



Description des profils de certificats et des CRL

IGC

Version	Date	Description	Auteurs	Société
0.2	17/02/2021	Description des profils de certificats et des CRL IGC	DIS_IAM_PKI	BPCE-IT
1.0	08/10/2021	Ajout ECDSA pour les certificats clients	B.MOLLARD	BPCE-IT
1.1	15/06/2022	Correction des gabarits de certificats	F.ROBERT	BPCE-IT
1.1	19/12/2022	Mise à jour Mentions Légales	F.ROBERT	BPCE-IT
1.1	16/03/2023	Ajout des données liées à l'algorithme Courbe Elliptique pour les certificats porteurs	F.ROBERT	BPCE-IT
1.1	19/06/2023	Changement du montant de capital social	F.ROBERT	BPCE-IT
1.1	05/06/2024	Ajout précisions champs subject Certificats Porteurs	F.ROBERT	BPCE-IT
1.1	07/08/2024	Ajout des données liées à l'algorithme Courbe Elliptique pour les cachets et les certificats d'horodatage	F.ROBERT	BPCE-IT
1.2	06/12/2024	Ajout des profils LCP	F.ROBERT	BPCE-IT

Etat du document – Classification	Référence
C1 - Public	Ref OID PC Signature Electronique : 1.3.6.1.4.1.40559.1.0.1.31.101.1.3 Ref OID PC Cachet Serveur : 1.3.6.1.4.1.40559.1.0.1.31.210.1.1 Ref OID PC Horodatage : 1.3.6.1.4.1.40559.1.0.1.31.211.1.1

Mentions Légales BPCE : voir document Mesures Communes [MCOM]

*Ce document est la propriété exclusive de BPCE SA.
Son usage est réservé à l'ensemble des personnes habilitées selon leur niveau de confidentialité.
Sa reproduction est régie par le Code de la propriété intellectuelle qui ne l'autorise qu'à l'usage privé du copiste.*

SOMMAIRE

1	INTRODUCTION.....	3
2	PROFILS	4
2.1	AC RACINE	4
2.2	AC SIGNATURE UTILISATEUR [USSE].....	5
2.3	AC CACHET	11
3	REFERENCES.....	15

1 INTRODUCTION

Le présent document décrit les profils des certificats produits par l'IGC BPCE, en conformité avec les documents suivants :

- œ RFC 3647, *X.509 Public Key Infrastructure certificate Policy certification Practise Statement Framework* de l'*Internet Engineering Task Force* (IETF) ;
- œ *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service providers issuing certificates ; Part 1: General requirements* (ETSI EN 319411-1).
- œ *Certificate profile for certificates issued to natural persons* (ETSI EN 319412-2)
- œ *Certificate profile for certificates issued to legal persons* (ETSI EN 319412-3)

2 PROFILS

2.1 AC Racine

Version	3 (0x2)
Serial Number	1 (0x1)
Signature Algorithm	sha256WithRSAEncryption
Issuer	C = FR O = BPCE OI = NTRFR-493455042 OU = 0002 493455042 CN = BPCERootCA
Not Before	Nov 25 12:33:43 2020 GMT
Not After	Nov 19 12:33:43 2045 GMT
Subject	C = FR O = BPCE OI = NTRFR-493455042 OU = 0002 493455042 CN = BPCERootCA
Public Key Algorithm	rsaEncryption
RSA Public-Key	(4096 bit)
Modulus	00c83021b36a8e71a0f19b2b622b58d61bbd8615f63f1d4c19b2e572840c16a0557ea40edc9d5e0f0a150f8566fb9100f5c70af1b3b5f57b8f8b4331f94da4b4ad00905d8862721f60160dbdee18ff92daba07a434c53c0a1a298011eca2cb5f40c0556807d6fd4170ef1f799a1a05e9d13b3606e3965b4023a9cf4d0180ce1551c4e905b8d757fa85570a6a4fc6c9a0efef44e64334e5a5550ca508c08926bd8f97e1973f0f00e98c13ce22611aa44f993225e373d024567cac60802905bcd088a7e6d9c53bf7d811c0cbc442debe9816646810c211626473d57aba43652fb433a0ed54d730076b31f1ea75092c8c7978b56b4bac271869e5bd2bf46bd957e1865f9308970cf96b7fa55d12c7b70b9ec0885018cd1a029a3094ad53969a56da987dbf3fc2c83b48cd5f0aec3f1766bb583c2d3872b04c003d2cbe758aee8db849e93e9f7f70abcc63afe7aad3fbff07244508ec65f356307aae89dc18ad13ee93f827184edbed0c551de4d3b53671a9a186d1e326b5c320c39b1bbf656d74bbf1e6b6d270e733bff410fe7634f1ff9e5aa831cc952a110bab0358c4f1d7211a75d07fc093471633bb358a5986e13739935bb5cd4d4be695788e61c9f21365daebb817870f9f56d2c6c0fa3fb2a7cf30f703327490214e1ea6f84c7a0956308efdda558a36cc2b2d6298437a66764990524c5391553eb1c71897ce432069da9187
Exponent	65537 (0x10001)
X509v3 Basic Constraints (critical)	CA:TRUE
X509v3 Subject Key Identifier	40:EB:C3:B1:D6:E7:A1:62:C9:9E:9B:E2:55:88:3C:9A:FC:24:FB:32
X509v3 Authority Key Identifier	keyid:40:EB:C3:B1:D6:E7:A1:62:C9:9E:9B:E2:55:88:3C:9A:FC:24:FB:32
X509v3 Certificate Policies	Policy: X509v3 Any Policy CPS: http://www.dossiers-securite.bpce.fr/
X509v3 Key Usage (critical)	Certificate Sign, CRL Sign
Signature Algorithm	sha256WithRSAEncryption

