5.2. THE USE OF THE PUBLIC KEY AND OF THE CERTIFICATE BY THE CERTIFICATE USER**


See the preceding section and section I.4. The certificate users must strictly observe the authorised uses of the certificates. If they fail to do so, they will be held liable.

### **IV.6. CERTIFICATE RENEWAL**

The lifetime of a certificate is three years. The CERTIMETIERSARTISANAT Certification Authority does not permit the renewal of its certificates.

The Bearer will be notified by post or by email at least one month prior to the expiry date of his or her certificate.



	<p><b>PUBLIC</b></p>	<p>Status: Official</p>
<p><b>CERTIMETIERSARTISANAT</b></p>	<p>Certification Policy</p>	<p>Last updated: 20/01/2012</p>

#### **IV.6.1. POSSIBLE GROUNDS FOR RENEWAL OF A CERTIFICATE**

Not applicable.

#### **IV.6.2. ORIGIN OF A REQUEST FOR RENEWAL**

Not applicable.

#### **IV.6.3. PROCEDURE FOR PROCESSING A REQUEST FOR RENEWAL**

Not applicable.

#### **IV.6.4. NOTIFYING THE BEARER OF THE ISSUE OF A NEW CERTIFICATE**

Not applicable.

#### **IV.6.5. PROCEDURE FOR ACCEPTING A NEW CERTIFICATE**

Not applicable.

#### **IV.6.6. PUBLICATION OF A NEW CERTIFICATE**

Not applicable.

#### **IV.6.7. NOTIFICATION OF OTHER ENTITIES BY THE CA OF THE ISSUE OF THE NEW CERTIFICATE**

Not applicable.

### **IV.7. DELIVERY OF A NEW CERTIFICATE FOLLOWING A CHANGE TO THE KEY PAIR**

*Note - in compliance with [RFC3647], this section addresses the delivery of a new certificate to the Bearer in connection with the generation of a new key pair.*

#### **IV.7.1. POSSIBLE GROUNDS FOR CHANGES TO A KEY PAIR**

Key pairs are renewed at least once every three years.


In addition, a key pair and a certificate may be renewed in advance, following the revocation of the Bearer certificate (see section IV.9 and in particular section IV.9.1.1 for the different possible causes of a revocation).

*Note: For the remainder of this section, the term used is "provision of a new certificate". Where it is generated by the CA, this term also covers the provision of the new key pair to the Bearer.*

#### **IV.7.2. ORIGIN OF A REQUEST FOR A NEW CERTIFICATE**

The Bearer will be notified by post or by email at least one month prior to the expiry date of his or her certificate.

The origin of a request for a new certificate is identical to that of an initial request.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

#### **IV.7.3. PROCEDURE FOR PROCESSING A REQUEST FOR A NEW CERTIFICATE**

The procedure for processing a request for a new certificate is identical to that for an initial request (see section IV.3.1)

#### **IV.7.4. NOTIFYING THE BEARER OF THE GENERATION OF A NEW CERTIFICATE**

See section IV.3.2.

#### **IV.7.5. PROCEDURE FOR ACCEPTING A NEW CERTIFICATE**

See section IV.4.1.

#### **IV.7.6. PUBLICATION OF A NEW CERTIFICATE**

See section IV.4.2.

#### **IV.7.7. NOTIFICATION OF OTHER ENTITIES BY THE CA OF THE ISSUANCE OF THE NEW CERTIFICATE**

See section IV.4.3.

### **IV.8. MODIFICATION OF THE CERTIFICATE**

*Note - in compliance with [RFC3647], the modification of a certificate refers to the modification of information without changing the public key (see section IV.7) and to changes other than those solely to the certificate's dates of validity (see section IV.6).*

Modifications to CERTIMETIERSARTISANAT certificates are not permitted.

#### **IV.8.1. POTENTIAL GROUNDS FOR MODIFYING A CERTIFICATE**

Not applicable.

#### **IV.8.2. ORIGIN OF A REQUEST TO MODIFY A CERTIFICATE**

Not applicable.

#### **IV.8.3. PROCEDURE FOR PROCESSING A REQUEST TO MODIFY A CERTIFICATE**

Not applicable.

#### **IV.8.4. NOTIFYING THE BEARER OF THE CREATION OF A MODIFIED CERTIFICATE**


Not applicable.

#### **IV.8.5. PROCEDURE FOR ACCEPTANCE OF THE MODIFIED CERTIFICATE**

Not applicable.

#### **IV.8.6. PUBLICATION OF THE MODIFIED CERTIFICATE**

Not applicable.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

#### **IV.8.7. NOTIFICATION OF OTHER ENTITIES BY THE CA OF THE DELIVERY OF THE MODIFIED CERTIFICATE**

Not applicable.

### **IV.9. REVOCATION AND SUSPENSION OF THE CERTIFICATE**

A CERTIMETIERSARTISANAT certificate can only exist in one of three states: valid, expired or revoked.

#### **IV.9.1. POSSIBLE GROUNDS FOR A REVOCATION**

##### **IV.9.1.1. Bearer certificates**

The following scenarios may be grounds for the revocation of a bearer certificate:

- the Bearer information listed on the certificate is not or is no longer correct prior to the normal expiry date of the certificate;
- the information included in the subscription file is no longer accurate or has been found to be fraudulent;
- the Bearer has failed to comply with the rules for the use of the certificate;
- the Bearer's private key is suspected of being compromised, has been compromised or has been lost;
- the cancellation or non-payment of the subscription contract;
- the Bearer, the CTA or the legal representative of the entity has requested that the certificate be revoked;
- the departure, transfer or death of the Bearer, or the cessation of the business activities of his or her company.

When one of the above circumstances has occurred and CA has become aware of such circumstance, the certificate concerned will be revoked and placed on the Certificate Revocation List (CRL).

##### **IV.9.1.2. PKI component certificates**

The following circumstances may be grounds for revoking the certificate of a PKI component (including certificates provided by the CA for issuing certificates or CRLs):

- the suspicion of the compromise, the compromise, loss or theft of the component's private key;
- the decision to terminate the PKI component following the detection of non-compliance of procedures within the component with those announced in the CPS (for example, following a negative qualification or compliance audit);
- cessation of the business activity of the entity operating the component.


#### **IV.9.2. ORIGIN OF A REQUEST TO REVOKE A BEARER CERTIFICATE**

##### **IV.9.2.1. Bearers' certificates**

A request to revoke a bearer certificate may be originated by:

- the Bearer in whose name the certificate was issued;
- the legal representative of the company;
- the Certification Agent;
- the CERTIMETIERSARTISANAT CA that issued the certificate or the RA.

*Note: The Bearer must be notified of the persons / entities that are qualified to submit a request to*

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

revoke his or her certificate.

#### **IV.9.2.2. PKI component certificates**

The decision to revoke a CA's certificate may only be made by the responsible entity of the CA or by the judicial authorities via a court order.

The decision to revoke certificates by other components is made by the entity operating the component concerned. This entity must notify the CA without delay.

### **IV.9.3. PROCEDURE FOR PROCESSING A REVOCATION REQUEST**

#### **IV.9.3.1. Revocation of a Bearer certificate**

The requirements for the identification and validation of a revocation request, performed offline or online by the revocation management service, are described in section III.4.

The revocation request must contain, at a minimum:

- the given name and surname of the revocation applicant;
- the identity of the Bearer;
- the DN of the Bearer or any other information (for example: the emergency revocation code of the certificate) that will make it possible to definitively identify the certificate to be revoked.

Requests for revocation by the Bearers, the CTAs and by companies' legal representatives may be made to the RA in person (during business hours), by sending a request in an electronic format signed with the use of a certificate issued by the CA, or by telephone (for Bearers, CTAs and legal representatives who possess a revocation code for the relevant certificate).

The emergency revocation code is emailed to the legal representative and to the CTA during the certificate registration phase. The Bearer must define the code via the website <https://services.certeurope.fr> when he or she uses his or her key for the first time. This code is required to make urgent revocation requests.

Without an emergency revocation code, it is not possible for an individual to self-authenticate using the online revocation service (website or phone), and he or she will therefore be unable to make an emergency request for processing within 24 hours. In this case, only authentications that take place in a face-to-face meeting or by signed letter will be accepted.

The revocation procedures are set out in the CPS.


Upon receipt of a revocation request, the applicant's authenticity is verified. This verification is carried out by the RA during a face-to-face meeting, by telephone or by the transfer of electronically signed documents.

If the request is admissible, the RA applies for the Certificate to be revoked by making a request to the CA to add the serial number and the date of revocation of the certificate to the Certificate Revocation List.

If the request is not admissible, the RA notifies the applicant of this fact.

The Bearer is notified of the publication of the revocation. The grounds for the revocation are not published.

The operation is recorded in the audit logs of the CERTIMETIERSARTISANAT CA.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

#### **IV.9.3.2. Revocation of certificate issued by a PKI component**

The procedures to be implemented in the event of a revocation of a certificate issued by a PKI component are described in the CPS associated with this CP.

In the event of the revocation of one of the certificates in a certification chain, the CA must notify all of the Bearers affected by this revocation, as rapidly as possible and by all means necessary, that their certificates are no longer valid.

Where the CA certificate was signed by a root certificate, revocation of the root certificate by the CA invalidates all of the Bearer's certificates.

The contact listed on the DGME/SDAE site (<http://www.references.modernisation.gouv.fr/>) is immediately notified in the event of the revocation of a certificate in the certification chain.

The DGME / SDAE reserves the right to disseminate information by any means to application developers within the administrative authorities and to users.

#### **IV.9.4. REVOCATION REQUEST GRACE PERIOD**

As soon as the Bearer (or an authorised person) becomes aware that one of the possible grounds for a revocation for one of his or her certificates is effective, he or she must submit a revocation request as promptly as possible.

#### **IV.9.5. TIME WITHIN WHICH THE CA MUST PROCESS A REVOCATION REQUEST**

##### **IV.9.5.1. Revocation of a bearer certificate**

A revocation request is inherently urgent and is processed as quickly as possible.

