Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

DIRECCIÓN DE SERVICIOS DIGITALES E INNOVACIÓN
DEPARTAMENTO CERES

DOCUMENTO DE PERFILES DE LA AC SERVIDORES SEGUROS
TIPO 1

Referencia:

Documento clasificado como: *Público*

Contenido

1. PERFILES

1.1. AC RAIZ FNMT-RCM SERVIDORES SEGUROS

Campo		Contenido	Ext. Critica
1. Version		2	
2. Serial Number		Número identificativo único del certificado.	
3. Signature Algorithm		ecdsa-with-SHA384 Claves: ECC P-384 bits	
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Raíz)	
	4.1. Country	C=ES	
	4.2 Organization	O=FNMT-RCM	
	4.3 Organization Unit	OU=Ceres	
	4.4 OrganizationIddentifier	VATES- Q2826004J	
	4.5 CommonName	cn=AC RAIZ FNMT-RCM SERVIDORES SEGUROS	
5. Validity		25 años	
6. Subject			
	6.1. Country	C=ES	
	6.2. Organization	O=FNMT-RCM	
	6.3. Organization Unit	OU=Ceres	
	6.4. OrganizationIddentifier	VATES- Q2826004J	
	6.5. CommonName	cn=AC RAIZ FNMT-RCM SERVIDORES SEGUROS	
7. Subject Public Key Info		ECC P-384 bits	
8. Subject Key Identifier		Identificador de la clave pública de la CA. Medio para identificar certificados que contienen una clave pública particular y facilita la construcción de rutas de certificación.	
9. Key Usage		Uso permitido de las claves certificadas.	Sí
	9.1. Digital Signature	0	
	9.2. Content Commitment	0	
	9.3. Key Encipherment	0	
	9.4. Data Encipherment	0	

Campo		Contenido	Ext. Critica
	9.5. Key Agreement	0	
	9.6. Key Certificate Signature	1	
	9.7. CRL Signature	1	
10. Basic Constraints			Sí
	10.1. cA	Valor TRUE (CA)	
	10.2. pathLenConstraint	Ninguna	

1.2. AC SERVIDORES SEGUROS TIPO1 (EV)

Campo		Contenido	Obligatoriedad
1. Version		2	Sí
2. Serial Number		Número identificativo único del certificado.	Sí
3. Signature Algorithm		SHA384withECDSA Claves: ECC P-384 bits	Sí
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Raíz)	Sí
	4.1. Country	C=ES	Sí
	4.2. Organization	O=FNMT-RCM	Sí
	4.3. Organization Unit	OU=Ceres	Sí
	4.4. OrganizationIdentifier	VATES- Q2826004J	Sí
	4.5. CommonName	cn=AC RAIZ FNMT-RCM SERVIDORES SEGUROS	Sí
5. Validity		15 años	Sí
6. Subject		Entidad emisora del certificado (CA Subordinada)	Sí
	6.1. Country	C=ES	Sí
	6.2. Organization	O=FNMT-RCM.	Sí
	6.3. Organizational Unit	OU=Ceres	Sí
	6.4. OrganizationIdentifier	VATES- Q2826004J	Sí
	6.5. Common Name	cn=AC SERVIDORES SEGUROS TIPO1	Sí
7. Authority Key Identifier		Identificador de la clave pública de la entidad raíz. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de esta CA Subordinada	Sí
8. Subject Public Key Info		ECC P-384 bits	Sí
9. Subject Key Identifier		Identificador de la clave pública de la CA de Componentes.	Sí
10. Key Usage		Uso permitido de las claves del certificado.	Sí
	10.1. Digital Signature	0	Sí
	10.2. Content Commitment	0	Sí

