Information technology — Security techniques — Entity authentication —
Part 3: Mechanisms using digital signature techniques

TECHNICAL CORRIGENDUM 1

As defined in ISO/IEC 9798-1, \( X || Y \) is used to mean the result of the concatenation of data items \( X \) and \( Y \) in the order specified. In cases where the result of concatenating two or more data items is signed as part of one of the mechanisms specified in this part of ISO/IEC 9798, this result shall be composed so that it can be uniquely resolved into its constituent data strings, i.e. so that there is no possibility of ambiguity in interpretation. This latter property could be achieved in a variety of different ways, depending on the application. For example, it could be guaranteed by (a) fixing the length of each of the substrings throughout the domain of use of the mechanism, or (b) encoding the sequence of concatenated strings using a method that guarantees unique decoding, e.g. using the distinguished encoding rules defined in ISO/IEC 8825-1 [1].
Add a bibliography on a new page after Annex A, as follows:

Bibliography