Review - ISO/IEC 24760-2:2015

IT Security and Privacy - A framework for identity management - Part 2: Reference architecture and requirements

"IT Security and Privacy - A framework for identity management - Part 2: Reference architecture and requirements," *International Organization for Standards*, Technical Committee ISO/IEC JTC 1, Subcommittee SC 27, June 2015, https://www.iso.org/standard/57915.html.

Reviewer: George Dobbs

Abstract

This is a summary of what is in ISO/IEC 24760-2:2015, one of the core ISO standards on IAM, along with an opinion on its suitability for use by the identity practitioner.

Review

This document is formal in nature and provides a rigorous model of an identity management system and a notion of what should be include in the design for that system. Those without architectural background may find the approach to be too academic, but if you are looking to add a degree of rigor to your plans, read on.

After the preliminaries the text jumps into a set of viewpoints that provide a minimally acceptable documented design; these are a context view and a functional view. The document then describes these views in terms of definitions, concerns, and models.

Moving on from viewpoints, the text takes up the two mandatory views in some detail. For the context view the text elaborates on stakeholders, actors, context model, use case model, and compliance and governance model. The elaboration regarding stakeholders may be useful as it identifies some of the stakeholders that are often forgotten, such as regulatory bodies, and the rarely mentioned consumer/citizen representative or advocate.

The text not only lists the set of stakeholders to consider; it also identifies their concerns. The text distinguishes between stakeholders and actors although there is significant overlap in the lists. Where stakeholders have concerns, the actors have responsibilities and, in some cases, provide capabilities, both of which are listed. The diligent reader may want to study the text of the actor section carefully as it is quite precise and conveys a lot of concepts in a small space.

The text moves on to the use cases. The text provides a simple use-case as an example, then describes several more specific classes of use-case (employee, employer, principal, and device). Interestingly enough, the text does not call out specific use case for Customer/Citizen, although it does for Employee. Instead these concepts are included in the Principal use cases section. Additional examples are given in Annex B. These examples should be useful. For a practitioner fluent in universal modeling language (UML) the diagrams and use-case section should be straightforward. For others, this may be harder hill to climb.

The context view is rounded out with a short section on what should be included in a compliance and governance model. This section provides a checklist.

Next up is the functional view. This section lists interactions expected between the actors and architectural elements in the system. It covers ten processes including maintenance of identity information, access to identity information, winding up with less common processes such as identity authority discovery and publication of identity information (under a policy). Again, these are tersely worded but should provide useful checklists to the practitioner. The functional components are laid out as a UML diagram in Annex C, which brings in a couple of new items such as “Trust Root”.

Before moving on to the requirements section, the text outlines 4 scenarios. The scenarios are used to determine the trust relationships that are needed. This brief section encourages the architect to design for confidentiality, integrity and trust needed by each scenario. There is very little detail provided. For instance, the federation scenario is described in abstract terms but there is no mention of the common notions of identity provider or relying party. But it does encourage the architect to at least consider what scenarios are desired, helping to establish requirements.

The main text wraps up with a listing of requirements, both functional and non-functional. This is an excellent source to use in establishing the requirements for a system.
In addition to Annexes A - C, the document provides Annex D, which elaborates on selected business processes including consent management, credential lifecycle management, configuration management (in a federation), policy management, and principal’s life cycle management.

Overall the document is very formal and structured, which enables consumption of the core foundation concepts of Identity Management. Access management is referenced only in a reflexive mode – to control the access to identity information itself. The more general access management may be covered in another ISO/IEC document: ISO/IEC 29146, *Information technology — Security techniques — A framework for access management.* This may lead the reader to a point of frustration if looking for details about authorization and authentication.

The reviewer finds this document to be valuable for the identity practitioner who is confronted with developing a new identity system or evaluating the current state of an identity system in order to mitigate gaps and shortcomings. It provides a structured framework of concepts that can be used to inform such work. That being said, it is a text that requires the reader to bring significant powers of mind and experience to the reading. The presentation does not cover access management; it focuses entirely on identity management. It refers to another ISO/IEC document for access management. There are a few other off-document references, but this reviewer feels those can be skipped without affecting the understanding too much. This document is appropriate for those seeking to build or revise a robust identity system and are seeking to compare their own thoughts to the work of others in order to gain assurance that a complete design has been produced.