

# Digital Signature Service Overview

## Committee Draft, 11 September 2006 (WD-04)

4 5	Document identifier: oasis-dss-1.0-overview-cd-r1.doc		
6 7	Location: http://docs.oasis-open.org/dss/v1.0/		
8 9 10	Editor: Nick Pope, individual Juan Carlos Cruellas, individual <cruellas@ac.upc.edu></cruellas@ac.upc.edu>		
11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27	Contributors:  Dimitri Andivahis, Surety Glenn Benson, JPMorganChase Juan Carlos Cruellas, individual Carlos Gonzalez-Cadenas, Netfocus, S.L Frederick Hirsch, Nokia Pieter Kasselman, Cybertrust Andreas Kuehne, individual Konrad Lanz, Austria Federal Chancellery <konrad.lanz@iaik.tugraz.at> Tommy Lindberg, individual Paul Madsen, Entrust John Messing, American Bar Association Tim Moses, Entrust Trevor Perrin, individual Nick Pope, individual Rich Salz, DataPower Ed Shallow, Universal Postal Union</konrad.lanz@iaik.tugraz.at>		
28 29 30	Abstract:  This document provides an overview of the set of specifications for "Digital Signature Services".		
31 32 33 34 35 36 37 38 39	Status:  This is a <b>Public review Draft</b> produced by the OASIS Digital Signature Service Technical Committee. Comments may be submitted to the TC by any person by clicking on "Send A Comment" on the TC home page at: <a href="http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss">http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss</a> For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Digital Signature Service TC web page at <a href="http://www.oasis-open.org/committees/dss/ipr.php">http://www.oasis-open.org/committees/dss/ipr.php</a> .		
<b>4</b> 0			

