

Review - ISO/IEC 24760-1:2019

"IT Security and Privacy - A framework for identity management - Part 1: Terminology and concepts," *International Organization for Standards*, Technical Committee ISO/IEC JTC 1, Subcommittee SC 27, May 2019, <https://www.iso.org/standard/77582.html>.

Reviewer: Corey Scholefield

Abstract

This review offers insight into the first part of the ISO standard for Identity Management, ISO/IEC 24760-1:2019, which covers terminology and concepts.

Review

ISO/IEC 24760-1:2019 provides an introduction to the vocabulary of the identity management space, with definitions of key terms in common usage within the community. Under review is the 2nd edition of the document, revised for 2019-May.

As stated in the introduction to the document:

The goal of this document is to specify the terminology and concepts for identity management, in order to promote a common understanding in the field of identity management.

According to its abstract:

It is applicable to any information system that processes identity information.

The document supports the goal by offering brief definitions of community-standard terms, such as:

- *identity*
- *attribute*
- *identifier*
- *principal*

- *identity-proofing*

While the tone of the document is slightly academic, the definitions themselves:

- are written using terms familiar to English-speakers;
- include other terms that appear in the document, with convenient links to access their definitions easily;
- include some examples to illustrate the usage of the term, or to illustrate the concept.

This document only includes terminology, concepts, and brief definitions and outlines. It is intended to be used as reference material.

The authors have taken some effort to ensure that these definitions can be applied to a broad set of use cases, i.e., definitions of identity for use within human and non-human (device) contexts. This treatment keeps some of the coverage at a high-level, causing the supporting examples to be quite helpful for providing a real-world abstraction of some concepts. That being said, this reader would have appreciated a few more examples to help support some of the definitions.

The article only contains one figure, which is supportive of the concept it depicts. The document could be improved by using more illustrations to outline concepts.

The bibliography section is excellent and provides links to many other foundational documents in the contemporary identity-management space. Many of those references are freely available for download. This document intends to provide authoritative definitions of terms and concepts, so other documents probably use to this one as a reference document.

A reader who needs a basic introduction to the common terms included in this document will find this material very helpful, as the terminology is very relevant in contemporary identity-management conversations.

The more-seasoned reader will also find a useful reference document but may also wonder about the omission of terms such as *persona*, *account*, or *authorization*. It could be that these terms (and others?) might not fall within a strict scope of *identity-management* that the authors wished to cover in this document. Instead, those terms may fall under the category of *access management*, a closely connected but separate body of information security knowledge.

The document does not support any treatment of identity in a social-science concept, so the definitions should be taken as they apply to identity-management in technical use cases.