ČESKÁ TECHNICKÁ NORMA

ICS 35.240.30 **Říjen 2016**

Elektronické podpisy a infrastruktury (ESI) – Postupy pro vytváření a ověřování platnosti digitálních podpisů AdES –
Část 1: Vytváření a ověřování platnosti

ČSN
ETSI EN 319 102-1
V1.1.1
87 4017

Electronic Signatures and Infrastructures (ESI) – Procedures for Creation and Validation of AdES Digital Signatures –
Part 1: Creation and Validation

Tato norma přejímá anglickou verzi evropské normy ETSI EN 319 102-1 V1.1.1:2016. Má stejný status jako
oficiální verze.

This standard implements the English version of the European Standard ETSI EN 319 102-1 V1.1.1:2016. It has the same status as the official version.

Anotace obsahu

Tento dokument stanovuje postupy pro:

- vytváření digitálních podpisů AdES (specifikovaných v ETSI EN 319 122-1, ETSI EN 319 132-1, ETSI EN 319 142-1);
- prokazování toho, zda je digitální podpis AdES technicky platný;

pokud je digitální podpis AdES založen na kryptografii s veřejným klíčem a podporován certifikáty veřejného klíče.

Nařízení EU č. 910/2014 definuje termíny elektronický podpis, zaručený elektronický podpis, elektronická pečeť a zaručená elektronická pečeť. Tyto podpisy a pečeti jsou obvykle vytvářeny pomocí technologie digitálních podpisů. Tento dokument se zaměřuje na podporu nařízení EU č. 910/2014 pro vytváření a ověřování platnosti zaručených elektronických podpisů a pečetí, pokud jsou tyto implementovány jako digitální podpisy AdES.

Tento dokument zavádí obecné zásady, objekty a funkce důležité při vytváření nebo ověřování platnosti podpisů na základě omezení při vytváření a ověřování platnosti podpisů a definuje obecné třídy podpisů, které umožňují dlouhodobou ověřitelnost.

Národní předmluva

Informace o citovaných dokumentech

IETF RFC 5280 nezavedena

ISO/IEC 9594-8:2014 nezavedena

IETF RFC 3161 nezavedena

ETSI TS 119 172-1 nezavedena

Společné specifikace PKI pro interoperabilní aplikace od T7 & Teletrust, specifikace část 9 SigG-profil, verze 2.0:2009 nezavedena

IETF RFC 4158 nezavedena

ETSI EN 319 122-1 zavedena v ČSN ETSI EN 319 122-1 V1.1.1 (87 4013) Elektronické podpisy a infrastruktury (ESI) – Digitální podpisy CAdES – Část 1: Stavební bloky a základní podpisy CAdES

ETSI EN 319 122-2 zavedena v ČSN ETSI EN 319 122-2 V1.1.1 (87 4013) Elektronické podpisy a infrastruktury (ESI) – Digitální podpisy CAdES – Část 2: Rozšířené podpisy CAdES

ETSI EN 319 132-1 zavedena v ČSN ETSI EN 319 132-1 V1.1.1 (87 4015) Elektronické podpisy a infrastruktury (ESI) – Digitální podpisy XAdES – Část 1: Stavební bloky a základní podpisy XAdES

ETSI EN 319 132-2 zavedena v ČSN ETSI EN 319 132-2 V1.1.1 (87 4015) Elektronické podpisy a infrastruktury (ESI) – Digitální podpisy XAdES – Část 2: Rozšířené podpisy XAdES

ETSI EN 319 142-1 zavedena v ČSN ETSI EN 319 142-1 V1.1.1 (87 4014) Elektronické podpisy a infrastruktury (ESI) – Digitální podpisy PAdES – Část 1: Stavební bloky a základní podpisy PAdES

ETSI EN 319 142-2 zavedena v ČSN ETSI EN 319 142-2 V1.1.1 (87 4014) Elektronické podpisy a infrastruktury (ESI) – Digitální podpisy PAdES – Část 2: Dodatečné profily podpisů PAdES

IETF RFC 5652 nezavedena

IETF RFC 4998 nezavedena

IETF RFC 6283 nezavedena

IETF RFC 6960 nezavedena

ETSI EN 319 422 zavedena v ČSN ETSI EN 319 422 V1.1.1 (87 4012) Elektronické podpisy a infrastruktury (ESI) – Protokol pro vyznačení času a profily časového razítka

ECRYPT II Roční zpráva o algoritmech a velikostech klíčů, revize 1.0:2011 nezavedena

IETF RFC 3852 nezavedena

POZNÁMKA Pokud jsou v originálu normy citovány nezaváděné dokumenty ETR, TBR, ES, EG, TS, TR a GSM, jsou dostupné v Informačním centru ÚNMZ.

Vypracování normy

Zpracovatel: MAREŠKA Praha, IČ 86983555, Ing. Antonín Mareška

Technická normalizační komise: TNK 96 Telekomunikace

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Jan Křivka