## **Table of Contents**

42       1 Introduction         43       1.1 Overview of DSS         44       1.2 DSS Specifications         45       2 Current DSS Profiles         46       2.1 Time-stamp Profile         47       2.1.1 Overview         48       2.1.2 Relationship to other Profiles         49       2.2 Asynchronous Profile         50       2.2.1 Overview         51       2.2.2 Relationship to other Profiles         52       2.3 Code-Signing Profile         53       2.3.1 Overview         54       2.3.2 Relationship to other Profiles         55       2.4 J2ME code-signing profile         56       2.4.1 Overview         57       2.4.2 Relationship to other Profiles         58       2.5 Entity Seal Profile         59       2.5.1 Overview         60       2.5.2 Relationship to other Profiles         61       2.6 Electronic Postmark (EPM) Profile         62       2.6 Can Relationship to other Profiles         63       2.6.2 Relationship to other Profiles         64       2.7 German Signature Law Profile         65       2.7.2 Relationship to other Profiles         66       2.7.2 Relationship to other Profiles         67       2.8 AdES		
44       1.2 DSS Specifications.         45       2 Current DSS Profiles.         46       2.1 Time-stamp Profile         47       2.1.1 Overview.         48       2.1.2 Relationship to other Profiles.         49       2.2 Asynchronous Profile         50       2.2.1 Overview.         51       2.2.2 Relationship to other Profiles.         52       2.3 Code-Signing Profile         53       2.3.1 Overview.         54       2.3.2 Relationship to other Profiles.         55       2.4 J2ME code-signing profile         56       2.4.1 Overview.         57       2.4.2 Relationship to other Profiles.         58       2.5 Entity Seal Profile         59       2.5.1 Overview.         60       2.5.2 Relationship to other Profiles.         61       2.6 Electronic Postmark (EPM) Profile         62       2.6.1 Overview.         63       2.6.2 Relationship to other Profiles.         64       2.7 German Signature Law Profile         65       2.7.1 Overview.         66       2.8.1 Overview.         67       2.8 AdES Profile         68       2.8.2 Relationship to other Profiles.         70       2.9 Signature Gateway Profile     <		3
45       2       Current DSS Profiles	;	3
46 2.1 Time-stamp Profile		3
2.1.1 Overview		5
2.1.2 Relationship to other Profiles.  2.2 Asynchronous Profile		5
2.2 Asynchronous Profile  2.2.1 Overview  2.2.2 Relationship to other Profiles  2.3 Code-Signing Profile  2.3.1 Overview  2.3.2 Relationship to other Profiles  2.4 J2ME code-signing profile  2.4.1 Overview  2.4.2 Relationship to other Profiles  2.5 Entity Seal Profile  2.5.1 Overview  2.5.2 Relationship to other Profiles  2.6 Electronic Postmark (EPM) Profile  2.6.1 Overview  3.6.2 Relationship to other Profiles  2.7 German Signature Law Profile  2.7.1 Overview  2.7.2 Relationship to other Profiles  2.8 AdES Profile  2.8 AdES Profile  2.8.1 Overview  3.9 Signature Gateway Profile  2.9 Signature Gateway Profile  2.9.2 Relationship to other Profiles  3.8 References  3.1 DSS Specifications  3.2 Other Specifications		5
2.2.1 Overview  2.2.2 Relationship to other Profiles.  2.3 Code-Signing Profile.  2.3.1 Overview.  3.2.2 Relationship to other Profiles.  2.4 J2ME code-signing profile.  2.4.1 Overview.  2.4.2 Relationship to other Profiles.  2.5 Entity Seal Profile.  2.5 Entity Seal Profile.  2.5 Electronic Postmark (EPM) Profile.  2.6 Electronic Postmark (EPM) Profile.  2.6.1 Overview.  3.6.2 Relationship to other Profiles.  2.7 German Signature Law Profile.  2.7 German Signature Law Profile.  2.8 AdES Profile.  2.8 AdES Profile.  2.8 AdES Profile.  2.9 Signature Gateway Profile.  2.9 Signature Gateway Profile.  3.1 DSS Specifications.  3.2 Other Specifications.		5
2.2.2 Relationship to other Profiles		5
2.3 Code-Signing Profile  2.3.1 Overview  2.3.2 Relationship to other Profiles  2.4 J2ME code-signing profile  5.5 2.4 J2ME code-signing profile  5.6 2.4.1 Overview  5.7 2.4.2 Relationship to other Profiles  2.5 Entity Seal Profile  5.9 2.5.1 Overview  6.0 2.5.2 Relationship to other Profiles  6.1 2.6 Electronic Postmark (EPM) Profile  6.2 2.6.1 Overview  6.3 2.6.2 Relationship to other Profiles  6.4 2.7 German Signature Law Profile  6.5 2.7.1 Overview  6.6 2.7.2 Relationship to other Profiles  6.7 2.8 AdES Profile  6.8 2.8.1 Overview  6.9 2.8.2 Relationship to other Profiles  7.0 2.9 Signature Gateway Profile  7.1 2.9.1 Overview  7.2 2.9.2 Relationship to other Profiles  7.3 3 References  7.4 3.1 DSS Specifications  7.5 3.2 Other Specifications		5
