ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T X.1411 (03/2023)

SERIES X: Data networks, open system communications and security

Secure applications and services (2) – Distributed ledger technology (DLT) security

Guideline on blockchain as a service (BaaS) security

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security (1)	X.1140–X.1149
Application Security (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1350–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1399
Distributed ledger technology (DLT) security	**X.1400–X.1429**
Application Security (2)	X.1450–X.1459
Web security (2)	X.1470–X.1489
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
Cyber Defence	X.1590–X.1599
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
Data protection	X.1770–X.1789
IMT-2020 SECURITY	X.1800–X.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1411

Guideline on blockchain as a service (BaaS) security

Summary

Recommendation ITU-T X.1411 provides generic security guidelines for blockchain as a service (BaaS). The security threats and vulnerabilities of BaaS are first analysed and then the security measures of BaaS are provided. The Recommendation also addresses security requirements and provides guidelines for all the activities in the construction, operation and use of BaaS.

Blockchain as a service (BaaS) has become mainstream in blockchain development due to its promising capabilities and the extensive support it has received from the industry, especially from top cloud providers. BaaS provides the fundamental service and resources for blockchain applications, however, it faces security challenges arising from both blockchain core technologies and cloud platforms. Guidance on Baas security is thus of great importance and a necessity.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1411	2023-03-03	17	11.1002/1000/15110

Keywords

Blockchain as a service, cloud computing environment, consensus protocol, smart contract, security.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Page

Recommendation ITU-T X.1411

Guideline on blockchain as a service (BaaS) security

1 Scope

This Recommendation specifies the guidelines on blockchain as a service (BaaS) security. It describes the definitions, structure, security threats and vulnerabilities, and measures of blockchain as a service. The security of the BaaS applications built on the BaaS is out of the scope of this Recommendation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1401] Recommendation ITU-T X.1401 (2019), *Security threats of distributed ledger technology*.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 blockchain as a service (BaaS) [b-ITU-T Y.3530]: A cloud service category in which the capabilities provided to the cloud service customer are the ability to set up blockchain platforms and develop decentralized applications using blockchain technologies.

3.1.2 cloud service customer [b-ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

3.1.3 cloud service provider [b-ITU-T Y.3500]: Party which makes cloud services available.

3.1.4 cloud service partner [b-ITU-T Y.3500]: Party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both.

3.1.5 consensus [b-ITU-T X.1400]: Agreement that a set of transactions is valid.

3.1.6 peer-to-peer [b-ISO 22739]: Relating to, using, or being a network of peers that directly share information and resources with each other without relying on a central entity.

3.1.7 proof of work [b-ITU-T X.1400]: Consensus process to solve a difficult (costly, time-consuming) problem that produces a result that is easy for others to verify.

3.1.8 smart contract [b-ITU-T X.1400]: Program written on the distributed ledger system which encodes the rules for specific types of distributed ledger system transactions in a way that can be validated and triggered by specific conditions.

3.1.9 threat [b-ISO/IEC 27000]: A potential cause of an unwanted incident, which may result in harm to a system or an organization.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 51% attack: An attack in which attackers control enough blockchain nodes or enough computational resources to revoke or rewrite the distributed ledger system ledger by controlling the generation of blocks.

3.2.2 network partition: A network connection scenario where the network is divided into more than one disconnected part.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
BaaS	Blockchain as a Service
BSC	Blockchain as a Service Customer
BSD	Blockchain as a Service Developer
BSP	Blockchain as a Service Provider
BSS	Blockchain as a Service Security developer
CPU	Central Processing Unit
CSC	Cloud Service Customer
CSN	Cloud Service partner
CSP	Cloud Service Provider
DDoS	Distributed Denial-of-Service
GPU	Graphics Processing Unit
IAM	Identity and Access Management
P2P	Peer-to-Peer
PII	Personally Identifiable Information
PoW	Proof of Work
SDK	Software Development Kit

5 Conventions

In this Recommendation:

The keywords "**is required**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

In the body of this Recommendation and its appendixes, the words "**shall**", "**shall not**", "**should**" and "**may**" sometimes appear, in which case they are to be interpreted, respectively, as is required to, is prohibited from, is recommended and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

6 Overview of blockchain as a service security

Blockchain as a service provides an integrated developing environment for both blockchain developers and customers to create, develop, test, host, deploy and operate blockchain related applications. As a result, BaaS customers can utilize the core blockchain components of the BaaS platform for efficient usage and easy deployment of blockchain networks and applications.

