DRAFT

An Introduction to the Provisioning Services Technical Committee

10/16/2001

Introduction

The purpose of the OASIS Provisioning Services Technical Committee (PSTC) is to define an XML-based framework for exchanging user, resource, and service provisioning information. The Technical Committee will develop an end-to-end, open, provisioning specification developed from several supporting XML specifications.

This document is intended to precede the formal standards definition process within the PSTC and set the stage for the initial discussions of the committee, compiling pre-existing XRPM and ADPR efforts, into a single, high level outline. It is intentionally devoid of much of the detail already defined and discussed in supporting materials. It aims provide a high level definition of provisioning within the context of the PSTC, an overview of the proposed scope, and a suggested road map for the first committee meeting.

NOTE: This document has no formal standing within the OASIS TC submission and ratification process. It is therefore informal, non-binding and unofficial in that context. It is not the intention of this document to lay out definitive definitions, terms or scope, but rather to provide context for wider ongoing discussion under the formal terms of the PSTC.

Terms

- For the purposes of this document the term “working group” will be used to refer to the original OASIS members that sponsored the formation of the PSTC.
- For the purposes of this document the term “resource” will be taken to refer to the target digital or non-digital systems” provisioned to.

What does provisioning mean?

Provisioning means many different things to many different people. Consider the following definition:

Etymology: Middle English, from Middle French, from Late Latin & Latin; Late Latin provision-, provisio act of providing, from Latin, foresight, from providEre to see ahead,

Definitions: 1a: the act or process of providing b: the fact or state of being prepared beforehand c: a measure taken beforehand to deal with a need or contingency; 2: a stock of needed materials or supplies; especially: a stock of food -- usually used in plural.

In our context, provisioning refers to the "preparation beforehand" of IT systems' "materials or supplies" required to carry out some defined activity. In general, it goes further than the initial "contingency" to the onward management lifecycle of the managed items. This could include the provisioning of purely digital services like user accounts and access privileges on systems, networks and applications. It could also include the provisioning of non-digital or "physical" resources like the requesting of office space, cell phones and credit cards.

The following short definition has been proposed by the working group (but is still under review and could possibly change).

"Provisioning is the automation of all the steps required to manage (setup, amend & revoke) user or system access and entitlement rights to electronic services".

What is a Provisioning System?

At this stage it is not necessary to define the implementation or physical makeup of a provisioning system. It should simply be assumed that a facility or capability exists within a network to carry out provisioning actions on a given set of resources. In many (but not mandatory to all) provisioning systems, the "system" denotes the capacity to take provisioning requests and to execute them in the context of some pre-defined flow of execution. In many cases (but not mandatory to all) the provisioning system encompasses a formal work-flow to implement these pre-defined business process.

Figure 1 shows a high-level schematic of two provisioning systems, each responsible for managing provisioning actions for a defined set of resources.

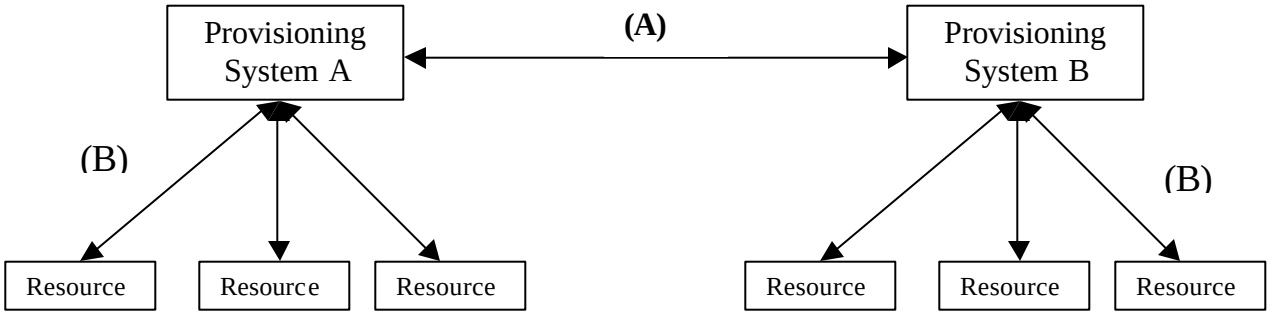

Figure 1. Provisioning Systems.

Why Do We Need Provisioning Standards?

There are several areas of provisioning systems that would benefit from standardization. XRPM [1] and ADPr [2] both adequately address the business needs and possible benefits for establishing standardization in this space. Each initiative identified this need at opposite ends of the provisioning scenario depicted in **Figure 1**. XRPM set out to define the set of standards required to facilitate interoperation and functioning at the Provisioning-System-to-Provisioning-System level (labeled "A" in **Figure 1**). In contrast, ADPr set out to define the set of standards required to facilitate interoperation and functioning at the Provisioning-Systems-to-Managed-Resource level (labeled "B" in **Figure 1**). The PSTC has been formed to work through both areas of potential standardization with the goals of defining a single XML-based framework for the exchange of information at both levels.

