EUROPEAN UNION AGENCY
FOR CYBERSECURITY

OVERVIEW OF STANDARDS

Specifying formats of advanced electronic signatures and seals

DECEMBER 2019

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

For contacting the authors please use trust@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

LEGAL NOTICE

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 2019/881.
This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.
Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Regulation (EU) No 910/2014[1] (hereafter the **eIDAS** Regulation[2]) provides the regulatory framework in the EU for electronic identification and trust services for electronic transactions in the internal market. The creation, verification, validation and preservation of electronic signatures or electronic seals relies (among others) on standards specifying formats of electronic signatures and seals to guarantee interoperability and their general usability within the Member States and across borders.

The scope of this document is to assess the suitability of the recently published European Norms (hereafter ENs) on advanced signatures formats (based on CMS, XML and PDF, and for Associated signature and seal containers) to fulfil the eIDAS Regulation requirements, and to describe the differences with the previous Technical Specifications (hereafter TSs), in view of a possible update of the list of standards referenced in the Commission Decisions in force. It also aims at evaluating the consequences of such update and defines the timeline for a possible transition to the exclusive usage of the new ENs.

The updated set of ENs, published by ETSI in April 2016, has a much higher stability and value in the standardization document hierarchy than TSs and guarantee that no other national standard can be developed or adopted overlapping these ones. The validation process included a public review (in addition to the enquiry stage already part of the ETSI process) and specific tests that led to the improvement of interoperability (also improving the text where it was not interpreted unambiguously by implementors), elimination of technical flaws and provision of new features proposed during the drafting and the approval process of the ENs. The extensive experience of ETSI TC ESI in developing standards for electronic signatures is also a guarantee for the quality of the standards and for their sustainability and maintenance.

In order to reduce the impact of updating the references, the European Commission should consider defining, with the Member States, an appropriate update path. The process could be stimulated with specific funding measures, such as CEF[3], during the adoption of the CEF eSignature building block. This should be possible until the end of 2020 when the CEF initiative is expected to terminate.

The update path should be adopted in a way should avoid any discontinuity and minimize the impact on provision of services by allowing enough time to implement the changes but also foreseeing a period of time of parallel use of the new ENs with the previous TSs.

It should be noted that ETSI will not deprecate the previous TSs unless serious flaws are identified. This is not likely to happen given that these standards where tested during a long time and are currently widely adopted.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910
[2] See Annex A.
[3] Connecting Europe Facility, https://ec.europa.eu/inea/en/connecting-europe-facility

1. INTRODUCTION

The Regulation (EU) No 910/2014[4] (hereafter the **eIDAS** Regulation[5]) provides the regulatory framework in the EU for electronic identification and trust services for electronic transactions in the internal market. The creation, verification, validation and preservation of electronic signatures or electronic seals relies (among others) on standards specifying formats of electronic signatures and seals to guarantee interoperability and their general usability within the Member States and across borders.

The eIDAS Regulation in recital 64 says: “When addressing formats of advanced electronic signatures and seals, the Commission should build on existing practices, standards and legislation […]” and sets the ground for Article 27 “Electronic signatures in public services” where the paragraph 5 reads: “By 18 September 2015, and taking into account existing practices, standards and Union legal acts, the Commission shall, by means of implementing acts, define reference formats of advanced electronic signatures […]”. Mutatis mutandis Article 37 “Electronic seals in public services” and its paragraph 5 requires the same for electronic seals. On this basis the Commission has published the Commission Implementing Decision (EU) 2015/1506[6] laying down specifications relating to the format of advanced electronic signatures and seals, defining the minimum requirements in terms of advanced electronic signatures and seals format recognition for the public sector.

The above mentioned Decision specifies in its Article 1 that the Member States shall recognize XML, CMS or PDF advanced electronic signatures based on the formats respectively named XAdES[7], CAdES[8] or PAdES[9], or associated signature containers based on ASiC[10] if they comply with the ETSI technical specifications (TSs) listed in the Decision Annex. The article 3 requires the same formats for electronic seals. It should be noted that the standards referenced are the same as in the Commission Decision 2011/130/EU[11], “establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC” (“on services in the internal market” or “Services Directive”[12]).

Some years after the publication of the technical specifications referenced in the mentioned Decisions, ETSI has published a set of European standards (ENs) taking into account the eIDAS Regulation requirements and addressing a number of issues that have been identified, based on the feedback received from the stakeholders, for example during CAdES/XAdES/PAdES/ASiC ETSI Plugtests™ events. These ENs are not listed in the mentioned Decisions, thus a consideration should be given for their update.

The scope of this document is to assess the suitability of the recently published ENs to fulfil the eIDAS Regulation requirements, and to describe the differences with the previous TSs, in view

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910
[5] See Annex A.
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015D1506
[7] XML Advanced Electronic Signature
[8] CMS Advanced Electronic Signature
[9] PDF Advanced Electronic Signature
[10] Associated Signature Container
[11] This document refers to Decision 2011/130/EU (available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011D0130) as amended by the Commission Implementing Decision 2014/148/EU (available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014D0148). The consolidated text is available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02011D0130-20141201
[12] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0123

of a possible update of the list of standards referenced in the Decisions in force. It also aims at evaluating the consequences of such update and defines the timeline for a possible transition to the exclusive usage of the new ENs.

The standards affected are those mentioned in the Annex of the Commission Decision 2011/130/EU and Commission Implementing Decision 2015/1506/EU:

- For XML advanced electronic signatures and seals the specification currently referenced is the XAdES baseline profile, specified in ETSI TS 103 171, which is now specified as “XAdES baseline signatures” in clause 6 of ETSI EN 319 132-1.
- For CMS advanced electronic signatures and seals the specification currently referenced is the CAdES baseline profile, specified in ETSI TS 103 173, which is now specified as “CAdES baseline signatures” in clause 6 of ETSI EN 319 122-1.
- For PDF advanced electronic signatures and seals the specification currently referenced is the PAdES baseline profile, specified in ETSI TS 103 172, which is now specified as “PAdES baseline signatures” in clause 6 of ETSI EN 319 142-1.
- For associated signature and seal container the specification currently referenced is the ASiC baseline profile, specified in ETSI TS 103 174, which is now specified as “ASiC baseline containers” in clause 5 of ETSI EN 319 162-1.

In this document (as well as in TR 119 112, see 3.1) the set of “old” technical specifications (i.e. ETSI TS 103 171/2/3/4) is collectively referenced as “previous TSs” while the “new” European Norms (i.e. ETSI EN 319 122/132/142/162) are collectively referenced as “AdES/ASiC ENs”.

2. OVERVIEW OF THE ADVANCED ELECTRONIC SIGNATURE AND SEAL FORMAT STANDARDS

This chapter gives an overview of electronic signature standards and some background information on what underpinned their development.

The Directive 1999/93/EC[13], known as the “Electronic Signatures Directive”, was in force before the eIDAS Regulation. The European legislative framework presented a continuous challenge for European standards bodies to address the needs of both, the public and private sectors, while keeping as much as possible the interoperability with global standards, when they exist.

