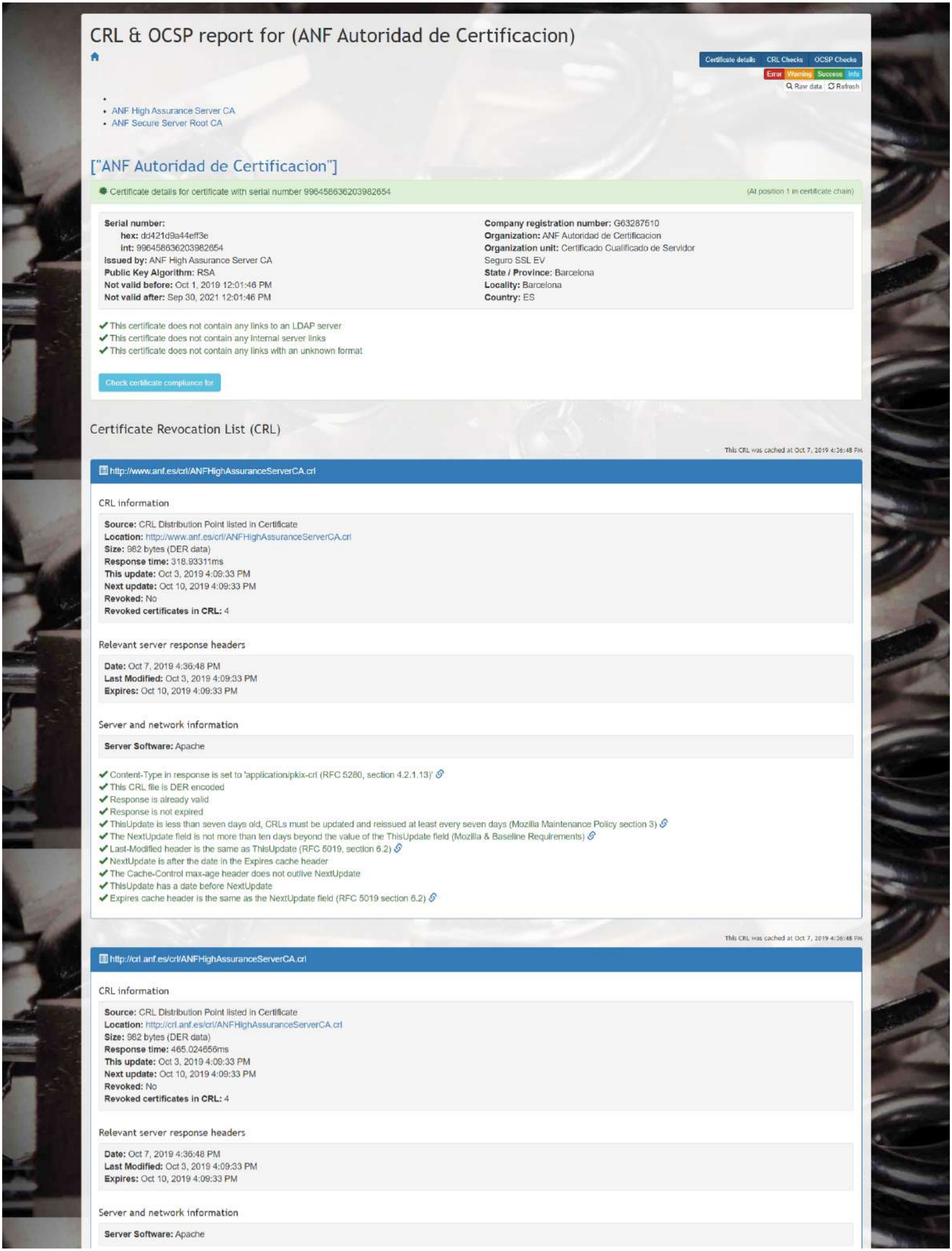


CRL & OCSP report for (ANF Autoridad de Certificacion)