Provisioning-System-to-Provisioning-System Interoperability

The need for Provisioning-System-to-Provisioning-System (P2P) standards is discussed fully in [3]. In summary, the intention is to define a standard XML dialog and supporting security infrastructure to enable the exchange of requests between provisioning systems. Several "modes of operation" may exist for this interaction. Issues around authentication, authorization, notification and general operational semantics all require discussion, qualification and definition by the PSTC.

Provisioning-Systems-to-Managed-Resource Standardization

The need for Provisioning-Systems-to-Managed-Resource (P2R) standards is discussed fully in [4]. In summary the intention is to define an XML vocabulary and schema for describing the structure and content of requests from the provisioning platform to the managed resource. ADPr also covers the notion of exchange between platforms (through the definition of authentication, authorization and administration information in the request structures).

Unified Scope

The PSTC sets out to define the schema and protocol under which both P2P and P2R provisioning requests can be securely issued between provisioning systems and from the provisioning system to the managed resources.

Common System Elements

A critical part of defining and ratifying standards in this space is agreeing upon common definitions for the data elements within the system. Before any dialog or exchange of provisioning data can be defined, the PSTC needs to set out extensible definitions of the key system elements. This will include (but is not limited to) system elements such as resources, organizations, requests and identities. Previous standards efforts have made progress in this regard [5]. The PSTC intends to leverage prior initiatives wherever prudent and possible.

Supporting Standards

Through OASIS and other standards initiatives, we now see the emergence of significant industry standards in and around XML. It is the stated intention of the working group to leverage relevant existing and emerging standards where ever possible. **Figure 2** shows how existing standards might be used in the context of **Figure1**. It depicts a SOAP transport envelope with SAML authentication (and implicit signing and encryption), with a PSTC provisioning request to make a DSML specified change to a directory resource. The working group believes the PSTC will be strongly influenced by (but not limited to) the standards initiatives listed below.

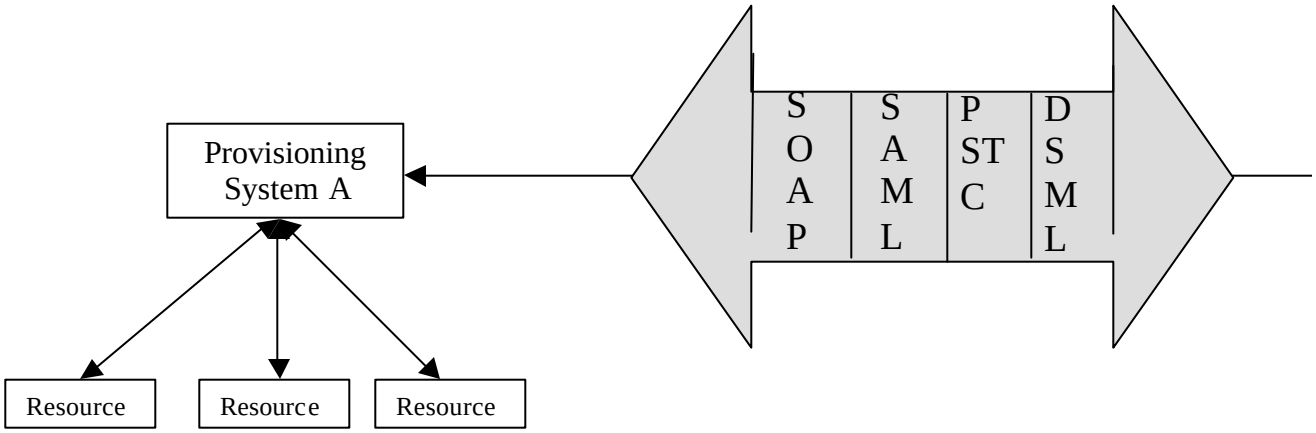

Figure 2. Possible Use of Existing Standards within This Effort

SOAP

SOAP [6] version 1.2 is a lightweight protocol for exchange of information in a decentralized, distributed environment. It is an XML-based protocol that consists of four parts: an envelope that defines a framework for describing what is in a message and how to process it, a transport binding framework for exchanging messages using an

underlying protocol, a set of encoding rules for expressing instances of application-defined data types and a convention for representing remote procedure calls and responses.

The working group envisions SOAP as one of the defined transports for provisioning requests. Other transports to consider are SMTP,….