2.3.1 Overview 2.3.2 Relationship to other Profiles 2.4 J2ME code-signing profile 5.2 2.4.1 Overview 5.3 2.4.2 Relationship to other Profiles 5.4 2.5 Entity Seal Profile 5.5 2.5 Entity Seal Profile 5.6 2.5.1 Overview 6.0 2.5.2 Relationship to other Profiles 6.1 2.6 Electronic Postmark (EPM) Profile 6.2 2.6.1 Overview 6.3 2.6.2 Relationship to other Profiles 6.4 2.7 German Signature Law Profile 6.5 2.7.1 Overview 6.6 2.7.2 Relationship to other Profiles 6.7 2.8 AdES Profile 6.8 2.8.1 Overview 6.9 2.8.2 Relationship to other Profiles 7.0 2.9 Signature Gateway Profile 7.1 2.9.1 Overview 7.2 2.9.2 Relationship to other Profiles 7.3 3 References 7.4 3.1 DSS Specifications 7.5 3.2 Other Specifications		5
2.3.2 Relationship to other Profiles.  2.4 J2ME code-signing profile		5
2.4 J2ME code-signing profile		5
2.4.1 Overview		5
2.4.2 Relationship to other Profiles.  2.5 Entity Seal Profile.  59		6
2.5 Entity Seal Profile  2.5.1 Overview  2.5.2 Relationship to other Profiles  2.6 Electronic Postmark (EPM) Profile  2.6.1 Overview  3.6.2 Relationship to other Profiles  2.7 German Signature Law Profile  2.7.1 Overview  3.7.2 Relationship to other Profiles  2.8 AdES Profile  2.8.1 Overview  2.8.2 Relationship to other Profiles  2.9 Signature Gateway Profile  2.9.1 Overview  2.9.2 Relationship to other Profiles  3.8 References  3.1 DSS Specifications  3.2 Other Specifications		6
2.5.1 Overview		6
2.5.2 Relationship to other Profiles 2.6 Electronic Postmark (EPM) Profile 2.6.1 Overview 3.6.2 Relationship to other Profiles 4.7 German Signature Law Profile 5.7.1 Overview 6.7.2 Relationship to other Profiles 6.7.2 Relationship to other Profiles 6.7.2 Relationship to other Profiles 6.8.1 Overview 6.9.2.8.2 Relationship to other Profiles 6.9.9 Signature Gateway Profile 6.9.1 Overview 6.9.2 Relationship to other Profiles 6.9.3 References 6.9.3 References 6.9.3 References 6.9.3 References 6.9.3 References 6.9.3 Specifications 6.9.3 Specifications		6
2.6 Electronic Postmark (EPM) Profile 2.6.1 Overview 3.6.2 Relationship to other Profiles 4.7 German Signature Law Profile 5.2.7.1 Overview 6.2.7.2 Relationship to other Profiles 7.2.8 AdES Profile 8.2.8.1 Overview 9.2.8.2 Relationship to other Profiles 9.2.9 Signature Gateway Profile 9.2.9.1 Overview 9.2.9.2 Relationship to other Profiles 9.3.1 DSS Specifications 9.3.2 Other Specifications		6
2.6.1 Overview		6
2.6.2 Relationship to other Profiles 2.7 German Signature Law Profile 2.7.1 Overview 6.2.7.2 Relationship to other Profiles 6.2.8 AdES Profile 6.2.8.1 Overview 6.2.8.2 Relationship to other Profiles 7.2.9 Signature Gateway Profile 7.2.9.1 Overview 7.2.9.2 Relationship to other Profiles 7.3 References 7.4 3.1 DSS Specifications 7.5 3.2 Other Specifications		6
2.7 German Signature Law Profile 2.7.1 Overview 2.7.2 Relationship to other Profiles 2.8 AdES Profile 2.8.1 Overview 2.8.2 Relationship to other Profiles 2.9 Signature Gateway Profile 2.9.1 Overview 2.9.2 Relationship to other Profiles 3 References 3 References 3.1 DSS Specifications 3.2 Other Specifications		6
2.7.1 Overview 2.7.2 Relationship to other Profiles 2.8 AdES Profile 2.8.1 Overview 2.8.2 Relationship to other Profiles 2.9 Signature Gateway Profile 2.9.1 Overview 2.9.2 Relationship to other Profiles 3 References 3 References 3.1 DSS Specifications 3.2 Other Specifications		6
2.7.2 Relationship to other Profiles 2.8 AdES Profile 2.8.1 Overview 2.8.2 Relationship to other Profiles 2.9 Signature Gateway Profile 2.9.1 Overview 2.9.2 Relationship to other Profiles 3 References 3.1 DSS Specifications 3.2 Other Specifications	······································	7
2.8 AdES Profile	······································	7
2.8.1 Overview 2.8.2 Relationship to other Profiles 2.9 Signature Gateway Profile 2.9.1 Overview 2.9.2 Relationship to other Profiles 3 References 3.1 DSS Specifications 3.2 Other Specifications		7
2.8.2 Relationship to other Profiles  2.9 Signature Gateway Profile  2.9.1 Overview  2.9.2 Relationship to other Profiles  3 References  3.1 DSS Specifications  3.2 Other Specifications	······································	7
70 2.9 Signature Gateway Profile	······································	7
71 2.9.1 Overview	······································	7
72 2.9.2 Relationship to other Profiles		7
73 3 References		7
<ul><li>74 3.1 DSS Specifications</li><li>75 3.2 Other Specifications</li></ul>		7
75 3.2 Other Specifications		8
•		8
76 Appendix A. Notices		8
		9

