BDOC
Format for digital signatures

BDOC
Digitaalallkirja vorming

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

NATIONAL FOREWORD

This Estonian standard

— is the identical English version of the Estonian Standard EVS 821:2014 and it has the same status as the original Estonian version. In case of interpretation disputes the original version applies;

— has been endorsed with a notification published in the June 2014 issue of the official bulletin of the Estonian Centre for Standardisation.

The proposition to prepare this standard has been presented by Technical Committee EVS/TK 4 “Information technology”, it has been coordinated by the Estonian Centre for Standardisation.

The standard and its English translation have been prepared by Certification Centre Ltd. (AS Sertifitseerimiskeskus) and the standard has been approved by EVS/TK 4.

This document is a revision of EVS 821:2009.

The main reason of this revision is harmonization with recently published standards from ETSI; also introduction of indication of signing policy in the signature and an update of cryptographic algorithms.

Feedback about the content of the standard can be given by using the feedback form on the home page of the Estonian Centre for Standardisation or by e-mail: standardiosakond@evs.ee.

ICS 35.040 Character sets and information coding

CONTENTS

INTRODUCTION

The European Directive 1999/93/EC on a community framework for electronic signatures defines an electronic signature as: “data in electronic form which is attached to or logically associated with other electronic data and which serves as a method of authentication”.

The present document is intended to cover electronic signatures for various types of transactions, including business transactions (e.g. purchase requisition, contracts and invoice applications). Thus the present document can be used for any transaction between an individual and a company, between two companies, between an individual and a governmental body, etc. The present document is independent of any environment. It can be used with different signature creation devices, e.g. smart cards, GSM SIM cards, special programs for electronic signatures, etc.

The ETSI standard TS 101 903 [1] (hereinafter: XAdES) defines formats for advanced electronic signatures that remain valid over long periods and incorporates additional useful information for common use cases (like indication of the role or resolution of the signatory). XAdES is XML-based and therefore suitable for the current ICT environment. The ETSI standard TS 103 171 [4] further profiles the XAdES signature by putting limitations on choices.

The ETSI standard TS 102 918 [3] (hereinafter: ASiC) defines the format of the container for encapsulation of signed files and signatures with extra information. The ETSI TS 103 174 [5] profiles it further on.

This BDOC specification is fully compliant with above-mentioned ETSI standards.

The present document:

- specifies profiles of XAdES by narrowing down choices of elements and value types in the standard;
- defines sets of XAdES elements for long-time validity of XAdES signature;
- specifies container format for embedding signed files and signatures based on ASiC.

For further reference, the term BDOC is used throughout the text to denote both the XAdES profile and the container format.

1 SCOPE

The present document defines XML formats for advanced electronic signatures that remain valid over long periods and incorporates additional useful information for common use cases. This includes evidence to its validity even if the signer or verifying party later attempts to deny (repudiates) the validity of the signature.

The present document builds on the following standards:

- ETSI TS 101 903 V1.4.2. XML Advanced Electronic Signatures (XAdES) [1]; and its Baseline Profile ETSI TS 103 171 V2.1.1 [4];
- ITU-T Recommendation X.509 [11];
- IETF RFC 3161. PKIX Time-Stamp protocol [7];
- IETF RFC 6960. Online Certificate Status Protocol [10];
- ETSI TS 102 918 V1.2.1. Associated Signature Containers (ASiC) [3]; and its Baseline Profile ETSI TS 103 174 V2.1.2 [5]. The latter is in turn based on OpenDocument [12] standard “OpenDocument V1.2 Part 3 – Packages”.

For a complete list of references, see Clause 2.

Clause 5 defines the basic profile of the BDOC format. This profile contains just the signature without any validation data.

Clause 6 defines two profiles of the BDOC format with validation data providing for “replacement of the handwritten signature”.

Clause 7 discusses and defines means for achieving long-time validity of the electronic signatures.

Clause 8 specifies container format for embedding signed files and signatures into one data unit.

2 NORMATIVE REFERENCES

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

[1] ETSI TS 101 903 V1.4.2 (2010-12). XML Advanced Electronic Signatures (XAdES)

[2] ETSI TS 102 023 V1.2.2 (2008-10). Policy requirements for time-stamping authorities

[3] ETSI TS 102 918 V1.2.1 (2012-02). Associated Signature Containers (ASiC)

[4] ETSI TS 103 171 V2.1.1 (2012-03). XAdES Baseline Profile

[5] ETSI TS 103 174 V2.1.1 (2012-03). ASiC Baseline Profile

[6] ETSI TS 102 176-1 V2.1.1 (2011-07). Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms

[7] IETF RFC 3161. Internet X.509 Public Key Infrastructure Time-Stamp protocol

[8] IETF RFC 3275. XML-Signature Syntax and Processing

[9] IETF RFC 5280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[10] IETF RFC 6960. Internet X.509 Public Key Infrastructure Online Certificate Status Protocol (OCSP)

[11] ITU-T Recommendation X.509. Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

[12] OASIS. Open Document Format for Office Applications (OpenDocument) Version 1.2. Part 3: Packages

3 DEFINITIONS AND ABBREVIATIONS

For the purposes of this document, the terms and definitions given in Clause 3 and Annex A of XAdES [1] apply.

4 OVERVIEW

Whereas XAdES has been around for several years and there are a number of implementations of this standard around, they remain incompatible. The reasons are the following:

- XAdES allows for a myriad of options. Implementations of XAdES usually do not support every non-mandatory building block or element which results in incompatibility of XAdES signatures;
- Use of XAdES optional building blocks heavily depends on security requirements of the application and PKI services provided. As those requirements and set of services tend to vary, corresponding XAdES profiles do as well.
- XAdES specifies just a signature format allowing the source data (to be signed) be anywhere and referenced only by URI. In practice it is often required for the source data and signatures to be bound together in a single data unit ("container" or "file"). Implementers have free choice here which results in incompatibility of digitally signed files.

Recent additions to ETSI standards have addressed the problem by introducing XAdES Baseline Profile [4] and by standardizing container format [3] and its Baseline Profile [5].

This specification uses new base standards and solves above-mentioned problems by defining:

- subset of XAdES elements and parameters – "BDOC profile of XAdES";
- requirement profiles for PKI, time-stamping and certificate validation services and corresponding XAdES building blocks;
- container format for embedding source data and signatures – "BDOC file format".

This document is based entirely on XAdES [1] and therefore is not self-consistent. The reader shall use this standard as a basis and follow references and profiling notes given in this document. Requirements from other standards (XAdES Baseline Profile [4], ASiC [3] and its Baseline Profile [5]) are covered by this specification but could give reader expanded insight.

Annex B contains an overview of use of XAdES element in different BDOC variations.

5 BDOC BASIC PROFILE

The BDOC Basic Profile is an XML structure containing a single cryptographic signature over a well-defined set of data. It does not contain any additional data for full signature validation such as timestamps or certificate validity confirmations. It just forms basis for other forms of BDOC described in the next clause.

The BDOC Basic profile is based on Basic Electronic Signature – XAdES-EPES (Explicit Policy Based Electronic Signature) – defined in clause 4.4.2 of XAdES [1].

Requirements for the usage of the elements are shown in further text by the labels given in table 1.