Since the introduction of the Electronic Signatures Directive, the standards on digital signatures and related trust services, i.e. the main technologies supporting electronic signatures and seals, are developed by the ETSI Technical Committee “Electronic Signatures and Infrastructures”[14] (ETSI TC ESI hereafter). In parallel, CEN developed standard protection profiles supporting certification of related products, such as qualified signature and seal creation devices, not in scope of this document.

2.1 FIRST SET OF TSS SPECIFYING ADVANCED ELECTRONIC SIGNATURES FORMAT

The ETSI ESI TC started the development of the signature format TSs when the Electronic Signatures Directive entered into force, based on the use of public key infrastructure (PKI) technology to produce digital signatures:

- ETSI TS 101 733[15] “CMS Advanced Electronic Signatures (**CAdES**)” that specifies formats for Advanced Electronic Signatures built on the IETF RFC 5652[16] “Cryptographic Message Syntax (**CMS**)”;
- ETSI TS 101 903[17] “XML Advanced Electronic Signatures (**XAdES**)” that specifies formats for Advanced Electronic Signatures built on the W3C Recommendation "XML Signature Syntax and Processing”[18] (**XMLDSig**);
- ETSI TS 102 778 “PDF Advanced Electronic Signature Profiles” (**PAdES**) a multipart standard (more specifically ETSI TS 102 778-3[19] and ETSI TS 102 778-4[20] are the basis for the PAdES Baseline Profile, see 2.2) that specifies formats for Advanced Electronic Signatures built on ISO-32000-1 "Document management - Portable document format"[21] (**PDF**);
- ETSI TS 102 918[22]“Associated Signature Containers (**ASiC**)” that specifies the use of container structures to bind together one or more signed objects with

[13] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31999L0093
[14] For more information see https://www.etsi.org/committee/esi
[15] All the references to ETSI TS 101 733 in this document refer to version 2.2.1 available at: https://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/
[16] Available at: https://tools.ietf.org/html/rfc5652
[17] All references to ETSI TS 101 903 in this document refer to version1.4.2 available at: https://www.etsi.org/deliver/etsi_ts/101900_101999/101903/01.04.02_60/
[18] Available at: https://www.w3.org/TR/2013/REC-xmldsig-core1-20130411/
[19] All references to ETSI TS 102 778-3 in this document refer to version 1.2.1 available at: https://www.etsi.org/deliver/etsi_ts/102700_102799/10277803/01.02.01_60/
[20] All references to ETSI TS 102 778-4 in this document refer to version 1.1.2 available at: https://www.etsi.org/deliver/etsi_ts/102700_102799/10277804/01.01.02_60/
[21] Available at: http://www.adobe.com/devnet/acrobat/pdfs/PDF32000_2008.pdf
[22] Available at: https://www.etsi.org/deliver/etsi_ts/102900_102999/102918/01.03.01_60/

either advanced electronic signatures or time-stamp tokens into one single digital container using package formats based on ZIP.

The first CAdES standard was published in 2000, the first XAdES in 2002, the first PAdES in 2009 and the first ASiC in 2011.

CMS, XMLDSig and PDF digital signatures are the formats for digital signatures most commonly used globally, but it was necessary to specify additional attributes to support the requirements of advanced electronic signatures as defined in the Electronic Signatures Directive, in force at that time.

The main gap identified in global standards was the lack of a consistent support for validation of the electronic signatures over long term, to protect them against key compromised or weakened algorithms. The signature validity evidence in case of disputes between signers and verifiers may occur many years after the signature creation. These issues were addressed in the global standards while keeping the basic compliance with them, i.e. using extension mechanisms that did not break the syntactical rules of the formats defined in the global standards. A number of successive versions were published as part of regular maintenance of the standards, to fix identified issues, support the business needs that were progressively emerging and to keep the suitability of the standards to support the evolving legal framework.

This led to the standards containing various options addressing long term protection but lacking a fully coherent approach to the different signature formats. This requirement emerged with the need to support the operation of Points of single contact, introduced with the Services Directive[23], and was addressed in the publication of the set of electronic signature profiles, as described in the next paragraph.

2.2 PUBLICATION OF A SET OF ELECTRONIC SIGNATURE BASELINE PROFILES ("PREVIOUS TSS")

The Services Directive required for the first time the cross border interoperability of advanced electronic signature formats to allow competent authorities[24] in each Member State to process electronic signatures created by competent authorities in another Member State. It was noted that they "may face technical difficulties due to the variety of signature formats used", as recognized in recital 3 of Commission Decision 2011/130/EU[25].

This led to the need to rationalize the different forms of signatures defined for each signature format (similar but not really equivalent) and develop and group a minimal number of sets of common properties to support the same features for long time validation, independently from the specific signature format.

In a similar way – when compared to the Services Directive – the eIDAS Regulation introduced in the article 27 "Electronic signatures in public services" (and article 37 for electronic seals) an obligation for the Member States, when they require advanced electronic signatures or seals, to support the standards referenced by the Decision 2015/1506 in their public services.

In addition, the eIDAS Regulation has introduced the electronic seals (i.e. signature by a legal persons), and, in article 37, the same obligations for member States as in the article 27 for advanced electronic signatures. The digital signature technology can support both electronic signatures and seals, and the standards developed for the advanced electronic signature

[23] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006L0123
[24] As defined in the Services Directive, i.e. any body or authority which has a supervisory or regulatory role in a Member State in relation to service activities
[25] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011D0130

formats work perfectly also for electronic seals. Only the certificates supporting signatures and seals have different content, to reflect the different nature of the subject to which the certificate is issued. In fact, the current version of the Decision 2015/1506 reference the same signature format standards specified in Decision 2011/130/EU.

In order to tackle the requirements of the Services Directive, ETSI has developed and published, in the scope the European Commission Mandate M/460[26], a set of Technical Specifications specifying Baseline Profiles for all the Advanced Electronic Signatures (CAdES, XAdES, PAdES) and for Associated Signature Containers (ASiC). These, correspond to the minimum requirements specified in Decision 2011/130/EU, and provide the same basic features with a minimal number of options. The same set of specification were found applicable by the Commission for the eIDAS Regulation and, specifically, for the purposes of the Decision 2015/1506.

Each profile specifies common set of options aiming at maximising interoperability and supporting not only the requirements of the Services Directive, but also a wide range of business and governmental use cases for electronic procedures and communications, applicable to a wide range of communities and across borders.

The Baseline Profile TSs, profiling the formats described in 2.1, are:

1. ETSI TS 103 171[27] “XAdES Baseline Profile”,
2. ETSI TS 103 172[28] “PAdES Baseline Profile”,
3. ETSI TS 103 173[29] “CAdES Baseline Profile”,
4. ETSI TS 103 174[30] “ASiC Baseline Profile”.

Each profile defines four different conformance levels addressing incremental requirements to maintain the validity of the signatures over the long term:

1. B-Level, for basic conformance, profiling a number of basic properties incorporated when the signature is generated;
2. T-Level, for Trusted time for signature existence conformance, profiling the generation, for an existing signature, of a trusted token allowing to prove that the signature itself actually existed at a certain date and time;
3. LT-Level, for Long Term conformance, profiling the incorporation of all the material required for validating the signature, to tackle the long term availability of such validation material;
4. LTA-Level, for Long Term with Archive time-stamps conformance, profiling the incorporation of time-stamp tokens that allow validation of the signature long time after its generation, to tackle the long term availability and integrity of the validation material.