	5f6730c893cce02c22c83950b855a65ec1a1d3d346ef0e7545b15101d0f4ceec18cead2ecf40cb6d36ef4bc7dd14afd458caa938a3d6cc079f6269e580fdefed64ca1312e75554abece6a2d7758b61465bd11ce0ed02f134d08e9c7917e35b99f19572e66bbde2433704d6b660ca1858a0037794939f50638a30f8a8ae4679b2469b8be1bc774d66a5422d84f28a6518a6e332cbdf4887ab20e07c6bfff9695c62b850715f2be1c93441b4746c7192771d154e9735bb6b879ff814db6db91e8003877556b66de0303f0101b9331d5dcc27a1cc99987ac64964e630f20f2ff5eb0b3c1d52bccac3c2f79946bfa6ff68e400eadab6a5f8b6a3e57fe406483bb32c122cefd5ee1463fe104bcf96423379a2177b7e83cdc995f5e98d36a55a3f0e51785db6ea7fc79bd5fe5da430a0b8ff2c19c6afa424f62d49bdf31660cb40e127f88fee5a5e423908ab08527a0bf16033e14d79a8e05e35005177c5111e92a110a969dc71636d88dff8051bc2b5e944503377ed856a774cd3f416304ff801897f9ee192ae7ee76f120b8533bfd29a31ff53c2e0d80b79915ee28d4d546899121a71ee6b1d2b8d7a85761afef88f9ad396d97246006ca36ef7e00ea53fff51f330165574c7b2377589be980734ae223fdd2aef8595272d097d809a2b0568a9b4e70380e9e379588643bfbbcca0f0ee362ce361febaefe9e4eb8c6b5cb36976c4be260
--	---

2.2 AC Signature Utilisateur du Service de Signature Electronique [USSE]

Les profils correspondent aux OID suivants, de la PC Signature Electronique [PC_SIG].

Niveau	Enregistrement		Population	OID
NCP	AGENCE	Face à Face en agence avec vérification de carte d'identité	Particulier	1.3.6.1.4.1.40559.1.0.1.31.111.1.1
NCP	AGENCE	Face à Face en agence avec vérification de carte d'identité	Professionnel s	1.3.6.1.4.1.40559.1.0.1.31.112.1.1
NCP	AGENCE	OTP CAP ou sur SMS ou SECUR'PASS	Particulier	1.3.6.1.4.1.40559.1.0.1.31.113.1.1
NCP	AGENCE	OTP CAP ou sur SMS ou SECUR'PASS	Professionnel s	1.3.6.1.4.1.40559.1.0.1.31.114.1.1
NCP+	AGENCE	OTP CAP (ex : avec Challenge) Certificat numérique sur support physique (Clé USB, carte à puce, etc...)	Particulier	1.3.6.1.4.1.40559.1.0.1.31.115.1.1
NCP+	AGENCE	OTP CAP (ex : avec Challenge) Certificat numérique sur support physique (Clé USB, carte à puce, etc...)	Professionnel s	1.3.6.1.4.1.40559.1.0.1.31.116.1.1
NCP	INTERNE T	OTP CAP ou sur SMS ou SECUR'PASS	Particulier	1.3.6.1.4.1.40559.1.0.1.31.117.1.1
NCP	INTERNE T	OTP CAP ou sur SMS ou SECUR'PASS	Professionnel s	1.3.6.1.4.1.40559.1.0.1.31.118.1.1
NCP+	INTERNE T	OTP CAP (ex : avec Challenge) PVID Certificat numérique sur support physique (Clé USB, carte à puce, etc...)	Particulier	1.3.6.1.4.1.40559.1.0.1.31.119.1.1