The revocation management service is available 24 hours a day, 7 days a week.


This service has a maximum period of non-availability due to service interruptions (breakdowns or maintenance) of 1 hour and a total maximum duration of non-availability per month of 4 hours.

Any request for the revocation of a bearer certificate must be processed within 24 hours. This period is calculated from the time that the authenticated request for revocation is received to the time that the revocation information is made available to the users.

##### **IV.9.5.2. Revocation of certificate issued by a PKI component**

The revocation of a certificate issued by a PKI component must be implemented immediately following the detection of an event that qualifies as grounds for the revocation of this type of certificate. The revocation of the certificate takes effect as soon as the serial number of the certificate is added to the Certificate Revocation List of the CA that issued the certificate.

The revocation of a CA's signature certificate (signature of certificates, CRLs/CCRLs) is effective immediately, particularly if the key has been compromised.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

#### **IV.9.6. VERIFICATION REQUIREMENTS FOR REVOCATIONS BY CERTIFICATE USERS**

The user of a bearer certificate is required to verify, prior to use, the status of the certificates throughout the relevant certification chain. The method used (CRL) is available to the user subject to its availability and to the constraints related to its use.

#### **IV.9.7. CRL ISSUANCE FREQUENCY**

CRLs are issued every 24 hours and every time a certificate is revoked.

#### **IV.9.8. MAXIMUM TIME LIMIT FOR PUBLISHING A CRL**

A CRL must be published no later than 30 minutes after it is issued.

#### **IV.9.9. AVAILABILITY OF AN ONLINE SYSTEM FOR VERIFYING REVOCATIONS AND THE STATUS OF CERTIFICATES**

There is no OCSP server.

#### **IV.9.10. REQUIREMENTS FOR THE ONLINE VERIFICATION OF CERTIFICATE REVOCATIONS BY CERTIFICATE USERS**

See section IV.9.6 above.

#### **IV.9.11. OTHER AVAILABLE MEANS OF OBTAINING INFORMATION REGARDING REVOCATIONS**

The Bearer may log on to the website <https://services.certeurope.fr/>, with his or her certificate, to verify the status of his or her certificate.

This service is based on the distribution points for CRLs in the trust chain.

#### **IV.9.12. SPECIFIC REQUIREMENTS FOR REVOCATIONS DUE TO COMPROMISED PRIVATE KEYS**

For bearer certificates, no specific requirements apply in the event that the Bearer's private key is compromised other than the revocation of the certificate.

In the event that the private key of a CA is compromised, information about the revocation of the certificate will be available on the APCM website: <http://www.artisanat.fr>.

Consequently, access to the portal for online certificate requests will be unavailable.

See section IV.9.3.2.

#### **IV.9.13. POSSIBLE GROUNDS FOR A SUSPENSION**


Suspension of certificates is not authorised.

#### **IV.9.14. ORIGIN OF A REQUEST FOR A SUSPENSION**

NOT APPLICABLE.

#### **IV.9.15. PROCEDURE FOR PROCESSING A REQUEST TO SUSPEND A CERTIFICATE**

NOT APPLICABLE.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

#### **IV.9.16. LIMITATIONS TO THE SUSPENSION PERIOD FOR A CERTIFICATE**

NOT APPLICABLE.

### **IV.10. CERTIFICATE STATUS INFORMATION SERVICE**

#### **IV.10.1. OPERATIONAL CHARACTERISTICS**

Access to the Certificate Revocation List is available via the two LDAP V3 directories and via a web server. These CRLs are in "CLR V2" format.

Access to the CA Certificate Revocation List (in this case, the CLR for the root certificate) is available via the two LDAP V3 directories and via a web server. These CRLs are in "CLR V2" format.

#### **IV.10.2. SERVICE AVAILABILITY**

The certificate status information service is available 24 hours per day, 7 days per week.

The maximum period of non-availability due to service interruptions (breakdowns or maintenance) is 2 hours and the total maximum duration of non-availability per month is 8 hours.

#### **IV.10.3. OPTIONAL PROCEDURES**

Not applicable.

### **IV.11. TERMINATION OF THE RELATIONSHIP WITH THE BEARER**

In the event of the termination of the contractual / hierarchical / regulatory relationship between the CA and the Bearer prior to the expiry of the certificate, whatever the reason the certificate will be revoked.

### **IV.12. KEY ESCROW AND RECOVERY**


The CA prohibits the escrow of Bearer keys.

#### **IV.12.1. POLICY AND PRACTICES FOR RECOVERY THROUGH KEY ESCROW**

Not applicable.

#### **IV.12.2. POLICY AND PRACTICES FOR RECOVERY THROUGH SESSION KEY ENCAPSULATION**

Not applicable.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

## V. NON-TECHNICAL SECURITY MEASURES

---

The various controls described herein aim to ensure, through appropriate risk management, a high level of confidence in the operation of the CERTIMETIERSARTISANAT CA.

### V.1. PHYSICAL SECURITY MEASURES

A risk analysis has been conducted by CERTIMETIERSARTISANAT. The security requirements are described in the OSC's Security Policy [CERT\_PS].

#### V.1.1. GEOGRAPHIC LOCATION AND SITE CONSTRUCTION

The geographic location of the production sites comply with the requirements of the document [CERT\_PS].

#### V.1.2. PHYSICAL ACCESS

The areas housing the computer systems of the CERTIMETIERSARTISANAT CA are physically protected against unauthorised external access.

There is a list of personnel who are authorised to access these areas. This list is strictly limited to those personnel who require access to ensure the correct operation of the service. Access by authorised personnel is physically monitored and recorded.

#### V.1.3. ELECTRICAL SYSTEMS AND AIR CONDITIONING

Electrical and air conditioning systems are adequate for the proper operation of the CERTIMETIERSARTISANAT CA's computer systems.

#### V.1.4. VULNERABILITY TO FLOOD DAMAGE

The CERTIMETIERSARTISANAT CA's computer systems are not located in a flood zone, and are not placed in a location that is vulnerable to damage due to flooding or faulty plumbing.

#### V.1.5. FIRE PREVENTION AND PROTECTION

The premises housing the CERTIMETIERSARTISANAT CA's computer systems are protected against fire (automatic detection and suppression). The physical distribution of the machines makes it possible to ensure maximum service availability.

#### V.1.6. MEDIA STORAGE

Backup media containing saved or archived data is retained with a level of security at least equal to that of the systems that generated the original data.


The means used to achieve this objective are stipulated in the CPS.

#### V.1.7. DECOMMISSIONING MEDIA

The destruction or resetting of media is executed with a level of security at least equal to that of the systems that generated the original data.

The means used to achieve this objective are stipulated in the CPS.



	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

### V.1.8. OFFSITE DATA BACKUP

The organisation of backup data will be structured in such a way as to ensure the most rapid disaster recovery possible, particularly for the services involved in the revocation of certificates.

The information stored offsite meets the requirements of this CP template with respect to preserving the confidentiality and integrity of such information.

The means used to achieve this objective are stipulated in the CPS.

## V.2. PROCEDURAL SECURITY MEASURES

Controls for these procedures have been implemented by the CERTIMETIERSARTISANAT CA and are stipulated in the CPS that corresponds to this CP, structured around the following themes:

### V.2.1. POSITIONS OF TRUST

Each component of the PKI identifies, at a minimum, the following positions of trust:

- **Head of security:** The head of security is responsible for implementing the component's security policy. He or she controls the physical access to the component's system equipment. He or she is authorised to read the archives and is responsible for analysing the audit logs in order to detect any incident, anomaly, compromise attempt, etc.;
- **Head of operations/application:** The head of operations is responsible, within the component to which he or she is attached, for implementing the PKI's certification policy and certification practice statement at the request level for which he or she is responsible. His or her responsibility covers all the services provided by this application and the corresponding performances;
- **Operator:** An operator within a PKI component ensures the use of applications for the services implemented by the component within his or her area of responsibility;
- **Systems engineer:** He or she is responsible for the initiation, configuration and technical maintenance of the component's IT equipment. He or she ensures the technical administration of the component's systems and networks;
- **Auditor / Controller:** The person designated by a competent authority whose role is to monitor, on a regular basis, the compliance of the implementation of the services provided by the component with respect to certification policies, the PKI's certification practice statements and the component's security policies.
- **Secret holder:** The person responsible for ensuring the confidentiality, integrity and availability of the private keys entrusted to them.

The general responsibilities of each of these roles are set out in the CPS.


### V.2.2. NUMBER OF PERSONS REQUIRED PER TASK

Depending on the task to be carried out, one or more persons must be present during the execution of the task.

The CPS will specify, in accordance with risk analysis for each of the tasks related to certificate administration, the number of people and the roles required.

### V.2.3. IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

Each component of the CA verifies the identity and the authorisations of the personnel who must participate, before:

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

- his or her name is added to the list of personnel who have physical access to the CA's IT systems;
- an account is opened for him or her on the CERTIMETIERSARTISANAT CA's IT systems;

#### **V.2.4. ROLES REQUIRING SEPARATION OF DUTIES**

More than one role may be assigned to the same person, to the extent that the combination of roles does not compromise security functions. For positions of trust, however, it is recommended that the same person not hold multiple roles and, at a minimum, the following restrictions regarding combinations of roles must be respected.

Regarding positions of trust, the following combinations of roles are prohibited:

- head of security and systems engineer/operator
- auditor/controller and any other role
- systems engineer and operator

The functions associated with each role are described in the CPS and comply with the security policy of the relevant component.

### **V.3. SECURITY MEASURES WITH RESPECT TO PERSONNEL**

#### **V.3.1. REQUIRED QUALIFICATIONS, SKILLS AND ABILITIES**

All personnel who work within a PKI component are subject to a confidentiality clause with respect to their employer.

Every entity that operates a PKI component ensures that the responsibilities allocated to its personnel who have been assigned to work within the component are appropriate to their professional skills.

The managerial staff must possess the appropriate expertise for their roles and must be familiar with the security procedures in place within the PKI.