As the blockchain fundamental platform and service is built on the cloud service, there are three major roles participating in the functioning of BaaS, in correspondence to the roles in the cloud service.

- **Blockchain as a service provider (BSP):** In correspondence to the cloud service provider (CSP) in the cloud computing environment, BSP comprises of blockchain infrastructure and platform providers which make blockchain as a service available. BSP simplifies the development and usage of blockchains and applications with fundamental blockchain related resources and functions in terms of storage, communication, computation and networking support. BSP is responsible for the security of the fundamental blockchain resources and developing tools provided to other roles of BaaS.
- **Blockchain as a service developer (BSD):** In correspondence to the cloud service partner (CSN) in the cloud computing environment, BSD is engaged in developing and operating BaaS core components to assist BSP in providing blockchain service. BSD is responsible for the security of the developed core components.
  - **Blockchain as a service security developer (BSS)** is a specific type of BSD. BSS assists BSP in enhancing BaaS security as a third-party security service provider. Security services provided by BSS include identity and access management (IAM), audit, intrusion detection and others.
- **Blockchain as a service customer (BSC):** In correspondence to the cloud service customer (CSC) in the cloud computing environment, BSC comprises of the blockchain customers who request, access and use the blockchain service or resource via the functions provided by BSP directly, or via the applications and services provided by BSD indirectly. BSC is responsible for following the security rules provided by BSP in running its own blockchain network and applications. BSC is also encouraged to cooperate with BSP in monitoring the security of customized blockchain networks and reporting security events if necessary.

Interactions between these roles are presented in Figure 1.

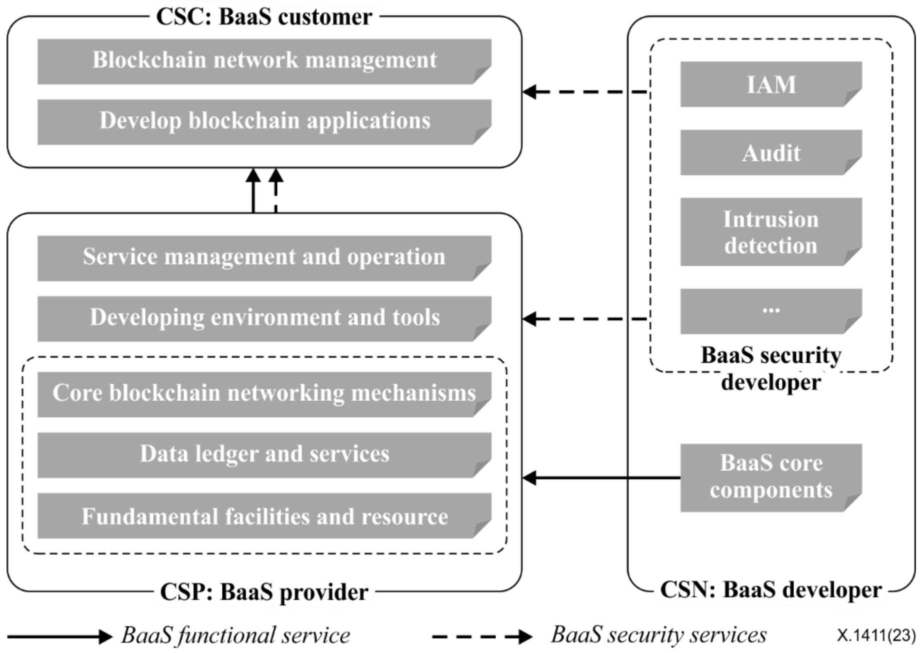

Figure 1 – Functions and interactions of roles in blockchain as a service

6.1 Overview of BSP security

BSP provides blockchain core functions including smart contracts, consensus protocols, peer-to-peer (P2P) connections, crypto algorithms, transaction records, ledger management, node and resource management, as well as the support of standardized development interfaces and security services. The functions of BSP and related security challenges are as follows.

