Disposition of comments to FDIS 17960 Source Code Signing ballot 2015

This document passed with no National Body Comments. Comments were received from SC 27 WG 3, and are addressed in this document.

We thank SC 27 WG 3 for their consideration of our FDIS. IS 17960 is moving forward to publication at this time. The issues raised in your comments should be on the agenda of our joint meeting in Jaipur, India in October 2015.

For clarity, we include your recommendations below in italics, followed by our responses.

We agree with the technical content of your comments, but note that the resolution of these could be incorporated in one or all of the three standards under discussion. We look forward to the discussions in Jaipur.

Recommendations

There are four recommendations as follows.

1) *The scope of ISO/IEC 17960 is extended to recommend certain best practices in developer CM system and production support procedures. A good example of these best practices is the set of ISO/IEC 15408 ALC_CMC family of requirements. If the best practices are followed, then the ISO/IEC 17960 requirement of cryptographic signing of the source code file hash code values can be made optional.*

   Response: SC 22 WG 23 agrees that the best practices as specified in IS 15408 are relevant to the production and use of code signing. We would like to work with SC 27 WG 3 to produce the relevant material needed for the next revisions of both standards. As a minimum, each standard should acknowledge the requirements of the other.

2) *The scope of ISO/IEC 17960 is also extended to include an option for the generation of cryptographic hash code values of source code files as the source code files are compiled to produce the software, especially in the case where the developer already follows the recommended best practices in CM system and production support procedures.*

   Response: WG 23 stayed away from producing such specifications in deference to SC 27 work. As a joint undertaking for the next revision of IS 17960 in conjunction with SC 27 technical experts, this seems achievable.

3) *ISO/IEC 17960 project investigates the potential to develop a set of best practices for working with the generic model of some of the leading open source revision control systems. For example, Git (http://www.git-scm.com/) is an open source distributed revision control system for software*

source code files. These revision control systems do not talk about source code files directly. They talk about repositories which are data structures of metadata for sets of file and/or directory structures (http://git-scm.com/book/en/v2/Getting-Started-Git-Basics). While Git supports the concept of signing a repository update through its git-commit and git-push commands, it covers only the update and not the whole repository. It is more beneficial to see a closer alignment between the generic model of some of the leading open source revision control systems and the ISO/IEC 17960 requirements.

Response: We agree that this would be a beneficial addition. We look forward to working with SC 27 WG 3 to accomplish this.

4) *ISO/IEC 15408 to consider a requirement within its ALC_CMC family that the TOE production support procedures shall be able to generate or record unique identifiers to the implementation representation.*

Response: We agree with the benefits of unique identifiers for TOE, but note that they are insufficient for the authentication that IS 17960 requires. We would prefer that the authentication requirements of IS 17960 were incorporated in TOE.