The CA must ensure that all members of staff who perform duties related to the operation of a CA:


- are appointed to their position in writing;
- are required by contract or by law to comply with the obligations of their position, particularly with respect to confidentiality;
- have no duties or interests that may conflict with their obligations with respect to the CA.

#### **V.3.2. BACKGROUND CHECK PROCEDURES**

Every entity that operates a PKI component uses all legal means necessary to ensure the honesty of the personnel who are assigned to work within the component.

These personnel must not have criminal records that would conflict with their duties. They must provide their employer with a copy of their criminal record check (bulletin n°3). Individuals holding positions of trust may not have any conflict of interest prejudicial to the impartiality of their duties.

These background checks must be carried out prior to the assignment of an individual to a position of trust and must be reviewed regularly (at least every 3 years).

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

### **V.3.3. INITIAL TRAINING REQUIREMENTS**

The CA must ensure that all personnel who perform duties related to the management of the CA have received appropriate training on the CA's principles of operation and security mechanisms, and are familiar with the latest safety rules.

### **V.3.4. REQUIREMENTS AND FREQUENCY WITH REGARD TO FURTHER TRAINING**

The relevant personnel will receive information and adequate training prior to any changes to systems, procedures, the structure of the organisation, etc., appropriate to the nature of these changes.

### **V.3.5. JOB ROTATION FREQUENCY AND SEQUENCE**

The CA does not require the rotation of its authorised personnel.

### **V.3.6. SANCTIONS FOR UNAUTHORISED ACTIONS**

In the event of known or suspected misconduct by a member of the CA in the fulfilment of his or her duties, the CA will block the access of the individual to the CA's systems and, where necessary, take all appropriate disciplinary action.

### **V.3.7. INDEPENDENT CONTRACTOR REQUIREMENTS**


The employees of independent contractors and external service providers who are present at the offices and / or the components of the PKI must also comply with the requirements of this section V.3. This requirement will be incorporated into appropriate clauses in contracts with any such independent contractor or external service provider.

### **V.3.8. DOCUMENTATION SUPPLIED TO PERSONNEL**

The CA will ensure that its personnel have access to all laws and contracts that apply to the positions that they hold.

Documents available to personnel include the following:

- the CP supported by the component to which the staff member belongs;
- the CPS appropriate to the area of certification;
- internal operating procedures;
- the user manuals for the hardware and software used.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

## V.4. AUDIT LOGGING PROCEDURES

Audit logging consists of recording events manually or electronically, through manual or automatic data input.

The resulting files, in paper or electronic format, make it possible to track and attribute operations.

### V.4.1. TYPES OF EVENTS RECORDED

Each entity that operates a component of the PKI must log the following events. These events must be logged automatically, in electronic format, from the moment of startup for all systems related to the functions that the entity operates within the PKI:


- creation / modification / deletion of user accounts (access rights) and the corresponding authentication data (passwords, certificates, etc.);
- startup and shutdown of computer systems and requests;
- events related to logging: startup and shutdown of the logging function, changes to log settings, actions taken following a failure of the logging function;
- log on and log off attempts by users in positions of trust, and any related unsuccessful attempts.

Other events are logged electronically or manually. These are events that concern security and that are not automatically created by the information technology system, notably:

- physical access;
- maintenance activities and changes in system configuration;
- staff changes;
- the destruction and re-initiation of media containing confidential information (keys, activation data, personal information about the Bearers, etc.).

In addition to these log requirements, which are common to all of the components and functions of the PKI, events specific to the various different functions of the PKI are logged, including:

- receipt of a request for a certificate (initial and renewal);
- approval/rejection of a request for a certificate;
- events related to signature keys and CA certificates (issuing (key ceremony), backup / recovery, revocation, renewal, destruction, etc.);
- where applicable, generation of the secret bearer elements (key pairs, activation codes, etc.);
- key pairs and bearer certificates;
- transmission of certificates to bearers and, as appropriate, explicit acceptances/rejections by the Bearers;
- where applicable, delivery of the authentication and signature device to the Bearer;
- publication and updating of information related to the CA (CP, CA certificates, general terms and conditions of use, etc.);
- receipt of a revocation request;
- approval/rejection of a revocation request;
- generation and subsequent publication of CRLs.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

Each registration of an event in an audit log contains, at a minimum, the following fields:

- type of event;
- name of the individual or system reference that caused the event;
- data and time of the event;
- result of the event (failure or success).

Accountability for action rests with the person, entity or system that executed the action. The name or identifier of the executor is explicitly noted in one of the fields in the audit log.

In addition, depending on the type of event, each record contains the following fields:

- recipient or addressee of the operation;
- name of the person who requested the operation or the reference of the system that made the request;
- name(s) of the individuals present (if the relevant operation required the presence of more than one individual);
- cause of the event;
- all information unique to the event (for example, for the generation of a certificate, the series number of the relevant certificate).

Logging operations are performed during the processes.

If the log is created manually, the log for the event must, without exception, be written on the same business day as the event.

#### **V.4.2. AUDIT LOG PROCESSING FREQUENCY**

Audit logs are activated on a daily basis, and are activated systematically in the event of the escalation of a discrepancy.

See section V.4.8

#### **V.4.3. AUDIT LOG RETENTION PERIOD**

Events logs are retained on site for a period of at least 1 month.

They are archived no more than 1 month after this period has elapsed.

#### **V.4.4. AUDIT LOG PROTECTION**

The logging process is designed and implemented to limit the risks of the circumvention, alteration or destruction of the audit logs. Integrity monitoring mechanisms make it possible to detect any alteration, intentional or accidental, of these logs.


The availability of these logs is protected (against theft and against partial or total destruction, whether deliberate or involuntary).

The event dating system complies with the requirements of section VI.8.

The sensitivity of the event logs is determined based on the nature of the information being processed and of the business. It can create a need for the protection of confidential data.

#### **V.4.5. BACKUP PROCEDURE FOR AUDIT LOGS**

Each entity operating a component of the PKI will implement the necessary measures to ensure the integrity and availability of the audit logs for the component concerned, in accordance with the requirements of the CERTIMETIERSARTISANAT Security Policy [CERT\_PS] and based on the results of the CA's risk analysis.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

#### **V.4.6. AUDIT LOG COLLECTION SYSTEM**

The collection system ensures the integrity, confidentiality and availability of the audit logs.

#### **V.4.7. NOTIFICATION OF EVENT RECORDING PROVIDED TO THE INDIVIDUAL RESPONSIBLE FOR THE EVENT**

This CP makes no specific requirements on this subject.

#### **V.4.8. VULNERABILITY ASSESSMENT**

Each entity operating a PKI component is equipped to detect any attempt to violate the integrity of that component.

Audit logs are checked at least once every 24 hours in order to identify discrepancies linked to failed attempts.

The logs are analysed in their entirety at least once per week and upon detection of a discrepancy. This analysis is used to create a summary in which the important elements are identified, analysed and explained. The summary will highlight any discrepancies or falsifications that may be discovered.

In addition, reconciliation between the various audit logs of services that interact with each other (the registration authority and the certificate generation service, the revocation management service and the certificate status information service, etc.) is performed at least once a month, in order to check the correlation between dependent events and thus help to reveal any discrepancies.

### **V.5. RECORDS ARCHIVAL**

#### **V.5.1. TYPES OF RECORDS TO BE ARCHIVED**

Archiving arrangements are made by the CA and the RA. By archiving its own data, the CA ensures the retention of the logs created by the various components of the PKI. This makes the retention of paper documentation related to certification operations possible, as well as ensuring the availability of these documents where necessary.


The records to be archived, at a minimum, are:

- software (executable files) and configuration files for IT equipment;
- CPs;
- CPSs;
- contractual agreements with other CAs;
- issued and published certificates and CRLs;
- receipts and notifications (for information purposes);
- undertakings signed by the CTAs;
- bearer identity documents and, where appropriate, the entities with which the Bearers are associated;
- audit logs of the various entities of the PKI.

#### **V.5.2. ARCHIVE RETENTION PERIOD**

##### **Certificate application files**

Approved certificate application files are archived for a period of 5 (five) years from the date on which the certificate was accepted by its bearer.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

During this period, the files are retained in order that they can be made available for all requests by authorised authorities.

The files are listed and classified so that they can be quickly linked to a certificate Bearer.

The content of the files makes it possible to identify the real identity of the Bearer of a certificate.

### **Certificates and CRLs issued by the CA**

Bearer certificates and CRLs/CCRLs are archived for ten years from the date on which they were generated.

#### **Audit logs**

The audit logs covered in section V.4 are archived for a period of 10 years from the date on which the log was generated.

#### **Other logs**

Other logs are archived for 5 years in the case of paper documents, and 10 years for electronic documents.

### **V.5.3. ARCHIVE PROTECTION**

Throughout the whole of the retention period, the archives and their backup copies are:

- protected, in terms of integrity of content;
- accessible to authorised persons;
- reviewed and used.

The means used to safely archive the documents are specified in the CPS.

### **V.5.4. BACKUP PROCEDURES FOR ARCHIVES**

This CP makes no specific requirements on this subject. The level of backup protection must be at least equivalent to the level of protection given to the archives.

### **V.5.5. REQUIREMENTS FOR TIME STAMPING OF RECORDS**

See section V.4.4 for dating requirements for the audit logs.


Section VI.8 stipulates the requirements with respecting to dating and time stamping.

### **V.5.6. ARCHIVE COLLECTION SYSTEM**

The system and the procedures for collecting the archives respect the requirements for the protection of the archives concerned. The collection procedures are set out in the CPS.

### **V.5.7. ARCHIVE RETRIEVAL AND AUDIT PROCEDURES**

Archives (paper and electronic) may be retrieved within a period of 2 business days, given that only the CA can access all of the archives (as opposed to an entity operating a component of the PKI, which can retrieve and view only the archives of the component in question).

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

## V.6. CA KEY CHANGEOVER

The CA key is valid for a period of 10 years.

As bearer certificates are valid for a period of 3 years, the renewal of the CA key takes place no later than three (3) years before the end of its period of validity. The CA reserves the right to renew its key prior to its expiry date. The decision to renew the key may be taken prior to its expiry date based on various criteria (improvements in cryptographic techniques, longer validity period, etc.).