## 1 Introduction

- 79 The OASIS Digital Signature Services (DSS) TC has produced a number of specification
- 80 documents. This document attempts to provide an overview of DSS and the roles played by the
- 81 various specifications.

78

82

100

#### 1.1 Overview of DSS

- The DSS specifications describe two XML-based request/response protocols a signing protocol
- 84 and a verifying protocol. Through these protocols a client can send documents to a server and
- 85 receive back a signature on the documents; or send documents and a signature to a server, and
- 86 receive back an answer on whether the signature verifies the documents.
- 87 These operations could be useful in a variety of contexts for example, they could allow clients to
- 88 access a single corporate key for signing press releases, with centralized access control,
- 89 auditing, and archiving of signature requests. They could also allow clients to create and verify
- 90 signatures without needing complex client software and configuration.
- 91 The signing and verifying protocols are chiefly designed to support the creation and verification of
- 92 XML signatures [XMLSig], , and CMS signatures [RFC3369]. These protocols can also be used
- 93 to create and verify time-stamps, either in binary format as defined in [RFC3161] or to an XML
- 94 time-stamp structure as defined in DSS. These protocols may also be extensible to other types of
- 95 signatures and timestamps, such as PGP signatures.
- 96 It is expected that the signing and verifying protocols will be *profiled* to meet many different
- 97 application scenarios. In anticipation of this, these protocols have only a minimal set of required
- 98 elements, which deal with transferring "input documents" and signatures back and forth between
- 99 client and server.

#### 1.2 DSS Specifications

- 101 The DSS specification consist of a "Core Protocols, Elements, and Bindings" specification (the
- 102 Core) and a number of profiles.
- 103 The Core specification provide the basic protocols and elements which are adapted to support
- specific use cases in the DSS profiles. The Core consists of:
- 105 Skeleton protocols for signing and verifying
- Optional elements that can be "mixed in" to the skeleton protocols to support the
   requirements of the different profiles. This includes an XML timestamp and elements to
   control a range of approaches to creation and verification of signatures,
- 109 A range of transport and security bindings that selected as required by profiles.
- 110 The DSS profiles specify the options and bindings to be used with the skeleton protocols to meet
- the requirements of a particular application or use case. A profile may also specify additional
- elements and / or bindings where necessary to meet its own particular needs.
- 113 Profiles are either abstract or concrete. Concrete profiles provide a complete selection of the
- options giving the basis for interoperability: products implementing concrete profiles should be
- 115 compatible at the level of protocol defined by DSS. Abstract profiles add some functionality or
- options to the core that can be inherited by concrete profiles, or by other abstract profiles (and in
- some cases, concrete profiles can be made more concrete through inheritance as well).
- These relationships can be visualized as an inheritance graph, with the core as the root node,
- and a directed acyclic graph of profiles and sub-profiles extending below it.
- 120 The DSS TC has produced several profiles so far, and is likely to produce further profiles in the
- 121 future. Below is a summary of the existing DSS profiles.

## 2 Current DSS Profiles

#### 124 **2.1 Time-stamp Profile**

- 125 **2.1.1 Overview**
- 126 The Time-stamp profile define the use of the DSS Core protocols to support creation and
- 127 verification of time-stamps. The profile includes support for the creation of XML Time-stamps as
- defined in the Core and binary time-stamps as defined in [RFC 3161].
- 129 2.1.2 Relationship to other Profiles
- 130 None.

