



BSI Standards Publication

Blockchain and distributed ledger technologies (DLTs) — Overview of trust anchors for DLT-based identity management

National foreword

This Published Document is the UK implementation of [ISO/TR 23644:2023](#).

The UK participation in its preparation was entrusted to Technical Committee DLT/1, Blockchain and Distributed Ledger Technology.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2023
Published by BSI Standards Limited 2023

ISBN 978 0 539 15639 3

ICS 35.030; 35.240.40; 35.240.99

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 May 2023.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

**Blockchain and distributed ledger
technologies (DLTs) — Overview
of trust anchors for DLT-based
identity management**





COPYRIGHT PROTECTED DOCUMENT

© ISO 2023, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	1
5 Types of trust anchors	2
5.1 Overview	2
5.2 Legal trust anchors	3
5.3 Data trust anchors	4
5.4 Cryptographic trust anchors	5
5.5 Cybersecurity trust anchors	5
5.6 Social trust anchors	6
6 Existing trust anchors for DLT-based identity management	7
6.1 Overview	7
6.2 Cryptographic trust anchors in public key infrastructures	8
6.3 Cryptographic trust anchors — Federated PKI	10
6.4 Social trust anchor architectures	12
6.5 Cryptographic trust anchors — Autonomic identifiers	13
6.6 Data trust anchors in eID regulations – eIDAS Regulation	13
6.7 Data trust anchors in non-PKI-based SSI solutions using DIDs	15
6.8 Data trust anchors in non-PKI-based, non-DID partial SSI solutions using ZKP	18
7 Using trust anchors	19
7.1 Representing multiple dimensions of risk	19
7.2 Chains of trust	21
7.2.1 General	21
7.2.2 Legal trust anchors	21
7.2.3 Data trust anchors	21
7.2.4 Cryptographic trust anchors	21
7.3 Use of trust anchors in applications	22
Bibliography	23

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 307, *Blockchain and distributed ledger technologies*, in collaboration with Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

In recent years, new decentralized digital identity management systems have emerged, some of them based in distributed ledger technologies (DLTs) providing support functions. As explained in [ISO/TR 23249](#), these include associating identifiers with public keys, supporting the attestation of credentials, enabling credentials revocation, defining common credential templates or implementing trust anchors.

DLT systems provide and rely on different types of trust anchors for DLT-based identity management, each being important in terms of some dimension of policy, technology, data, security, assurance, etc. Each trust anchor presents opportunities and risks to a DLT-based identity management system, and the DLT-based identity management system actors need guidance and standards to develop an appropriate operating model and risk mitigation strategy.

However, the DLT-based identity management system actors have also to take into account risks, including those shared with other organizations in chains of trust, and to have a governance model that is suitable for distributed and decentralized ecosystems formed by multiple actors. The DLT-based identity management system actors have to consider technological change and new types of technology with new risks that can address, create or result in opportunities and threats. The overall effectiveness of the DLT-based identity management system is critically dependent on the quality of the data it holds and shares; this is a high priority in DLT-based identity management system governance and operational models.

This document provides an overview of trust anchors for DLT-based identity management systems.

This page deliberately left blank

Blockchain and distributed ledger technologies (DLTs) — Overview of trust anchors for DLT-based identity management

1 Scope

This document describes concepts and considerations on the use of trust anchors for systems leveraging blockchain and distributed ledger technologies (DLTs) for identity management, i.e. the mechanism by which one or more entities can create, be given, modify, use and revoke a set of identity attributes.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

[ISO 22739:2020](#), *Blockchain and distributed ledger technologies — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in [ISO 22739:2020](#) apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

4 Abbreviated terms

AML	anti-money laundering
BIP	bitcoin improvement proposal
CA	certification authority
CAB	Certification Authority Browser (CA/Browser)
DID	decentralized identifier
DKMI	decentralized key management infrastructure
DKMS	decentralized key management system
DLT	distributed ledger technology
eIDAS	electronic identification, authentication and trust services
ETSI	European Telecommunication Standards Institute
EU	European Union
ID	identity