<i>Niveau</i>	Enregistrement		Population	OID
<i>NCP+</i>	INTERNE T	OTP CAP (ex : avec Challenge) PVID Certificat numérique sur support physique (Clé USB, carte à puce, etc...)	Professionnel s	1.3.6.1.4.1.40559.1.0.1.31.120.1.1
<i>LCP</i>	AGENCE	Face à Face en agence avec vérification de carte d'identité	Particulier	1.3.6.1.4.1.40559.1.0.1.31.311.1.1
	AGENCE	Face à Face en agence avec vérification de carte d'identité	Professionnel s	1.3.6.1.4.1.40559.1.0.1.31.312.1.1
<i>LCP</i>	AGENCE	OTP CAP ou sur SMS ou SECURPASS	Particulier	1.3.6.1.4.1.40559.1.0.1.31.313.1.1
<i>LCP</i>	AGENCE	OTP CAP ou sur SMS ou SECURPASS	Professionnel s	1.3.6.1.4.1.40559.1.0.1.31.314.1.1
<i>LCP</i>	AGENCE	OTP CAP (ex : avec Challenge) Certificat numérique sur support physique (Clé USB, carte à puce, etc...)	Particulier	1.3.6.1.4.1.40559.1.0.1.31.315.1.1
<i>LCP</i>	AGENCE	OTP CAP (ex : avec Challenge) Certificat numérique sur support physique (Clé USB, carte à puce, etc...)	Professionnel s	1.3.6.1.4.1.40559.1.0.1.31.316.1.1
<i>LCP</i>	INTERNE T	OTP CAP ou sur SMS ou SECURPASS	Particulier	1.3.6.1.4.1.40559.1.0.1.31.317.1.1
<i>LCP</i>	INTERNE T	OTP CAP ou sur SMS ou SECURPASS	Professionnel s	1.3.6.1.4.1.40559.1.0.1.31.318.1.1
<i>LCP</i>	INTERNE T	OTP CAP (ex : avec Challenge) PVID Certificat numérique sur support physique (Clé USB, carte à puce, etc...)	Particulier	1.3.6.1.4.1.40559.1.0.1.31.319.1.1
<i>LCP</i>	INTERNE T	OTP CAP (ex : avec Challenge) PVID Certificat numérique sur support physique (Clé USB, carte à puce, etc...)	Professionnel s	1.3.6.1.4.1.40559.1.0.1.31.320.1.1

2.2.1 Certificats d'AC

Remarque : Il existe quatre certificats d'AC différents.

Champ	Description	
Version	2 (=version 3)	
Serial number	BPCE Sign 01 CA	ea:13:be:bc:35:59:87:17:54:f8:b9:c6
	BPCE Sign 02 CA	ea:13:be:bc:1a:ae:07:31:dd:59:61:34

Champ	Description
	BPCE Sign 03 CA ea:13:be:bc:e6:3e:80:53:45:9b:ec:b2
	BPCE Sign 04 CA ea:13:be:bc:70:30:d5:7f:5c:bf:ff:26
Issuer	CN=BPCE Root CA OU=0002 493455042 OI=NTRFR-493455042 O=BPCE C=FR
NotBefore	Nov 25 14:38:29 2020 GMT
NotAfter	Nov 19 12:33:43 2045 GMT
Subject	CN=BPCE Sign 0x CA OU=0002 493455042 OI=NTRFR-493455042 O=BPCE C=FR
<i>Le « x » prend la valeur 1, 2, 3 ou 4, en fonction de l'AC qui a émis le certificat (BPCE Sign 01 CA, BPCE Sign 02 CA, BPCE Sign 03 CA, ou BPCE Sign 04 CA)</i>	
Subject Public Key Info	(rsaEncryption) 1.2.840.113549.1.1.1
Key size	4096
Modulus	Voir ci-dessous
Signature (algorithm & OID)	SHA256WithRsaEncryption
Authority Key Identifier	keyid:40:EB:C3:B1:D6:E7:A1:62:C9:9E:9B:E2:55:88:3C:9A:FC:24:FB:32
Subject Key Identifier	BPCE Sign 01 CA 1C:94:10:74:45:74:D9:38:41:FC:D6:E4:BB:A2:12:B5:E2:83:E8:5C
	BPCE Sign 02 CA 2E:75:1E:34:CB:A6:B7:DB:E1:09:27:C5:F7:A0:D9:48:A9:08:6F:40
	BPCE Sign 03 CA A3:EE:4E:D3:37:FB:89:A1:FA:50:61:C2:60:8F:5A:AB:C2:00:42:00
	BPCE Sign 04 CA FE:D2:45:19:6B:25:CD:06:9F:94:0B:E6:AC:45:28:7C:AF:32:A6:09
Key Usage (critical)	keyCertSign, cRLSign
Certificate Policies (critical)	
policyIdentifier	2.5.29.32.0 (AnyPolicy)
policyQualifier-cps	http://www.dossiers-securite.bpce.fr/
X509v3	
Basic Constraint (critical)	CA:True pathLenConstraint:0
CRL Distribution Points	
distributionPoint	URL http://pro.d00.pki02.bpce.fr/BPCERootCA.crl URL http://pro.d01.pki02.bpce.fr/BPCERootCA.crl URL http://pro.d02.pki02.bpce.fr/BPCERootCA.crl
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.2 (Autorité de certification émettrice)
Alternative Name	URL http://pro.d00.pki02.bpce.fr/bpce-root-ca.crt

 BPCE	Description des profils de certificats et des CRL
--	--

Les modules de chacune des AC sont :

