Chapter 9

Conclusions

Secure production and storage of digital documents in an office environment is an important problem to be studied as a major step towards realization of paper-less offices. Security, production and storage are the three aspects of the problem. In the present work, these aspects are studied, different issues are identified in each aspect and solutions for them are provided.

The perimeter of the study is defined by three frameworks: production framework, storage framework and security framework. Documents in an office are termed as Multi-Part Multi-Signature Documents (MPMSD) and are produced as cases of a Document Production Workflow (DPW). Based on the frameworks, a conceptual three-tier architecture for a DPW is presented. It is found that to address the security issues, involvement of an in-line TTP is mandatory. A protocol for production of MPMSDs as cases of a DPW, with an arbiter as an in-line TTP, is presented. This protocol addresses the security issues identified in the problem. Since the arbiter is a TTP and also in-line, therefore it is always an intermediary between two communicating parties. A communication between a sender and a receiver via the arbiter is an aggregation of communication between the sender and the arbiter and
the arbiter and the receiver. As a result the arbiter becomes one of the two communicating parties. Therefore, a digital signature scheme based on signed session key, suitable for such a scenario is proposed. This signature scheme is more efficient than RSA-based signature schemes used in existing solutions for office automation.

The context of creation of a document in an office is an important component of the organizational memory of an office. But hitherto this aspect has not been incorporated in any of the existing solutions for office automation. In the present work a study on this important component of document production is done. A multi-dimensional model, named Page Cube, for storage and retrieval of MPMSDs in an office with the contexts as the binding elements, is proposed. Documents are modelled in the scheme as pages or a tree of pages. A page is a point in the space defined by a set of orthogonal dimension hierarchies. The points are linked by bidirectional links forming dimensional graphs as well as inter dimensional graphs. Query languages to query pages from a Page Cube are also proposed. From the dimensional graph for the category dimension, the context can be produced. Algorithms to produce the dynamic context of a DPW as well as to produce a previous state of a context are discussed. The scheme to label the edges of the graphs with time stamps provide us the ability to recreate the previous states of a page. A model for dynamic authorization for DPW is also proposed as an extension of the Page Cube model. Implementation strategies of a DPW system, using state-of-the art technology have been provided. The implementation of a DPW system is meaningful if it is integrated as a subsystem of existing office automation software. Integration is easy in the CORBA framework. The output of the present work, which is academic in nature, may be input to future commercial paper-less office software. Here only a
guideline of implementation is given. The scope of the study is limited to a single office, where the office is considered as a single trust domain. But in real life, document production may be across multiple domains. The study of such inter-domain DPWs with multiple arbiters remains for the future.