IDP	identity provider
IETF	Internet Engineering Task Force
IoT	internet of things
IP	internet protocol
KERI	key event receipt infrastructure
KYC	know your customer
LoA	level of assurance
LoIP	level of identity proofing
MPC	multi-party computation
OID	object identifier
PDP	policy decision point
PKI	public key infrastructure
RFC	request for comments
RP	relying party
SED	self-encrypting drive
SSI	self-sovereign identity
ToIP	trust over IP
TPM	trusted platform module
UID	unique identifier
VC	verifiable credential
ZKP	zero knowledge proof
ZVE	zero knowledge proof verification engine

5 Types of trust anchors

5.1 Overview

Identity management is defined in ISO/IEC 24760-1:2019, 3.4.1, as the “processes and policies involved in managing the lifecycle and value, type and optional metadata of attributes in identities known in a particular domain”. ISO/IEC 24760-1:2019, 3.1.2, defines identity as a “set of attributes related to an entity”, and ISO/IEC 24760-1:2019, 3.1.3, defines an attribute as a “characteristic or property of an entity”. Parties involved in identity management, such as relying parties (RPs), typically have trust relationships among them based in various features, which can be collectively designated as trust anchors.

There is no single definition of a trust anchor because it can mean different things to different people.

NOTE Some authors identify different types of trust anchors, including government trust anchors (i.e. see Reference [38]).

However, for the purposes of this document, the following five different types of trust anchor are described that exist within any governance model, even if they are not obvious (there can be more):

- Legal trust anchors are the trust anchors established and/or recognized by the legislation and regulations of relevant jurisdictions, by the contractual agreements and organizational by-laws. They set a legal foundation for the trust frameworks and underpin the operating rules and procedures. Legal trust anchors can mention or include references to other trust anchors.
- Data trust anchors are authoritative data sources that relate to the entities and attributes to be processed, where very high data quality is vitally important.
- Cryptographic trust anchors, which provide the roots of cryptographic trust and enable cryptographic binding, revocation, authentication, signing, encryption and other trust functions.
- Cybersecurity trust anchors, which monitor, detect and respond to policy violations, and enforce policy compliance. This includes assurance, testing and certification regimes, possibly augmented by the combined effort of a group responsible for defending an enterprise's use of information systems by maintaining its security (so-called "blue team"), known to the defenders, and a group of mock attackers ("red team"), unknown to the defenders.
- Social trust anchors. Subjective trust anchors can exist, particularly in the context of social situations and informal relationships where each individual can have a different view on the assessed risks and the requirements for risk mitigation or legal remedy.

In this document, reference is made to different levels of assurance, borrowed from [ISO/IEC 29115](#) and reflected in other ISO and ISO/IEC standards (maybe using different words) in order to provide a spectrum of risk mitigation measures in response to internal, external and shared risks. Broadly speaking, these are as follows:

- a) Level 1. Low assurance. Little confidence in identity, cybersecurity, counter fraud, data quality, etc. No significant risk mitigation strategy. No government-issued identity (ID) documents. Requires repeatability, e.g. user ID, email address. Major use case: social media.
- b) Level 2. Medium assurance. Medium confidence. Consumer-centric low-cost risk mitigation strategy for low-value financial risks. Expect failures. Some/increasing use of government-issued ID documents. Major use case: consumer credit/debit cards.
- c) Level 3. High assurance. High confidence. Strong risk mitigation strategy to address financial and non-financial risks, with the goal of preventing failures. Good use of government-issued ID documents and real-time authentication/validation. Major use case: employer/employee binding for employees acting digitally internally and externally on behalf of the organization.
- d) Level 4. Very high assurance. Very high confidence. Multiple government ID documents or real-time authentication/validation. Major use cases involve danger to life, public safety, high economic risk and national security.

There are other ways to convey this information, such as vectors of trust, as defined in IETF RFC 8485, that essentially provide the assurance information in a more granular way, considering different components or categories of information relevant in the context of authentication processes.

5.2 Legal trust anchors

Trust frameworks exist to describe the policies, procedures and mechanisms for the operation of digital trust across a community of trust, whether that exists in a legally binding agreement or whether it is mandatory across the nation or jurisdiction under the rule of law. In almost all cases, the starting point for a trust framework is the legal baseline upon which a policy framework is built, which forms the core of the trust framework. These policies, based upon legislation, are encapsulated and implemented in rulesets within the technological system, which are controlled through architectural components such as policy decision points (PDPs) and policy enforcement points (PEPs). Legal trust anchors underpin the operating rules.