**Section A: Nomination**

**To be completed by nominator:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Standard Name: | eXtensible Access Control Markup Language Version 3.0 (Core specification) | | | | Acronym: | XACML 3.0 | | |
| Standards Developer (SD): | OASIS | | SD Status on Standards Developer Inventory : | | Not on Standards Developer Inventory | | | |
| Approved  Declined  Approval rescinded | | **Date of SCC decision:** | |
| 3/20/2015 | |
| Description of standard: | XACML is a general-purpose access control policy language. This means that it provides a syntax (defined in XML) for managing access to resources based on applicable policies combined with asserted facts about (“attributes” of) an authenticated user, the type of access requested, the protected information resource, and the environment or context of the transaction. XACML is used to implement attribute-based access control (ABAC.) | | | | | | | |
| Date initially published: | 1/22/2013 | Current version: | | XACML 3.0 | | **Date published:** | | 1/22/2013 |

|  |  |  |
| --- | --- | --- |
| **Relevance to the IDEF:** | XACMLv3 is referenced as an example of public, open standards in IDEFv1 Requirements INTEROP-3. STANDARDIZED CREDENTIALS and INTEROP-4. STANDARDIZED DATA EXCHANGES | |
| **Compatible with NSTIC Guiding Principles:**  ***(minimum of one)*** | Privacy Enhancing and Voluntary  Secure and Resilient  Interoperable  Cost Effective and Easy-to-use | Privacy-enhancing.—ABAC as implemented with XACML enhances privacy by: (1) eliminating the need for relying-party systems to maintain user accounts with names and other identifying information; (2) supporting implementations that require only the minimum user information required by an access policy; and (3) enabling consistent and detailed compliance with policies on access to privacy-sensitive data of relying parties.  Secure and resilient.—XACML lets custodians of protected information resources enforce compliance with all policies applicable to access to a protected resource at an arbitrarily precise level, e.g, an individual row in a database or even individual data elements within a record. This can dramatically reduce the damage done by malevolent insiders or other attackers who have obtained an authentication credential.  Interoperable.—Via Profiles (nominated separately), XACMLv3 is used in conjunction with SAMLv2, JSON and REST. Implementers have also deployed XACML-based authorization solutions that leverage User attributes in OAUTH2 tokens. Cost-effective and Easy-to-Use.—XACML is not encountered directly by end-users. Enterprises implementing ABAC with XACML leverage tools available from multiple vendors that implement XACML “under the covers” while presenting user-friendly interfaces to access-policy administrators. There is no licensing cost for use of the XACML specification by tool developers or by implementing enterprises. |

|  |  |  |  |
| --- | --- | --- | --- |
| Stakeholder communities using proposed standard: | Privacy/Civil Liberties  Usability and Human Factors  Consumer Advocates  US Federal Government  US State, Local, Tribal, and Territorial Government  Research, Development, Education, and Innovation  Identity and Attribute Providers  Interoperability | | IT Infrastructure  Regulated Industries  Small Business, Entrepreneurs  Security  Relying Parties  Unaffiliated Individuals  Other, Please Specify: Healthcare; International |
| **Required by regulation?** | Yes  No  Unsure | If Yes, click here to list applicable regulations. | |
| **Trust Framework(s) adopted****?** | Yes  No  Unsure | US Federal Government  Healthcare | |

|  |  |  |  |
| --- | --- | --- | --- |
| Nominator name: | Martin Smith | Internal IDESG sponsor  *(if applicable)* | IDESG Security Committee |
| Nominator email: | Bfc.mclean@gmail.com | Date of submission: | Click here to enter a date. |

**To be completed by SCC:**

|  |  |  |  |
| --- | --- | --- | --- |
| **SCC Review of Nomination** | | | |
| SCC review completion date: | Click here to enter a date. | **Progress to evaluation?** | Yes  No |
| SCC comments:  *(if not progressing, explain the reason)* | Click here to enter text. | | |