Campo		Contenido	Obligatoriedad
	10.3. Key Encipherment	0	Sí
	10.4. Data Encipherment	0	Sí
	10.5. Key Agreement	0	Sí
	10.6. Key Certificate Signature	1	Sí
	10.7. CRL Signature	1	Sí
11. Certificate Policies		Política de certificación	Sí
	11.1. Policy Identifier	2.5.29.32.0 (anyPolicy)	Sí
12. CRL Distribution Point			Sí
	12.1. Distribution Point 1	Punto de distribución 1 de la CRL http://www.cert.fnmt.es/crls/ARLSERVIDORESSEGUROS.crl	Sí
13. Basic Constraints			
	13.1. Subject Type	CA	
	13.2. Path Length	0	
14. Authority Info Access			Sí
	14.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	
	14.2. Acces Location 1	http://ocspfnmtssr.cert.fnmt.es/ocspssr/OcspResponder	
	Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	
	Access Location 2	http://www.cert.fnmt.es/certs/ACRAIZSERVIDORESSEGUROS.crt	

1.3. CERTIFICADOS DE AUTENTICACIÓN DE SITIOS WEB

1.3.1. Certificado EV

Campo		Contenido	Obligatoriedad
1. Version		2	Sí
2. Serial Number		Número identificativo único del certificado.	Sí
3. Signature Algorithm		SHA384withECDSA Claves: ECC P-384 bits	Sí
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí
	4.1. Country	C=ES	Sí
	4.2. Organization	O=FNMT-RCM.	Sí
	4.3. organizationalUnit	OU=Ceres	Sí
	4.4. OrganizationIdentifier	VATES- Q2826004J	Sí
	4.5. Common Name	cn=AC SERVIDORES SEGUROS TIPO1	Sí
5. Validity		1 año	Sí
6. Subject		Identificación/descripción del responsable de las claves certificadas	Sí
	6.1. Country	C=ES	Sí
	6.2. stateOrProvinceName	Nombre del estado o Provincia	Sí
	6.3. LocalityName	Nombre de la localidad del suscriptor	Sí
	6.4. Organization	Denominación del suscriptor	Sí
	6.5. SerialNumber	NIF del suscriptor	Sí
	6.6. BusinessCategory (OID 2.5.4.15)	Los valores de este campo deberán ser uno de los siguientes literales: "Private Organization", "Government Entity", "Business Entity" o "Non-Commercial Entity"	Sí
	6.7. jurisdictionCountryName	jurisdictionCountryName=ES	Sí
7. Authority Key Identifier		Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente.	Sí

Campo			Contenido	Obligatoriedad
8. Subject Public Key Info			ECC P-384 bits	Sí
9. Subject Key Identifier			Identificador de la clave pública del componente.	Sí
10. Key Usage			Uso permitido de las claves certificadas.	Sí
	10.1. Digital Signature		1	
	10.2. Content Commitment		0	
	10.3. Key Encipherment		0	
	10.4. Data Encipherment		0	
	10.5. Key Agreement		0	
	10.6. Key Certificate Signature		0	
	10.7. CRL Signature		0	
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí
	11.1. Server Authentication		1.3.6.1.5.5.7.3.1	Sí
	11.2. Client Authentication		1.3.6.1.5.5.7.3.2	Si
12. Qualified Certificate Statements			Extensiones cualificadas.	Sí
	12.1. QcCompliance. (0.4.0.1862.1.1)		Certificado cualificado	Sí
	12.2. QcEuRetentionPeriod (0.4.0.1862.1.3)		15 años	Sí
	12.3. id-qcspkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)		semanticsId-Legal (0.4.0.194121.1.2)	No
	12.4. QcType (0.4.0.1862.1.6)		qct-web (0.4.0.1862.1.6.3)	Sí
	12.5. QcPDS (0.4.0.1862.1.5)		{https://www.cert.fnmt.es/pds/PDS_SS1_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_SS1_en.pdf, en}	Sí
13. Certificate Policies			Política de certificación	Sí
	13.1. Policy Identifier		ev-guidelines (2.23.140.1.1)	Sí
	13.2. Policy Identifier		evcp (0.4.0.2042.1.4)	Sí
	13.3. Policy Identifier		QCP-w (0.4.0.194112.1.4)	Sí
	13.4. Policy Identifier		1.3.6.1.4.1.5734.3.16.1.2	Sí
	13.4.1 Policy Qualifier Id			Sí
		13.4.1.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí

Campo		Contenido	Obligatoriedad
14. SignedCertificateTimestampList (SCT)			
	14.1. signed_certificate_timestamp (OID 1.3.6.1.4.1.11129.2.4.2)	SCT (Octet String) obtenidos al publicar en un log el pre-certificado. Se obtendrá un SCT por cada log en el que se publique este certificado.	Sí
15. Subject Alternative Names			Sí
	15.1. DNSName	Nombre de dominio	Sí
16. CRL Distribution Point		Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí
	16.1. Distribution Point 1	Punto de publicación de la CRL1. http://www.cert.fnmt.es/crlsservseguros/CRLT1.crl	Sí
17. Authority Info Access			Sí
	17.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí
	17.2. Acces Location 1	http://ocspfnmtss1.cert.fnmt.es/ocspss1/OcspResponder	Sí
	17.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí
	17.4. Access Location 2	http://www.cert.fnmt.es/certs/ACSS1.crt	Sí
18. Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí
	18.1. Subject Type	Valor FALSE (entidad final)	

1.3.2. Certificado SAN EV

Campo		Contenido	Obligatoriedad
1. Version		2	Sí
2. Serial Number		Número identificativo único del certificado.	Sí
3. Signature Algorithm		SHA384withECDSA Claves: ECC P-384 bits	Sí
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí
	4.1. Country	C=ES	Sí
	4.2. Organization	O=FNMT-RCM.	Sí
	4.3. organizationalUnit	OU=Ceres	Sí
	4.4. OrganizationIdentifier	VATES- Q2826004J	Sí
	4.5. Common Name	cn=AC SERVIDORES SEGUROS TIPO1	Sí
5. Validity		1 año	Sí
6. Subject		Identificación/descripción del responsable de las claves certificadas	Sí
	6.1. Country	C=ES	Sí
	6.2. stateOrProvinceName	Nombre del estado o Provincia	Sí
	6.3. LocalityName	Nombre de la localidad del suscriptor	Sí
	6.4. Organization	Denominación del suscriptor	Sí
	6.5. SerialNumber	NIF del suscriptor	Sí
	6.6. BusinessCategory (OID 2.5.4.15)	Los valores de este campo deberán ser uno de los siguientes literales: "Private Organization", "Government Entity", "Business Entity" o "Non-Commercial Entity"	Sí
	6.7. jurisdictionCountryName	jurisdictionCountryName=ES	Sí
7. Authority Key Identifier		Identificador de la clave pública de la CA de Componentes. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar el certificado de componente.	Sí
8. Subject Public Key Info		ECC P-384 bits	Sí