123

#### 131 2.2 Asynchronous Profile

- 132 **2.2.1 Overview**
- 133 Although most applications of the OASIS Digital Signature Service supply the results
- immediately, there is a demand for deferred delivery of results. For example, the German
- 135 Signature Law explicitly requires the commitment of the certificate holder or at least a time slot for
- 136 the certificate holder to deny the signing request.
- 137 This abstract profile defines a simple mechanism for asynchronous signing and verification
- 138 requests. Concrete profiles that use this abstract profile allow the client to submit a request which
- the server doesn't respond to right away. Instead, the client can poll the server until the response
- 140 is ready.

157

#### **2.2.2 Relationship to other Profiles**

142 This profile is a parent of the code-signing profile.

#### 143 **2.3 Code-Signing Profile**

- 144 **2.3.1 Overview**
- 145 Code-signing allows the recipient of a software program to receive assurances regarding the
- 146 origin and integrity of a program. The recipient may use this information to make a trust decision
- on whether to install or execute the program.
- 148 Centralizing the generation of signatures in the code-signing process allows for the roles of the
- 149 software developer and the code signer to be separated. This has the advantage that keys used
- 150 for signing software programs can be better managed, access to the keys can be better
- 151 controlled, audit trails can be centrally kept, event records can be reliably archived, and signing
- 152 policies can be rigorously enforced.
- 153 This abstract profile provides a basic framework for code-signing independent of any specific
- 154 signature schemes or formats. Specifying the use of specific signature schemes and formats is
- 155 left to concrete sub-profiles. For instance, a code-signing profile should be defined for Java 2
- 156 Micro Edition code-signing and Authenticode code-signing.

#### 2.3.2 Relationship to other Profiles

This profile is a child of the asynchronous profile, and a parent of the J2ME code-signing profile.

### 2.4 J2ME code-signing profile

- 160 **2.4.1 Overview**
- 161 This specification provides a concrete profile based on the Code-Signing Profile for requesting
- the generation of signatures as specified in the Java 2 Micro Edition (J2ME), Mobile Information
- 163 Device Profile 2.0 [MIDP 2.0].

#### 164 2.4.2 Relationship to other Profiles

This profile is a child of the asynchronous profile, and the code-signing profile.

166

159

#### 167 **2.5 Entity Seal Profile**

#### 168 **2.5.1 Overview**

- 169 This profile supports creation and validation of a "seal" created by a given Entity or Organization
- 170 on electronic data.
- 171 The seal is a form of electronic signature which:
- a) protects the integrity of the document,
- b) includes the time at which the seal was applied proving that the data existed at the given time,
- 175 c) includes the identity of the entity requesting the seal,
- may include a statement of intent for applying the seal.
- 177 This profile is concrete except for the security binding, which must be specified before using this
- in a particular environment.

### 179 2.5.2 Relationship to other Profiles

180 None.

181

182

## 2.6 Electronic Postmark (EPM) Profile

#### 183 **2.6.1 Overview**

- 184 The Electronic PostMarking service [EPM] is a Universal Postal Union (UPU) endorsed standard
- aimed at providing generalized signature creation, signature verification, timestamping, and
- 186 receipting services for use by and across Postal Administrations and their target customers.
- 187 Although the total scope and functional coverage of the EPM's service offering are outside the
- 188 immediate scope of the DSS initiative, the UPU wishes to offer its client base a DSS-compliant
- 189 subset of the EPM for clients who wish to maintain OASIS compliance in the core areas of
- 190 signature and timestamp creation and verification.