BPCE Sign 01 CA	bfee525aecab513f4fe6852628af63d864f8903e643e8af87492c5a6ef8ae699b00176ec45e58a07c109c5db715d4ea93f163580ec81c0fdce49b7504e2dddc7401911d1e43e15dcb6fdf6dd995fe3fed6f09fc55aa62fd6fa847439943107d40a46a7eba007f934c584e0c936f187416f1fd6d75a864111a1be4818595d29ca45d954d33c536ebabf41b94e11c90bc7f0c8739d2bb5b9f8c767e222a6566573ffeff75bf406826818f0c4ac1e18369fb210b6361475eace4bd5adb9107bb08221c1f6a182f871811795bec4b66c8e8b2b6bc79500503ddf46b1eab29389de7c08a375d7391dc151541e4ac7af7b22ae2dd4ea53f7a764429ca3478355af98b70f3be03a8a2e397c20aeac0e6f2f04467ff590413f7309a2f2da726738675a1529a99b65b3c8207db8484ba352dc177b976d72f558dff8432cc8f316b3133bb7f3c1d88a89fb1a44e58d9ecf1bc0b84b21097e06c4c80d6e1c581020c05614bed8673b0c6ffbf6a10a689c1d831e2a344c7c8a7e5dd385b013ba419078ad13a5106c8f42537c9c561034ee15474daafdedcc1188c163ec59a8e4e84b5de7dcc09c28782cdc393e8bf3d6254bde6f9d77fb3cc96a28fe7959a48d2c12d17ad0b38efd5cdcd836a8be117e6e16199bd6db9afc99e38b0b592d4373bee7c318139ae94dbe97d32dd9ec8e89f3b0cc74d2e66e688bac97e6446596b4479a435711d
BPCE Sign 02 CA	c1c7b4461649ede0bc085dddc706f28a47805b051942d9da44ce818632d246119714394ee846ff994dd101c9883179133669367108b1271cde8a49dbdbba73a444b24828323a264db37556da30bcd8e381f864670b053edbed2e769ab1055c1ba76d7d0328fe52cbf0396def19da5f0b3a87831189caf0b68a28ed45b4e808fe5091147efd4e4eb04c2d1daa18693a008e3ebbd310464d5621de969ce0234daa2d7c7ea9662621bb456a7bf2703244d76c99a0dcff379a5785016b7b2895c504f2304491b6542f68d0433f5d134529270451945f824a93ec34fd247f28383f8a07a5756a8d8f94983107df295621749acf07626d933b8051e00587b44c7cec1ede11a4916fe706baef3870063e62ceac88323561acc9fa561b64bd1b5fe4a35eb6982f8ec6cedc3a4d5f2ca3f1f5fa8b7ca958a46827276e841d1757b0217bf86c5c438b269e3945cfff287d1f515de720e83db53a6759f949b1ad445cce1260fc27a4222a8f205fd3c6131261dfea326a7c715c39cc06d2ab4e22790ae27f6576a41d8588ba9c8bf3dbf3e822f9d253db6330c5c0eda60d6ae422cf0566cd04467d4e6bdd4feea26ce6be02156bdec7c88a9bd72688022a0b3163660cf579e0371e47770ebd5e0b115b14019e7d5bdd9cb3ce8690e72a45ad30a759f9adf62cad16203946f2294685c8a469936ae53e0fbdf5444a7b12aec69666c178981f9b0d
BPCE Sign 03 CA	b20d025b52770e13fe836e37740ba3554fe53e38187850886d1df705584035acefc7c284207f8e45b3568d2d316830941bb0c330759134c1ba443e002ab7ca6e91e4eb453c859d219a3059be2ca9a49351e3138810fc8380bb1f6c99e8ed508a68d7359d5df4254bd3c47e43148339b816e5b3191e6612565e101414c9c9e3f19af4e3bdc3f3c7d83f28e323d66472bbd1380429e0db8288060ae72d591c7be8d0b8d777d69bc3e35ecf5175bf4bb56867ba66e5ba53b30f882488ba4159b9379a8fa22a652758df2b8cf10899824fba7417fca8ce8d8ac614f43f2c30cfe0aca30ab09da8cd8eadd684e23e84f144b0a14a55e3b30460cc9d6b66a94fb79613452a93a3d190e142acc27b3d9428dddb7064202569da3efcc17f1a10555f3873ce7a0902343fc15f575b1fd9dd3f162019dc88297b2fdafebb05924f740cc9b8d15b551ccd699e74aa47c39f234d4f3b68468165c4e93755d7e06e57fd897b3244fe33a78a6f4309c19ccde81ac6822104d3e90681fa827d9f3b9768f0738ce6bd574ad82dd4d36ee6d62d273e6e4d8cfff95a6944fe3f5b0b970d3d2335f9ccb81d594f038e2feee2875365d1696565d1d987e0a09d035764f36beaa9cb979ef8207e51580ae188d022caed74d4585b51155bc2422d2976a7169aed4a963df3b086402e2ac1e708093da18919d1937e6169a77b2951b1d46ec5804c3eba7423
BPCE Sign 04 CA	a9fdb59563a30197dd2e9400ba1d8e56eafe5d1f426bdea8634b81829b0324c9ab585d7887ed11078fb1d26307c93c88d8839192e258e91638d18afe1e3c93df537b78de1d6c5394145491e4509532ab43a099fcd3f01c0a9691d61b36801d1f7c22c8c12dff517f13fa8a5b61dfd3026f933a1bbdea0e3830d7aace767a60aedd1b75e324c841b925244c8fffd111e135274944b965b044019ab71b0a48e6a24ddb3baa9cabe1dfbd7151d8fcf453d06d7f05b7311000974dd44f5be90d469bf863adf2719ce06ab695a007954baf4ec7673e7d70db634ed4d175b404f71cbfc05a04c37aa440eb21dace7fd867257bd6431d78fdfeaea8a63cf3cbfaf5addf80ae84fe1e3a308f6d8e63237ae77fa23410a8c6e1b5e7b2d425645c3391d1330eb2ac63886f2aeef1a292e38319b7292f3f867743b46c9bfe82155906f0163a0e4230fc42275e9bb8a336cc36be85c0bb5f908332f2619789776e1a13aba46550f6a6a41c5d605ec958f1a91de39f39054db106423ee91786d060db7885dc6f2414be5f2c0621281698adcdecaec48b230a07cabe6991f514e991ba83c1ff7584c4cddd013c2ac7aea7491dae4eb874d2ac33c1b07e01cb52f90feef54cb34d17e1759eed26e75ca8e92d6d0624d15969e6b07499e90a7e127309650c302da28a043cea34b8447dcc5b5c82702cc913727aebbf6199680052a35f61caffa3

