

ISO/TR 24374:2023-04 (E)

Financial services - Security information for PKI in blockchain and DLT implementations

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols and abbreviated terms	2
5	Relevant issues - Distributed Ledger Technology (DLT) / Blockchain and PKI	3
5.1	DLT/Blockchain data security and privacy concerns	3
5.1.1	General	3
5.1.2	From centralised to decentralized	3
5.1.3	Instant exploitation	3
5.1.4	Protecting the key is critical	3
5.2	Problems and attacks associated with PKI systems	4
5.2.1	Current Challenges of Public Key Infrastructure	4
5.2.2	Attacks to PKI	4
5.3	Security objectives	5
5.4	Summary of the use of asymmetric key cryptography in blockchain networks	5
5.5	Private key storage	6
6	Security and privacy activities	6
6.1	Cryptographic tools	6
6.2	Governance activities	7
6.3	Operation activities	7
7	Blockchain and DLT controls	7
7.1	Technical Controls	7
8	Security and privacy processes	8
8.1	General	8
8.2	Standard advice on organisation security and privacy processes	8
8.2.1	General	8
8.2.2	Standard advice on risk analysis	8
8.3	Technical Design Elements	9
8.4	Legal Risk	9
9	Blockchain based PKI implementations	10
Annex A (Informative)		11
Annex B (Informative)		15
Bibliography		17