ISO/IEC 23264-1:2021 (E)

Information security — Redaction of authentic data — Part 1: General

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Symbols and conventions

4.1 Symbols
4.2 Conventions

5 General model and processes

5.1 General
5.2 Parties and processes
5.3 General model
5.4 Specification of processes
5.4.1 Key generation process
5.4.2 Redactable attestation process
5.4.3 Redaction process
5.4.4 Verification process

6 Cryptographic properties of redactable attestation schemes

6.1 Required cryptographic properties
6.1.1 Correctness
6.1.2 Unforgeability
6.1.3 Privacy
6.2 Optional cryptographic properties
6.2.1 Undetectability of redactions
6.2.2 Detectability of redactions
6.2.3 Unlinkability of redactions
6.2.4 Disclosure control
6.2.5 Consecutive redaction control
6.2.6 Mergeability

Page count: 11