-
- ANF High Assurance Server CA
- ANF Secure Server Root CA

["ANF Autoridad de Certificacion"]

Certificate details for certificate with serial number 996458636203982654 (At position 1 in certificate chain)

Serial number:
hex: dd421d9a44eff3e
int: 996458636203982654
Issued by: ANF High Assurance Server CA
Public Key Algorithm: RSA
Not valid before: Oct 1, 2019 12:01:46 PM
Not valid after: Sep 30, 2021 12:01:46 PM

Company registration number: G63287510
Organization: ANF Autoridad de Certificacion
Organization unit: Certificado Cualificado de Servidor Seguro SSL EV
State / Province: Barcelona
Locality: Barcelona
Country: ES

✓ This certificate does not contain any links to an LDAP server
✓ This certificate does not contain any internal server links
✓ This certificate does not contain any links with an unknown format

Certificate Revocation List (CRL)

This CRL was cached at Oct 7, 2019 4:36:48 PM

http://www.anf.es/crl/ANFHighAssuranceServerCA.crl

CRL information

Source: CRL Distribution Point listed in Certificate
Location: http://www.anf.es/crl/ANFHighAssuranceServerCA.crl
Size: 982 bytes (DER data)
Response time: 318.93311ms
This update: Oct 3, 2019 4:09:33 PM
Next update: Oct 10, 2019 4:09:33 PM
Revoked: No
Revoked certificates in CRL: 4

Relevant server response headers

Date: Oct 7, 2019 4:36:48 PM
Last Modified: Oct 3, 2019 4:09:33 PM
Expires: Oct 10, 2019 4:09:33 PM

Server and network information

Server Software: Apache

✓ Content-Type in response is set to 'application/pkix-crl (RFC 5280, section 4.2.1.13)'
✓ This CRL file is DER encoded
✓ Response is already valid
✓ Response is not expired
✓ ThisUpdate is less than seven days old, CRLs must be updated and reissued at least every seven days (Mozilla Maintenance Policy section 3)
✓ The NextUpdate field is not more than ten days beyond the value of the ThisUpdate field (Mozilla & Baseline Requirements)
✓ Last-Modified header is the same as ThisUpdate (RFC 5019, section 6.2)
✓ NextUpdate is after the date in the Expires cache header
✓ The Cache-Control max-age header does not outlive NextUpdate
✓ ThisUpdate has a date before NextUpdate
✓ Expires cache header is the same as the NextUpdate field (RFC 5019 section 6.2)

This CRL was cached at Oct 7, 2019 4:36:48 PM

http://crl.anf.es/crl/ANFHighAssuranceServerCA.crl

CRL information

Source: CRL Distribution Point listed in Certificate
Location: http://crl.anf.es/crl/ANFHighAssuranceServerCA.crl
Size: 982 bytes (DER data)
Response time: 465.024656ms
This update: Oct 3, 2019 4:09:33 PM
Next update: Oct 10, 2019 4:09:33 PM
Revoked: No
Revoked certificates in CRL: 4

Relevant server response headers

Date: Oct 7, 2019 4:36:48 PM
Last Modified: Oct 3, 2019 4:09:33 PM
Expires: Oct 10, 2019 4:09:33 PM

Server and network information

Server Software: Apache

✓ Content-Type in response is set to 'application/pkix-crl (RFC 5280, section 4.2.1.13)' 🔗
✓ This CRL file is DER encoded
✓ Response is already valid
✓ Response is not expired
✓ ThisUpdate is less than seven days old, CRLs must be updated and reissued at least every seven days (Mozilla Maintenance Policy section 3) 🔗
✓ The NextUpdate field is not more than ten days beyond the value of the ThisUpdate field (Mozilla & Baseline Requirements) 🔗
✓ Last-Modified header is the same as ThisUpdate (RFC 5019, section 6.2) 🔗
✓ NextUpdate is after the date in the Expires cache header
✓ The Cache-Control max-age header does not outlive NextUpdate
✓ ThisUpdate has a date before NextUpdate
✓ Expires cache header is the same as the NextUpdate field (RFC 5019 section 6.2) 🔗