Les signatures de chacun des certificats sont :

BPCE Sign 01 CA	003f2fb928b2a515129dcf80720e0585e4b81663a5f22dc18e9dd80cbc096f8698092f0927671bbe80ac93f8217b90832adf9d89dbbc478dd08f75a279ab6456f347a6822de08fd98fcdcb00557e2a2838b693325bf21742bba99af8bfb4ed75af086dfa615f8defeb36b774b4b0660e32718f508a9abcf341b1eb9a5d56b9c6358b50d6a383b150b1a5639dc608f3c7f783c9015074e5fb49a1406d6da136acf4b4c79a0bd5c658972aaade849c796682535fec029840159213c948ae47b1d06708c41c4b87148cd22e977c2b189e975f30f6abe494fce32eac5adccf670c62616e30785eebd27e883f4e5aebc8d32ce5ad409ef6bf0fb444a4fb1a7f01314c045e9ac4678d5b8ef836b026bf41dfbfebfbe3eaf0cfed79cc646e21481ccb73054d6500e1464a768ef9ef0331c1a837874a33599c9a936c68c396df69e6608864e3fc06ad8ab41f647a7a3452112dc924dc511624e781d6b43d31b4c80546bbc42d262532d0d7bed73cb7344b68c4865114bf90ea3d565c69f0f0fb0ac082d56925e887d81e3d6921047e4c2c4e0dc87a43d26c369428dae8b85c54d9d9188f07bc6d8547d45173fce8ab7d0e1aac395e37c1dbadf544bd16484d2a5d5fbc32e46a72591a453132c18bb955ac3ad14f4c72a8cdab74c52d9ec4c81abfbc4c717c5e21862d2cdac974fc72e4a7df5e332eda20e25c74d057 6b03a31c63196916
BPCE Sign 02 CA	07be9b37c07e8a022173f39fbd4e3c70ae8d7c3bba1fdfd169dc5ae824374e36d184267efe5d5fdeedcaa683747f98d7cae3dd2073dd27a5b43de8cf188cf61b63dcb6818b686c9de7737f7be5ad9d2c8b9ae3559ed6184eae2ee30b20ba235a320decddade40a7e0d1ce8304554f768a5e15b0e53606d9a66b03c8a00ef23d38b9abe9099386e0415b1b7548b90c20f6e8caab9e978ec1ffe67fdac31aed0662b55a5aa5109367f9428dd5e47ceb8b007ba77c84da14d44ef4bb336d00f7baecdddf58775558a7b81cf6209ff0739d94f0b0dc662478654f283cc73ebcd89354d573bf6be74103ed9a5227b27afca5d60106443fb4b4cc2aaab7bb9cc0b6963e4a3d2e3ed55b9f2c2aa48f27d662e376a2b5c42343798b7624b4120a97ec8ab2abf198dac048a171416f0b23153b74765c0289b0dc05d2520bddac08b3e677c51268cd83ef5f77fa9d00dcb852d634d283de9c9e566389a3ff15aa9a87b5f4f00c38fd71ee36dff05efaf1edb46c29a18496fcb410cd2d5259ceb2f1682abb3a13e65065280263f57774eed257c44b5e8a28f9ae1d42952da3b4e08c0c5e5781c398c42c766f02b8181e779665ad712ca800889cdd3b7e0487c9beb47eebe041b3f8580d5a00fc3712db9a17993b57b775c597a022075fc2e146265d9507b6f19e09b09d47612266049ce9cb62fa41c94cfd3f6405d3c9722 1dbbba5988d16a4b
BPCE Sign 03 CA	b824488bf2e3b8f4be0940386089dd500987625f1e5f4c8d9952d6612ceb40b71a13c3bb935c8c662cd3b40d474d36fc12de8dd63b1675c494f03acc471f320017c7354edbef35750104e37c1970fe9cbf2bc522957e8fb4f67d112d41bbcd49e10c22e069aa38c84dbd4bc7ed0049a9a75d194681dad45f1d70c4e7da0ed5b6a04903d009a5d34d0d44aaef8357c61b229cda0eff9cc9d80f52d03a575cba4704a0667dbaa209889d86fe5e1e97a91d9009dff03504f85b2dd8046c763613d4514f229316443797632112cc41d16a97ae27025fef5631167169dadb706715131a1ff8f1355b6731625db81ed84bac3081fd8cb4c2b92c0bb60807bc888af7425a9fd7df2cc80fa2565369ed57edc8afe2152207679f606756efff032693f710007fc3e3cec743889b6de44fabe333cddb6b422024f6e19be9cc17b28a71a6b519a30caeb44872eab0bd2ffdf8532b463224721776d617ee3588d190f418259851709b453633bcc3ebee8918fb54b5f8e8de4d09b90bffd0918caeb22e61de46bb12cc3ec6fd1f941a83bc4699e872c0ed52182581718701181828f1ab71468ac35b3a726b154c5e557f8b2f48618f265dded6ba5eae5b89431154652550a19bbd3b172b1d210957a14c40f0820e903e95b96c2c0b4cb82263d8c757232c6e819daa1a63d333c7cf549aa0aa43278346b595b5d7bd775 a7ffa9489e6fb8a9
BPCE Sign 04 CA	1cfc5968c9f7cb105a40e74d9f7b7a37ecac147b007714c232a3dd1230e508a55b90b298e6a0d2717deaf836a28df9f45627b9aed3932d8062c5f726afca337476184cf1ae0a9b336ba45ad04f80fee0d87594a1991a20f63cbd396f59c1d81c539b63dafa21ff8a2917cdfb23b205d220531fdbbb1f43c2e5ead79d9185d40c43ad6964165893cae78cf71b5b3a84680ef2608548999648387c8a13070efcf25faee03f81fced88323ef902f668fc7c2e580bf84265402d9287bb88d2d9b3989eb254548e673b0d2020ecf6ee106c4488c3d7ae8884a6dc6eb873a73f4f81d3b7dd43e48ab7bc906990981bf391c5127acee2ebfe2a8a26c743dd73870df65fcfab750aea5b7ff3d51775337e0ec9ccf592395b06ac051c2f2159b53b9bbe8c681f9cbb74c6375aa76cab2a22adb69303a3d57ee31aeb6a84a5f57ae5759f4856a1ca183ebca5fec43ea45cb25becf56baa5d90b6b61f95a87cc9bab42b030e725dac88cc1e266623a2b6e9e7f045c80beb21086433cab8cbdbfb9ee1cb0f662007eacb22272e25df8cbd8bf335790f1702de1def79b7c1e9d04930e967aa7815c7037e8f205faabc2ee6cba910508b061173cabe9734b69a478fa32743a66566252096dc50e5dbda4907aa2521bda05df5cd0007a4f5d159d14a86654ad2afcebb251963a31d54a776de2b31ef44763b7f36e9118cc059 a588d07cce71a3e8