The new key pair that is generated may be used to sign new Bearer Certificates and CRLs.

The previous certificate will continue to be usable for validating certificates issued prior to the renewal date until such time as all certificates signed with the corresponding private key have expired.

## V.7. COMPROMISE AND DISASTER RECOVERY

### V.7.1. INCIDENT AND COMPROMISE HANDLING PROCEDURES

Each entity operating a PKI component has established procedures and methods for reporting and processing incidents, including through the awareness and training of its personnel and through the analysis of various audit logs.

In the event of a major incident, such as the loss, suspicion of compromise, compromise or theft of the CA's private key, the triggering event is the discovery of the incident at the level of the component concerned, which immediately notifies the CA. It is imperative that a major incident be handled as soon as it is detected. If the certificate is revoked, this information is published immediately by any available effective means (media, website, etc.).

### V.7.2. RECOVERY PROCEDURES IN THE EVENT OF CORRUPTION OF IT RESOURCES (HARDWARE, SOFTWARE AND / OR DATA)

Each PKI component has a business continuity plan enabling it to meet the availability requirements of the various PKI functions set out in this CP, the CA's undertakings in its own CP and the results of the PKI's risk analysis, particularly with regard to the functions related to the publication and / or the revocation of certificates.

This plan is tested at least once a year.

The RA workstations used for certificate revocation are distributed across the infrastructure of the RA and the CO to ensure optimum availability of the revocation service.


### V.7.3. RECOVERY PROCEDURES IN THE EVENT OF COMPROMISE OF A COMPONENT'S PRIVATE KEY

The infrastructure and control keys are distributed across the CA, RA and CO components.

#### RA Component

The RA has keys available for its personnel who are authorised to generate and revoke certificates.



	<p><b>PUBLIC</b></p>	<p>Status: Official</p>
<p><b>CERTIMETIERSARTISANAT</b></p>	<p>Certification Policy</p>	<p>Last updated: 20/01/2012</p>

In the event that one of these keys is compromised, the RA notifies the CA, who applies to the OC in order to revoke the RA's certificate and, if necessary, to generate a new one.

#### **CA Component**

The CA has keys for its personnel who are authorised to monitor the production and revocation of certificates.

In the event that one of these keys is compromised, CA applies to the OC in order to revoke the CA's certificate and, if necessary, to generate a new one.


#### **CO Component**

The CO has keys available for its personnel who are authorised to administer IT resources as well as to carry out urgent revocations.

In the event that one of these keys is compromised, the CO notifies the CA and proceeds to revoke the certificate and, if necessary, to generate a new one.

#### **V.7.4. BUSINESS CONTINUITY CAPABILITIES FOLLOWING A DISASTER**

The various PKI components have the necessary means available to ensure the continuity of their business, in compliance with the requirements of this CP (see section V.7.2).

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

## V.8. PKI TERMINATION

One or more components of the PKI may cease its activities or transfer these activities to another entity.

The transfer of an activity is defined as the cessation of activity of a PKI component that does not affect the validity of certificates issued prior to the transfer in question, and the resumption of the activity is organised by the CA in collaboration with the new entity.

Cessation of activity is defined as the end of the activity of a PKI component, with a bearing on the validity of certificates issued prior to the termination.

### Transfer of activity or cessation of activity affecting a PKI component

The CA components that can terminate their activity without jeopardising the PKI are: the RAs and the CO.

To the extent that the proposed changes may have repercussions on its commitments vis-à-vis certificate bearers or users, the CA will notify them as soon as necessary and, in any event, within 15 days of the signing of the transfer agreement or of the company being placed into receivership or bankruptcy.

#### RA Component

When an RA terminates its activity, the RA must notify the CA with sufficient advance notice for the activities and functions performed by the RA to be transferred to another RA without impacting the certificates issued by the RA.

In particular, the CA will:


- Create an action plan and address the risk analysis for the CA. In particular, the action plan must address the:
  - o transfer of records under the responsibility of the RA: certificate application files, various letters, etc.
  - o transfer of services provided by the RA: revocation, issuance, etc.
  - o communication to the Bearers and to other PKI components,
  - o communication to the certificate users,
  - o revocation of certificates to authorised personnel.
- Communicate the action plan to the DGME/SDAE contact, together with any changes that may arise during the transfer.

#### CO component

The contract between the CO and the CA includes a reversibility clause enabling the CA to change operators. In the event of the CO terminating its activity, the CA undertakes to transfer the services provided by the CO to another CO.

In particular, the CA will:

- Create an action plan and address the risk analysis for the CA. In particular, the action plan must address the:
  - o transfer of the records archived under the responsibility of the CO,
  - o transfer of services provided by the CO,
  - o continuity of services during the transfer,
  - o transfer of the CA's keys hosted by the CO,
  - o cancellation of the CO's authorisations to provide emergency revocations,
  - o modification of the CA's documentary standards: CP, CPS, etc.
  - o training of authorised CA personnel
  - o communication to other PKI components,

	<p><b>PUBLIC</b></p>	<p>Status: Official</p>
<p><b>CERTIMETIERSARTISANAT</b></p>	<p>Certification Policy</p>	<p>Last updated: 20/01/2012</p>


- communication to the Bearers and the certificate users,
- Communicate the action plan to the DGME/SDAE contact, together with any changes that may arise during the transfer.

### **Cessation of activity affecting the CA**

In the event of a total cessation of activity, the CA or, if this is not possible, any entity that can be substituted by virtue of a law, regulation, court decision or an agreement previously reached with this entity, will ensure the revocation of the certificates and the publication of the CRLs in accordance with commitments made in this CP.

During the shutdown of its service, the CA undertakes to:

- 1) refrain from transmitting the private key that enabled it to issue certificates;
- 2) take all necessary steps to destroy or disable the private key;
- 3) revoke its certificate;
- 4) revoke all of the certificates that it has signed and that are still valid;
- 5) notify all of the CTAs and/or bearers of certificates that have been revoked or that are to be revoked, as well as the entities with which they are affiliated, where necessary (see section III.2.3).

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

## VI. TECHNICAL SECURITY CONTROLS

---

### VI.1. KEY PAIR GENERATION AND INSTALLATION

#### VI.1.1. KEY PAIR GENERATION

##### VI.1.1.1. CA keys

CERTIMETIERSARTISANAT CA signature keys are generated in a secure environment (see section V).

The CERTIMETIERSARTISANAT CA signature keys are generated and incorporated into an encryption module that meets the requirements of section XI below for the relevant level of security.

The generation of the CA's signature keys is carried out in fully controlled circumstances, by staff members holding positions of trust (see section V.2.1), as part of a "key ceremony". These ceremonies follow predefined scripts.

As applicable, the initialisation of the PKI and / or the generation of the CA's signature keys may take place at the same time as the generation of the PKI's secret data. This secret data is data that makes it possible to manage and manipulate the CA's private signature keys, subsequent to the key ceremony, including the ability to subsequently initialise new cryptographic modules using the CA's signature keys.

Following their generation, this secret data is given to certificate bearers who have been previously identified and authorised by the CA for this position of trust. Regardless of the media format (paper, magnetic media or saved to a smart card or USB key), a Bearer may not hold more than one unit of secret data from a given CA at any given time. Each unit of secret data is implemented by its bearer.

Key ceremonies take place under the control of at least two people in positions of trust and in the presence of several witnesses, at least one of whom is external to the CA and is impartial. These witnesses can attest, in an objective and factual manner, to the way in which the ceremony was executed relative to the predefined script.

##### VI.1.1.2. Bearer keys generated by the CA

The key pair is generated directly in the authentication and signature device by the RA and cannot be removed from it. From this point on, the protection of the key pair depends on the authentication and signature device protection mechanisms. The authentication and signature device meets the requirements of section XII.

##### VI.1.1.3. Bearer keys generated by the Bearer


Not applicable.

#### VI.1.2. DELIVERY OF THE PRIVATE KEY TO ITS OWNER

The private key is delivered to its owner during the face-to-face meeting in which the authentication and signature device, which contains the Bearer's protected private key, is delivered.

#### VI.1.3. DELIVERY OF THE PUBLIC KEY TO ITS OWNER

Not applicable. The key pair is not generated by the Bearer.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

#### **VI.1.4. DELIVERY OF THE CA'S PUBLIC KEY TO THE CERTIFICATE USERS.**

The CA's public key can be downloaded from the CA's website.

The "fingerprint" of the CA's public key certificate makes it possible to establish its authenticity.

The CPS stipulates the terms of access to the CA's certificate.

#### **VI.1.5. KEY SIZE**

The RSA bearer keys used have a size of 2048 bits, and will be upgraded as and when changes in technology and/or legislation arise.

The size of the CERTIMETIERSARTISANAT CA's key is 2048 bits.

#### **VI.1.6. KEY PAIR PARAMETER GENERATION AND QUALITY VERIFICATION**

The Bearers' cryptographic modules use standard or standardised parameters to ensure random key pair generation.

The Bearers' cryptographic modules verify the quality of the key pairs generated by these devices.

The CA's key pair (for the signature of certificates and CRLs) is generated and protected by a hardware encryption module.

Generating or renewing the CA's key pair using this module requires the presence of at least 3 people.

#### **VI.1.7. KEY USAGE PURPOSES**

The use of the CERTIMETIERSARTISANAT CA's private key and its associated certificate is strictly limited to the signature of certificates, CRLs/LARs (see section I.4.1.2 and the document [PROFILS]). The use of the Bearer's private key and its associated certificate is strictly limited to authentication and signature services (see section I.4.1.1, IV.5 and the document [PROFILS]).

### **VI.2. SECURITY MEASURES FOR THE PROTECTION OF PRIVATE KEYS AND CRYPTOGRAPHIC MODULES**


#### **VI.2.1. SECURITY MEASURES AND STANDARDS FOR CRYPTOGRAPHIC MODULES**

##### **VI.2.1.1. The CA's cryptographic modules**

The cryptographic modules used by the CA to generate and initiate its signature keys are cryptographic modules that meet the EAL4+ Common Criteria and therefore meet the requirements of section XI below with respect to the level of security of these modules \*\*.