6.1.1 Fundamental facilities and resources

BSP provides fundamental facilities to provide basic computation, communication, and other resources in supporting blockchain networking and application development. Such facilities can be physical devices or virtualized devices such as virtual machines and containers.

Fundamental facilities face challenges including environmental risks to physical facilities, backdoor injections, shared resources among tenants, etc.

6.1.2 Data ledger and services

BSP provides both on-chain and off-chain data services such as storage, management, enquiry of the customer and system data for BSC. Here, the on-chain data ledger guarantees tamper-resistance while the off-chain database supports efficient data services.

In terms of data security, BSP faces the following security challenges:

– unavailable data services, include inconsistent on-chain and off-chain data storage caused by network partitions, data loss caused by the breakdown of database and storage facilities, unauthorized revisions of data ledger, etc.

– privacy leakage, including unauthorized access to individual data, derivation of sensitive information from data, unsuccessfully destroyed private data, etc.

6.1.3 Blockchain core networking mechanisms

BSP provides a set of options in blockchain core networking mechanisms to simplify the set-up of customized blockchain networks. Blockchain core networking mechanisms comprise of consensus protocols, P2P connection protocols, and crypto algorithms. BSC can choose a specific set of networking components from all options and set corresponding parameters to quickly set up a customized blockchain network.

BSP is responsible for tackling security challenges to blockchain core networking mechanisms. These challenges affect the security of customized blockchain networks and even the blockchain applications built upon the BaaS platform, as BSC directly uses the blockchain core networking mechanisms to develop blockchain networks and applications. Here, security challenges include unauthorized access to blockchain resources, network partitions, malicious nodes, etc. For example, network partitions caused by unavailable blockchain services might lead to an unacceptable delay in reaching a consensus among the distributed blockchain network.

6.1.4 Developing environment and tools

BSP provides an integrated developing environment supplied with an application programming interface (API), development toolkit and other development tools, for simplifying blockchain application development. As the smart contract is an instinctive blockchain mechanism in developing blockchain applications, BSP also simplifies the deployment of smart contracts and provides a set of smart contracts for common functions, such as identity and access management.

Related challenges include inappropriate access control of the API, incompatible interfaces, unexpected running of smart contracts, etc.

6.1.5 Service management and operation

BSP is responsible for monitoring and alarming the blockchain service status, in terms of physical facilities, blockchain nodes, network connections and allocated resources, as well as IAM and other security management functions. BSP also supports and manages blockchain-related functions provided by BSD.

Related security challenges include unavailable management functions, inappropriate access management, unauthorized administration access, an explosion of consumed resources, and risks in blockchain-related components provided by BSD.

6.2 Overview of BSD security

BSD develops BaaS core components for BSP or provides security services for all roles.

6.2.1 Develop BaaS core components

BSD provides BaaS core components such as smart contracts, cryptographic algorithms, consensus protocols and crypto algorithms as a third-party provider.

Related security challenges and threats include incompatible interfaces, insecure protocol designs, backdoors in protocol implementations, etc.

6.2.2 Security services

BSS serves as the third-party security service provider for all roles in the BaaS ecosystem. For example, BSS can provide intrusion detection for BSP, code audit for BSDs, and IAM for BSC.

Security challenges include outdated security rules, improper operations of BSS employees, etc.

6.3 Overview of BSC security

BSC uses services provided by BSP and BSD to build up a customized blockchain network and blockchain applications. There are two types of BSC: one is the administrator that builds up and manages customized blockchain networks, and the other is the member which joins a customized blockchain network. For a specific BSC, it can be the administrator in one customized blockchain network and the member in another customized blockchain network.

All types of BSC face security challenges in key management and usage. The administrator also faces security challenges in the setup and management of customized blockchain networks, such as the improper setting of blockchain nodes, connections and other resources.

7 Security threats to blockchain as a service

Threats to BSP, BSD and BSC can be classified into three types:

- insecure technical designs, implementation flaws and inappropriate management of fundamental resources, blockchain core functions and blockchain service systems;
- insecure interactions among BSC, BSD and BSP, including incompatible interfaces, and an insecure supply chain;
- improper operations of employees, including inappropriate usage and storage of passwords.