2.2.2 Certificats Utilisateurs [USSE]

Champ	Description
Version	2 (=version 3)
Serial number	Défini par l'outil
Issuer	Voir [PC_SIG]
NotBefore	AAAA/MM/JJ HH:MM:SS Z (date d'émission du certificat)

Ce document est la propriété du Groupe BPCE. Ne peut être reproduit par des tiers sans son autorisation écrite.
Classification C1 - Public

Champ	Description
NotAfter	AAAA/MM/JJ HH:MM:SS Z (10 minutes après la date d'émission du certificat)
Subject (Utilisateurs [USSE] Professionnel)	C = <code pays de l' Utilisateur [USSE]> O = <libellé de l'organisation personne morale> OU = <Identification de l'entité légale de l' Utilisateur [USSE]> OI = <Identification eIDAS de l'entité légale de l' Utilisateur [USSE]> serialNumber = <identifiant de transaction> GN = <prénom de l' Utilisateur [USSE] personne physique, représentant la personne morale> SN = <nom de l' Utilisateur [USSE] personne physique, représentant la personne morale> CN = <nom et prénom de l'Utilisateur [USSE]personne physique, représentant la personne morale > Voir [PC_SIG]
Subject (Utilisateur [USSE] Particulier)	C = FR serialNumber = <identifiant de transaction> GN = <prénom de l'Utilisateur [USSE]> SN = <nom de l'Utilisateur [USSE] > CN = <nom et prénom de l'Utilisateur [USSE] > Voir [PC_SIG]
Subject Public Key Info	(rsaEncryption) 1.2.840.113549.1.1.1 (secp384r1) 1.3.132.0.34
Key size	2048 ou P-384
Signature (algorithm & OID)	SHA256WithRsaEncryption Ou ECDSA_P-384
Authority Key Identifier	Identification de la clé publique de l'A.C. émettrice
Subject Key Identifier	Identification de la clé publique du porteur
Key Usage (critical)	contentCommitment, digitalSignature
Certificate Policies (critical)	
policyIdentifier	L'un des OID ci-dessus.
policyQualifier-cps	http://www.dossiers-securite.bpce.fr/
X509v3	
Basic Constraint	CA:False
CRL Distribution Points	
distributionPoint	URI http://pro.d00.pki02.bpce.fr/bpcesign0xca.crl URI http://pro.d01.pki02.bpce.fr/bpcesign0xca.crl URI http://pro.d02.pki02.bpce.fr/bpcesign0xca.crl