##### **VI.2.1.2. Bearer authentication and signature devices**

The Bearers' authentication and signature devices, which are used for initiating their private authentication and signature keys, meet the EAL4+ common criteria and thus comply with the requirements of section XII below with respect to the level of security\*\*.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

### **VI.2.2. CONTROL OF THE PRIVATE KEY BY MORE THAN ONE PERSON**

This chapter addresses the control of the CA's private key for exporting/importing out of/into a cryptographic module. The generation of the key pair is discussed in section VI.1.1.1, activation of the private key in section VI.2.8 and its destruction in section VI.2.10.

The control of the CA's private signature keys is ensured by personnel in positions of trust (the PKI's secret keepers) and through the use of a tool that implements the sharing of these secrets (systems that require that minimum of 3 of the 5 authorised users must authenticate themselves).

### **VI.2.3. ESCROW OF THE PRIVATE KEY**

The CERTIMETIERSARTISANATCA does not permit either the CA's or the Bearers' private keys to be held in escrow.

### **VI.2.4. PRIVATE KEY BACKUP**

The CA does not make any backup copies of private bearer keys.

A backup copy of the private CA key is made, either in a cryptographic module that complies with the requirements of section XI below, or outside of a cryptographic module, but in an encrypted form incorporating an integrity control mechanism. The encryption offers a level of security that is equivalent or superior to storage in a cryptographic module and, in particular, is based on an algorithm, key length and operating mode capable of resisting decryption attacks for at least the lifespan of the protected key. The encryption and decryption operations are performed inside the cryptographic module in such a way that the CA's private keys are never in plain form outside of the cryptographic module.

Operational control of encryption/decryption complies with the requirements of section VI.2.2. Copying procedures are described in the CPS.

### **VI.2.5. PRIVATE KEY ARCHIVAL**

The CA's private keys are not archived.

The Bearers' private keys are not archived by either the CA or by any PKI component.


### **VI.2.6. TRANSFER OF THE PRIVATE KEY INTO/FROM THE ENCRYPTION MODULE**

Private bearer keys are never transferred. They are generated within the cryptographic module and cannot be exported.

For the private CA keys, any transfer must take place in encrypted format, in accordance with the requirements of section VI.2.4.

### **VI.2.7. PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULES**

Private CA keys are stored on cryptographic modules that meet the requirements of section XI below for the relevant level of security.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

## **VI.2.8. PRIVATE KEY ACTIVATION METHOD**

### **VI.2.8.1. Private CA Keys**

The activation method of the CA's private key in a cryptographic module makes it possible to meet the requirements set out in section XI for the relevant level of security.

The activation of the CA's private keys in a cryptographic module is controlled through the use of activation data (see section VI.4) and requires the participation of at least two people in positions of trust.

### **VI.2.8.2. Private bearer keys**

The activation method for a Bearer's private key complies with the requirements set out in section XII for the relevant level of security.

## **VI.2.9. METHOD FOR DEACTIVATING THE PRIVATE KEY**

### **VI.2.9.1. Private CA keys**

Deactivation of private CA keys on cryptographic modules takes place automatically as soon as the module's environment changes: module stoppage or disconnection, logging off by the operator, etc.

### **VI.2.9.2. Private bearer keys**

The conditions for the deactivation of a private bearer key comply with the requirements set out in section XII for the relevant level of security.

## **VI.2.10. METHOD FOR DESTROYING PRIVATE KEYS**

### **VI.2.10.1. Private CA Keys**

The method for destroying private CA keys complies with the requirements set out in section XII for the relevant level of security.

At the end of the life of a private CA key, whether through normal expiry or in advance (revocation), the key is systematically destroyed, together with any copies and any elements that could make it possible to reconstitute the key.


### **VI.2.10.2. Private bearer keys**

At the end of the life of a private bearer key, the method for the destruction of the key complies with the requirements set out in section XII for the relevant level of security.

## **VI.2.11. ASSESSMENT OF THE LEVEL OF SECURITY OF THE CRYPTOGRAPHIC MODULE**

The CA's cryptographic modules are assessed at security level EAL4+, corresponding to their anticipated use, as specified in section XI below.

Bearer authentication and signature devices are assessed at security level EAL4+, corresponding to their anticipated use, as specified in section XII below.

	<p><b>PUBLIC</b></p>	<p>Status: Official</p>
<p><b>CERTIMETIERSARTISANAT</b></p>	<p>Certification Policy</p>	<p>Last updated: 20/01/2012</p>

## **VI.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT**

### **VI.3.1. PUBLIC KEY ARCHIVAL**

The public CA keys and the public bearer keys are archived as part of the archival of the corresponding certificates.

### **VI.3.2. CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS**

The life of key pairs and bearer certificates provided by the CERTIMETIERSARTISANAT CA is 3 years, non-renewable.

The life of CA key pairs and bearer certificates of the CERTIMETIERSARTISANAT CA is 10 years.


## **VI.4. ACTIVATION DATA**

### **VI.4.1. ACTIVATION DATA GENERATION AND INSTALLATION**

#### **VI.4.1.1. Activation data generation and installation for the CA private key**

The generation and installation of data on a PKI cryptographic module is performed during the initialisation and customisation phase of the module. If the activation data is not personally chosen and entered by the individuals who are responsible for the data, this data is sent to the responsible individuals in a manner that ensures the confidentiality and integrity of the data. This activation data is known only by the appointed individuals who have been identified with respect to in the roles assigned to them (see chapter V.2.1).



	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

#### **VI.4.1.2. Activation data generation and installation for the Bearer private key**

The authentication and signature devices are provided to the Bearers and are protected by an activation code (PIN code). The PIN codes are generated by the CA in a way that makes it impossible to predict the codes. The length of the code is 6 figures. The PIN code is transmitted directly to the Bearer on the day following its generation.

#### **VI.4.2. ACTIVATION DATA PROTECTION**

##### **VI.4.2.1. Activation data protection for the CA private key**

Following the CA key ceremony, the CA activation data are delivered to several bearers who have the responsibility of ensuring the data's confidentiality, integrity and availability.

##### **VI.4.2.2. Activation data protection for the Bearer private keys**

The integrity and confidentiality of the activation data for the Bearer authentication and signature devices generated by the CA are protected until they are delivered to the Bearers.

The integrity and confidentiality of the activation data stored by the CA is protected.

#### **VI.4.3. OTHER ASPECTS OF ACTIVATION DATA**

The CA does not retain the Bearer activation codes for longer than one month following their delivery by courier.

### **VI.5. COMPUTER SECURITY CONTROLS**

The security measures with respect to computer systems satisfy the security objectives designed based on the risk analysis that must be conducted by the CA (see section I.3.1).

#### **VI.5.1. SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS**


The workstations of PKI components require an optimal level of security. This level of security is stipulated in the CPS and makes it possible to meet the following needs:

- identification and authentication of workstation users,
- management of user sessions (logout following a period of inactivity, access to files controlled by role and by name of user),
- protection against computer viruses,
- network protection (confidentiality, integrity, etc.),
- audit functions,
- accountability.

The minimum level of security achieved meets these security objectives. Applications using the services of the components may have additional security requirements, which must be taken into account in determining the minimum level of security provided by the workstations.

#### **VI.5.2. COMPUTER SECURITY RATING**

No specific requirements have been established.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

## **VI.6. LIFE CYCLE TECHNICAL CONTROLS**

### **VI.6.1. SYSTEM DEVELOPMENT CONTROLS**

CA applications have been implemented in strict compliance with the preliminary risk analysis and with the resulting security policy.

The implementation of the CA and its hosting platform has been documented.

Any modification to the CA or its hosting platform will be documented.

### **VI.6.2. SECURITY MANAGEMENT CONTROLS**

Any changes to the systems are recorded in the CA's activity log and are reported.

### **VI.6.3. LIFE CYCLE SECURITY CONTROLS RATING**


Not applicable.

## **VI.7. NETWORK SECURITY CONTROLS**

The CA is built on a network protected by at least two levels of security gateways (firewalls). These gateways are configured in such a way as to accept only essential flows.

## **VI.8. TIME STAMPING / DATING SYSTEM**

To date events, the various PKI components use the PKI's time system, ensuring the synchronisation of the clocks within the PKI system to within one minute, and, with respect to a reliable source of UTC time, to the nearest second. For operations that are conducted offline (e.g.: administration of a Root CA), this level of precision of synchronisation with respect to UTC time is not required. The system orders events with sufficient accuracy. Synchronization with respect to time UTC refers to a system that includes two independent time feeds.