#### 191 2.6.2 Relationship to other Profiles

192 None.

#### 2.7.1 Overview 195 This abstract profile supports creation and validation of qualified signatures according to the 196 guidelines given by the German signature law [SigG] and its associated regulations. The EU has 197 certified that the German signature law complies with the European legal framework, so this 198 199 profile may be used as a template for national profiles all over Europe. 200 2.7.2 Relationship to other Profiles 201 None. 202 203 2.8 AdES Profile 204 2.8.1 Overview 205 This set of profiles supports the creation and verification of XML and binary Advanced Electronic 206 Signatures as defined in [XAdES] and [TS 101 733]. 207 2.8.2 Relationship to other Profiles 208 209 None. 210 2.9 Signature Gateway Profile 211 2.9.1 Overview 212 213 The Signature Gateway profile specifies the use of DSS to support the transform of a signature. 214 This Signature Gateway transforms both signing technology and credential logistics. The signing 215 technology specifies the mechanisms through which one creates and verifies a signature. 216 Example technologies include, but are not limited to photocopied signatures, signatures using 217 public key infrastructures, and signatures defined using symmetric keying material. Credential 218 logistics, describes the means to distribute credentials to remote parties; and the associated 219 vehicle for distributing trust. Although electronic means allows communication at a distance, 220 geographic separation increases the difficulty of trusting one's peers. Credentials overcome many of the geographic impediments to trust; and the associated logistics securely define the 221 222 means of managing the credential lifecycle, e.g., distribution, revocation, renewal, and retirement. 2.9.2 Relationship to other Profiles 223 224 None. 225 226

2.7 German Signature Law Profile

## 3 References

227

228

231232

254

## 3.1 DSS Specifications

- The current list of DSS Specifications are available through the OASIS DSS home page:
- 230 http://www.oasis-open.org/committees/tc\_home.php?wg\_abbrev=dss

## 3.2 Other Specifications

233 234 235	[XMLSig]	D. Eastlake et al. <i>XML-Signature Syntax and Processing</i> . W3C Recommendation, February 2002. http://www.w3.org/TR/1999/REC-xml-names-19990114
236	[RFC 3369]	R. Housley. <i>Cryptographic Message Syntax</i> . IETF RFC 3369, August
237		2002.
238		http://www.ietf.org/rfc/rfc2459.txt.
239	[TS 101733]	Advanced Electronic Signatures. ETSI TS 101 733.
240	[XAdES]	XML Advanced Electronic Signatures. ETSI TS 101 903
241	[RFC 3161]	C. Adams, P. Cain, D. Pinkas, R. Zuccherato. Internet X.509 Public Key
242		Infrastructure Time-Stamp Protocol (TSP). IETF RFC 3161, August
243		2001.
244		http://www.ietf.org/rfc/rfc3161.txt.
245	[MIDP 2.0]	Mobile Information Device Profile for Java™ 2 Micro Edition Version 2.0,
246		JSR 118 Expert Group
247	[EPM]	Universal Postal Union, Electronic PostMark Web Service Description
248		Language (WSDL) the UPU's Postal Technology Centre
249		http://www.ptc.upu.int/.
250	[SigG]	Framework for Electronic Signatures, Amendment of Further Regulations
251		Act (Signaturgesetz – SigG).
252		http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/119.pdf
253		

## **Appendix A. Notices**

- 256 OASIS takes no position regarding the validity or scope of any intellectual property or other rights 257 that might be claimed to pertain to the implementation or use of the technology described in this 258 document or the extent to which any license under such rights might or might not be available; 259 neither does it represent that it has made any effort to identify any such rights. Information on 260 OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS 261 website. Copies of claims of rights made available for publication and any assurances of licenses 262 to be made available, or the result of an attempt made to obtain a general license or permission 263 for the use of such proprietary rights by implementors or users of this specification, can be obtained from the OASIS Executive Director. 264
- OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to implement this specification. Please address the information to the OASIS Executive Director.
- 268 Copyright © OASIS Open 2006. All Rights Reserved.
- 269 This document and translations of it may be copied and furnished to others, and derivative works 270 that comment on or otherwise explain it or assist in its implementation may be prepared, copied, 271 published and distributed, in whole or in part, without restriction of any kind, provided that the 272 above copyright notice and this paragraph are included on all such copies and derivative works. 273 However, this document itself does not be modified in any way, such as by removing the 274 copyright notice or references to OASIS, except as needed for the purpose of developing OASIS 275 specifications, in which case the procedures for copyrights defined in the OASIS Intellectual 276 Property Rights document must be followed, or as required to translate it into languages other 277 than English.
- The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.
- This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

285286287288