All the requirements addressed at a certain level are always addressed also by the levels above. Each level requires the presence of certain properties, specified in each profile TS to reduce as much as possible the optionality. All the properties used in a signature profile for a given signature format are specified in the TS listed in 2.1 that specifies that format.

The specific level to be used depends on the period of time after signature creation for which technical validity of signature has to be preserved, taking into account certificate expiration, revocation and/or algorithm obsolescence. Each signature conformance level should be

[26] https://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=442
[27] All references to ETSI TS 103 171 in this document refer to version 2.1.1 available at: https://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/
[28] All references to ETSI TS 103 172 in this document refer to version 2.2.2 available at: https://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/
[29] All references to ETSI TS 103 173 in this document refer to version 2.2.1 available at: https://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60
[30] All references to ETSI TS 103 174 in this document refer to version 2.2.1 available at: https://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60

increased as needed to guarantee that the relying parties can always trust the signature. This process in called “signature augmentation”.

2.3 PUBLICATION OF THE ADES/ASIC ENS

The requirements for electronic signatures in the Signatures Directive and in the eIDAS Regulation are very similar. The difference between advanced electronic signatures and seals in the Regulation did not put any additional technical requirements on formats[31]. As part of the rationalization of the electronic signature standards, requested by the mandate M/460 published by the European Commission, all the technical specifications were restructured, and a set of European Standards (ENs) were developed. The aim of this exercise was to replace the previous Technical Specifications (TSs) limiting as much as possible the foreseen impact on existing implementations of the adoption of the new standards.

The development of ENs had a number of implications and resulted in:

- better guarantee of taking into account the market needs: a TS is approved in ETSI with a procedure that involves only the relevant Technical Committee, while an EN has additional steps, including one or more enquiry and weighted votes by the EU National Standardization Organizations (NSOs), guaranteeing a wider stakeholder involvement through national mirror committees. The AdES/ASiC ENs had undergone also a public review, required by the European Commission as part of mandate m/460, where all the stakeholders had the possibility to comment on the drafts. Reaching approval took significantly more time, as an EN should be published only when its content is mature enough, and, because of its nature, it does not require frequent changes;
- better support of the Digital Single Market: no national standard can be drafted by an European NSO if an EN exists or is under development on the same topic (i.e. the “standstill” applies). When the EN is approved, the existing national standards must be withdrawn.

AdES/ASiC ENs have been published by ETSI after throughful considerations, which included involved a far bigger representation of stakeholders than while drafting the previous TSs, approved at ETSI ESI TC level only. They reached unanimous approval at their final vote. It should also be noted that ETSI run regular Plugtests™, interoperability events conducted remotely, in order to prove interoperability of implementations and enhance standards robustness, either on CAdES/XAdES/PAdES/ASiC and on signature validation. Plugtests™ events use a dedicated portal developed by the ETSI independent testing unit CTI (Centre for Testing and Interoperability)[32].

Each EN in the signature format set of standards is divided into two parts, as follows:

- EN 319 122 “CAdES digital signatures”
  - Part 1: “Building blocks and CAdES baseline signatures”[33]
  - Part 2: “Extended CAdES signatures”[34]
- EN 319 132 “XAdES digital signatures”
  - Part 1: “Building blocks and XAdES baseline signatures” [35]

[31] See clause A.3 of this document for a short overview on advanced electronic signature and seal requirements
[32] See https://portal.etsi.org/Services/CentreforTestingInteroperability.aspx
[33] All references to ETSI EN 319 122-1 in this document refer to version 1.1.1 available at: https://www.etsi.org/deliver/etsi_en/319100_319199/31912201/01.01.01_60/
[34] All references to ETSI EN 319 122-2 in this document refer to version 1.1.1 available at: https://www.etsi.org/deliver/etsi_en/319100_319199/31912202/01.01.01_60/
[35] All references to ETSI EN 319 132-1 in this document refer to version 1.1.1 available at: https://www.etsi.org/deliver/etsi_en/319100_319199/31913201/01.01.01_60/

  - Part 2: “Extended XAdES signatures”[36]
- EN 319 142 “PAdES digital signatures”
  - Part 1: “Building blocks and PAdES baseline signatures” [37]
  - Part 2: “Extended PAdES signatures” [38]
- EN 319 162 “Associated Signature Containers (ASiC)”
  - Part 1: “Building blocks and ASiC baseline containers” [39]
  - Part 2: “Additional ASiC containers” [40]

All the AdES/ASiC ENs clearly delimit their scope to the technological level, i.e. digital signatures supported by PKI and public key certificates.

This approach allows keeping the legal details apart from the scope of a technical standard, to target the applicable technical requirements stemming from the eIDAS Regulation for both advanced electronic signatures and seals. In general, avoiding to have a strict link with legislation aims to make the standards more easily usable for the international community. More specifically, the AdES/ASiC ENs aim at supporting electronic signatures, advanced electronic signatures, qualified electronic signatures, electronic seals, advanced electronic seals, and qualified electronic seals as defined in the eIDAS Regulation.

This approach is fully in line with the eIDAS Regulation and its technical neutrality: in fact, the link between the Regulation and specific technologies that fulfil the requirements specified therein, is established only by the implementing acts.

Each first part the of the AdES/ASiC ENs specifies the “building blocks” for that signature format, then defines four levels of baseline signatures addressing incremental requirements to maintain the validity of the signatures over the long term, in a way that a given level always addresses all the requirements addressed at levels that are below.

Each level requires the presence of certain attributes, defined in the “building blocks” section, profiled for reducing any optionality as much as possible to maximise interoperability.

Each first part the of the AdES/ASiC ENs is then self-contained, including both – the basic information that was available in each format specifications (the ones listed in 2.1), and the baseline content that was specified in in the previous TSs. For example, in the current version of the Commission implementing Decision (EU) 2015/1506, a reference to ETSI TS 103 173 is given for the CMS advanced electronic signatures and seals. Then ETSI TS 103 173 references the ETSI TS 101 733 for the format itself, i.e. the parts that in EN 319 122-1 are specified for CAdES in the building blocks section. This allows an easier implementation, as all the required information for CAdES can be found in a single document, which helps avoiding mistakes in using the right version of the format specification.

All the second parts of the standards include the former additional forms present in the signature format TSs (listed in 2.1). Unless otherwise specified, in this document only the first Parts for each signature format EN are referenced.