	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

## **VII. CERTIFICATE AND CRL PROFILES**


---

### **VII.1. CERTIFICATES PROFILES**

CERTIMETIERSARTISANAT CA certificates contain the following primary fields and extensions:

	PUBLIC	Status: Official
CERTIMETIERSARTISANAT	Certification Policy	Last updated: 20/01/2012

Field	Value	Value constraint	Explanation
Version	V3	2	Certificate version X.509
Serial number	15 06 38 D4		The unique serial number of the certificate generated by the cryptographic module
Signature algorithm	Sha1RSA = 1.3.14.3.2.29		CA signature algorithm identifier
Issuer	/C=FR /O=APCM /OU=0002 187500046 /CN=CERTIMETIERSARTISANAT		The name of the issuing CA is the Distinguished Name (X.500) of the CA that signed the certificates
Valid from	Start date = x (no earlier than the start date of the life of the CERTIMETIERSARTISANAT CA)		Dates and hours of activation and expiry of the certificate
Valid until	Valid until x+ 3 years (no later than the end date for the life of the CERTIMETIERSARTISANAT CA)		
Subject	E = <a href="mailto:emartin@apcm.fr">emartin@apcm.fr</a> 1.2.250.1.191.20.1 = APCM Description = 01234567891 2.5.4.15 = 10.71C SN = 5e4be36a5566813d7b0ee92c4e01189a9abcd6ad CN = ERIC MARTIN OU = 0002 124562390 O = AAA Company C = FR		Unique name of the identified entity
Public key	RSA(2048 Bits)		Identifier of the algorithm used for the public key contained in the certificate, and the value of the public key
Base constraint	Subject Type=End Entity Path Length Constraint=None		
Other Name of the subject	Nom RFC822=emartin@apcm.fr		
Distribution point of the CRL	CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://lcr1.certimetiersartisanat.fr/CN=CERTIMETIERSARTISANAT, OU=0002 187500046, O=APCM, C=FR? Certificate Revocation List URL=ldap://lcr2.certimetiersartisanat.fr/CN=CERTIMETIERSARTISANAT, OU=0002 187500046, O=APCM, C=FR? Certificate Revocation List URL= <a href="http://lcr.certimetiersartisanat.fr/reference/certimetiersartisanat.crl">http://lcr.certimetiersartisanat.fr/reference/certimetiersartisanat.crl</a>		

	PUBLIC	Status: Official
CERTIMETIERSARTISANAT	Certification Policy	Last updated: 20/01/2012

Certificate Policies	Certificate Policy: Policy Identifier=1.2.250.1.191.1.1.1.2 Policy Qualifier Info: Policy Qualifier Id= Qualifier=	OBJECT IDENTIFIER ' OBJECT IDENTIFIER cps <a href="http://pc.certimetiersartisanat.fr/referenc&lt;br/&gt;e/pc-certimetiersartisanat_v1.3_en.pdf">http://pc.certimetiersartisanat.fr/referenc e/pc-certimetiersartisanat_v1.3_en.pdf</a>	Certification Policy Identifier
Digital Signature Algorithm	Sha1 = 1.3.14.3.2.29		
Digital Signature	07F2 AC3F 4E3A 30D5 277C 2A1A 6AD2 6BA4 F019 E130	8C 62 E9 57 0B 94 DF EB 73 14 AE 15 0F A9 36 2B 22 84 81 28 0F 25 06 FF 1C D3 10 EC A5 BC 43 1C AB 02 1D CD 7E 9E D7 B9 A0 DA 13 59 22 26 DF 72 EB 6D B3 AA 4E 2C B0 B3 1B 38 A4 E5 C4 3A 4C 15 2F E2 B2 AD 1C 9D 8F 5A FE D6 05 BC 6D 2E 81 D4 67 96 3D 74 BB F1 3F 37 7C 27 75 8C 9A 9A 9D 56 63 F1 BD 1E 76 89 09 ED 71 AA E1 F0 65 E1 A5 C8 0E DC AE 50 E1 C6 0D BF 76 6F A8 EC D0 D7 55 B9	Octet field characterising the CA certificate that signed the certificate

## VII.2. CRL PROFILE

### VII.2.1. CRL FIELDS

The CERTIMETIERSARTISANAT CA CRLs contain the following fields:

- Version: the version of the CRL. For this CA, this is version 2;
- Signature: the signature algorithm identifier for the CA is SHA1-RSA;
- Issuer: the name of the CA that signs the certificates is the CERTIMETIERSARTISANAT CA;
- This Update: issue date of the CRL;
- Next Update: the next date on which the CRL is scheduled to be updated;
- Revoked Certificates: the list of the serial numbers of revoked certificates;
- User Certificate: the serial number of the revoked certificate;
- Revocation Date: the date on which a given certificate was revoked;
- crl Extensions: list of CRL extensions.

### VII.2.2. CRL EXTENSIONS

The CERTIMETIERSARTISANAT CA CRLs contain two extensions:

- authorityKeyIdentifier: this non-critical extension identifies the public key to be used to verify the validity of the CRL. This identifier has the same value as the SubjectKeyIdentifier field for certificates issued by the CERTIMETIERSARTISANAT CA;
- CRLNumber: this non-critical extension contains the serial number of the CRL.


## VII.3. OCSP PROFILE

### VII.3.1. VERSION NUMBER

Not applicable

### VII.3.2. OCSP EXTENSIONS

Not applicable

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

## **VIII. COMPLIANCE AUDIT AND OTHER ASSESSMENTS**

---

The operations of the CA are based, on the one hand, on the processing of requests for certificates submitted by chambers of trades and crafts in their capacity as delegated registration authorities, and on the other hand, on the technical services provided by CertEurope.

CertEurope undertakes, under the general terms and conditions of the contract, to comply with the CPS of Certimetiersartisanat.

### **VIII.1. FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT**

The CERTIMETIERSARTISANAT CA has arranged for a compliance audit concerning the operation of its PKI to be conducted by LSTI, an external entity accredited by COFRAC. Compliance audits will continue to be conducted every two years by an external entity accredited by COFRAC. In addition, the CA will conduct a check of the compliance of each Delegated Registration Authority. These checks will take the form of surveys.

### **VIII.2. IDENTITY/QUALIFICATIONS OF THE ASSESSORS**

The internal assessments will be carried out by employees of the APMC's legal department, which participated in the establishment and participates in the operating of the PKI.

### **VIII.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITIES**

APCM's assessors are independent of the chambers of trades and crafts that they audit.

### **VIII.4. TOPICS COVERED BY THE ASSESSMENTS**


The periodic assessments conducted by an external entity accredited by COFRAC cover the whole of the architecture of the PKI. Spot checks conducted by the APMC will take place in accordance with the procedure described in the document entitled "Certimetiersartisanat CA Assessment and Monitoring Procedure" version1.

### **VIII.5. ACTIONS TAKEN FOLLOWING THE CONCLUSION OF THE ASSESSMENTS**

Following the assessments, corrective actions will be taken in accordance with the outline set out below: At the conclusion of the compliance assessment, the audit team provides the assessed entity with an audit report. Any non-compliance issues detected during the audit will be classified as "notes", "minor non-compliance" or "major non-compliance".


The "notes" and the "minor non-compliance" issues will be corrected based on the recommendations and within the time frame suggested by the audit team. The assessed entity will specify how and under what time frame the non-compliance issues will be resolved.

The "major non-compliance" issues must be resolved as rapidly as possible, under penalty of the temporary or permanent termination of the activity, depending on the recommendations of the audit team.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

## VIII.6. COMMUNICATION OF RESULTS

The results of the compliance audits will be made available to the qualification organisation responsible for qualifying the CA.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

## **IX. OTHER BUSINESS AND LEGAL MATTERS**

---

### **IX.1. FEES**

#### **IX.1.1. CERTIFICATE ISSUANCE OR RENEWAL FEES**

Please refer to the specific terms and conditions of the subscription contract.

#### **IX.1.2. CERTIFICATE ACCESS FEES**

Access to the certificates is free of charge.

#### **IX.1.3. REVOCATION OR STATUS INFORMATION ACCESS FEES**

There is free access to the three CRL distribution points.

#### **IX.1.4. FEES FOR OTHER SERVICES**

Not applicable.

#### **IX.1.5. REFUND POLICY**

Not applicable.

### **IX.2. FINANCIAL RESPONSIBILITY**

#### **IX.2.1. INSURANCE COVERAGE**

The CA declares that it has purchased professional indemnity insurance covering its electronic certification services.

#### **IX.2.2. OTHER ASSETS**

Not applicable.

#### **IX.2.3. EXTENDED WARRANTY COVERAGE**

Not applicable.


### **IX.3. CONFIDENTIALITY OF BUSINESS INFORMATION**

#### **IX.3.1. SCOPE OF CONFIDENTIAL INFORMATION**

The following information is considered to be confidential:

- the private keys associated with the certificates;
- the Bearer PIN codes;



	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

- the identification data or other personal information of the Bearer contained in his or her certificate, except:
  - if the Bearer has explicitly given his or her prior consent to the publication of the certificate;
  - if the publication of this data has been requested by a judicial or government authority;
- the grounds for the revocation of the certificates;
- the audit log for the components of the CERTIMETIERSARTISANAT PKI;
- the Bearer's certificate application file, especially the personal data (with the exception of information of a personal nature contained in the certificates);
- the audit reports;
- the CPS.

This data will not be used and will not be the subject of external communication except for the sole purpose of the requirements of the management of operations in implementing the CPS associated with this CP, to meet legal requirements or for the execution of works or the provision of services entrusted to the service providers.

The individuals to whom the personal information refers have the right to obtain copies of this information from the RA, and to request correction of this information, if necessary, as specified in Law No. 7817 of 6 January 1978 relating to information technology, files and freedoms.

The individuals whose personal data are collected and processed are also entitled to object specifically to the use of their data for purposes other than those stipulated in this CP, in a letter addressed to the address given above.

### **IX.3.2. INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION**

Not applicable.

### **IX.3.3. RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION**

The CA is required to comply with the laws and regulations in force on French territory.

## **IX.4. PROTECTION OF PERSONAL INFORMATION**

### **IX.4.1. POLICY FOR THE PROTECTION OF PERSONAL INFORMATION**

The CA's corresponding policy with respect to information technology and freedoms has included this procedure in the list of procedures carried out by the CA.

### **IX.4.2. PERSONAL INFORMATION**


Information that is considered to be personal information is:

- The grounds for the revocation of the Bearer certificate.
- The Bearer's registration file.

### **IX.4.3. INFORMATION NOT WITHIN THE SCOPE OF PERSONAL INFORMATION**

Information that is not considered to be personal information is data that do not include information about the identity of the Bearer, such as:

- The audit logs containing the serial number of a certificate.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

- The LRCs (the grounds for the revocation of a certificate are not published in the LRCs).

#### **IX.4.4. RESPONSIBILITY TO PROTECT PERSONAL INFORMATION**

The components of the PKI undertake to protect any data of a personal nature they are required to handle for management purposes by:

- using a safe with locking device to protect paper documents (registration file, correspondence with the Bearer or the Subscriber, etc.);
- using a physical and logical safety device for files containing personal data.

#### **IX.4.5. NOTICE AND CONSENT TO USE PERSONAL INFORMATION**

Pursuant to Law No. 78-17 of 6 January 1978, referred to as the law on "Information technology, files and freedoms", the subscriber has an individual right to access and rectify information that concerns him or her. He or she may request changes by sending a letter to APCM at the following address: 12 Avenue Marceau, 75008 Paris, or by e-mail to info@apcm.fr.

