

Altres disposicions

Decret 382/2021, del 24 de novembre del 2021

Decret 382/2021, del 24-11-2021, pel qual s'aproven els números de referència de normes relatives a dispositius de signatura electrònica i de segell electrònic, i altres sistemes, mitjans i productes relacionats.

Exposició de motius

La Llei 35/2014, del 27 de novembre, de serveis de certificació i confiança electrònica, modificada per la Llei 9/2021, del 29 d'abril, regula, entre altres aspectes, els serveis de confiança electrònica i els seus efectes substantius en l'àmbit de les relacions privades i en el de les administracions públiques, l'activitat dels prestadors de serveis de confiança electrònica qualificats i les condicions de supervisió que s'hi apliquen.

Respecte a la signatura electrònica i al segell electrònic, els articles 5.5 i 7.4, respectivament, de la Llei 35/2014 autoritzen el Govern a dictar disposicions reglamentàries per definir els seus diversos nivells de seguretat, així com a establir números de referència de normes relatives als mateixos nivells, que han de ser publicats al *Butlletí Oficial del Principat d'Andorra*.

En relació amb els certificats qualificats de signatura electrònica i de segell electrònic, i d'autenticació de lloc web, els articles 6.4, 8.4 i 19.2, respectivament, de la Llei 35/2014 autoritzen el Govern a dictar disposicions reglamentàries per definir-ne els requisits de forma més precisa, així com a establir números de referència de normes relatives als mateixos certificats, que han de ser publicats al *Butlletí Oficial del Principat d'Andorra*.

Pel que fa als dispositius de creació de signatura electrònica i de segell, l'article 9.3 de la Llei 35/2014 autoritza el Govern a establir números de referència de normes relatives a dispositius de signatura electrònica i de segells electrònics, i altres sistemes, mitjans i productes relacionats a què es refereix aquesta Llei, que han de ser publicats al *Butlletí Oficial del Principat d'Andorra*, previsió que cal posar en relació amb l'article 26.8 de la mateixa Llei. Aquesta Llei autoritza el Govern a establir números de referència de normes per a sistemes i productes dignes de confiança electrònica, atès que la gestió de les dades de creació de signatura electrònica i segell electrònic qualificat en nom del seu titular ha d'anar a càrrec d'un prestador qualificat, en compliment del que disposa l'article 10.3 de la Llei.

En ús d'aquesta habilitació legal, mitjançant el Decret del 22-4-2015 es van aprovar els números de referència de normes relatives a dispositius de signatura electrònica i de segell electrònic, i altres sistemes, mitjans i productes relacionats.

En relació amb la validació de les signatures electròniques qualificades i dels segells electrònics qualificats, l'article 14.2 de la Llei 35/2014 autoritza el Govern a dictar disposicions reglamentàries per definir-ne els requisits de forma més precisa, així com a establir números de referència de normes relatives a la mateixa validació, que han de ser publicats al *Butlletí Oficial del Principat d'Andorra*. Quan la validació s'ofereix com a servei a càrrec d'un prestador qualificat, conforme a l'article 15.2 de la Llei 35/2014, el Govern pot dictar disposicions reglamentàries per definir-ne de forma més precisa els requisits, així com establir números de referència de normes relatives al mateix servei qualificat de validació, que han de ser publicats al *Butlletí Oficial del Principat d'Andorra*.

Respecte a la conservació de les signatures electròniques qualificades i dels segells electrònics qualificats, l'article 16.2 de la Llei 35/2014 autoritza el Govern a dictar disposicions reglamentàries per definir-ne els requisits de forma més precisa, així com a establir números de referència de normes relatives a la mateixa conservació, que han de ser publicats al *Butlletí Oficial del Principat d'Andorra*.