Security threats to each role are presented in clauses 7.1 to 7.3.

7.1 Security threats to BSP

7.1.1 Threats to cloud service

Since BSP provides fundamental blockchain resources based on the cloud services, therefore BSP faces challenges and threats inherited from the cloud service, as presented in clauses 7 and 8 in [ITU-T X.1601]. For example, unauthorized access to a partition of another tenant's resource in the shared environment of cloud services could lead to blockchain forks of that tenant's blockchain system by rewriting or revising its data ledgers.

7.1.2 Threats to blockchain core networking mechanisms

Threats to consensus protocols, P2P connection protocols and crypto engines can be caused by vulnerabilities in protocol designs, flaws in mechanisms implementations, and inappropriate management. Details could be referred to in clause 6 in [ITU-T X.1401].

7.1.3 Unreliable data service

Threats to distributed data ledger include insufficient blockchain resources, flaws in the storage system and insecure storage management, which may lead to an inconsistent data record, data loss, data tampering and data leakage. For example, the system and blockchain data of a customized blockchain network expands when the blockchain network operates. In the case where BSP does not provide enough storage resources for the customized blockchain network to meet the data expansion, the customized blockchain network will overwrite the old data with new data or drop the new data directly, leading to data loss in the customized blockchain network. Another example is where, communication or storage facility failures could lead to inconsistent data storage at the distributed data ledgers. If the failures last a long time, the resultant network partitions lead to unexpected delays in block generations, data inquiry and other data services.

7.1.4 Threats to the developing environment

The integrated developing environment, compilation environment, smart contracts, APIs, software development kit (SDKs), and other development accessibility functions provided by BSP face threats in the process of designs, implementations, configurations, and operations of these development functions. For example, authentication flaws of the API could lead to unauthorized access and usage of the fundamental blockchain resource. Besides, smart contracts face security vulnerabilities in the logic design, contracts implementations and code management, such as integer overflows and underflows in a smart contract, resulting in unexpected running results.

7.1.5 Insecure third-party functions

BSP supports third-party functions provided by BSD and integrates them into the BaaS platform via APIs. Here, flaws and malwares in the third-party functions, as well as incompatible APIs and inappropriate access control of APIs, could lead to the disorder of the BaaS system.

7.1.6 Insecure system access

Insecure system access includes a lack of access control or inappropriate access control to the blockchain facilities, data ledger, network and applications. It could lead to blockchain data tampering, intrusions into customized blockchain networks, and leakage of private information.

7.1.7 Insider threats

BSP employees may accidentally or deliberately perform malicious behaviours, such as sharing passwords with unauthorized persons, leaving passwords in insecure areas, exposing personal information, etc. Insider threats could lead to leakage of private information, unauthorized access to customized blockchain networks and unavailable blockchain services.

7.1.8 Unreliable supply chain

The blockchain service platform uses software and hardware components supplied by various suppliers. A discontinued supply of software and hardware will undermine the abilities of computation, connections, and other resources of blockchain services. In this case, the availability of blockchain services is at risk. For example, the consensus protocol proof of work (PoW) relies on the competition of computation abilities among online blockchain nodes, therefore the discontinued supply of computation and connection abilities could affect the consensus results of PoW-based blockchain networks.

Besides, malware and exploitable vulnerabilities in software and hardware, as well as in open source blockchain architectures, could lead to unexpected block generations, denial of services, data leakage and misuse and so on.

7.1.9 Threats to physical environment

Fire, flood, thunder, and other environmental disasters to fundamental facilities could lead to the unavailability of physical facilities in providing communication, computation, and other fundamental resources. For example, a deliberate or an accidental power outage may result in a partition of blockchain nodes offline. In this case, the consensus process is under the control of a smaller number of blockchain nodes, leading to incorrect consensus results and extra delay in the block generation.

7.2 Security threats to BSD

7.2.1 Threats to third-party functions

BSD provides blockchain core components, blockchain security mechanisms, and blockchain application developing functions as a third-party provider. Related threats include inherent security vulnerabilities of blockchain core components, implementation flaws of these third-party functions, incompatible interfaces, and insecure access control of interfaces.

