

ISO/TS 32002:2022-10 (E)

Document management - Portable Document Format - Extensions to Digital Signatures in ISO 32000-2 (PDF 2.0)

Contents		Page
Foreword		iv
Introduction		v
1 Scope		1
2 Normative references		1
3 Terms and definitions		1
4 Extension Schema Details		2
5 Digital signature enhancements		2
5.1 Elliptic curve cryptography		2
5.1.1 Specification of allowed elliptic curve algorithms		2
5.1.2 Proposed changes to ISO 32000-2:2020 Table 260 – SubFilter value algorithm support		2
5.1.3 Specification of allowed elliptic curves		3
5.1.4 Hash algorithm congruence for message digest and signed attribute digest		3
Bibliography		4