En relació amb la marca de temps electrònica qualificada, l'article 18.2 de la Llei 35/2014 autoritza el Govern a dictar disposicions reglamentàries per definir de forma més precisa els requisits per a la vinculació exacta de la data i l'hora amb les dades, i una font d'informació temporal exacta, així com a establir números de referència de normes relatives a les mateixes dades, que han de ser publicades al *Butlletí Oficial del Principat d'Andorra*.

Respecte als serveis de lliurament electrònic qualificats, l'article 21.2 autoritza el Govern a dictar disposicions reglamentàries per definir-ne els requisits de forma més precisa, així com a establir números de referència de normes relatives als mateixos serveis, que han de ser publicats al *Butlletí Oficial del Principat d'Andorra*.

Pel que fa a la digitalització documental, l'article 23.4 de la Llei 35/2014 autoritza el Govern a dictar disposicions reglamentàries per definir de forma més precisa els requisits dels processos de digitalització qualificada, així com a establir números de referència de normes relatives als mateixos processos, que han de ser publicats al *Butlletí Oficial del Principat d'Andorra*.

Finalment, l'article 26.8 de la Llei 35/2014 autoritza el Govern a establir números de referència de normes per a sistemes i productes dignes de confiança electrònica, a l'efecte de complir el que disposa l'article 26.1, en els epígrafs b i c.

Des que es va aprovar la Llei 35/2014, els organismes europeus de normalització, significativament el Comitè Europeu de Normalització (CEN) i l'Institut Europeu de Normes de Telecomunicacions (ETSI), han produït un cos normatiu tècnic ampli referit als serveis de confiança regulats a la Llei 35/2014, orientat a establir condicions de seguretat i qualitat suficients en relació amb els serveis i les institucions jurídiques als quals els mateixos serveis ofereixen suport, així com a garantir-ne la interoperabilitat, cosa que fa convenient que s'aprovi conforme a les previsions de la Llei 35/2014 corresponents.

L'adopció d'aquests estàndards per part del Govern d'Andorra, així mateix, facilita el reconeixement directe a Andorra dels serveis de confiança oferts per prestadors de la Unió Europea conforme al Reglament (UE) núm. 910/2014, del Parlament Europeu i del Consell, del 23 de juliol, relatiu a la identificació electrònica i als serveis de confiança per a les transaccions al mercat interior.

D'altra banda, la Llei 9/2021, del 29 d'abril, ha incorporat diversos serveis de confiança addicionals als previstos inicialment per la Llei 35/2014.

En relació amb la identificació electrònica d'una persona física i d'una persona jurídica, els articles 5 *bis*.5 i 7 *bis*.5, respectivament, de la Llei 35/2014 autoritzen el Govern a dictar disposicions reglamentàries per definir els diversos nivells de seguretat, així com a establir números de referència de normes relatives als mateixos nivells, que han de ser publicats al *Butlletí Oficial del Principat d'Andorra*.

Respecte a la presentació electrònica d'un atribut verificat d'identitat de persona física o jurídica, l'article 21 *bis*.5 autoritza el Govern a dictar disposicions reglamentàries per definir de forma més precisa els requisits de la presentació electrònica d'un atribut d'identitat verificat de persona física o jurídica, així com a establir números de referència de normes relatives a la mateixa presentació electrònica, que s'han de publicar al *Butlletí Oficial del Principat d'Andorra*.

Pel que fa als certificats electrònics qualificats d'atributs verificats, l'article 21 *ter*.4 autoritza el Govern a dictar disposicions reglamentàries per definir-ne els requisits de forma més precisa, així com a establir números de referència de normes relatives als mateixos certificats, que s'han de publicar al *Butlletí Oficial del Principat d'Andorra*.

En relació amb els repositoris electrònics personals de dades qualificats, l'article 21 *quater*.2 autoritza el Govern a dictar disposicions reglamentàries per definir-ne els requisits de forma més precisa, així com a establir números de referència de normes relatives als mateixos repositoris, que s'han de publicar al *Butlletí Oficial del Principat d'Andorra*.