Online Certificate Status Protocol (OCSP)

This OCSP response was cached at Oct 7, 2019 4:36:48 PM

http://ocsp.anf.es/spain/AV (GET)

OCSP response information

Source: OCSP server listed in Certificate
Location: http://ocsp.anf.es/spain/AV
Size: 2476 bytes (DER)
Response time: 315.486495ms
Signature algorithm: SHA256-RSA
Signature type: CA Delegated
Signed by: ANF High Assurance Server CA Responder 1293
Issued by: ANF High Assurance Server CA
Signing certificate validity: Sep 5, 2019 6:37:08 PM - Jul 1, 2020 6:37:08 PM
Signing certificate algorithm: SHA256-RSA
Reported statuses: 1
This update: Oct 7, 2019 4:36:48 PM
Next update: Oct 14, 2019 4:36:48 PM
Produced at: Oct 7, 2019 4:36:48 PM
Server status: Success
Status: Good

Relevant server response headers

Date: Oct 7, 2019 4:36:48 PM
Last Modified: Oct 7, 2019 4:36:48 PM
Expires: Oct 14, 2019 4:36:48 PM

✓ OCSP requests is smaller than 255 bytes 🔗
✓ OCSP signing certificate is already valid
✓ OCSP signing certificate is not expired
✓ OCSP signing certificate does not expire before NextUpdate
✓ OCSP signing certificate does contain the Extended Key Usage for OCSP Signing
✓ OCSP signing certificate does contain the OCSP No Check extension
✓ Content-Type in response is set to 'application/ocsp-response'
✓ Response is already valid
✓ Response is not expired
✓ ThisUpdate is less than four days old, OCSP information must be updated at least every four days (Mozilla & Baseline Requirements) 🔗
✓ The NextUpdate field is not more than ten days beyond the value of the ThisUpdate field (Mozilla & Baseline Requirements) 🔗
✓ Last-Modified header is the same as ThisUpdate (RFC 5019, section 6.2) 🔗
✓ NextUpdate is after the date in the Expires cache header
✓ The Cache-Control max-age header does not outlive NextUpdate
✓ ThisUpdate has a date before NextUpdate
✓ Expires cache header is the same as the NextUpdate field (RFC 5019 section 6.2) 🔗

This OCSP response was cached at Oct 7, 2019 4:36:48 PM

http://ocsp.anf.es/spain/AV (POST)