Besides that, the malicious behaviour of BSD employees could also lead to the leakage of private information, backdoors in third-party functions, and unexpected operations of security functions.

7.3 Security threats to BSC

7.3.1 Key leakage and loss

BSC manages keys by themselves or via a third-party service. Improper storage of keys, key file corruption, or unreliable third-party key services may lead to the loss or leakage of keys, resulting in the loss of BSC assets, private disclosure and disordered customized blockchain networks.

7.3.2 Improper management of customized blockchain networks

BSC sets up its own customized blockchain networks and deploys security mechanisms based on the blockchain functions provided by BSP and BSD. Here, improper configurations of customized blockchain networks and security mechanisms will threaten customized blockchain networks. For example, if BSC allocates non-sufficient storage resources for the operations of the customized blockchain network, the customized blockchain network could fail in updating blockchain data, finally leading to inconsistent blockchain data ledgers.

8 Security requirements of blockchain as a service

8.1 Security configuration of a customized blockchain network

BSP is recommended to provide recommendations on configurations of a customized blockchain network to meet the security requirements of BSC. Besides, BSP is recommended to provide recommendations on deploying necessary security mechanisms to the customized blockchain networks.

a) BSP is required to specify the recommended range of the total number of nodes.

b) BSP is required to specify the minimum number of online nodes to avoid 51% of threats and other known threats to the blockchain network.

c) BSP is required to specify the minimum number of neighbours of each node to avoid the blockchain network partition.

d) BSP is recommended to specify recommended types of nodes, with the number and rights of each type specified.

e) BSP is recommended to specify the minimum storage resource, central processing unit (CPU), and graphics processing unit (GPU) of each type of nodes.

f) BSP is recommended to specify the recommended consensus protocols and peer-to-peer protocols according to the node configurations.

g) BSP is recommended to provide basic security functions, including IAM and key management to the customized blockchain network.

h) BSP can optionally provide the security assessment of customized blockchain network configurations. BSP shall provide related security suggestions and solutions to BSC.

8.2 Identity and access management

BSP is recommended to provide identity and access management functions for the BaaS system and the customized blockchain network. Identity and access management functions are deployed not only to protect identities, but to also facilitate access management, authentication and authorization.

a) BSP is required to provide identity registration and deregistration functions for the BaaS system.

b) BSP is recommended to provide identity registration and deregistration functions for the customized blockchain network.

c) BSP is required to provide account access management for the BaaS system to differentiate BSP, BSC, and BSD.

d) BSP is recommended to provide account access management in the customized blockchain network. Any customized blockchain network shall have one or more roles of customers with various access rights.

e) BSP is required to provide access authentication for the BaaS system. Each identity can only access the resource according to its access right.

f) BSP is recommended to provide access authentication for the customized blockchain network.

g) BSP can optionally provide fine-grained access management functions, such as role-based access control functions.

h) BSP can optionally monitor the access activity frequency of the access IP, access account, access devices and others. Access activities include registration, deregistration, key update and others.

8.3 Key management

BSP is recommended to provide key management functions to protect the security of key generation, storage, distribution, usage, backup, recovery and revocation.

a) BSP is required to provide comprehensive key management schemes, clarifying the information of keys and the management procedure.

b) BSP is required to assess the security of random number algorithms and other parameters that are used to generate keys. Random number algorithms shall satisfy randomness and unpredictability.

c) BSP is recommended to support third-party key management functions. The security of third-party key management functions shall be assessed and guaranteed before being provided to BSC.

d) BSP is recommended to provide key revocation functions for deregistered and suspicious accounts.

e) BSP is recommended to provide key retrieval functions for lost keys. Only authenticated accounts can access key retrieval functions.

f) BSP is recommended to require BSC to update keys periodically. The update period shall be different according to the security levels.

g) BSC is recommended to deploy a key management function in the customized blockchain network.

h) BSC is required to master and follow the secure procedures of key usage, storage, retrieval and revocation, according to the key management function deployed in the customized blockchain network.

i) BSC is recommended to report the suspicious key usage to BSP as predefined in the key management function.

j) BSP can optionally use a two-party or multi-parties key storage scheme for the main keys and secret keys.