Finalment, respecte dels nodes qualificats de sistemes de tecnologia de registre distribuït, l'article 21 *quinques*.2 autoritza el Govern a dictar disposicions reglamentàries per definir-ne els requisits de forma més

precisa, així com a establir números de referència de normes relatives als mateixos nodes qualificats, que s'han de publicar al *Butlletí Oficial del Principat d'Andorra*.

En tots els casos esmentats, l'efecte jurídic de l'adopció de normes tècniques és establir una presumpció del compliment dels requisits legals, per la qual cosa es preserva plenament el caràcter voluntari propi de les normes tècniques i no es crea cap barrera per a la innovació, ja que és possible obtenir la qualificació d'un servei sense adoptar cap norma tècnica. Tanmateix, el valor d'adequar-se a les normes tècniques és indubtable, ja que facilita el compliment de les obligacions legals, aporta un nivell més gran de seguretat, redueix riscos per a totes les parts i proporciona un nivell adequat d'interoperabilitat.

Per altra banda, i com a novetat, l'article 27.4 de la Llei 35/2014, incorporat per la Llei 9/2021, autoritza els prestadors de serveis de confiança a fer ús de sistemes de tecnologia de registre distribuït en la provisió dels serveis i exigeix que quan el servei de confiança sigui qualificat, si es basa en sistemes de tecnologies de registre distribuït, els prestadors han de fer servir exclusivament xarxes formades per nodes qualificats. Degut al caràcter innovador i, en alguns casos, experimental que tenen les tecnologies de registre distribuït, resulta especialment necessari incorporar especificacions tècniques sense el caràcter formal de norma, com les que es produeixen en determinades comunitats d'usuaris.

En virtut de les competències atribuïdes pels articles indicats anteriorment de la Llei 35/2014, del 27 de novembre, de serveis de certificació i confiança electrònica, i a proposta del cap de Govern, el Govern, en la sessió del 24 de novembre del 2021, aprova aquest Decret amb el contingut següent:

Article 1. *Nivells de seguretat de la signatura electrònica i del segell electrònic*

1. Als efectes del que es determina als articles 5.5 i 7.4 de la Llei 35/2014, s'estableixen quatre nivells de seguretat:

- a) Bàsic.
- b) Amb marca de temps.
- c) Amb disponibilitat a llarg termini del material de validació.
- d) Amb disponibilitat a llarg termini i integritat del material de validació.

2. Els nivells de seguretat s'implementen mitjançant l'ús dels formats de signatura electrònica i segell electrònic aprovats pel Govern.

3. Les signatures i els segells electrònics han de fer servir els algorismes criptogràfics aprovats pel Govern.

Article 2. *Establiment i aprovació de normes i altres especificacions tècniques*

1. S'estableixen i s'aproven els números de referència de les normes i altres especificacions tècniques conforme a l'annex d'aquest Decret.

2. La Comissió Nacional d'Acreditació ha de concretar les versions corresponents de les normes i altres especificacions tècniques indicades a l'annex i la seva validesa temporal.

Article 3. *Publicació*

La Comissió Nacional d'Acreditació ha de publicar a la seva pàgina web la llista actualitzada de normes i altres especificacions tècniques establertes i aprovades pel Govern, amb la indicació del període temporal d'aplicació corresponent a cada versió de cada norma i especificació tècnica i l'enllaç a l'organisme corresponent.

Disposició transitòria

Els serveis que hagin obtingut la qualificació emprant el número de referència de normes aprovades conforme al Decret del 22-4-2015 s'han d'adequar al que disposa aquest Decret en el termini màxim d'un any, moment en què l'aprovació quedarà automàticament revocada.

Transcorregut aquest període, no es produirà l'efecte jurídic de presumpció de compliment dels requisits jurídics corresponents.