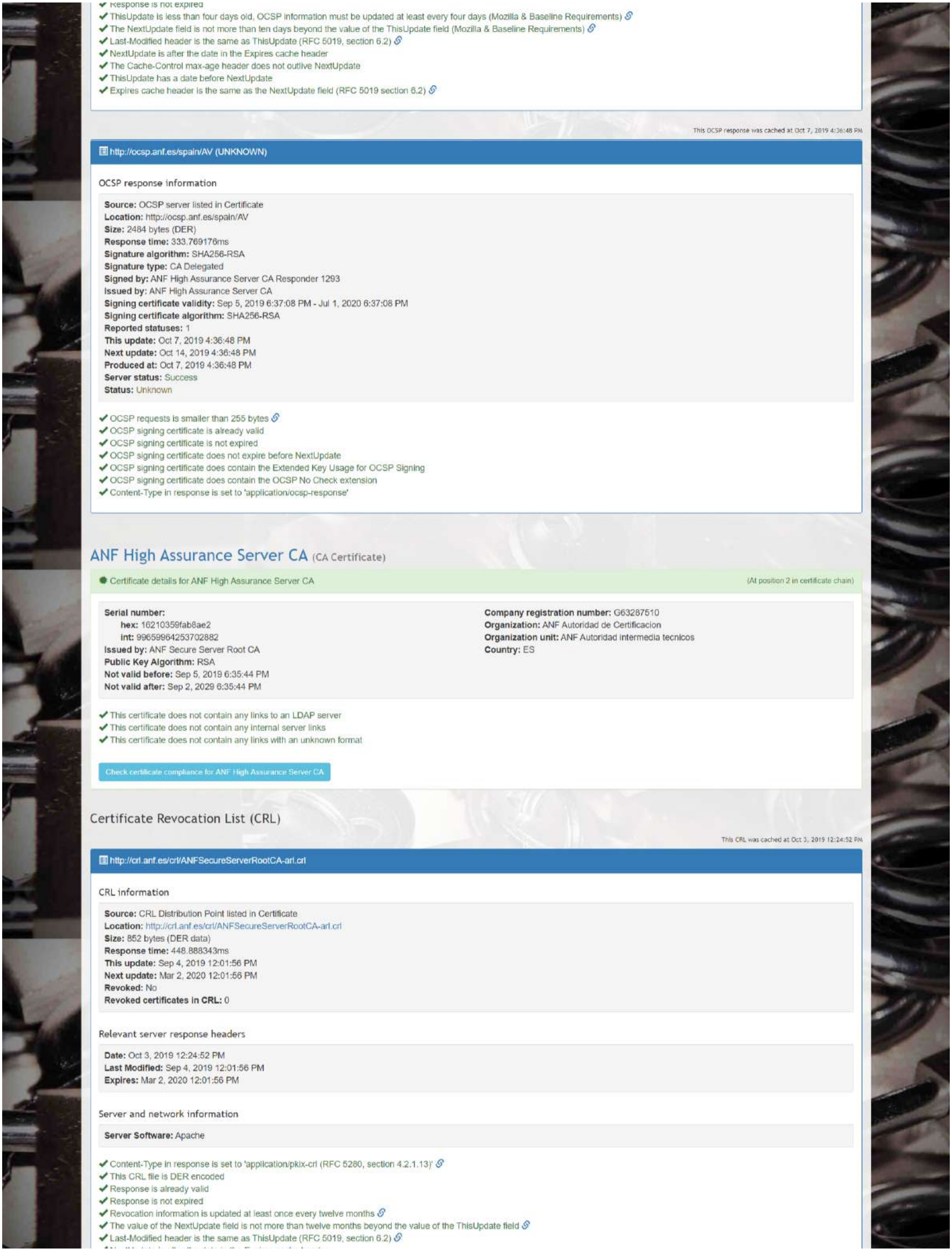
OCSP response information

Source: OCSP server listed in Certificate
Location: http://ocsp.anf.es/spain/AV
Size: 2476 bytes (DER)
Response time: 318.225707ms
Signature algorithm: SHA256-RSA
Signature type: CA Delegated
Signed by: ANF High Assurance Server CA Responder 1293
Issued by: ANF High Assurance Server CA
Signing certificate validity: Sep 5, 2019 6:37:08 PM - Jul 1, 2020 6:37:08 PM
Signing certificate algorithm: SHA256-RSA
Reported statuses: 1
This update: Oct 7, 2019 4:36:48 PM
Next update: Oct 14, 2019 4:36:48 PM
Produced at: Oct 7, 2019 4:36:48 PM
Server status: Success
Status: Good

Relevant server response headers

Date: Oct 7, 2019 4:36:48 PM
Last Modified: Oct 7, 2019 4:36:48 PM
Expires: Oct 14, 2019 4:36:48 PM

✓ OCSP signing certificate is already valid
✓ OCSP signing certificate is not expired
✓ OCSP signing certificate does not expire before NextUpdate
✓ OCSP signing certificate does contain the Extended Key Usage for OCSP Signing
✓ OCSP signing certificate does contain the OCSP No Check extension
✓ Content-Type in response is set to 'application/ocsp-response'
✓ Response is already valid
✓ Response is not expired