Champ	Description
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.2 (Autorité de certification émettrice)
Alternative Name	http://pro.d00.pki02.bpce.fr/BPCESIGN0xCA.crt

Le « x » prend la valeur 1, 2, 3 ou 4, en fonction de l'AC qui a émis le certificat (*BPCE Sign 01 CA*, *BPCE Sign 02 CA*, *BPCE Sign 03 CA*, ou *BPCE Sign 04 CA*).

2.3 AC Cachet

2.3.1 Certificats d'AC

Champ	Description
Version	2 (=version 3)
Serial number	ea:13:be:bc:ab:2d:00:55:f4:32:35:82
Issuer	CN=BPCE Root CA OU=0002 493455042 OI=NTRFR-493455042 O=BPCE C=FR
NotBefore	Nov 25 14:44:23 2020 GMT
NotAfter	Nov 19 12:33:43 2045 GMT
Subject	CN= BPCE Seal Time 01 OU=0002 493455042 OI=NTRFR-493455042 O=BPCE C=FR
Subject Public Key Info	(rsaEncryption) 1.2.840.113549.1.1.1
Key size	4096
Modulus	e7bbc140adf8d56e89996e90cd8eeb30b81fe893bdfbbe91df2e7de187beeb 201b40b3331fbd65c8eb1ef77ebdfa77dd6e8ad6f1f19ecaf03d141d0107ae7 5ae9e6702282fc88879a7577c8d9783c2783c1d080e558d225ea2ce33e2cbdf c245fbd60d66525372027978023378357ea96161a97a32a1e1caf3a491a8525 9cfa2155699a1feef38a5132d4676d138e27db921485fe466936b1c2c60f199 b131ae7916baf1a116e43135f4b3f7c6225c0f96d2200e81e96359aedf0a559 a09038811e618d7c12b264902ab3c9bc4582519b10a5620d8a14105222f9dbf 1b54e728bca506d8001008c5d6f53c9af67c8c135200aaf0c79f083aa0700f9 c53c78071fb4d8026e28c1a8a796c1f242cf1f2dd4ef20280210b0f2f8d533e 1a0f24abe4b0b56e668d83e2f9c48840d61f73106839248cf6b69822cdcd48e 32d21e16fdfeb844078ab2aea8d1800dc6382a8c99d771d21c8ff7bbc73526c 649d6f90b2cf39fb720f8383735393a95788fb672a50feefa7543e5f2c6fd30 74e2bcb91e12edfacc9c108e99cd8c3c0967564ab3216b902b57a21897a77d4 8675032cc00f067a28a190390e69fa97eb21fa49dfad01f1c4f4ca31edcd226 5042a29ed63937cbc4c2887942903ee020525aad963c391463f6ad8167d3d01 c548a0625fe71ac81726ab655a0bf41ffe3bcc2c767e857108ac6fbb5449109 88226b470acc2b8d
Signature (algorithm & OID)	SHA256WithRsaEncryption
Authority Key Identifier	keyid:40:EB:C3:B1:D6:E7:A1:62:C9:9E:9B:E2:55:88:3C:9A:FC:24:FB:32
Subject Key Identifier	57:BD:85:17:9F:3E:BC:A9:02:59:61:B9:FC:95:03:4B:1B:22:2D:77
Key Usage (critical)	keyCertSign, cRLSign

Champ	Description
Certificate Policies (critical)	
policyIdentifier	2.5.29.32.0 (AnyPolicy)
policyQualifier-cps	http://www.dossiers-securite.bpce.fr/
X509v3	
Basic Constraint (critical)	CA:True pathLenConstraint:0
CRL Distribution Points	
distributionPoint	URL http://pro.d00.pki02.bpce.fr/BPCERootCA.crl URL http://pro.d01.pki02.bpce.fr/BPCERootCA.crl URL http://pro.d02.pki02.bpce.fr/BPCERootCA.crl
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.2 (Autorité de certification émettrice)
Alternative Name	URL http://pro.d00.pki02.bpce.fr/bpce-root-ca.crt
Signature	3a59031cb1b41ae67e80adc518beb6a79e9ae88f1c4e9f0c825da8d89e7335b ce919033eea194a90e67d6990b482aff44f748cc835f6d624f9de6f1c3e6561 4871cf024477abe89af7bb6a8b2faf1be1cb7d14b0d80d8200ed612531fdd8d cc04478f4165ae594e7241c6c22c7ad103a563597c4804d85df3bc431748f9b a7a1fd408d617081e911f27201551dd45f7b7e80d7b19bab82f14e7ea917fda d41dbd1252399614fc20eed25798d97eefde9c41dfd6cc7c4cac86bb54890f 20c6ba2dba3b6dd3e94700d745f9f8f30c44c4007361bc78c9426bb28a605b5 86aeec73ffb21472c40d4a5e2e28a50217cb2370c742be987cf9cc9551666cc 7a1cdd06c2fb8c04ce63879bc0f4931754267d767a71bab3f2c8e90f12aa942 b70f00c6a33f69106458debe06a89fc4515096243a0c2a8454360b50ddc9ea5 e5c3928171e1d8b276a388c0e19bbb5b173be1c0f73c285ed3d4ab0b6c98bc0 58d24dda039ac092a92b28bc45b1d5b57afb327b752698620ff23d558b6cac 3d0721bc26fb17afda3d386b8b7debbb457835627e27f127e9384cab17a9328 e68c5fb4a33683a13883d076aca5ad9e335f487c71d9c79b0eb0d2c66b2ec87 485fe325821cfdd98d42d4e77cf920b7a17e22fc56b272c33878e062481f5bd 1b5b38c092074987a6430b2386c87d963e6ada86b63bb26cb7fa5fb0c424bd7 4514f036e0b31638