Disposició derogatòria

Es deroga el Decret del 22-4-2015 pel qual s'aproven els números de referència de normes relatives a dispositius de signatura electrònica i de segell electrònics, i altres sistemes, mitjans i productes relacionats.

Disposició final

Aquest Decret entrarà en vigor l'endemà de ser publicat al *Butlletí Oficial del Principat d'Andorra*.

Cosa que es fa pública per a coneixement general.

Andorra la Vella, 24 de novembre del 2021

Xavier Espot Zamora
Cap de Govern

Annex

	Normes i especificacions
Article 5.5 Article 7.4	ETSI EN 319 122-1. Electronic Signatures and Infrastructures (ESI); CAAdES digital signatures; Part 1: Building blocks and CAAdES baseline signatures. ETSI TS 103 173. Electronic Signatures and Infrastructures (ESI); CAAdES Baseline Profile. ETSI EN 319 132-1. Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures. ETSI TS 103 171. Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile. ETSI EN 319 142-1. Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures. ETSI TS 103 172. Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile. ETSI EN 319 162-1. Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers. ETSI TS 103 174. Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile. ETSI TS 119 182-1. Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures. La referència del nivell corresponent s'ha de fer conforme al que disposa ETSI TS 119 192. Electronic Signatures and Infrastructures (ESI); AdES related Uniform Resource Identifier. Algorismes aprovats: ETSI TS 119 312. Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
Article 5 bis.5 Article 7 bis.5	UNE 71307-1:2020. Tecnologías Habilitadoras Digitales. Modelo de Gestión de Identidades Descentralizadas sobre Blockchain y otras Tecnologías de Registros Distribuidos. Parte 1: Marco de referencia. W3C Proposed Recommendation. Decentralized Identifiers (DIDs) v1.0. OpenID Self-Issued OpenID Provider v2. DIF DID Authentication Profile for SIOP. DIF DIDComm Messaging, amb Hyperledger Aries Interop Profile 2.0.
Article 6.4	ETSI EN 319 412-1. Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures. ETSI EN 319 412-2. Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons. ETSI EN 319 412-5. Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.
Article 8.4	ETSI EN 319 412-1. Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures. ETSI EN 319 412-3. Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons. ETSI EN 319 412-5. Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements. Requisits específics per a banca oberta: ETSI TS 119 495. Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking.

Article 9.3	CEN/TR 419200:2017. Guidance for signature creation and other related devices. CEN/TR 419210:2019. Applicability of CEN Standards to Qualified Electronic Seal Creation Device under the EU Regulation N°910/2014 (eIDAS). CEN EN 419211-1:2014. Protection profiles for secure signature creation device - Part 1: Overview. CEN EN 419211-2:2013. Protection profiles for secure signature creation device - Part 2: Device with key generation. CEN EN 419211-3:2013. Protection profiles for secure signature creation device - Part 3: Device with key import. CEN EN 419211-4:2013. Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted channel to certificate generation application. CEN EN 419211-5:2013. Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted channel to signature creation application. CEN EN 419211-6:2014. Protection profiles for secure signature creation device - Part 6: Extension for device with key import and trusted channel to signature creation application. CEN EN 419212-1:2017. Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 1: Introduction and common definitions. CEN EN 419212-2:2017. Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 2: Signature and Seal Services. CEN EN 419212-3:2017. Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 3: Device authentication protocols. CEN EN 419212-4:2018. Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 4: Privacy specific Protocols. CEN EN 419212-5:2018. Application Interface for Secure Elements for Electronic Identification, Authentication and Trusted Services - Part 5: Trusted eService. En cas de gestió de dades de creació de signatura electrònica o segell electrònic per compte de tercers i suport a la creació remota de signatura o segell electrònics: CEN EN 419241-1:2018. Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements. CEN EN 419241-2:2019. Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing. ETSI TS 119 431-1. Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev. ETSI TS 119 431-2. Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation. ETSI TS 119 432. Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation. En cas de gestió centralitzada de dades de creació de signatura o segell pel mateix titular: CEN/TS 419221-6:2019. Conditions for use of EN 419221-5 as a qualified electronic signature or seal creation device.
Article 14.2	ETSI TS 119 101. Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation. ETSI EN 319 102-1. Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation. ETSI TS 119 102-2. Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report. ETSI TS 119 172-4. Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists, amb les adaptacions apropiades a la Llei 35/2014.
Article 15.2	ETSI TS 119 441. Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services. ETSI TS 119 442. Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services.
Article 16.2	ETSI TS 119 511. Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques. ETSI TS 119 512. Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services.
Article 18.2	ETSI EN 319 421. Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. ETSI EN 319 422. Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles, amb les adaptacions oportunes a la Llei 35/2014.