[36] All references to ETSI EN 319 132-2 in this document refer to version 1.1.1 available at: https://www.etsi.org/deliver/etsi_en/319100_319199/31913202/01.01.01_60/
[37] All references to ETSI EN 319 142-1 in this document refer to version 1.1.1 available at: https://www.etsi.org/deliver/etsi_en/319100_319199/31914201/01.01.01_60/
[38] All references to ETSI EN 319 142-2 in this document refer to version 1.1.1 available at: https://www.etsi.org/deliver/etsi_en/319100_319199/31914202/01.01.01_60/
[39] All references to ETSI EN 319 162-1 in this document refer to version 1.1.1 available at: https://www.etsi.org/deliver/etsi_en/319100_319199/31916201/01.01.01_60/
[40] All references to ETSI EN 319 162-2 in this document refer to version 1.1.1 available at: https://www.etsi.org/deliver/etsi_en/319100_319199/31916202/01.01.01_60/

3. MOST SIGNIFICANT DIFFERENCES BETWEEN ADES/ASIC ENS AND PREVIOUS TSS

As explained in Section 2.3, the eIDAS Regulation relies on implementing acts to specify standards that complies with the requirements specified therein.

The repealed Electronic Signatures Directive did not use this mechanism, therefore the previous TSs had to reference explicitly the advanced electronic signatures, while the AdES/ASiC ENs can, more correctly, reference the specific technology (i.e. digital signature) on which they are based.

Below are listed the most important differences between each signature format standards and the corresponding previous TSs.

3.1 ETSI TR 119 112

ETSI published a Technical Report (ETSI TR 119 112) on “Most significant differences between AdES/ASiC ENs and previous TSs” that has been used to compile the paragraphs from 3.2 to 3.5 and covers specifically the technical differences between the formats specified in the previous TSs and the ones specified in the AdES/ASiC ENs. This is, in fact, an important element to consider to assess the impact of introducing the new standards and in defining a strategy to possibly replace the previous TSs, minimizing the impact on implementations.

Only the relevant parts of ETSI TR 119 112 were considered: as explained in 2.3, only first parts of each EN specifie the baseline signatures, which corresponds to the “baseline profiles” described in 2.2 and are referenced in the Decisions published by the Commission. As explained in the section dedicated to ASiC, in case of associated signatures and seals containers some of the baseline profiles present in ETSI TS 103 174 are not present in EN 319 162-1 but in EN 319 162-2, for this reason also the latter were taken into account.

3.2 XADES DIGITAL SIGNATURES

This paragraph uses the URI namespaces and the prefixes associated to these XML namespaces listed in Table 1.

Table 1: Namespaces with constant prefixes

XML Namespace URI	Prefix
http://www.w3.org/2000/09/xmldsig#	ds
http://uri.etsi.org/01903/v1.3.2#	xades
http://uri.etsi.org/01903/v1.4.1#	xadesv141

The main differences of ETSI EN 319 132-1 in comparison to ETSI TS 101 903 and ETSI TS 103 171 are:

- Specification of the new qualifying properties for them to replace in the future the qualifying properties that had been specified by ETSI TSs.
- Specification of the new qualifying properties, with semantics that none of the qualifying properties already specified by ETSI TSs did not offer.
- Clarification of the semantics of certain qualifying properties already specified within the different ETSI TSs.
- Definition of a new set of signature levels specified in ETSI EN 319 132-1 that comes from the revision of the baseline signatures defined in ETSI TS 103 171.
- Redistribution of material:
  - ETSI EN 319 132-1 contains the definition of the semantics and the syntax of the new set of XAdES qualifying properties, and the specification of the XAdES baseline signature levels.
  - ETSI TS 101 903 contains the definition of the semantics and the syntax of all the previous set of XAdES qualifying properties.
  - ETSI TS 103 171 contains the specification of levels for XAdES baseline signatures old formats.

The following clauses will provide further details on some of the aforementioned changes.

3.2.1 New qualifying properties substituting previously defined ones

The XML Signature W3C Recommendation, which specifies the semantics and syntax of XML signatures, on which XAdES signatures are built, deprecated an element which was used in ETSI TS 101 903 and ETSI TS 103 171, namely the `ds:X509IssuerSerial` element, due to reported problems by XML validators when dealing with very high integer values. Indeed, the problem was not related to the specification of the element, but a problem of implementations of certain XML validators.

As has been mentioned, a number of qualifying properties specified in ETSI TS 101 903 contained the aforementioned element.

ETSI TC ESI decided not to keep in its new specifications an element that XML Signature W3C Recommendation had labelled as deprecated. This forced to define new XAdES qualifying properties for substituting:

1) all the previously defined ones containing the ds:X509IssuerSerial element; and
2) any previously defined qualifying property whose semantics depended on the properties included in bullet 1).

Table 2 shows the XAdES qualifying properties specified in the ETSI TS 101 903 and the new ones specified by ETSI EN 319 132-1.

Table 2: ETSI EN 319 132-1 new qualifying XAdES properties replacing ETSI TS 101 903 XAdES qualifying properties due to deprecation of ds:X509IssuerSerial in XML Signature W3C Recommendation

New XAdES qualifying properties specified in ETSI EN 319 132-1	XAdES qualifying properties specified in ETSI TS 101 903 replaced by the former ones
`xades:SigningCertificateV2`	`xades:SigningCertificate`
`xadesv141:CompleteCertificateRefsV2`	`xades:CompleteCertificateRefs`
`xadesv141:AttributeCertificateRefsV2`	`xades:AttributeCertificateRefs`
`xadesv141:SigAndRefsTimeStampV2`	`xades:SigAndRefsTimeStamp`
`xadesv141:RefsOnlyTimeStampV2`	`xades:RefsOnlyTimeStamp`
`xades:SignatureProductionPlaceV2`	`xades:SignatureProductionPlace`

Qualifying properties `xades:SigningCertificate`, `xades:CompleteCertificateRefs`, and `xades:AttributeCertificateRefs` included `ds:X509IssuerSerial` as component.

In these components, the deprecated `ds:X509IssuerSerial` element was replaced by the so-called `xades:IssuerSerialV2` element, which contains the base-64 encoding of one DER-encoded instance of type `IssuerSerial` type defined in IETF RFC 5035. In essence it contains the same information than the `ds:X509IssuerSerial` but in its original encoding within the X509 certificate, which first, keeps the information, and second, avoids any problem appearing by the conversion of a Distinguished Name into a String.

In addition to this, ETSI EN 319 132-1 clearly specifies that this new element is "only a hint, that can help to identify the certificate whose digest matches the value present in the reference. But the binding information is the digest of the certificate", which clearly states that applications cannot rely on this value for matching a reference to the purportedly referenced certificate. Instead, they are required to use the digest value. This was not stated in ETSI TS 101 903 nor in ETSI TS 103 171.

Qualifying properties `xades:SigAndRefsTimeStamp` and `xades:RefsOnlyTimeStamp` depended on some of the properties in the list before.

Table 3 shows new XAdES qualifying properties specified in ETSI EN 319 132-1, some of which replace already existing XAdES qualifying properties specified in ETSI TS 101 903, for the reasons explained in the table, others just allow to incorporate new features into the XAdES signatures.

