公的個人認証サービス

プロファイル仕様書

3.0 版

令和 5 年 3 月 31 日

② 個人番号カード用署名用電子証明書のプロファイル拡張領域（Extension）

項目	項目の意味	データ型	設定値	説明･備考
Extensions				
authorityKeyIdentifier	電子証明書発行者の公開鍵に関する情報	-	-	
extnID		OBJECT IDENTIFIER	2 5 29 35（固定）	「authorityKeyIdentifier」の OID
critical		BOOLEAN	FALSE（固定）	
extnValue		OCTET STRING	-	
authorityKeyIdentifier		-	-	
[0]keyIdentifier		OCTET STRING	（公開鍵の識別子（16進数））	
[1]authorityCertIssuer		-	-	
[4]directoryName		-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6（固定）	「countryName」の OID
value		PrintableString	JP（固定）	「日本国」の意味
organizationName		-	-	
type		OBJECT IDENTIFIER	2 5 4 10（固定）	「organizationName」の OID
value		UTF8String	JPKI（固定）	「公的個人認証サービス」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11（固定）	「organizationalUnitName」の OID
value		UTF8String	JPKI for digital signature（固定）	「公的個人認証サービス署名用認証局」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11（固定）	「organizationalUnitName」の OID

項目	項目の意味	データ型	設定値	説明･備考
value		UTF8String	Japan Agency for Local Authority Information Systems (固定)	「地方公共団体情報システム機構」の意味
[2]authorityCertSerialNumber		INTEGER	(公開鍵のシリアル番号 (16 進数))	認証局の公開鍵を一意に識別するための正の値
keyUsage	鍵の使用目的			
extnID		OBJECT IDENTIFIER	2 5 29 15 (固定)	「keyUsage」の OID
critical		BOOLEAN	TRUE (固定)	
extnValue		OCTET STRING	-	
keyUsage		BIT STRING	110000000 (固定)	鍵用途を示すビット列 「digitalSignature(0) & nonRepudiation(1)」の意味
subjectAltName	利用者日本語表記	-	-	
extnID		OBJECT IDENTIFIER	2 5 29 17 (固定)	「subjectAltName」の OID
critical		BOOLEAN	FALSE (固定)	
extnValue		OCTET STRING	-	
[0]otherName	氏名	-	-	
commonName		-	-	
type		OBJECT IDENTIFIER	1 2 392 200149 8 5 5 1 (固定)	「commonName」の OID (独自)
[0]value		UTF8String	(氏名 　姓名、姓名 (通称) 、姓 [旧氏] 名)	JIS 第 1 水準、第 2 水準、補助漢字以外の文字は代替文字に変換 通称ならびに旧氏は当該住民に係る住民票の記載にしたがってセパレート文字と共に氏名に追加･変更される。 最大文字数 100 文字 (セパレート文字を含む)
[0]otherName	生年月日	-	-	
dateOfBirth		-	-	
type		OBJECT IDENTIFIER	1 2 392 200149 8 5 5 4 (固定)	「dateOfBirth」の OID (独自)

項目	項目の意味	データ型	設定値	説明･備考
[0]value		UTF8String	(生年月日 EYYYYMMDD)	設定値を和暦に変換して表示 E (年号コード) 1:明治、2:大正、3:昭和、4:平成、5:令和、0:不明 YYYY (西暦年) MM (月) A1:春、A2:夏、A3:秋、A4:冬、00:不明 DD (日) A1:上旬、A2:中旬、A3:下旬、00:不明
[0]otherName	性別	-	-	
gender		-	-	
type		OBJECT IDENTIFIER	1 2 392 200149 8 5 5 3 (固定)	「gender」の OID (独自)
[0]value		UTF8String	(性別 1:男、2:女、3:不明)	
[0]otherName	住所	-	-	
address		-	-	
type		OBJECT IDENTIFIER	1 2 392 200149 8 5 5 5 (固定)	「address」の OID (独自)
[0]value		UTF8String	(住所)	JIS 第 1 水準、第 2 水準、補助漢字以外の文字は代替文字に変換 全角ハイフン設定可能 最大文字数 200 文字
[0]otherName	利用者の氏名代替文字の使用位置情報	-	-	
substituteCharacterOfCommonName		-	-	
type		OBJECT IDENTIFIER	1 2 392 200149 8 5 5 2 (固定)	「substituteCharacterOfCommonName」の OID (独自)
[0]value		UTF8String	(代替文字使用位置を示す数字の文字列)	0 代替文字でない 1 代替文字
[0]otherName	利用者の住所代替文字の使用位置情報	-	-	
substituteCharacterOfAddress		-	-	
type		OBJECT IDENTIFIER	1 2 392 200149 8 5 5 6 (固定)	「substituteCharacterOfAddress」の OID (独自)

項目	項目の意味	データ型	設定値	説明･備考
[0]value		UTF8String	(代替文字使用位置を示す数字の文字列)	0 代替文字でない 1 代替文字
issuerAltName	発行者の日本語表記	-	-	
extnID		OBJECT IDENTIFIER	2 5 29 18 (固定)	「issuerAltName」の OID
critical		BOOLEAN	FALSE (固定)	
extnValue		OCTET STRING	-	
[4]directoryName		-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6 (固定)	「countryName」の OID
value		PrintableString	JP (固定)	「日本国」の意味
organizationName		-	-	
type		OBJECT IDENTIFIER	2 5 4 10 (固定)	「organizationName」の OID
value		UTF8String	公的個人認証サービス (固定)	
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
value		UTF8String	公的個人認証サービス署名用 (固定)	
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
value		UTF8String	地方公共団体情報システム機構 (固定)	
cRLDistributionPoints	CRL 配布点に関する情報	-	-	
extnID		OBJECT IDENTIFIER	2 5 29 31 (固定)	「cRLDistributionPoints」の OID
critical		BOOLEAN	FALSE (固定)	
extnValue		OCTET STRING	-	
[0]distributionPoint		-	-	
[0]fullName		-	-	

項目	項目の意味	データ型	設定値	説明･備考
[4]directoryName		-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6 (固定)	「countryName」の OID
value		PrintableString	JP (固定)	「日本国」の意味
organizationName		-	-	
type		OBJECT IDENTIFIER	2 5 4 10 (固定)	「organizationName」の OID
value		UTF8String	JPKI (固定)	「公的個人認証サービス」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
value		UTF8String	JPKI for digital signature (固定)	「公的個人認証サービス署名用認証局」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
value		UTF8String	CRL Distribution Points (固定)	
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
value		UTF8String	都道府県名 (ローマ字)	
commonName		-	-	
type		OBJECT IDENTIFIER	2 5 4 3 (固定)	「commonName」の OID
value		UTF8String	市区町村名 (ローマ字) CRLDP	
certificatePolicies	証明書ポリシ	-	-	

項目	項目の意味	データ型	設定値	説明･備考
extnID		OBJECT IDENTIFIER	2 5 29 32 (固定)	「certificatePolicies」の OID
critical		BOOLEAN	TRUE (固定)	
extnValue		OCTET STRING	-	
policyIdentifier		OBJECT IDENTIFIER	1 2 392 200149 8 5 1 1 20	公的個人認証サービスの個人番号カード用署名用電子証明書ポリシの OID
policyQualifiers		-	-	
policyQualifierId		OBJECT IDENTIFIER	1 3 6 1 5 5 7 2 1 (id-qt-cps)	「CPS」の OID
pqualifier		IA5String	http://www.jpki.go.jp/cps.html	CPS を掲載する URL
subjectKeyIdentifier	電子証明書利用者の公開鍵の識別子	-	-	
extnID		OBJECT IDENTIFIER	2 5 29 14 (固定)	「subjectKeyIdentifier」の OID
critical		BOOLEAN	FALSE (固定)	
extnValue		OCTET STRING	-	
subjectKeyIdentifier		-	-	
keyIdentifier		OCTET STRING	(公開鍵のハッシュ値 (16 進数))	ハッシュ関数は sha-1 を使用