Campo			Contenido	Obligatoriedad
9. Subject Key Identifier			Identificador de la clave pública del componente.	Sí
10. Key Usage			Uso permitido de las claves certificadas.	Sí
	10.1. Digital Signature		1	
	10.2. Content Commitment		0	
	10.3. Key Encipherment		0	
	10.4. Data Encipherment		0	
	10.5. Key Agreement		0	
	10.6. Key Certificate Signature		0	
	10.7. CRL Signature		0	
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí
	11.1. Server Authentication		1.3.6.1.5.5.7.3.1	Sí
	11.2. Client Authentication		1.3.6.1.5.5.7.3.2	Si
12. Qualified Certificate Statements			Extensiones cualificadas.	Sí
	12.1. QcCompliance. (0.4.0.1862.1.1)		Certificado cualificado	Sí
	12.2. QcEuRetentionPeriod (0.4.0.1862.1.3)		15 años	Sí
	12.3. id-qcspkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)		semanticsId-Legal (0.4.0.194121.1.2)	No
	12.4. QcType (0.4.0.1862.1.6)		qct-web (0.4.0.1862.1.6.3)	Sí
	12.5. QcPDS (0.4.0.1862.1.5)		{https://www.cert.fnmt.es/pds/PDS_SS1_es.pdf, es},{https://www.cert.fnmt.es/pds/PDS_SS1_en.pdf, en}	Sí
13. Certificate Policies			Política de certificación	Sí
	13.1. Policy Identifier		ev-guidelines (2.23.140.1.1)	Sí
	13.2. Policy Identifier		evcp (0.4.0.2042.1.4)	
	13.3. Policy Identifier		QCP-w (0.4.0.194112.1.4)	Sí
	13.4. Policy Identifier		1.3.6.1.4.1.5734.3.16.1.3	Sí
	13.4.1 Policy Qualifier Id			Sí
		13.4.1.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí

Campo		Contenido	Obligatoriedad
14. SignedCertificateTimestampList (SCT)			
	14.1. signed_certificate_timestamp (OID 1.3.6.1.4.1.11129.2.4.2)	SCT (Octet String) obtenidos al publicar en un log el pre-certificado. Se obtendrá un SCT por cada log en el que se publique este certificado.	Sí
15. Subject Alternative Names			Sí
	15.1. DNSName	Id Campo / Valor: NombreDNS = Dominio_1	Sí
	15.2. DNSName	Id Campo / Valor: NombreDNS = Dominio_2	Sí
	15.3. DNSName	Id Campo / Valor: NombreDNS = Dominio_n	Sí
16. CRL Distribution Point		Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí
	16.1. Distribution Point 1	Punto de publicación de la CRL. http://www.cert.fnmt.es/crlsservseguros/CRLT1.crl	Sí
17. Authority Info Access			Sí
	17.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí
	17.2. Acces Location 1	http://ocspfnmtss1.cert.fnmt.es/ocspss1/OcspResponder	Sí
	17.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí
	17.4. Access Location 2	http://www.cert.fnmt.es/certs/ACSS1.crt	Sí
18. Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí
	18.1. Subject Type	Valor FALSE (entidad final)	

1.3.3. Certificado de Sede Electrónica EV

Campo		Contenido	Obligatoriedad
1. Version		2	Sí
2. Serial Number		Número identificativo único del certificado. Este número se asigna de forma aleatoria.	Sí
3. Signature Algorithm		SHA384withECDSA Claves: ECC P-384 bits.	Sí
4. Issuer Distinguish Name		Entidad emisora del certificado (CA Subordinada)	Sí
	4.1. Country	C=ES	Sí
	4.2. Organization	O=FNMT-RCM.	Sí
	4.3. Organizational Unit	OU=Ceres	Sí
	4.4. OrganizationIdentifier	VATES- Q2826004J	Sí
	4.5. Common Name	cn=AC SERVIDORES SEGUROS TIPO1	Sí
5. Validity		1 año	Sí
6. Subject		Identificación/descripción del responsable de las claves certificadas	Sí
	6.1. Country	C=ES	Sí
	6.2. stateOrProvinceName	Nombre del estado o Provincia	Sí
	6.2. LocalityName	Nombre de la localidad del suscriptor (organización)	Sí
	6.3. Organization	Denominación (nombre “oficial” de la organización) del suscriptor de servicios de certificación	Sí
	6.4. SerialNumber	NIF del suscriptor	Sí
	6.5. BusinessCategory (OID 2.5.4.15)	businessCategory=Government Entity	Sí
	6.6. jurisdictionCountryName	jurisdictionCountryName=ES	Sí
7. Authority Key Identifier		Identificador de la clave pública del PSC. Medio para identificar la clave pública correspondiente a la clave privada utilizada por la CA para firmar un certificado.	Sí
8. Subject Public Key Info		ECC P-384 bits	Sí
9. Subject Key Identifier		Identificador de la clave pública de la sede.	Sí
10. Key Usage		Uso permitido de las claves certificadas.	Sí