8.4 Privacy protection

BSP is recommended to provide protection on the collection, access, and other operations of personally identifiable information (PII).

a) BSP is required to abide by national and local regulations, policies and legislation related to privacy protection such as PII collection and PII storage.

b) BSP is required to provide de-identification on displayed PII.

c) BSP is required to deploy security measures to guarantee that on-chain PII can be deleted completely when required by BSC, such as using chameleon hash algorithm based blockchain technology, or to store PII off-chain.

d) BSP is recommended to invite professional organizations to perform audits on sensitive operations of PII.

8.5 Crypto engines security

BSP is recommended to guarantee the security of crypto engines that are deployed in customized blockchain networks.

a) BSP is required to support mainstream crypto algorithms, where security has been publicly verified.

b) BSP is required to invite professional organizations to audit the security of crypto engines.

c) BSP is recommended to support crypto engines provided by BSD. BSD is recommended to provide security assessment results of crypto engines.

8.6 Peer-to-peer connection security

BSP is recommended to guarantee that peer-to-peer connections resist against unreliable and malicious nodes.

a) BSP is required to provide authentication schemes to manage access to peer-to-peer networks.

b) BSP is required to use cryptographic technology to establish secure transmission channels between distributed nodes.

c) BSP is required to support peer-to-peer protocols with reliability and scalability. Reliability indicates that disconnected nodes keep consistency with other nodes after reconnecting. Scalability indicates that protocols support dynamically, or statically adding or deleting nodes with blockchain networks running normally.

d) BSP is required to support peer-to-peer protocols in any node that has more than one neighbour.

e) BSP is recommended to support peer-to-peer protocols so that any disconnected node will not lead to network partitions.

f) BSP is recommended to provide real-time topology of the peer-to-peer network.

g) BSP is recommended to provide an alert if the peer-to-peer network faces partitions or malicious nodes.

8.7 Consensus mechanism security

BSP is recommended to guarantee that the design and operations of the consensus mechanism are secure.

a) BSP is required to provide consensus algorithms where security has been publicly proved or assessed.

b) BSP is required to support BSC to deploy consensus algorithms provided by BSD.

c) BSP is required to provide security assessment of consensus algorithms to BSC. The security assessment shall include the threshold number of consensus nodes, the recommended consensus frequency and others.

d) BSP is required to guarantee that consensus nodes are authenticated before joining the consensus.

e) BSP is required to monitor the consensus process and assess the consensus period, consensus node and the consensus result.

f) BSP is recommended to provide alerts and solutions when the monitored consensus process is assessed as abnormal.

8.8 Smart contract security

BSP is recommended to provide comprehensive life cycle management for smart contracts, including smart contract creation, deployment, upgrade, trigger, execution and abolishment.

a) BSP is required to provide code specifications, logic requirements and other normative guidance on smart contracts.

b) BSP is recommended to provide a trusted isolated environment, such as a sandbox, for running smart contracts.

c) BSP is required to provide appropriate access management for smart contracts to restrict malicious operations or prevent wrong smart contracts from infecting other contracts.

d) BSP is required to support security emergency response mechanisms for smart contracts.

e) BSP is required to limit the complexity of smart contracts in terms of resource consumption and execution time.

f) BSP is recommended to monitor and control the excessive consumption of blockchain resources by smart contracts.

g) BSP is recommended to support the termination of smart contracts when smart contracts exceed the resource restriction.

h) BSP is recommended to provide technical solutions to prevent distributed denial-of-service (DDoS) attacks related to the smart contract.

i) BSP is recommended to have BSD to provide functions to automatically detect the security vulnerabilities of smart contract source code and smart contract byte code.

j) BSP is recommended to have BSD monitor smart contract activities for discovering early warning abnormal behaviours of smart contracts.