- ✓ Response is not expired
- ✓ ThisUpdate is less than four days old, OCSP information must be updated at least every four days (Mozilla & Baseline Requirements)
- ✓ The NextUpdate field is not more than ten days beyond the value of the ThisUpdate field (Mozilla & Baseline Requirements)
- ✓ Last-Modified header is the same as ThisUpdate (RFC 5019, section 6.2)
- ✓ NextUpdate is after the date in the Expires cache header
- ✓ The Cache-Control max-age header does not outlive NextUpdate
- ✓ ThisUpdate has a date before NextUpdate
- ✓ Expires cache header is the same as the NextUpdate field (RFC 5019 section 6.2)

This OCSP response was cached at Oct 7, 2019 4:36:48 PM

http://ocsp.anf.es/spain/AV (UNKNOWN)

OCSP response information

Source: OCSP server listed in Certificate
Location: http://ocsp.anf.es/spain/AV
Size: 2484 bytes (DER)
Response time: 333.769176ms
Signature algorithm: SHA256-RSA
Signature type: CA Delegated
Signed by: ANF High Assurance Server CA Responder 1293
Issued by: ANF High Assurance Server CA
Signing certificate validity: Sep 5, 2019 6:37:08 PM - Jul 1, 2020 6:37:08 PM
Signing certificate algorithm: SHA256-RSA
Reported statuses: 1
This update: Oct 7, 2019 4:36:48 PM
Next update: Oct 14, 2019 4:36:48 PM
Produced at: Oct 7, 2019 4:36:48 PM
Server status: Success
Status: Unknown

- ✓ OCSP requests is smaller than 255 bytes
- ✓ OCSP signing certificate is already valid
- ✓ OCSP signing certificate is not expired
- ✓ OCSP signing certificate does not expire before NextUpdate
- ✓ OCSP signing certificate does contain the Extended Key Usage for OCSP Signing
- ✓ OCSP signing certificate does contain the OCSP No Check extension
- ✓ Content-Type in response is set to 'application/ocsp-response'

ANF High Assurance Server CA (CA Certificate)

Certificate details for ANF High Assurance Server CA (At position 2 in certificate chain)

Serial number:
hex: 16210359fab8ae2
int: 99659964253702882
Issued by: ANF Secure Server Root CA
Public Key Algorithm: RSA
Not valid before: Sep 5, 2019 6:35:44 PM
Not valid after: Sep 2, 2029 6:35:44 PM

Company registration number: G63287510
Organization: ANF Autoridad de Certificacion
Organization unit: ANF Autoridad intermedia tecnicos
Country: ES

- ✓ This certificate does not contain any links to an LDAP server
- ✓ This certificate does not contain any internal server links
- ✓ This certificate does not contain any links with an unknown format

Check certificate compliance for ANF High Assurance Server CA

Certificate Revocation List (CRL)

This CRL was cached at Oct 3, 2019 12:24:52 PM

http://crl.anf.es/crl/ANFSecureServerRootCA-arl.crl

CRL information

Source: CRL Distribution Point listed in Certificate
Location: http://crl.anf.es/crl/ANFSecureServerRootCA-arl.crl
Size: 852 bytes (DER data)
Response time: 448.888343ms
This update: Sep 4, 2019 12:01:56 PM
Next update: Mar 2, 2020 12:01:56 PM
Revoked: No
Revoked certificates in CRL: 0

Relevant server response headers

Date: Oct 3, 2019 12:24:52 PM
Last Modified: Sep 4, 2019 12:01:56 PM
Expires: Mar 2, 2020 12:01:56 PM

Server and network information

Server Software: Apache

- ✓ Content-Type in response is set to 'application/pkix-crl (RFC 5280, section 4.2.1.13)'
- ✓ This CRL file is DER encoded
- ✓ Response is already valid
- ✓ Response is not expired
- ✓ Revocation information is updated at least once every twelve months
- ✓ The value of the NextUpdate field is not more than twelve months beyond the value of the ThisUpdate field
- ✓ Last-Modified header is the same as ThisUpdate (RFC 5019, section 6.2)