Table 3: Additional ETSI EN 319 132-1 new qualifying XAdES properties

New XAdES qualifying properties specified in ETSI EN 319 132-1	XAdES qualifying properties specified in ETSI TS 101 903 replaced by the former ones	Reason for replacement OR for their incorporation (if they do not replace none in ETSI TS 101 903)
`xades:SignatureProductionPlaceV2`	`xades:SignatureProduction Place`	Add new element for including the street address.
`xades:SignerRoleV2`	`xades:SignerRole`	Add new element able to contain signed assertions. This would be signed by a third party, stronger than claimed assertions but less restrictive than attribute certificates. Add new element able to contain not only X509 attribute certificates but any hypothetical attribute certificate in a different format.
`xadesv141:SignaturePolicyStore`	--	Allow incorporating the full signature policy document, not only its identifier and a pointer to the location where this signature policy document is stored. For self-contained long-lasting signatures in prevision of difficulties to access to the signature policy location.
`xadesv141:RenewedDigests`	--	For countering the risk of break of digests used in computation of archive time-stamp tokens on signed data objects that are detached of the XAdES signature. This property forces the computation of the digest of such objects with a different algorithm to the one that is suspected to be broken soon.

3.2.2 Clarification of qualifying properties semantics

The semantics of a number of qualifying properties (listed in Table 4) have been clarified. Most of these properties either contained validation material (certificates, CRLs, OCSP responses), or references to this kind of validation material.

In most cases the clarification consisted in describing which specific validation values, or references to the validation values, may be present in each qualifying property.

Table 4: Qualifying XAdES properties whose semantics has been clarified

XAdES qualifying properties whose semantics has been clarified	Clauses in ETSI EN 319 132-1
`xades:CertificateValues`	5.4.1
`xades:RevocationValues`	5.4.2
`xades:AttrAuthoritiesCertValues`	5.4.3
`xades:AttributeRevocationValues`	5.4.4
`xades:CompleteRevocationRefs`	A.1.2
`xades:AttributeRevocationRefs`	A.1.4

3.2.3 New set of levels

ETSI EN 319 132-compliant signature levels differentiate from the ETSI TS 103 171-compliant XAdES baseline signatures. ETSI EN 319 132-1 in fact defines a set of levels replacing XAdES baseline signatures specified in ETSI TS 103 171, as indicated in Table 5.

Table 5: Correspondence between levels in ETSI EN 319 132-1 and XAdES baseline signatures in ETSI TS 103 171

New levels specified in ETSI EN 319 132-1	XAdES baseline signatures in ETSI TS 103 171
`XAdES-B-B`	`XAdES-B-Level`
`XAdES-B-T`	`XAdES-T-Level`
`XAdES-B-LT`	`XAdES-LT-Level`
`XAdES-B-LTA`	`XAdES-LTA-Level`

3.3 CADES DIGITAL SIGNATURES

The main differences of ETSI EN 319 122-1 in comparison to ETSI TS 101 733 and ETSI TS 103 173 are:

- Specification of new attributes to replace in the future attributes that had been specified by ETSI TSs.
- Specification of new attributes, with semantics that the attributes already specified by ETSI TSs did not offer.
- Clarification of the semantics of certain attributes already specified within the different ETSI TSs.
- Deprecation of a number of attributes specified in ETSI TS 101 733.
- Definition of a new sets of signature levels specified in ETSI EN 319 122-1 that come from the revision of the baseline signatures defined in ETSI TS 103 173.
- Redistribution of material:
    - ETSI EN 319 122-1 contains the definition of the semantics and the syntax of the new set of CAdES attributes, and the specification of the CAdES baseline signature levels.
    - ETSI TS 101 733 contains the definition of the semantics and the syntax of all the previous set of CAdES attributes.
    - ETSI TS 103 173 contains the specification of levels for CAdES baseline signatures old formats.

The following clauses provide further details on some of the aforementioned changes.

3.3.1 New attributes substituting previously defined ones

Table 6 shows new CAdES attributes specified in ETSI EN 319 122-1: some of them also replace already existing CAdES attributes specified in ETSI TS 101 733, for the reasons explained in the table, others just allow to incorporate new features into the CAdES signatures.

Table 6: Additional ETSI EN 319 122-1 new qualifying CAdES properties

New CAdES attributes specified in ETSI EN 319 122-1	CAdES attributes specified in ETSI TS 101 733 replaced by the former ones	Reason for replacement OR for their incorporation (if they do not replace none in ETSI TS 101 733)
`signer-attributes-v2`	`signer-attributes`	Add new element able to contain signed assertions. This would be signed by a third party, stronger than claimed assertions but less restrictive than attribute certificates. Add new element able to contain not only X509 attribute certificates but any hypothetical attribute certificate in a different format.
`signature-policy-store`	--	Allow incorporating the full signature policy document, not only its identifier and a pointer to the location where this signature policy document is stored. For self-contained long-lasting signatures in prevision of difficulties to access to the signature policy location.
`ats-hash-index-v3`	`ats-hash-index`	Allow or addition of a value within the set of values in `Attribute.attrValues` field within a certain attribute after the already present values within the aforementioned set had been time-stamped by a former `archive-time-stamp-v3`. This is achieved by computing digests on octets "resulting from concatenating the `Attribute.attrType` field and one of the instances of `AttributeValue` within the `Attribute.attrValues` within the `unsignedAttrs` field". It is worth to mention that `ats-hash-index` attribute is not used in any of the signature profiles that are mentioned in the Commission Implementing Decision (EU) 2015/1506.
`SigPolicyQualifierInfo in signature-policy-identifier`	`SigPolicyQualifierInfo in signature-policy-identifier`	A third and new qualifier for the signature policy have been identified so far: an identifier of the technical specification that defines the syntax used for producing the signature policy document (an element of type SPDocSpecification).

3.3.2 Clarification of attributes semantics

A relevant effort was made by the ETSI TC ESI in clarifying the semantics of a number of attributes. Most of these properties either contained validation material (certificates, CRLs, OCSP responses) or references to this kind of validation material.

In most cases the clarification consisted in describing which specific validation values, or references to which validation values may be present in each attribute.

It is worth mentioning that none of the attributes listed in Table 7 is used in any of the levels that were mentioned in the Commission Implementing Decision (EU) 2015/1506.

Table 7: Qualifying CAdES properties whose semantics has been clarified

CAdES attributes whose semantics has been clarified	Clauses in ETSI EN 319 122-1
`certificate-values`	A.1.1.2
`revocation-values`	A.1.2.2
`complete-certificate-references`	A.1.1.1
`complete-revocation-references`	A.1.2.1
`attribute-certificate-references`	A.1.3
`attribute-revocation-references`	A.1.4
These attributes are not part of the signature profiles mentioned in the Commission Implementing Decision (EU) 2015/1506.	

In addition to this ETSI EN 319 122-1 clearly specifies that its `IssuerSerial` component of ESS `signing-certificate-v2` attribute is "only a hint, that can help to identify the certificate whose digest matches the value present in the reference. But the binding information is the digest of the certificate", which clearly states that applications cannot rely on this value for matching a reference to the purportedly referenced certificate; instead, they are required to use the digest value. This was not stated in ETSI TS 101 733 nor ETSI TS 103 173.

3.3.3 Deprecated attributes

Table 8 shows the attributes deprecated by ETSI EN 319 122-1.

Table 8: Attributes deprecated by ETSI EN 319 122-1

`other-signing-certificate`
`signer-attributes`
`archive-time-stamp (ATSv2)`
`long-term-validation`
`ats-hash-index`
`time-mark`
These attributes are not part of the signature profiles mentioned in the Commission Implementing Decision (EU) 2015/1506.

