Digital Signature Service Overview

Committee Draft, 11 September 2006 (WD-04)

Document identifier:

oasis-dss-1.0-overview-cd-r1.doc

Location:

http://docs.oasis-open.org/dss/v1.0/

Editor:

Nick Pope, *individual*

Juan Carlos Cruellas, *individual* <cruellas@ac.upc.edu>

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

Abstract:

This document provides an overview of the set of specifications for “Digital Signature Services”.

Status:

This is a **Public review Draft** 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:
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss

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 http://www.oasis-open.org/committees/dss/ipr.php.

Table of Contents

1 Introduction

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

1.1 Overview of DSS

The DSS specifications describe two XML-based request/response protocols – a signing protocol and a verifying protocol. Through these protocols a client can send documents to a server and receive back a signature on the documents; or send documents and a signature to a server, and receive back an answer on whether the signature verifies the documents.

These operations could be useful in a variety of contexts – for example, they could allow clients to access a single corporate key for signing press releases, with centralized access control, auditing, and archiving of signature requests. They could also allow clients to create and verify signatures without needing complex client software and configuration.

The signing and verifying protocols are chiefly designed to support the creation and verification of XML signatures **[XMLSig]**, , and CMS signatures **[RFC3369]**. These protocols can also be used to create and verify time-stamps, either in binary format as defined in [RFC3161] or to an XML time-stamp structure as defined in DSS. These protocols may also be extensible to other types of signatures and timestamps, such as PGP signatures.

It is expected that the signing and verifying protocols will be *profiled* to meet many different application scenarios. In anticipation of this, these protocols have only a minimal set of required elements, which deal with transferring “input documents” and signatures back and forth between client and server.

1.2 DSS Specifications

The DSS specification consist of a “Core Protocols, Elements, and Bindings” specification (the Core) and a number of profiles.

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:

- 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,
- A range of transport and security bindings that selected as required by profiles.

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.

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 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.

The DSS TC has produced several profiles so far, and is likely to produce further profiles in the future. Below is a summary of the existing DSS profiles.

122

123 # 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
128 defined in the Core and binary time-stamps as defined in **[RFC 3161]**.

129 ### 2.1.2 Relationship to other Profiles

130 None.

131 ## 2.2 Asynchronous Profile

132 ### 2.2.1 Overview

133 Although most applications of the OASIS Digital Signature Service supply the results
134 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
139 the server doesn't respond to right away. Instead, the client can poll the server until the response
140 is ready.

141 ### 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
147 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.

157 ### 2.3.2 Relationship to other Profiles

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

2.4 J2ME code-signing profile

2.4.1 Overview

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 Device Profile 2.0 **[MIDP 2.0]**.

2.4.2 Relationship to other Profiles

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

2.5 Entity Seal Profile

2.5.1 Overview

This profile supports creation and validation of a “seal” created by a given Entity or Organization on electronic data.

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,

c) includes the identity of the entity requesting the seal,

may include a statement of intent for applying the seal.

This profile is concrete except for the security binding, which must be specified before using this in a particular environment.

2.5.2 Relationship to other Profiles

None.

2.6 Electronic Postmark (EPM) Profile

2.6.1 Overview

The Electronic PostMarking service [EPM] is a Universal Postal Union (UPU) endorsed standard aimed at providing generalized signature creation, signature verification, timestamping, and receipting services for use by and across Postal Administrations and their target customers.

Although the total scope and functional coverage of the EPM’s service offering are outside the immediate scope of the DSS initiative, the UPU wishes to offer its client base a DSS-compliant subset of the EPM for clients who wish to maintain OASIS compliance in the core areas of signature and timestamp creation and verification.

2.6.2 Relationship to other Profiles

None.

2.7 German Signature Law Profile

2.7.1 Overview

This abstract profile supports creation and validation of qualified signatures according to the guidelines given by the German signature law [**SigG**] and its associated regulations. The EU has certified that the German signature law complies with the European legal framework, so this profile may be used as a template for national profiles all over Europe.

2.7.2 Relationship to other Profiles

None.

2.8 AdES Profile

2.8.1 Overview

This set of profiles supports the creation and verification of XML and binary Advanced Electronic Signatures as defined in **[XAdES]** and **[TS 101 733]**.

2.8.2 Relationship to other Profiles

None.

2.9 Signature Gateway Profile

2.9.1 Overview

The Signature Gateway profile specifies the use of DSS to support the transform of a signature. This Signature Gateway transforms both *signing technology* and *credential logistics*. The signing technology specifies the mechanisms through which one creates and verifies a signature. Example technologies include, but are not limited to photocopied signatures, signatures using public key infrastructures, and signatures defined using symmetric keying material. Credential logistics, describes the means to distribute credentials to remote parties; and the associated vehicle for distributing trust. Although electronic means allows communication at a distance, 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 means of managing the credential lifecycle, e.g., distribution, revocation, renewal, and retirement.

2.9.2 Relationship to other Profiles

None.

3 References

3.1 DSS Specifications

The current list of DSS Specifications are available through the OASIS DSS home page:

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss

3.2 Other Specifications

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

Appendix A. Notices

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification, can be obtained from the OASIS Executive Director.

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.