#### **IX.4.6. DISCLOSURE TO JUDICIAL OR ADMINISTRATIVE AUTHORITIES**

The CA exercises its business activity under French law. If requested to do so by a competent authority, the CA may be required to provide certain confidential information in accordance with law L90-1170.

#### **IX.4.7. OTHER CIRCUMSTANCES IN WHICH PRIVATE INFORMATION MAY BE DISCLOSED**

Upon request by the Bearer, the CA may provide him or her with the personal information concerning him or her that it possesses, in accordance with Law No. 7817 of 6 January 1978 on information technology, files and freedoms.

### **IX.5. INTELLECTUAL PROPERTY RIGHTS**

During the execution of the services defined in this document and/or other contractual document relating to the certification service, material protected by copyright laws may be provided.


These materials, together with the copyright attached thereto, shall remain the property of the relevant copyright holder. The beneficiary of these services shall have the right to reproduce these materials for his or her internal use. However, he or she may not, without the prior authorisation of the copyright holder, make available to third parties, extract or reuse in whole or in part, these materials or derivative works or copies thereof, especially software or databases.

Subject to the provisions of this section of the CP, no license, express or implied, is granted by the holder of rights regarding inventions, patents or patent applications owned by him or her and created outside of this document and/or any other contractual document relating to the certification service.

### **IX.6. REPRESENTATIONS AND WARRANTIES**

The obligations common to the components of the PKI are the following:

- to protect and ensure the integrity and confidentiality of their private keys;
- to use their public and private keys only for the purposes for which they were issued and with the specified tools, in accordance with this Certification Policy;
- to respect and apply the CP and the CPS with which it is associated with respect to those sections that apply to them;

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

- to submit to compliance checks conducted by APCM or any other entity mandated by APCM, and to respect the findings and address the non-compliance that these checks may reveal;
- to respect the agreements or contracts that bind them to each other as well as to the companies and certificate bearers;
- to document their internal operating procedures;
- to implement the means (technical and human) required to achieve the services that they have undertaken to provide, under conditions that ensure quality and security.

### IX.6.1. CERTIFICATION AUTHORITIES

The CERTIMETIERSARTISANAT CA guarantees its compliance with the requirements stipulated in this CP as well as in the associated CPS. Where the CA employs external entities to carry out its certification activity, the CA guarantees the compliance of each of these entities with these requirements.


As part of its operational functions, which it may undertake directly or outsource to external entities, the requirements incumbent on the CERTIMETIERSARTISANAT CA, as the head of the PKI as a whole are the following:

- To be a legal entity as defined under French law.
- To be in a contractual / hierarchical / regulatory relationship with the entity for which it administers the certificates of the entity's bearers. The CA may also, where appropriate, be in a contractual / hierarchical / regulatory relationship with the certification agents chosen by the entity.
- To make accessible all the services set out in the CP to promoters of digitised transfer applications for the government, bearers, certificate users etc. that implement its certificates.
- To ensure that the requirements of the CP and procedures of the CPS are applied by each PKI component and are adequate and in compliance with its standards.
- To conduct a risk analysis to determine the specific security objectives necessary to cover the business risks of the whole of the PKI and the corresponding technical and non-technical security measures to be implemented. The CPS is developed based on this analysis.
- To implement the various services identified in the CP, especially with regard to the generation of certificates, delivery to the Bearer, and the administration of revocations and of the certificate status information service.
- To implement everything that is necessary in order to meet the commitments set out in the CP, especially in terms of reliability, quality and security.
- To generate, and renew when necessary, its key pairs and corresponding certificates (signature certificates, CRL and OCSP responses), or arrange for these certificates to be renewed if the CA is attached to a hierarchically superior CA. Distribute its CA certificates to the Bearers and the certificate users.

The CERTIMETIERSARTISANAT CA has an obligation to:

- be able to demonstrate to applications using its certificates that it has issued a certificate for a given bearer and that this bearer has accepted the certificate, in accordance with § IV.4;
- make available for the Bearers and users the list of certificates that have been revoked. This list is published as a CRL;
- ensure the consistency between the CP and the associated CPS;
- ensure that its bearers are aware of their rights and obligations regarding the use and administration of keys and certificates as well as of the equipment and software used for the purposes of the PKI.

The relationship between a Bearer and the CERTIMETIERSARTISANAT CA is regulated by a document entitled "Certimetiersartisanat Electronic Signature Subscription Contract", which specifies the rights and obligations of the parties and in particular the guarantees provided by the CA.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

### IX.6.2. REGISTRATION SERVICE

The registration service is represented by the RA.

When the RA receives a request for a certificate, it:

- verifies with all due care the appearance of conformity and consistency of the supporting documentation, as well as the accuracy of the information that establishes the identity of the Bearer and the company in accordance with the procedures;

*Note: The RA may rely on a CTA appointed and placed under the responsibility of the client to perform all or part of the information verification operations (see section I.3.5.2). In this case, the RA ensures that applications are complete and accurate and made by a duly authorised CTA.*

- initiates the generation of bearer key pair on a blank authentication and signature device.
- transfers the request for a certificate to the certificate generation service;
- transfers the authentication and signature devices to the Bearers;

*Note: The RA cannot use the Bearer certificate, as the RA does not know the activation code for the authentication and signature device.*

When the RA receives a request to revoke a certificate, it must:

- verify with all due care the appearance of conformity and consistency of the origin of the request,
- take the necessary steps to process the revocation request,

The RA archives all the documentation contained in the Bearer registration and revocation files (in electronic and/or paper format) in the manner described in this CP.


Only the CERTIMETIERSARTISANAT CA may call into question the responsibility of the RA, which explicitly excludes any commitment by the RA towards the client companies, the Bearers or the end users.

### IX.6.3. CERTIFICATE BEARERS

The Bearer has an obligation to:

- provide accurate information when applying for a certificate;
- notify the RA or the CERTIMETIERSARTISANAT CA in the event of changes to this information;
- protect his or her private key, using means that are appropriate to the environment in which the key will be kept, against loss, disclosure, compromise, modification or unauthorised use;
- set his or her revocation code. It is essential for this code to be set immediately upon receipt of the PIN by the Bearer, so that the Bearer is able to request an emergency revocation of his or her certificate. The procedure for the setting this code is provided in the letter accompanying the PIN code. In the event the Bearer fails to set the revocation code, emergency revocation of the certificate will not be possible.
- protect his or her PIN code and emergency revocation code;
- transmit his or her emergency revocation code to the CTA if one exists;
- respect the terms of use of his or her private key and the corresponding certificate;
- immediately inform the CTA, RA or the CERTIMETIERSARTISANAT CA in the event of the compromise or suspected compromise of his or her private key.

The relationship between the Bearer and the CERTIMETIERSARTISANAT CA is regulated by a contractual agreement with the Bearer.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

#### **IX.6.4. CERTIFICATE USERS**

User applications and certificate users:

- verify and comply with the purpose for which a certificate was issued;
- check that the certificate issued by the CA is listed at the level of security and for the service of trust required by the application;
- check the digital signature of the CERTIMETIERSARTISANAT CA that issued the certificate as well as that of the CA CERTIMETIERSARTISANAT Root CA 2;
- verify the validity of the certificate (validity date and revocation status);
- verify and comply with the certificate user obligations described in this CP.

#### **IX.6.5. OTHER PARTICIPANTS**

Not applicable.

#### **IX.7. DISCLAIMERS OF WARRANTIES**

Not applicable.

#### **IX.8. LIMITATIONS OF LIABILITY**

Not applicable.

#### **IX.9. INDEMNITIES**

Not applicable.

#### **IX.10. TERM AND TERMINATION**

##### **IX.10.1. TERM**

The CP remains applicable at least until the end of life of the last certificate issued under this CP.

##### **IX.10.2. TERMINATION**


The publication of a new version of this CP template may, depending on the changes introduced, require the CA to update the corresponding CP.

Depending on the nature and extent of changes made to the PC type, the deadline for bringing the CP into compliance will be determined in accordance with procedures prescribed by applicable regulations.

In addition, bringing the CP into compliance does not require the early renewal of licenses already issued, except in exceptional cases related to security.

##### **IX.10.3. EFFECT OF TERMINATION AND SURVIVAL**

This CP makes no specific requirements on this topic.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

## **IX.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS**

In the event of changes of any kind in the composition of the PKI, the CA will:

- no later than one month prior to the start of the operation, validate this change by commissioning a technical expert to assess the impact on the quality and security of the functions of the CA and its various components.
- no later than one month following the end of the operation, notify the qualification entity.

## **IX.12. AMENDMENTS TO THE CP**

### **IX.12.1. AMENDMENT PROCEDURES**

The CA will verify that any proposed change in its CP will remain in compliance with the requirements of this CP Template and any supplementary GSS documentation. In the event of a significant change, the CA will call upon a technical expert to monitor the impact.

### **IX.12.2. NOTIFICATION MECHANISM AND PERIOD**

This CP makes no specific requirements on this topic.

### **IX.12.3. CIRCUMSTANCES UNDER WHICH THE OID MUST BE CHANGED**

As the OID of the CA's CP is included in the certificates that it issues, any change to this CP that has a significant impact on previously issued certificates (e.g., increased requirements with respect to registration for bearers, which cannot be applied to previously certificates) will result in a change in the OID, so that users can clearly distinguish which certificates correspond to which requirements. A system of versions makes it possible to assess the level of change: major or minor (e.g.: 1.2). The first digit changes when a major change takes place, and the second digit changes if the change is minor.

## **IX.13. DISPUTE RESOLUTION PROVISIONS**

See the general terms and conditions of subscription.

## **IX.14. GOVERNING LAW**

See the general terms and conditions of subscription.


## **IX.15. COMPLIANCE WITH APPLICABLE LAWS AND REGULATIONS**

See the general terms and conditions of subscription.

## **IX.16. MISCELLANEOUS PROVISIONS**

### **IX.16.1. ENTIRE AGREEMENT**

Not applicable.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

#### **IX.16.2. ASSIGNMENT**

See section V.8

#### **IX.16.3. SEVERABILITY**

Not applicable.