3.3.4 New sets of levels

ETSI EN 319 122-compliant signatures levels are differentiated from ETSI TS 103 171-compliant CAdES baseline signatures. ETSI EN 319 122-1 defines a set of levels replacing levels specified in ETSI TS 103 173 as indicated in Table 9.

Table 9: Correspondence between levels in ETSI EN 319 122-1 and CAdES baseline signatures in ETSI TS 103 173

New levels specified in ETSI EN 319 122-1	Levels in ETSI TS 103 173
CAdES-B-B	CAdES-B-Level
CAdES-B-T	CAdES-T-Level
CAdES-B-LT	CAdES-LT-Level
CAdES-B-LTA	CAdES-LTA-Level

3.4 PADES DIGITAL SIGNATURES

The main differences of ETSI EN 319 142-1 in comparison to ETSI TS 102 778 and ETSI TS 103 172 are:

- Specification of new attributes to replace in the future attributes that had been specified by ETSI TSs.
- Clarification of the usage and encoding of certain attributes already specified within the different ETSI TSs whenever ETSI ESI considered worth to implement such clarifications.
- Deprecation of a number of attributes specified in ETSI TS 102 778.
- Definition of a new set of signature levels specified in ETSI EN 319 142-1 that comes from the revision of the baseline signatures defined in ETSI TS 103 172.
- Redistribution of material:
    - ETSI EN 319 142-1 contains the definition of the semantics and the syntax of the new set of PAdES attributes, and the specification of the PAdES baseline signature levels.
    - ETSI TS 102 778 contains the definition of the semantics and the syntax of all the previous set of PAdES attributes.
    - ETSI TS 103 172 contains the specification of levels for PAdES baseline signatures old formats.
    - ETSI TS 102 778-1 contains an overview of the set of profiles for PDF Advanced Electronic Signatures specified in the other ETSI TS 102 778 parts. Its content was not included in ETS EN 319 142.
    - ETSI TS 102 778-6 contains recommendations for the visual representations of advanced electronic signatures (AdES) in PDFs. Its content was not included in ETSI EN 319 142.

The following clauses provide further details on some of the aforementioned changes.

3.4.1 New attributes substituting previously defined ones

Table10 shows a new attribute whose usage is specified in ETSI EN 319 142-1. It replaces an already existing CAdES attribute specified in ETSI TS 101 733. It may be present in the DER-encoded SignedData object included as the PDF signature in the entry with the key Contents of the Signature Dictionary, by reasons explained in Table 10.

Table 10: Additional ETSI EN 319 142-1 new qualifying PAdES properties

New PAdES attributes specified in ETSI EN 319 142-1	PAdES attributes specified in ETSI TS 102 778 replaced by the former ones	Reason for replacement OR for their incorporation
`signer-attributes-v2`	`signer-attributes`	Add new element able to contain signed assertions. This would be signed by a third party, stronger than claimed assertions but less restrictive than attribute certificates. Add new element able to contain not only X509 attribute certificates but any hypothetical attribute certificate in a different format.

3.4.2 Clarification of attributes usage and encoding

A relevant effort was made by ETSI TC ESI in clarifying the usage and encoding of a number of attributes, listed in Table 11. Most of these properties either contained information provided by the signer to enable a recipient to identify or contact the signer itself, or explained the reasons for the signing or properties that contain validation material (certificates, CRLs, OCSP responses).

Most of the times the clarification consisted in describing when specific attributes may be present in the PAdES signature.

Table 11: Qualifying PAdES properties whose usage and encoding has been clarified

PAdES attributes whose usage and encoding has been clarified	Clauses in ETSI EN 319 142-1
`Filter`	6.3
`Location`	6.3
`Name`	6.3
`ContactInfo`	6.3
`Reason`	6.3
`commitment-type-indication`	6.3
`Certs (DSS Dictionary)`	5.4.2.2
`OCSPs (DSS Dictionary)`	5.4.2.2
`CRLs (DSS Dictionary)`	5.4.2.2
`Cert (VRI Dictionary)`	5.4.2.3
`CRL (VRI Dictionary)`	5.4.2.3
`OCSP (VRI Dictionary)`	5.4.2.3

3.4.3 Deprecated attributes

Table 12 shows the attributes deprecated by ETSI EN 319 142-1.

Table 12: Attributes deprecated by ETSI EN 319 142-1

signer-attributes
time-mark

3.4.4 New set of levels

ETSI EN 319 142-compliant PAdES signatures levels are differentiated from ETSI TS 103 172-compliant PAdES baseline signatures. ETSI EN 319 142-1 defines a set of levels replacing levels specified in ETSI TS 103 172, as indicated in Table 13.

Table 13: Correspondence between levels in ETSI EN 319 142-1 and levels in ETSI TS 103 172 (PAdES baseline signatures)

New levels specified in ETSI EN 319 122-1	Levels in ETSI TS 103 173
PAdES-B-B	PAdES-B-Level
PAdES-B-T	PAdES-T-Level
PAdES-B-LT	PAdES-LT-Level
PAdES-B-LTA	PAdES-LTA-Level

3.5 ASIC CONTAINERS

The main differences of ETSI EN 319 162-1 in comparison to ETSI TS 102 918 and ETSI TS 103 174 are:

- Updated reference to ETSI EN 319 122-1 instead of ETSI TS 101 733 and ETSI TS 103 173 for ASiC containers based on CAdES. See clause 3.3 of this document for specific information about differences related to CAdES standards.
- Updated reference to ETSI EN 319 132-1 instead of ETSI TS 101 903 and ETSI TS 103 171 for ASiC containers based on XAdES. See clause 3.2 of this document for specific information about differences related to XAdES standards.
- Definition of a new set of baseline container levels specified in ETSI EN 319 162-1 from the revision of a subset of ASiC profiles defined in ETSI TS 103 174; the ASiC profiles that were not included among the ASiC baseline containers have been specified in ETSI EN 319 162-2 as additional profiles
- Support of IETF RFC 4998 and IETF RFC 6283 evidence records in ETSI EN 319 162-1 building blocks (this affects only additional profiles specified in ETSI EN 319 162-2).
- Introduction of new specific Manifest files for long term availability for containers types where this feature cannot be achieved with direct use of signature or time assertion formats attributes/qualifying properties (this affects only additional profiles specified in ETSI EN 319 162-2).
- Clarification of text to eliminate ambiguities.

3.5.1 New set of container levels

ETSI EN 319 162-1 defines a set of baseline container levels replacing a subset of container profiles specified in ETSI TS 103 174 as indicated in Table 14. ETSI TS 103 174 is referenced by the Commission Implementing Decision (EU) 2015/1506.

It should be noted that ETSI TS 103 174 specifies baseline profiles also for ASiC-S with Time stamp token, ASiC-E with CAdES and ASiC-E with Time stamp token that have no correspondence in ETSI EN 319 162-1 but are present as extended containers in ETSI EN 319 162-2.