**(Continued on next page)**

**Section B: Evaluation**

**To be completed by evaluator:**

|  |  |  |
| --- | --- | --- |
| Standard Evaluation Criteria | | |
| **Relevance to Identity Ecosystem:** | XACML 3.0 specifies the implementation of several of the fundamental components of the IDESG Functional Model of the Identity Ecosystem. In the Governance & Accountability layer it defines the language in which Policies and Rules may be expressed. In Administration it facilitates Policy Development. In the Functional layer, it specifies how Authorization is done.  In addition to the requirements mentioned in the Application (INTEROP-3. STANDARDIZED CREDENTIALS and INTEROP-4. STANDARDIZED DATA EXCHANGES) XACML 3.0 addresses many of the other IDESG requirements. A few examples suffice.PRIVACY-2 PURPOSE LIMITATION – the language and the Purpose Attribute defined in the Privacy Profile make it easy to compare the Purpose for which data was collected with the Purpose of use before allowing access. PRIVACY-12 ANONYMITY – XACML Policies can be based on any available attribute data. There is no requirement that a set of attributes uniquely identify an individual. SECURE-14 SECURITY LOGS – the Obligation feature of the XACML language makes it simple to enable logging on specific requests, whether successful , unsuccessful or either. SECURE-15 SECURITY AUDITS – the use of a logical language like XACML rather than a Turing-complete language like Java or C++ makes it possible to create tools to analyze policies. Several such tools currently exist. | **Meets:** |
| **No vendor lock-in:** | XACML is designed to be used in any access control environment from an embedded system to the open Internet. The language allows attribute information to be structured and represented in almost any conceivable way. No particular language or design is mandated. | **Meets:** |
| **Affordability:** | Access to the specification documents is completely free and unrestricted. The contributors to the specifications have pledged to license any necessary IPR royalty-free. There are more than a dozen implementations including at least 3 open source versions. | **Meets:** |
| **Compatible with NSTIC Guiding Principles:**  ***(minimum of one)*** | **Standard directly addresses one or more of the NSTIC Guiding Principles:** | |
| **Privacy Enhancing:**  XACML 3.0 has many privacy-enhancing features as noted above. | |
| **Voluntary:**  XACML 3.0 is designed to work with any source or format of attribute data and any scheme for attribute distribution. | |
| **Secure and Resilient:**  XACML as a standard cannot insure that systems are but considerable effort has been made to enable these characteristics. For example, the PDP is stateless, the policy language has been defined to avoid endless loops the handling of various kinds of errors and their reporting has been extensively analyzed to handle everything from missing data to internal policy errors. | |
| **Interoperable:**  XACML supports two primary points of interoperability. The policy language and the decision request interface. The standard specifies in detail how policies are evaluated, so that results from different implementations are compatible. The decision request interface allows a local or remote PEP to request a decision whether to allow access. The ability of multiple XACML implementations to interoperate in these ways has been repeatedly demonstrated at a number of public interoperability demonstrations. | |
| **Cost Effective:**  As stated elsewhere, XACML is inexpensive to use and is designed to work with the technology which is already deployed. | |
| **Easy-to-use:**  End users do not directly interface with XACML, but its integration features make it possible to seamlessly integrate into existing IT infrastructures without subjecting users to obscure, complex or otherwise onerous procedures. | |
| **For NSTIC guiding principles not addressed by the standard,**  **the standard supports and does not work against these NSTIC Guiding Principles:**  If the standard does work against one or more NSTIC Guiding Principles, click here and provide a summary of how. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Evaluator Recommendation to SCC** | | | | |
| **Evaluator name:** | **Date of submission to SCC:** | **Accept** | **More info needed** | **Reject** |
| Harold W. Lockhart | Click here to enter a date. |  |  |  |
| **Evaluator comments:**  ***(if not approved, explain the reason for the decision)*** | Click here to enter text. | | | |

**To be completed by SCC:**

|  |  |  |  |
| --- | --- | --- | --- |
| **SCC Review of Evaluation** | | | |
| **SCC review completion date:** | Click here to enter a date. | **Progress to Privacy for privacy review?** | Yes  No |
| **SCC Comments:**  ***(if not progressing, explain the reason)*** | Click here to enter text. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **SCC Recommendation to IDESG Plenary following Privacy Report Review** | | | |
| **SCC Privacy Report review date:** | Click here to enter a date. | **Recommendation to IDESG:** | Adopt  Do not adopt |
| **SCC Comments:**  ***(if recommending to not adopt, explain the reason)*** | Click here to enter text. | | |