✓ NextUpdate is after the date in the Expires cache header
✓ The Cache-Control max-age header does not outlive NextUpdate
✓ ThisUpdate has a date before NextUpdate
✓ Expires cache header is the same as the NextUpdate field (RFC 5019 section 6.2)

This CRL was cached at Oct 3, 2019 12:24:52 PM

http://www.anf.es/crl/ANFSecureServerRootCA-arl.crl

CRL information

Source: CRL Distribution Point listed in Certificate
Location: http://www.anf.es/crl/ANFSecureServerRootCA-arl.crl
Size: 852 bytes (DER data)
Response time: 296.501084ms
This update: Sep 4, 2019 12:01:56 PM
Next update: Mar 2, 2020 12:01:56 PM
Revoked: No
Revoked certificates in CRL: 0

Relevant server response headers

Date: Oct 3, 2019 12:24:52 PM
Last Modified: Sep 4, 2019 12:01:56 PM
Expires: Mar 2, 2020 12:01:56 PM

Server and network information

Server Software: Apache

✓ Content-Type in response is set to 'application/pkix-crl (RFC 5280, section 4.2.1.13)'
✓ This CRL file is DER encoded
✓ Response is already valid
✓ Response is not expired
✓ Revocation information is updated at least once every twelve months
✓ The value of the NextUpdate field is not more than twelve months beyond the value of the ThisUpdate field
✓ Last-Modified header is the same as ThisUpdate (RFC 5019, section 6.2)
✓ NextUpdate is after the date in the Expires cache header
✓ The Cache-Control max-age header does not outlive NextUpdate
✓ ThisUpdate has a date before NextUpdate
✓ Expires cache header is the same as the NextUpdate field (RFC 5019 section 6.2)

Online Certificate Status Protocol (OCSP)

This OCSP response was cached at Oct 3, 2019 12:24:52 PM

http://ocsp.anf.es/spain/AV (GET)

OCSP response information

Source: OCSP server listed in Certificate
Location: http://ocsp.anf.es/spain/AV
Size: 2740 bytes (DER)
Response time: 303.536714ms
Signature algorithm: SHA256-RSA
Signature type: CA Delegated
Signed by: ANF Secure Server Root CA Responder 1289
Issued by: ANF Secure Server Root CA
Signing certificate validity: Sep 4, 2019 12:05:36 PM - Jun 30, 2020 12:05:36 PM
Signing certificate algorithm: SHA256-RSA
Reported statuses: 1
This update: Oct 3, 2019 12:24:52 PM
Next update: Oct 10, 2019 12:24:52 PM
Produced at: Oct 3, 2019 12:24:52 PM
Server status: Success
Status: Good