In case of the containers meant to associate data with time-stamp tokens (ASiC-S with Time stamp token and ASiC-E with Time stamp token) they cannot be considered as associated electronic signature or seal containers and therefore they are out of scope of the decisions 2015/1506 and 2011/130/EU. In the case of ASiC-E with CAdES, given the feedback received during the consultations that was in the direction to simplify and reduce the number of containers, ETSI ESI TC decided to not include it among the baseline containers.

Table 14: Correspondence between levels in ETSI EN 319 162-1 and ASiC baseline containers in ETSI TS 103 174

New levels specified in ETSI EN 319 162-1	ASiC baseline containers in ETSI TS 103 174
ASiC-S with CAdES B-B level	ASiC-S with CAdES B-Level
ASiC-S with XAdES B-B level	ASiC-S with XAdES B-Level
ASiC-E with XAdES B-B level	ASiC-E with XAdES B-Level
ASiC-S with CAdES B-T level	ASiC-S with CAdES T-Level
ASiC-S with XAdES B-T level	ASiC-S with XAdES T-Level
ASiC-E with XAdES B-T level	ASiC-E with XAdES T-Level
ASiC-S with CAdES B-LT level	ASiC-S with CAdES LT-Level
ASiC-S with XAdES B-LT level	ASiC-S with XAdES LT-Level
ASiC-E with XAdES B-LT level	ASiC-E with XAdES LT-Level
ASiC-S with CAdES B-LTA level	ASiC-S with CAdES LTA-Level
ASiC-S with XAdES B-LTA level	ASiC-S with XAdES LTA-Level
ASiC-E with XAdES B-LTA level	ASiC-E with XAdES LTA-Level

3.5.2 Evidence records

ETSI EN 319 162-1 building blocks use the term "Time Assertion" to encompass both time stamp tokens and evidence records as specified in IETF RFC 4998 and IETF RFC 6283.

Evidence records are also supported in ASiC manifest files allowing to specify the data object(s) to which the evidence records apply.

Evidence records are not used in ASiC baseline containers specified in ETSI EN 319 162-1.

3.5.3 New ASiC Manifest files for long term availability

ASiCArchiveManifest was added to protect long term time stamp tokens and ASiCEvidenceRecordManifest was added to reference a set of files to which an evidence record applies, allowing an LTA equivalent level also for ASiC containers with time assertions.

ASiC Manifest files are not used in ASiC baseline containers specified in ETSI EN 319 162-1.

4. CONCLUSIONS

4.1 OPPORTUNITY AND SUITABILITY TO REFERENCE THE ADES/ASIC ENS

The signature format TSs were introduced when the Electronic Signatures Directive was in force. Given the similar requirements for the signature formats in the Directive and in the Regulation, and for both, advanced electronic signatures and seals, the profiles published by ETSI in 2012 (i.e. the previous TSs) are still usable today.

In April 2016 ETSI has published an updated set of European standards (the AdES/ASiC ENs). The European Norms have a much higher stability and value in the standardization document hierarchy and they guarantee that no other national standard can be developed or adopted overlapping the ones developed by ETSI for electronic signature and seal formats based on CMS, XML and PDF and for Associated signature and seal containers. As explained in 2.3 the process included a public review (in addition to the enquiry stage already part of the ETSI process) and Plugtests™ that led to changes that improved interoperability (also improving the text where it could not be interpreted unambiguously by implementors), eliminated technical flaws and provided new features proposed during the drafting and the approval process of the ENs.

The extensive experience of ETSI TC ESI in developing standards for electronic signatures is also a guarantee for the quality of the standards, and for their sustainability and maintenance.

It should also be noted that even if the Commission Implementing Decision (EU) 2015/1506 applies only to the public sector, the standards listed become a reference also for the private sector: this is an additional reason for updating the Decision, otherwise also the private sector adoption of the standards could be compromised. ETSI TC ESI in fact developed a comprehensive framework of standards supporting electronic signatures and seals and eIDAS trust services: it is therefore important that the referenced standards take into account the evolution of the framework, to maximize the benefits for all the actors involved. Signature format standards are in fact cross referenced by many other standards.

Moreover, the CEF e-signature building block is based on the AdES/ASiC ENs[41] and funded already a number of projects that implemented it. This means on one hand that a number of implementations based on the AdES/ASiC ENs already exist and the public and private sector organizations that participated (or are participating) to CEF projects are ready to use the new AdES/ASiC ENs. On the other hand there is a risk that the positive effect expected from these funding measures is reduced, in case the references to the signature format standards are not updated.

Also the Commission Decision 2011/130/EU should be considered for update. In fact the recital 8 of the eIDAS Regulation says that “Directive 2006/123/EC of the European Parliament and of the Council (5) requires Member States to establish ‘points of single contact’ (PSCs) to ensure that all procedures and formalities relating to access to a service activity and to the exercise thereof can be easily completed, at a distance and by electronic means, through the appropriate PSC with the appropriate authorities. Many online services accessible through PSCs require electronic identification, authentication and signature.” Keeping the Decisions

[41] See https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature+standards for more information

2015/1506 and 2011/130/EU not aligned would result in additional complexity,especially for the public sector.

The Commission Decision 2011/130/EU is also referenced in the article 22(6)(c)(i) of the Directive 2014/24/EU on public procurement[42], in case a contracting entity requires advanced electronic signatures supported by a qualified certificate for the electronic transmission and receipt of tenders, and for the electronic receipt of requests to participate. Lack of alignment of the Decisions 2015/1506 and 2011/130/EU can introduce additional costs to both, the private and he public sectors.

Specific consideration is reserved to the ASiC. As explained in 3.5.1, ETSI EN 319 162-1 clause 5 does not include some of the profiles specified in TS 103 174, referenced by decisions 2015/1506 and 2011/130/EU, namely:

- ASiC-S Time stamp token and ASiC-E Time stamp token, as these were not specifying associated signature or seal but associate containers with time-stamp tokens;
- ASiC-E CAdES, as there was no evidence for its adoption and this was considered to be in contrast with the principle of maximum reduction of options present in the mandate.

In case it is agreed to include also these containers in the update of decisions 2015/1506 and/or 2011/130/EU, then specific clauses of ETSI EN 319 162-2 can be introduced according to the specific need. In order to avoid putting excessive requirements on the public services, it is however recommended to avoid or to limit referencing the ETSI EN 319 162-2 unless there is a clear evidence that the containers now moved in this part of the standard have been adopted by a high number of public services, and to deprecate the creation of ASiC containers compliant with the profiles listed above.

The European Commission is then advised to revise its Decisions 2015/1506 and 2011/130/EU, referencing the new ENs and taking into account a transition period to allow to update the software involved and to migrate the applications, as proposed in the next paragraph.

Reference should be made to ETSI EN 319 122-1 clause 6, ETSI EN 319 132-1 clause 6, ETSI EN 319 142-1 clause 6 where the baseline signatures are specified and ETSI EN 319 162-1 clause 5 where baseline containers are specified.

4.2 POSSIBLE WAY FORWARD MINIMIZING IMPACT

The previous paragraph is focused on the reasons for updating decisions 2015/1506 and 2011/130/EU. This has of course an impact that needs to be minimized.

