

# ISO/TS 32002:2022-10 (E)

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

---

<b>Contents</b>		<b>Page</b>
<b>Foreword</b>		<b>iv</b>
<b>Introduction</b>		<b>v</b>
<b>1</b>	<b>Scope</b>	<b>1</b>
<b>2</b>	<b>Normative references</b>	<b>1</b>
<b>3</b>	<b>Terms and definitions</b>	<b>1</b>
<b>4</b>	<b>Extension Schema Details</b>	<b>2</b>
<b>5</b>	<b>Digital signature enhancements</b>	<b>2</b>
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
<b>Bibliography</b>		<b>4</b>