Relevant server response headers

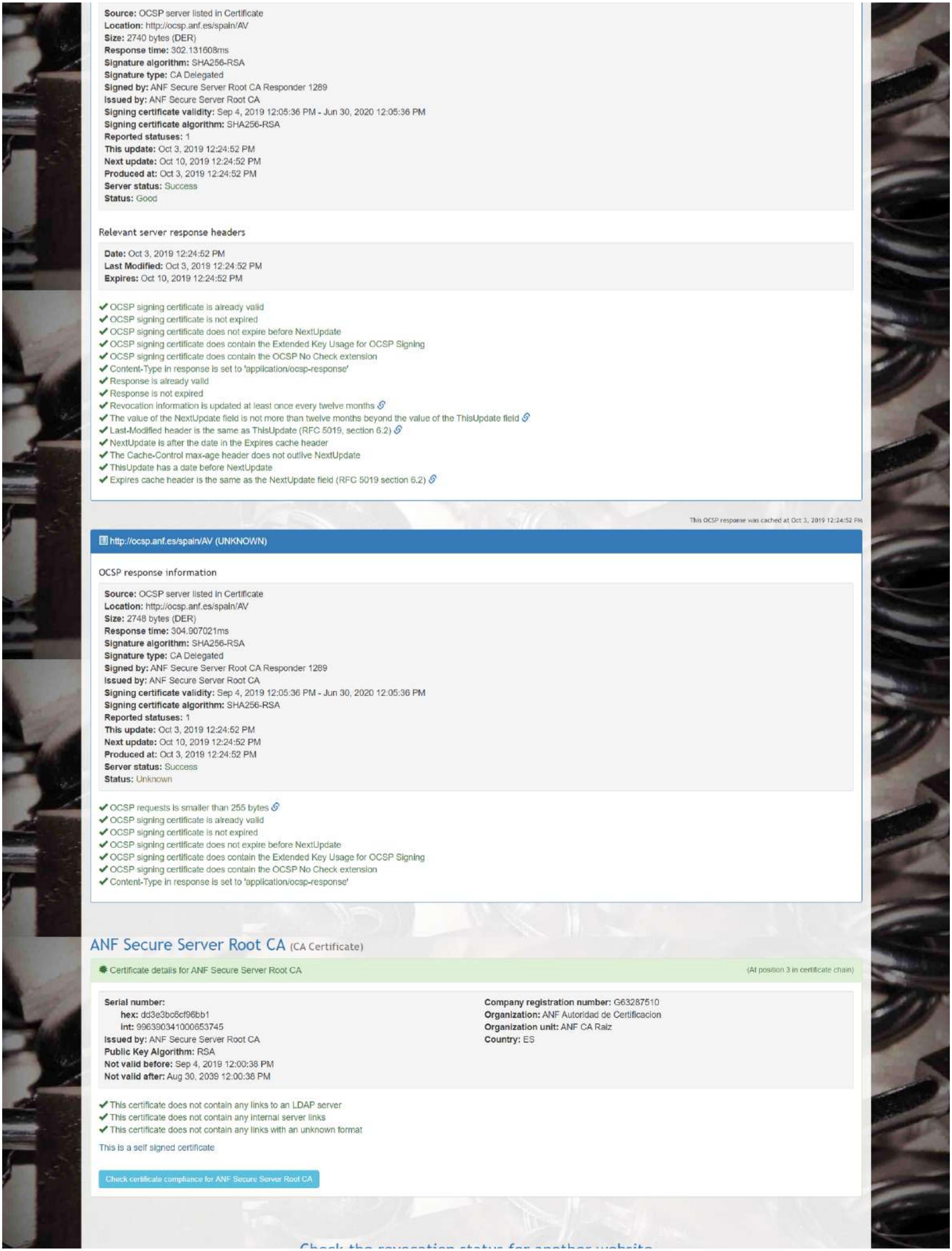
Date: Oct 3, 2019 12:24:52 PM
Last Modified: Oct 3, 2019 12:24:52 PM
Expires: Oct 10, 2019 12:24:52 PM

✓ OCSP requests is smaller than 255 bytes
✓ OCSP signing certificate is already valid
✓ OCSP signing certificate is not expired
✓ OCSP signing certificate does not expire before NextUpdate
✓ OCSP signing certificate does contain the Extended Key Usage for OCSP Signing
✓ OCSP signing certificate does contain the OCSP No Check extension
✓ Content-Type in response is set to 'application/ocsp-response'
✓ Response is already valid
✓ Response is not expired
✓ Revocation information is updated at least once every twelve months
✓ The value of the NextUpdate field is not more than twelve months beyond the value of the ThisUpdate field
✓ Last-Modified header is the same as ThisUpdate (RFC 5019, section 6.2)
✓ NextUpdate is after the date in the Expires cache header
✓ The Cache-Control max-age header does not outlive NextUpdate
✓ ThisUpdate has a date before NextUpdate
✓ Expires cache header is the same as the NextUpdate field (RFC 5019 section 6.2)

This OCSP response was cached at Oct 3, 2019 12:24:52 PM

http://ocsp.anf.es/spain/AV (POST)