2.3.2 Certificats cachet serveur

Champ	Description
Version	2 (=version 3)
Serial number	Défini par l'outil
Issuer	Voir ci-dessus
NotBefore	AAAA/MM/JJ HH:MM:SS Z (date d'émission du certificat)
NotAfter	AAAA/MM/JJ HH:MM:SS Z (3 ans après la date d'émission du certificat)
Subject	Voir [PC_CHT]
Subject Public Key Info	(rsaEncryption) 1.2.840.113549.1.1.1 (secp384r1) 1.3.132.0.34
Key size	2048 et 3072 ou P-384
Signature (algorithm & OID)	SHA256WithRsaEncryption Ou ECDSA_P-384
Authority Key Identifier	Identification de la clé publique de l'A.C. émettrice
Subject Key Identifier	Identification de la clé publique du porteur

Champ	Description
Key Usage	digitalSignature
Certificate Policies (critical)	
policyIdentifier	1.3.6.1.4.1.40559.1.0.1.31.210.1.1
policyQualifier-cps	http://www.dossiers-securite.bpce.fr/
X509v3	
Basic Constraint (critical)	CA:False
Extended Key usage	1.2.840.113583.1.1.5 (Adobe CDS AuthenticDocumentsTrust)
CRL Distribution Points	
distributionPoint	URI http://pro.d00.pki02.bpce.fr/bpcesealtime01ca.crl
	URI http://pro.d01.pki02.bpce.fr/bpcesealtime01ca.crl
	URI http://pro.d02.pki02.bpce.fr/bpcesealtime01ca.crl
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.2 (Autorité de certification émettrice)
Alternative Name	http://pro.d00.pki02.bpce.fr/BPCESEALTIME01.crt

2.3.3 Certificats horodatage

Champ	Description
Version	2 (=version 3)
Serial number	Défini par l'outil
Issuer	Voir ci-dessus
NotBefore	AAAA/MM/JJ HH:MM:SS Z (date d'émission du certificat)
NotAfter	AAAA/MM/JJ HH:MM:SS Z (4 ans après la date d'émission du certificat)
Subject	Voir [PC_CHT]
Subject Public Key Info	(rsaEncryption) 1.2.840.113549.1.1.1 (secp384r1) 1.3.132.0.34
Key size	2048 et 3072 ou P-384
Signature (algorithm & OID)	SHA256WithRsaEncryption Ou ECDSA_P-384
Authority Key Identifier	Identification de la clé publique de l'A.C. émettrice
Subject Key Identifier	Identification de la clé publique du porteur
Key Usage (critical)	digitalSignature
Certificate Policies (critical)	
policyIdentifier	1.3.6.1.4.1.40559.1.0.1.31.211.1.1
policyQualifier-cps	http://www.dossiers-securite.bpce.fr/

Champ	Description
X509v3	
Basic Constraint (critical)	CA:False
Extended Key usage	1.3.6.1.5.5.7.3.8 (id-kp-timeStamping)
CRL Distribution Points	
distributionPoint	URI http://pro.d00.pki02.bpce.fr/bpcesealtime01ca.crl
	URI http://pro.d01.pki02.bpce.fr/bpcesealtime01ca.crl
	URI http://pro.d02.pki02.bpce.fr/bpcesealtime01ca.crl
Authority Information Access	
Access Method	1.3.6.1.5.5.7.48.2 (Autorité de certification émettrice)
Alternative Name	http://pro.d00.pki02.bpce.fr/BPCESEALTIME01.crt

3 RÉFÉRENCES

- [MCOM] *Mesures communes*, publié à l'adresse www.dossiers-securite.bpce.fr
- [PC_SIG] *Politique et pratiques de certification – Signature Electronique*, publiée à l'adresse www.dossiers-securite.bpce.fr
- [PC_CHT] *Politique et pratiques de certification – Cachet Serveur & Horodatage*, publiée à l'adresse www.dossiers-securite.bpce.fr
- [USSE] *Utilisateur du Service de Signature Electronique*