OASIS Digital Signature Services TC

Statement of Purpose:

The Digital Signature Services Technical Committee has as its mandate the development of techniques to support the processing of digital signatures. This mandate includes defining an interface for requesting that a web service produce and/or verify a digital signature on a given piece of data and techniques for proving that a signature was created within its ~~private~~ key validity period.

The TC will develop a protocol for a digital signature creation web service. Providing digital signatures via such a web service facilitates policy-based control of the provision of the signatures.

The TC will also develop a protocol for a centralized digital signature verification web service that can verify signatures in relation to a given policy set.

Finally, the TC will develop an XML-based protocol to produce cryptographic time stamps that can be used for determing whether or not a signature was created within the associated ~~public~~ key's validity period or before revocation. This is required as part of the signature verification algorithm.

More generally there is a need for XML-based techniques for proving that data existed at a particular point in time. While this more general problem is not, strictly speaking, within the scope of the TC, the ability of the proposed solutions to solve this problem will be considered, as much as possible, while remaining consistent with the scope of the TC.

Relationship to Existing Activities:

Many efforts related to digital signatures and related technologies are underway throughout the industry. The following work may be relevant to this Digital Signature Services TC:

- OASIS Access Control TC (XACML)
- OASIS Rights Language TC (XrML)
- OASIS Security Services TC (SAML)
- OASIS Web Services Security TC (WSSTC)
- OASIS Election and Voter Services TC
- OASIS LegalXML eNotary TC
- OASIS XML Common Biometric Format TC (XCBF)
- W3C XML Signature
- W3C XML Key Management
- W3C XML Encryption
- ETSI Electronic Signatures and Infrastructures Technical Committee
- ANSI X9F4 X9.95 (Trusted Time Stamps)
- ISO/IEC JTC1/SC27 18014

Technical Committee Deliverables
The new TC will have the following deliverables:

1. an XML-based protocol, including a time stamping protocol, providing a method or methods of proving that a ~~private~~ key was used during its validity period,
2. a SOAP binding for the protocol elements in 1)

2. a SOAP binding for the protocol elements in 1),
3. a WS-Security profile for the elements in 1),
4. an interface for a ~~centralized~~ digital signature creation web service,
5. an interface for a ~~centralized~~ digital signature verification web service.

Language in Which the TC will Conduct Business
English