Japanese Positions on Digital Signatures for OOXML

Japan
2016-09-10

ETSI SR 019 020 shows signing scenarios and validation scenarios. In particular, it shows both local signing scenarios (the signing key is held with the signer's personal device) and server signing scenarios (the signing key is held in a shared server). ETSI SR 019 020 further identifies several actors playing roles in these scenarios.

Japan believes that standardization of XAdES for OOXML should allow interoperability in these scenarios. Actors different from office suites should be allowed to interwork with other actors. Note that addition of archive timestamps is typically done by servers, and batch validation of multiple documents is also done by servers

However, interoperability is hampered if too many options are allowed. Japan believes that such options should be minimized.

As an example, ISO/IEC 29500 as of now does not specify which OPC part in a WML/SML/PML document should be signed. As a result, it is possible to digitally sign a WML document without signing document.xml. Even if validation succeeds for the WML document, its content might be significantly modified after the WML document was signed.

As another example, both OPC and XAdES provide mechanisms for counter signatures. In OPC, counter signatures can be created as different signature parts, some of which are signed by others. XAdES allows counter signatures by nested signatures. Japan believes that having both mechanisms complicates validation services and hampers interoperability without introducing any advantages.

To maximize interoperability, Japan has the following proposals:

1) Create amendments to 29500-1 and 29500-4 and specify which OPC part is signed
2) Prohibit those XAdES features (such as counter signatures) which are not useful in the context of OPC
3) Provide guidelines for multiple signatures (including counter signatures) in OPC.
4) Allow timestamped-but-not-signed OPC (see XMLERS). Note that PAdES-DT (ISO 14533-3) of PDF already provides timestamped-but-not-signed PDF documents.