Campo			Contenido	Obligatoriedad
	10.1. Digital Signature		1	
	10.2. Content Commitment		0	
	10.3. Key Encipherment		0	
	10.4. Data Encipherment		0	
	10.5. Key Agreement		0	
	10.6. Key Certificate Signature		0	
	10.7. CRL Signature		0	
11. Extended Key Usage			Uso mejorado o extendido de las claves	Sí
	11.1. Server Authentication		1.3.6.1.5.5.7.3.1	Sí
	11.2. Client Authentication		1.3.6.1.5.5.7.3.2	Si
12. Qualified Certificate Statements			Extensiones cualificadas.	Sí
	12.1. QcCompliance (0.4.0.1862.1.1)		Certificado cualificado	Sí
	12.2. QcEuRetentionPeriod (0.4.0.1862.1.3)		15 años	Sí
	12.3. id-qcspkixQCSyntax-v2 (1.3.6.1.5.5.7.11.2)		semanticsId-Legal (0.4.0.194121.1.2)	No
	12.4. QcType(0.4.0.1862.1.6)		qct-web (0.4.0.1862.1.6.3)	
	12.5. QcPDS (0.4.0.1862.1.5)		{https://www.cert.fnmt.es/pds/PDS_SS1_es.pdf, es}, {https://www.cert.fnmt.es/pds/PDS_SS1_en.pdf, en}	
13. Certificate Policies			Política de certificación	Sí
	13.1. Policy Identifier		ev-guidelines (2.23.140.1.1)	Sí
	13.2. Policy Identifier		evcp (0.4.0.2042.1.4)	Sí
	13.3. Policy Identifier		QCP-w (0.4.0.194112.1.4)	Sí
	13.4. Policy Identifier		2.16.724.1.3.5.5.2	Sí
	13.5. Policy Identifier		1.3.6.1.4.1.5734.3.16.1.1	Sí
	13.5.1 Policy Qualifier Id			Sí
		13.5.1.1 CPS Pointer	http://www.cert.fnmt.es/dpcs/	Sí
14. SignedCertificateTimestampList (SCT)				

Campo		Contenido	Obligatoriedad
	14.1. signed_certificate_timestamp (OID 1.3.6.1.4.1.11129.2.4.2)	SCT (Octet String) obtenidos al publicar en un log el pre-certificado. Se obtendrá un SCT por cada log en el que se publique este certificado.	Sí
15. Subject Alternative Names		Identificación/ descripción de Identidad Administrativa	Sí
	15.1. DNS Name	Nombre de Dominio (DNS) de la Sede	Sí
16. CRL Distribution Point		Informa acerca de cómo se obtiene la información de la CRL asociada al certificado.	Sí
	16.1. Distribution Point 1	Punto de publicación de la CRL. http://www.cert.fnmt.es/crlsservseguros/CRLT1.crl	Sí
17. Authority Info Access			Sí
	17.1. Access Method 1	Identificador de método de acceso a la información de revocación: 1.3.6.1.5.5.7.48.1 (ocsp)	Sí
	17.2. Acces Location 1	http://ocspfnmtss1.cert.fnmt.es/ocspss1/OcspResponder	Sí
	17.3. Access Method 2	Identificador de método de acceso a la información de certificados adicionales necesarios para la validación: 1.3.6.1.5.5.7.48.2 (ca cert)	Sí
	17.4. Access Location 2	http://www.cert.fnmt.es/certs/ACSS1.crt	Sí
18. Basic Contraints		Esta extensión sirve para identificar si el sujeto de certificación es una CA así como el máximo nivel de "profundidad" permitido para las cadenas de certificación".	Sí
	18.1. Subject Type	Entidad final (valor FALSE)	