8.9 Resource monitoring

BSP is recommended to monitor the resource consumption in BaaS and provide an alert when the resource status is abnormal.

a) BSC is recommended to allow BSP to monitor the resource consumption of nodes in the customized blockchain networks, in terms of storage, computation, CPU, network connections, online status, online duration and others.

b) BSP is recommended to provide a resource shortage alert to BSC when the nodes of the customized blockchain network face resource shortages. BSP shall provide BSC solutions to relieve the resource shortage.

c) BSC is recommended to allow BSP to monitor the network status of customized blockchain networks in terms of block generation rate, block generators, block size and others.

d) BSP is recommended to provide an intrusion alert to BSC when the network status is monitored as abnormal. BSP shall provide BSC with the according abnormal analysis, related abnormal node information and recommended solutions.

8.10 Intrusion detection system

BSP is recommended to provide and update mechanisms to prevent malicious code and other intrusions.

a) BSP is required to provide smart contract security rules and a vulnerability library. BSP shall provide access interfaces in a common form for vulnerability detection.

b) BSP is required to install anti-malware software or configure software with corresponding functions to detect and remove malware.

c) BSP is recommended to provide malicious code prevention in each blockchain node and eliminate the malicious code before accessing the blockchain network.

d) BSP is recommended to provide regulations on the malicious code prevention mechanisms, including periodically upgrading the malicious code library, and regularly checking and killing malicious code.

e) BSP is recommended to have BSD regularly assess the effectiveness of technical measures against malicious code attacks.

8.11 Security audit

BSP is recommended to have one or more BSDs to perform a security audit on blockchain infrastructure, source code and other basic functions.

a) BSP is recommended to select more than one BSD to perform security assessment and audit on blockchain basic software, network and other operating environments before blockchain service online, to ensure that the security risks at the infrastructure level are controllable.

b) BSP is recommended to have at least one BSD to perform a security audit of source code, which mainly focuses on the risks and quality problems at the source code level.

c) BSD is recommended to provide the source code audit report to BSP with compliance / violation items and revision suggestions for the source code listed.

d) BSP is recommended to have BSD assess IAM functions to ensure that there are no risks such as private key leakage and user information leakage.

8.12 Third-party functions management

BSP is recommended to guarantee third-party functions operate securely as predefined.

a) BSP is required to clarify the security and functional requirements of the third-party providers.

b) BSP is required to sign service component cooperation agreements with third-party service providers and clarify their obligations and responsibilities.

c) BSP is recommended to monitor or audit the service of the third-party services and assess its services with the signed agreement.

8.13 Supply chain security

BSP is recommended to guarantee that its supply chain is robust against malicious providers and provider change.

a) BSP is required to develop supply chain security management policies and procedures, including security management criteria of supply chain participants.

b) BSP is required to assess its supply chain vulnerability in infrastructure, and open source usage in the system on a routine base.

c) BSP is recommended to inform BSC about the supply chain risks in the blockchain as a service system.

d) BSP is required to confirm the diversity of its providers of the indispensable software and hardware.

Table 1 – Security requirements of BaaS

Security threats		Security requirements												
		Security configuration	IAM	Key management	Privacy protection	Crypto engines security	P2P connection security	Consensus mechanism security	Smart contract security	Resource monitoring	Intrusion detection system	Security audit	Third-party functions management	Supply chain security
BSP	7.1.1	✓	✓	✓	✓				✓			✓	✓	✓
	7.1.2					✓	✓	✓	✓		✓	✓	✓	✓
	7.1.3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	7.1.4							✓	✓	✓	✓			
	7.1.5										✓	✓	✓	✓
	7.1.6		✓	✓										
	7.1.7		✓										✓	
	7.1.8											✓	✓	✓
	7.1.9												✓	
BSD	7.2.1			✓	✓	✓	✓	✓		✓	✓		✓	
BSC	7.3.1		✓	✓										
	7.3.2	✓								✓			✓	

Bibliography

[b-ITU-T X.1400] Recommendation ITU-T X.1400 (2020), *Terms and definitions for distributed ledger technology*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[b-ITU-T Y.3530] Recommendation ITU-T Y.3530 (2020), *Cloud computing – Functional requirements for blockchain as a service*.

[b-ISO 22739] ISO 22739:2020, *Blockchain and distributed ledger technologies – Vocabulary*.
<https://www.iso.org/standard/73771.html>

[b-ISO/IEC 27000] ISO/IEC 27000:2018(en), *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.
<https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2023