OCSP response information



Source: OCSP server listed in Certificate
Location: http://ocsp.anf.es/spain/AV
Size: 2740 bytes (DER)
Response time: 302.131608ms
Signature algorithm: SHA256-RSA
Signature type: CA Delegated
Signed by: ANF Secure Server Root CA Responder 1289
Issued by: ANF Secure Server Root CA
Signing certificate validity: Sep 4, 2019 12:05:36 PM - Jun 30, 2020 12:05:36 PM
Signing certificate algorithm: SHA256-RSA
Reported statuses: 1
This update: Oct 3, 2019 12:24:52 PM
Next update: Oct 10, 2019 12:24:52 PM
Produced at: Oct 3, 2019 12:24:52 PM
Server status: Success
Status: Good

Relevant server response headers

Date: Oct 3, 2019 12:24:52 PM
Last Modified: Oct 3, 2019 12:24:52 PM
Expires: Oct 10, 2019 12:24:52 PM

✓ OCSP signing certificate is already valid
✓ OCSP signing certificate is not expired
✓ OCSP signing certificate does not expire before NextUpdate
✓ OCSP signing certificate does contain the Extended Key Usage for OCSP Signing
✓ OCSP signing certificate does contain the OCSP No Check extension
✓ Content-Type in response is set to 'application/ocsp-response'
✓ Response is already valid
✓ Response is not expired
✓ Revocation information is updated at least once every twelve months
✓ The value of the NextUpdate field is not more than twelve months beyond the value of the ThisUpdate field
✓ Last-Modified header is the same as ThisUpdate (RFC 5019, section 6.2)
✓ NextUpdate is after the date in the Expires cache header
✓ The Cache-Control max-age header does not outlive NextUpdate
✓ ThisUpdate has a date before NextUpdate
✓ Expires cache header is the same as the NextUpdate field (RFC 5019 section 6.2)

This OCSP response was cached at Oct 3, 2019 12:24:52 PM

http://ocsp.anf.es/spain/AV (UNKNOWN)

OCSP response information

Source: OCSP server listed in Certificate
Location: http://ocsp.anf.es/spain/AV
Size: 2748 bytes (DER)
Response time: 304.907021ms
Signature algorithm: SHA256-RSA
Signature type: CA Delegated
Signed by: ANF Secure Server Root CA Responder 1289
Issued by: ANF Secure Server Root CA
Signing certificate validity: Sep 4, 2019 12:05:36 PM - Jun 30, 2020 12:05:36 PM
Signing certificate algorithm: SHA256-RSA
Reported statuses: 1
This update: Oct 3, 2019 12:24:52 PM
Next update: Oct 10, 2019 12:24:52 PM
Produced at: Oct 3, 2019 12:24:52 PM
Server status: Success
Status: Unknown

✓ OCSP requests is smaller than 255 bytes
✓ OCSP signing certificate is already valid
✓ OCSP signing certificate is not expired
✓ OCSP signing certificate does not expire before NextUpdate
✓ OCSP signing certificate does contain the Extended Key Usage for OCSP Signing
✓ OCSP signing certificate does contain the OCSP No Check extension
✓ Content-Type in response is set to 'application/ocsp-response'

ANF Secure Server Root CA (CA Certificate)

Certificate details for ANF Secure Server Root CA (At position 3 in certificate chain)

Serial number:
  hex: dd3e3bc6cf96bb1
  int: 996390341000653745
Issued by: ANF Secure Server Root CA
Public Key Algorithm: RSA
Not valid before: Sep 4, 2019 12:00:38 PM
Not valid after: Aug 30, 2039 12:00:38 PM

Company registration number: G63287510
Organization: ANF Autoridad de Certificacion
Organization unit: ANF CA Raiz
Country: ES

✓ This certificate does not contain any links to an LDAP server
✓ This certificate does not contain any internal server links
✓ This certificate does not contain any links with an unknown format

This is a self signed certificate

Check the revocation status for another website

Check the revocation status for another website

Created by Paul van Brouwershaven

◆ 2015 - 2019 Digitorus B.V.

Revoked certificates can't and should not be trusted, these certificate will cause errors like "NET::ERR_CERT_REVOKED" in browsers and expose a security risk.