SAML

SAML [7] is an XML-based security standard for exchanging authentication and authorization information. It is being defined by the Security Services TC (SSTC) under OASIS. The SSTC will produce set of one or more Committee Specifications that cover use cases and requirements, core assertions, protocols, bindings and a conformance suite, all of the aforementioned to be examined with respect to security considerations. The work takes into consideration the S2ML specification and the intended submission of AuthXML, along with other relevant and timely submissions. The goal (subject to revision) is to publish a substantially complete set of Committee Specifications by 1 Dec 2001, and submit a Committee Specification to the OASIS membership for its approval by 1 March 2002.

The working group envisions SAML as the exchange definition for authentication and authorization information.

XACML

XACML [8] is a core schema for representing authorization and entitlement policies n XML. It is being defined by the XACML Technical Committee under OASIS. XACML is expected to address fine grained control of authorized activities, the effect of characteristics of the access requestor, the protocol over which the request is made, authorization based on classes of activities, and content introspection (i.e. authorization based on both the requestor and potentially attribute values within the target where the values of the attributes may not be known to the policy writer). XACML is also expected to suggest a policy authorization model to guide implementers of the authorization mechanism.

DSML

DSML [9] is an XML specification for marking up directory services information. It is being defined by the Directory Services TC under OASIS. The Directory Services Markup Language (DSML) bridges the world of directory services with the world of XML. DSML 1.0 provided a means of representing directory information in XML. This Technical Committee is working on DSML 2.0 which will add support for querying and modifying directories

CIM

The DMTF Common Information Model (CIM) [10] is an approach to the management of systems and networks that applies the basic structuring and conceptualization techniques of the object-oriented paradigm. The approach uses a uniform modeling formalism that—together with the basic repertoire of object-oriented constructs—supports the cooperative development of an object-oriented schema across multiple organizations.

A management schema is provided to establish a common conceptual framework at the level of a fundamental typology—both with respect to classification and association, and with respect to a basic set of classes intended to establish a common framework for a description of the managed environment. The management schema is divided into these conceptual layers:

XML Signatures

The mission of this working group [11] is to develop an XML compliant syntax used for representing the signature of Web resources and portions of protocol messages (anything referenceable by a URI) and procedures for computing and verifying such signatures. This is a joint Working Group of the IETF and W3C

XML Encryption

The mission of this Working Group [12] (WG) is to develop a process for encrypting/decrypting digital content (including XML documents and portions thereof) and an XML syntax used to represent the (1) encrypted content and (2) information that enables an intended recipient to decrypt it.

The Proposed Charter

One of the first jobs of the PSTC will be to establish quorum and agree upon a formal charter for the group. The following was put forward by the working group.

> **Provisioning Services Technical Committee (PSTC) Proposal**
>
> **Name of the TC:**
> **OASIS Provisioning Services Technical Committee (PSTC)**
>
> **Statement of purpose:**
> **The purpose of the OASIS Provisioning Services Technical Committee (PSTC) is to define an XML-based framework for exchanging user, resource, and service provisioning information. The Technical Committee will develop an end-to-end, open, provisioning specification developed from Provisioning specifications including the following: (The following specifications are of public knowledge, accessible, and freely distributed).**
>
> **- Active Digital Profile (ADPr)**

- eXtensible Resource Provisioning Management (XRPM)
- Information Technology Markup Language (ITML)

And any other relevant and timely submissions will be taken into consideration.

Proposed list of deliverables and projected dates (subject to change): The PSTC will produce a set of one or more Committee Specifications that will cover the following:

- Use cases and requirements
- Information model
- Protocol(s)
- Bindings
- Conformance

All of the aforementioned are to be examined with respect to security considerations.

The goal (subject to revision) is to submit a Committee Specification to the OASIS membership for its approval by September 2002.

References

[1] XRPM web site at http://www.xrpm.org
[2] ADPr web site at http://www.adpr-spec.org
[3] "Peer-to-Peer Provisioning", XRPM discussion document, http://www.xrpm.org/docs/pstc/PSTC.zip
[4] "The Thinking Behind the Active Digital Profile", ADPr discussion document, http://www.adpr-spec.org/profile/initiative.htm
[5] "The Common Information Model", DMTF, http://www.dmtf.org/standards/standard_cim.php
[6] http://www.w3.org/TR/2001/WD-soap12-part1-20011002/
[7] http://www.oasis-open.org/committees/security/
[8] http://www.oasis-open.org/committees/xacml/
[9] http://www.oasis-open.org/committees/dsml/
[10] http://www.dmtf.org/standards/cim_spec_v22/
[11] http://www.w3.org/Signature/
[12] http://www.w3.org/Encryption/2001/