#### **IX.16.4. APPLICATION AND WAIVER**


Not applicable.

#### **IX.16.5. FORCE MAJEURE**

All events usually held by the French courts to be acts of force majeure shall be held to be force majeure events under the terms of this CP, including events that are irresistible, insurmountable and unpredictable.

#### **IX.17. OTHER PROVISIONS**

Not applicable.


	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

## X. ANNEX 1 – REFERENCE DOCUMENTS

### X.1. REGULATIONS

- Law No. 78-17 of 6 January 1978 relating to information technology, files and freedoms
- Law No. 2000-230 of 13 March 2000 adapting the right of proof to information technologies and relating to electronic signatures
- Decree No. 2001-272 of 30 March 2001 with respect to article 1316-4 of the civil code and relating to electronic signatures
- Decree No. 99-199 of 17 March 1999 establishing the categories of cryptographic devices and services for which the procedure of advance declaration is substituted for that of authorisation.
- Decree No. 99-200 of 17 March 1999 establishing the categories of cryptographic devices and services dispensing with all advance formalities.
- Order of 17 March 1999 establishing the form and content of the file concerning the declarations or applications for authorisation with respect to cryptographic devices and services.
- Order defining the specific provisions that may be provided in the authorisation for providing a cryptographic device or service, no PRMX9802730A of 13 March 1998
- Order defining the form of prior notification by the supplier of the identities of intermediaries used for the provision of cryptographic devices or services submitted for approval, no PRMX9802732A of 13 March 1998.
- Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (J.O.C.E. , No. L 281 of 23 November 1995, p. 31);
- Directive 96/9/EC of the European Parliament and Council of 11 March 1996 on the protection of databases (J.O.C.E. No. L 77 of 27 March 1996, p. 20);
- Directive 1999/93/EC of the European Parliament and Council of 13 December 1999 on a Community framework for electronic signatures (J.O.C.E. No. L 013 of 19 January 2000, p. 12 et seq.)
- Directive 2000/31/EC of the European Parliament and Council of 8 June 2000 on certain legal aspects of information society services, and in particular electronic commerce, in the Internal Market ("Directive on electronic commerce") (J.O.C.E. No. L 178 of 17 July 2000, p. 1 et seq.);
- Directive 2002/58/EC of the European Parliament and Council of 12 July 2002 concerning the processing of personal data and protecting privacy in the electronic communications sector ("Directive on privacy and electronic communications") (J.O.C.E. No. L 201 of 31 July 2002, p. 37);
- Decision 2003/511/EC of the European Parliament and the Council of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/511/EC of the European Parliament and Council (J.O.C.E. No. L 175 of 15 July 2003, p. 45);
- Law No. 2004-575 of 21 June 2004 on confidence in the digital economy;
- Decree No. 2007-663 of 2 May 2007 for the application of Articles 30, 31 and 36 of Law No. 2004-575 of 21 June 2004 on confidence in the digital economy and on cryptographic methods and services;
- Decree No. 2005-973 of 10 August 2005 amending Decree No. 56-222 of 29 February 1956 concerning the status of bailiffs;
- Decree No. 2002-535 of 18 April 2002 on the evaluation and certification of the security provided by information technology products and systems;
- Decree of 25 May 2007 defining the form and content of the declaration and request for authorisation of operations related to cryptologic methods and services;
- Decree of July 26 2004 on the recognition of the qualifications of providers of certification services and the accreditation of organisations that conduct their assessment.




	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

## X.2. TECHNICAL DOCUMENTS

Reference	Version	Document titles
[PC RGS V2.3]		CP - GSS standard
[PROFILS]	V2.11 1/2006	PRIS – Certification Policy Templates– Profiles of Certificates, CRLs, OCSP and cryptographic algorithms
[ETSI_CERT].		
[RFC3647]		
[RFC3739]		
[DCSSI_ALGO].		Rules and recommendations regarding the selection and the dimensioning of cryptographic mechanisms with standard levels of robustness, DCSSI, Version  See PRIS-Repository of versions of applicable documents  See <a href="http://www.ssi.gouv.fr">www.ssi.gouv.fr</a>
[LSTI_OSC]	8031 v1.0	Qualification contract based on the GSS of a Trusted Third Party service provider (No. 8031)
[CERT_PS]		CertEurope – Security Policy

### OSC Documents:

- [1] Certeurope – Certeurope PKI security procedures
- [2] Certeurope – Certeurope PKI operating procedures
- [3] Certeurope – Security policy
- [4] Certeurope – Optilian contract
- [5] Certeurope – TéléHouse contract
- [6] Certeurope – Continuity Plan
- [7] Certeurope – Optilian contract
- [8] Certeurope – Roles and Authorisations
- [10] Certeurope – PKI inventory
- [11] Certeurope – Media support life cycle
- [12] Certeurope – Backup procedure
- [13] Certeurope – Hiring procedure
- [14] Certeurope – Training plan
- [15] Certeurope – Information technology charter
- [16] Certeurope – Internal regulations
- [17] Certeurope/APCM – Contract for the provision of an electronic certification service
- [18] Certeurope – LSTI contract

	<p><b>PUBLIC</b></p>	<p>Status: Official</p>
<p><b>CERTIMETIERSARTISANAT</b></p>	<p>Certification Policy</p>	<p>Last updated: 20/01/2012</p>

[19] Certeurope – Qualifying rules for ECSPs

[20] Certeurope – Incident management

[21] Certeurope – RA life cycle

Documents AC:

[21] CERTIMETIERSARTISANAT - KeyCeremony\_v1.0.doc

[22] CERTIMETIERSARTISANAT – RA life cycle

[23] CERTIMETIERSARTISANAT – RA-DRA Agreement

[24] CERTIMETIERSARTISANAT – Subscription contract – Specific Terms and Conditions

[25] CERTIMETIERSARTISANAT – General Terms and Conditions

[26] CERTIMETIERSARTISANAT – Authorisation of request for certificate

[27] CERTIMETIERSARTISANAT – Legal representative mandate – Appointment of a certification agent

[28] CERTIMETIERSARTISANAT – Certificate receipt

[29] CERTIMETIERSARTISANAT – Revocation request

[30] CERTIMETIERSARTISANAT – Archiving

[31] CERTIMETIERSARTISANAT – RA Guide

[32] CERTIMETIERSARTISANAT – APCM Statute


[33] CERTIMETIERSARTISANAT – General organisation memo

[34] CERTIMETIERSARTISANAT – Roles and organisations

[35] CERTIMETIERSARTISANAT – Information technology charter

[36] CERTIMETIERSARTISANAT – LSTI contract

[37] CERTIMETIERSARTISANAT – Risk analysis

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

## **XI. ANNEX 2: SECURITY REQUIREMENTS FOR THE CA'S CRYPTOGRAPHIC MODULE**

### **XI.1. REQUIREMENTS REGARDING SECURITY OBJECTIVES**


The cryptographic module used by the CA to generate and implement the signature keys (for generating electronic certificates and CRLs) meets the following security requirements:

- ✓ ensures the confidentiality and integrity of the CA's private signature keys throughout the whole of their life cycle and ensure their complete destruction at the end of their life cycle;
- ✓ is capable of identifying and authenticating its users;
- ✓ limits the access to its services with reference to the function of the user and the role to which he or she has been assigned;
- ✓ is capable of running a series of tests to verify that it is functioning correctly and that it enters security mode if it detects an error;
- ✓ is able to create a secure electronic signature for signing the certificates generated by the CA, which do not reveal the CA's private keys and which cannot be falsified without the knowledge of these private keys;
- ✓ creates audit log entries for each change that affects security;
- ✓ ensures the confidentiality and integrity of the backed up data and establish, at a minimum, a dual level of controls over the backup and restore operations.

The CA's cryptographic module detects physical attempts to make alterations and enters into a secure mode when an alteration attempt is detected.

### **XI.2. CERTIFICATION REQUIREMENTS**

The cryptographic module used by the CA is, under the conditions anticipated by Decree No. 2002-535 of 18 April 2002 relating to the evaluation and the certification of the security offered by information technology products and systems, certified by the Prime Minister as being in compliance with the requirements of section XI.1 above.

	<b>PUBLIC</b>	Status: Official
<b>CERTIMETIERSARTISANAT</b>	Certification Policy	Last updated: 20/01/2012

## **XII. ANNEX 3: SECURITY REQUIREMENTS FOR THE AUTHENTICATION AND SIGNATURE DEVICE**

---

### **XII.1. REQUIREMENTS REGARDING SECURITY OBJECTIVES**

The authentication and signature device used by the Bearer to store and implement his or her private key and to generate his or her key pair meets the following security requirements:

- ✓ ensures that the generation of the authentication and signature bearer key pairs is executed exclusively by authorised users and ensure the cryptographic robustness of the key pair that is generated;
- ✓ detects faults during the phases of initialisation, personalisation and operation and have reliable techniques for destroying the private key in the event of the regeneration of the private key;
- ✓ ensures the confidentiality and integrity of the private key;
- ✓ ensures the correspondence between the private key and the public key;
- ✓ generates an authentication or a signature that cannot be falsified without knowledge of the private key;
- ✓ ensures the authentication and signature function for the legitimate user only and protect the private key against any use by a third party;
- ✓ make it possible to ensure the authenticity and integrity of the public key during its export out of the device.

*Note: physical devices must respect these requirements. In particular, the technical specifications stipulated in the shared socket [Socle\_IAS] (Identification, Authentication, Signature) take all of the security requirements into account. A microchip-enabled card that meets the requirements of the shared socket, subject to its certification at the appropriate level (see the following section) would therefore meet the security requirements listed above.*

### **XII.2. CERTIFICATION REQUIREMENTS**

The authentication and signature module used by the Bearer is, under the conditions anticipated by Decree No. 2002-535 of 18 April 2002 relating to the evaluation and the certification of the security offered by information technology products and systems, certified by the Prime Minister as being in compliance with the requirements of section XII.1 above.