Article 19.2	ETSI EN 319 412-1. Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures. ETSI EN 319 412-4. Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates. ETSI EN 319 412-5. Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements. Requisits específics per a banca oberta: ETSI TS 119 495. Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Certificate Profiles and TSP Policy Requirements for Open Banking.
Article 21.2	ETSI EN 319 521. Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers. ETSI EN 319 522-1. Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture. ETSI EN 319 522-2. Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic contents. ETSI EN 319 522-3. Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 3: Formats. En cas d'ús del protocol de transmissió AS4: ETSI EN 319 522-4-1. Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 1: Message delivery bindings. ETSI EN 319 522-4-2. Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 2: Evidence and identification bindings. ETSI EN 319 522-4-3. Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 3: Capability/requirements bindings. En cas d'utilització de correu electrònic: ETSI EN 319 531. Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers. ETSI EN 319 532-1. Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 1: Framework and architecture. ETSI EN 319 532-2. Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 2: Semantic contents. ETSI EN 319 532-3. Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 3: Formats. ETSI EN 319 532-4. Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 4: Interoperability profiles.
Article 21 bis.5	UNE 71307-1:2020. Tecnologías habilitadoras digitales. Modelo de gestión de identidades descentralizadas sobre blockchain y otras tecnologías de registros distribuidos. Parte 1: Marco de referencia. European Blockchain Services Infrastructure ESSIF. Alastria Identity Reference Model.
Article 21 ter.4	W3C Recommendation. Verifiable Credentials Data Model 1.0. Algorismes aprovats (addicionals als articles 5.5 i 7.4): Camenisch Lysyanskaya signature, Boneh Boyen Shacham (BBS+), ECDSA i ECDH Secp256k1, Boneh Lynn Shacham (BLS) signature.
Article 21 quater.2	No se n'estableixen.
Article 21 quinquies.2	Hyperledger BESU, amb Istanbul Bizantine Fault Tolerant Protocol (IBFT) 2.0. Hyperledger Indy, amb Plenum Byzantine Fault Tolerant Protocol. Hyperledger Fabric, amb RAFT Protocol. Algorand (Pure Proof-of-Stake) amb Certified Vote (pendent de revisió).
Article 23.4	AFNOR NF Z42-026:2017. Définition et spécifications des prestations de numérisation fidèle de documents sur support papier et contrôle de ces prestations. ISO/TR 13028. Information and documentation - Implementation guidelines for digitization of records.
Article 26.2.e	ETSI TS 119 461. Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects.
Article 26.8	CEN/TS 419261:2015. Security requirements for trustworthy systems managing certificates and time-stamps. CEN/TS 419221-1:2016. Protection Profiles for TSP cryptographic modules - Part 1: Overview. CEN/TS 419221-2:2016. Protection Profiles for TSP cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup. CEN/TS 419221-3:2016. Protection Profiles for TSP Cryptographic modules - Part 3: Cryptographic module for CSP key generation services. CEN/TS 419221-4:2016. Protection Profiles for TSP cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup. CEN EN 419221-5:2018. Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services. CEN EN 419231:2019. Protection profile for trustworthy systems supporting time stamping.