The following measures should be considered by the Commission to reduce the impact of updating the references:

- defining, with member States, an appropriate update path. Some advice is given hereafter;
- stimulate the process with specific funding measures, such as CEF, the adoption of the CEF eSignature building blocks. This should be possible until the end of 2020 when the CEF initiative is expected to terminate;

[42] Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0024

- take benefit from the execution of ETSI Plugtests™: the next edition for electronic signature validation is foreseen in November 2019.

The update path to be adopted should avoid any discontinuity and minimize the impact on provision of services by allowing enough time to implement the changes, but also to foresee a period of time of parallel use of the new AdES/ASiC ENs standards with the previous TSs.

The number of technical differences is quite limited and new attributes are designed in a way that they can be implemented in parallel with the old ones.

Therefore, a possible way forward could be:

- To establish a first deadline to:
  - mandate acceptance of the new AdES/ASiC ENs standards, in parallel with the previous TSs;
  - recommend the use the new AdES/ASiC ENs standards to create signatures.
- Optionally, to establish a second deadline to deprecate the creation of signatures with the previous TSs;
- To establish a final deadline, after which previous TSs shall not be accepted any more. This final deadline should be chosen by balancing the time needed to introduce the new standards when creating signatures and the cost of maintaining implementations supporting both the new AdES/ASiC ENs standards and the previous TSs.

It should be noted that ETSI will not deprecate the previous TSs, unless serious flaws are identified. This situation is not likely to happen, given the long time when the standards where tested and widely adopted.

ETSI could give a “historical” status to the previous TSs after the last deadline is passed, as it was the case for other standards changed or replaced in frame of the mandate M/460. This would give a clear message to the market and all the stakeholders to use only the new AdES/ASiC ENs standards.

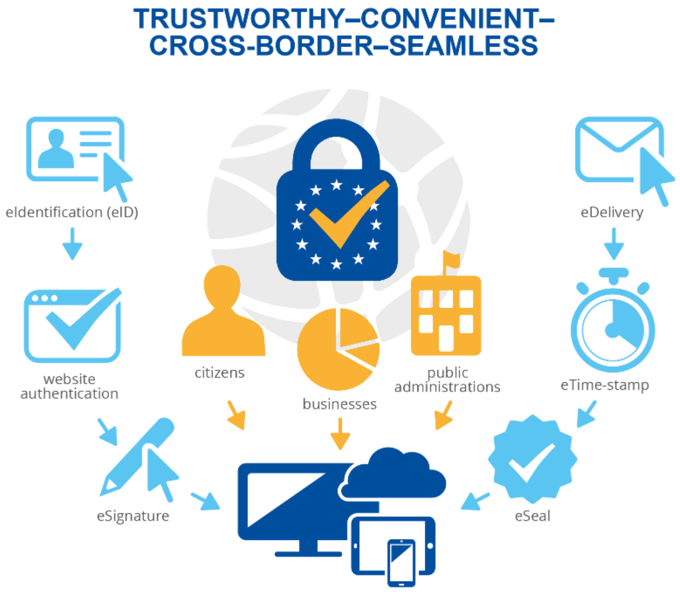
ANNEX A: BASIC CONCEPTS

A.1 GENERAL CONTEXT: THE EIDAS REGULATION AND TRUST SERVICES

eIDAS is the acronym used to refer to Regulation (EU) No 910/2014 on electronic identification (eID) and trust services for electronic transactions in the internal market. The eIDAS Regulation is about trust, seamless user experience and convenience in online cross-border transactions.

It is possible to use those trust services as well as electronic documents as evidence in legal proceedings in all EU Member States contributing to their general cross-border use. Courts (or other bodies in charge of legal proceedings) cannot discard them as evidence only because they are electronic but have to assess these electronic tools in the same way they would do for their paper equivalent.

Figure 15: Trustworthy-Convenient-Cross-Border-Seamless



Whether you are a large company, a SME or a citizen trying to complete an electronic transaction in another EU country, e.g. submit a call for tender or register as a student in another EU Member State (MS), besides reducing time and costs, the eIDAS Regulation ensure cross-border recognition of electronic trust services supporting your electronic transaction.

Since 1 July 2016, the eIDAS Regulation provisions related to trust services are directly applicable in all the EU Member States overcoming problems of fragmented national regimes. It provides legal certainty and fosters the usage of electronic trust services for online transactions at EU level.

The eIDAS Regulation creates an EU wide internal market for electronic trust services by ensuring their recognition and workability across borders and are considered equivalent to traditional paper-based processes.

A.2 TRUST SERVICES DEFINED BY THE EIDAS REGULATION

In its Art.3.16, the eIDAS Regulation defines a 'trust service' as an electronic service normally provided for remuneration, which consists of:

- the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
- the creation, verification and validation of certificates for website authentication; or
- the preservation of electronic signatures, seals or certificates related to those services.

A.3 ADVANCED ELECTRONIC SIGNATURES AND SEALS

An advanced electronic signature meets the requirements specified in article 26 of the eIDAS Regulation, namely:

- it is uniquely linked to the signatory;
- it is capable of identifying the signatory;
- it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
- it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

It should be noted that the requirements on advanced electronic signatures in the eIDAS Regulation does not introduce new requirements in terms of format with regard to the former Electronic Signatures Directive[43]. For this reason, the previous TSs, developed while the Directive was in force, continued to be usable without change when the eIDAS Regulation become applicable.

An advanced electronic seal meets the requirements specified in article 36 of the eIDAS Regulation, namely:

- it is uniquely linked to the creator of the seal;
- it is capable of identifying the creator of the seal;
- it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and
- it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.

The requirements in terms of signature/seal format are part of points a, b and d (for both the lists above) and remained unchanged from the Electronic Signatures Directive.

All the ETSI signatures and seal format standards (old and new) are based on PKI, a specific technology. This is not the only possible technical way to achieve the advanced electronic signature or seal level, but it is the only technology that allow full interoperability thanks to a complete set of standards. Electronic signatures and seals based on different technologies and on commonly recognized standards are therefore not presently possible. Moreover, no other technology is known to achieve the qualified level for advanced electronic signatures and seals.

[43] Directive 1999/93/EC, article 2(2) reads: "advanced electronic signature" means an electronic signature which meets the following requirements:
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control; and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

However, in case this will change in the future, the eIDAS Regulation is technologically neutral and foresee the possibility, by updating the implementing acts, to reference new standards implementing technologies that could emerge in the future.

ANNEX B: GLOSSARY

ENISA – European Union Agency for Cybersecurity

ETSI – European Telecommunications Standards Institute

ETSI TC ESI - ETSI Technical Committee for Electronic Signatures and Infrastructures

eIDAS – Regulation (EU) No 910/2014 on electronic identification (eID) and trust services for electronic transactions in the internal market

Electronic Signatures Directive – Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures

Services Directive – Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market

TSs – Technical Specifications

ENs – European Norms

AdES – Advanced Electronic Signature

XAdES – XML Advanced Electronic Signature

CAdES – CMS Advanced Electronic Signature

PAdES – PDF Advanced Electronic Signature

ASiC – Associated Signature Container

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu