Work items in ITU-T SG17Q14

ITU Workshop on DLT security, identity management and privacy

20 February 2023, Geneva, Switzerland (Remote)

Ke WANG, ITU-T SG17Q14

Standardization System

Security protection of DLT

X.1401:**Security threats** to distributed ledger technology

X.1402:**Security framework** for distributed ledger technology

X.1404:**Security assurance** for distributed ledger technology

X.sc-dlt:**Security controls** for distributed ledger technology

TR.qs-dlt: Guidelines for **quantum-safe** DLT systems

X.srscm-dlt: Security requirements for **smart contract** management based on DLT

Security protection of DLT based applications

X.1405:Security threats and requirements for **digital payment services** based on DLT

X.1406:Security threats to **online voting** systems using DLT

X.1407:Security requirements for **digital integrity proofing** service based on DLT

X.1408:Security threats and requirements for **data access and sharing** based on the DLT

X.1410:Security architecture for **data-sharing management** based on DLT

X.1403:Security guidelines for using distributed ledger technology for **decentralized identity management**

Using DLT for security

X.1409:**Security services** based on distributed ledger technology

Terms and Definitions

X.1400 :Terms and definitions for distributed ledger technology

X.1400: Terms and definitions for distributed ledger technology

Status: Published on 2020-10

Summary:

X.1400 contains a baseline set of terms and definitions for distributed ledger technology (DLT).

account	address	application	asset	bitcoin	block	**block header**	blockchain	**blockchain system**	blockchain as a service(BaaS)
Byzantine fault tolerance	compliance	consensus	consensus mechanism	crash fault tolerance	decentralized application	decentralized autonomous organization (DAO)	**decentralized system**	delegated proof of stake (DPoS)	digital signature
distributed ledger	**distributed ledger technology (DLT)**	**DLT system**	DLT oracle	fork	genesis block	governance	hard fork	hash function	hashing
hybrid permission	**immutability**	**incentive mechanism**	inter ledger interoperability	intra ledger interoperability	ledger	Merkle tree	node	nonfungible token (NFT)	**off-chain**
on-chain	participant	**peer-to-peer**	permission	**permissioned**	**permissionless**	permissioned distributed ledger system	permissionless distributed ledger system	proof of work	proof of stake
public key cryptography	**public DLT system**	**private DLT system**	**sidechain**	smart contract	soft fork	**subchain**	stateful contract	stateless contract	stateful execution of contract
stateless execution of contract	token	token ecosystem	tokenomics	transaction	wallet				

- **Security protection of DLT**
- Security protection of DLT based applications
- Using DLT for security

X.1401:Security threats to distributed ledger technology

Status: Published on 2020-7

Introduction:

A distributed ledger system may still faces kinds of security threats to its components.

X.1401 provides a structured and systematic threat analysis method and lists threats to protocol, network, data components.

Each of the threat is described in dimensions:

– targeted component;

– attacks;

– attack impact;

– attack likelihood;

– an index to each security threat with attack methods or vulnerabilities to be referenced.

Ind #	IDCOMPONENT CLASS THREATS	COMPONENT THREATS	COMPONENT VULNERABILITYATTACKS	ACRONYM
1.0	ProtocolThreat Class (PTC)	PTC Threats	Protocol Component Attacks (PCA)	
1.1	P-CMT	Consensus Mechansim Threats		CM
1.1.1	P-CM-51		51% Attack	CM-51A
1.1.2	P-CM-TM		Timestamp Manipulation Attack	CM-TMA
1.1.3	P-CM-B		Bribing Attack	CM-BA
1.1.4	P-CM-SM		Selfish Mining Attack	CM-SMA
1.1.5	P-CM-CH		Chain Hopping Attack	CM-CHA
1.1.6	P-CM-BW		Block Withholding Attack	CM-BWA
1.1.7	P-CM-DS		Double-Spending Attack	CM-DSA
1.2	P-SCT	Smart Contract Threats		SC
1.2.1	P-SC-TD		Timestamp Dependence Attack	SC-TDA
1.2.2	P-SC-ME		Mishandled Exceptions Attack	SC-MEA
1.2.3	P-SC-IO		Integer Overflow Attack	SC-OIA
1.2.4	P-SC-PRN		Predictable Random Number Attack	SC-PRNA
1.3	P-VMT	Virtual Machine Threats		VM
1.3.1	P-VM-E		Escape Attack	VM-EA
1.3.2	P-VM-FH		Fault Handling Attack	VM-FHA
1.3.3	P-VM-MC		Memory Corruption Attack	VM-MCA
1.4	P-CHAT	Cryptographic Hash Algorithm Threats		CHA
1.4.1	P-CHA-C		Collision Attack	CHA-HCA
1.4.2	P-CHA-SP		Second Preimage Attack	CHA-SPA
1.4.3	P-CHA-PE		Preimage Attack	CHA-FPA
1.5	P-ACAT	Asymmetric Cryptographic Algorithm Threats		ACA
1.5.1	P-ACA-WKMA		Weak Key Material Attack	ACA-WKMA
1.5.2	P-ACA-BA		Backdoor Attack	ACA-BA
1.5.3	P-ACA-MCCA		Mathematical Cryptanalysis Cracking Attack	ACA-MCCA
1.5.4	P-ACA-PMMA		Protocol Message Manipulation Attack	ACA-PMMA
1.6	P-PQCT	Practical Quantum Computers Threats		PQC
1.6.1	P-PQC-CPA		Cryptographic Protocol Attack	PQC-CPA
1.6.2	P-PQC-BFCA		Brute Force Cracking Attack	PQC-BFCA
1.6.3	P-PQC-DSA		Digital Signature Attack	PQC-DSA
2.0	Network Threat Class (NTC)	Network Components Threats	Network Component Attacks (NCA)	
2.1	N-NRTT	Node Routing Table Threat		NRT
2.1.1	N-NRT-EA		Eclipse Attack	NRT-EA
2.2	N-DDOST	Network DDOS Threat		DDOST
2.2.1	N-DDOS-DA		DDoS attack	N-DDOSA
2.3	N-NIT	Node Identity Threats		NNI
2.3.1	N-NI-SA		Sybil Attack	NNI-SA
2.3.2	N-NI-FNIA		Fraudulent Node Identity Attack	NNI-FNIA
2.4	NRT	Network Routing Threats		NRT
2.4.1	NR-PA		Partition Attack	ISP-PA
2.4.2	NR-DA		Delayed Attack	ISP-DA
3.0	Data Threat Class (DTC)	Data Component Threats	Data Component Attacks (DCA)	
3.1	D-ATDT	Account Data & Transaction Data Threats		ATD
3.1.1	D-ATD-PSDA		Public Sensitive Data Attack	ATD-PSDA
3.1.2	D-ATD-AA		Analysis Attack	ATD-AA
3.1.3	D-ATD-UAA		Unauthorized Access Attack	ATD-UAA
3.2	D-PKLeT	Private Key Leakage Threats		PKLeT
3.2.1	D-PKLe-SCA		Software Client Attack	PrK-SCA
3.2.2	D-PKLe-PA		Physical Attack	PrK-PA
3.3	D-PKLoT	Private Key Loss Threats		PKLoT
3.3.1	D-PKLo-MA		Malware Attack	PrK-MA
3.3.2	D-PKLo-FUD		Forget Unlocking Data	PrK-FUD
3.3.3	D-PKLo-UL		Unlocking Loss	PrK-UL
3.3.4	D-PKLo-PCL		Paper Private Key Code Loss	PrK-PCL
3.4	D-TT	Transactions Threat		TT
3.4.1	D-TT-SBA		Spam Block Attack	TD-SBA

X.1402:Security framework for distributed ledger technology

Status: Published on 2020-7

Introduction:

Based on analysis of security threats and security requirements to DLT, X.1402 describes security capabilities list that could mitigate the related security threats and specifies a methodology to determine security capabilities to a specific DLT system.

A security framework analysis for commodity tracing as a service on a private distributed ledger system

		Security capabilities																
Security requirement	Security threat	Merkle tree	Time stamp	Digital signature	Data encryption	Security storage	Routing attack defence	Sybil attack defence	Eclipse attack defence	DDoS attack defence	Consensus mechanism	51% Attack defence	Selfish mining attack defence	Double-spending attack defence	Identity Authentication	Authorization	Multi-signature	Smart contract security design
Data	Private key leakage				Y	Y												
	Data leakage	Y	Y	Y	Y	Y												
Network	DDoS attack																	
	Sybil attack on network							Y										
	Routing attack						Y											
	Eclipse attack																	
Consensus	51% Attack										Y							
	Double-spending attack										Y							
	Selfish mining attack										Y							
Application	Smart contract attack														Y	Y		Y

X.1404: Security assurance for distributed ledger technology

Status: Published on 2020-10

Introduction:

Assurance of DLT is defined as the degree of confidence that the process or deliverable meets defined characteristics or objectives. An assurance level could be considered as a quantitative expression of assurance agreed among the relevant parties.

- X.1404 defines three levels(low-medium-high) of security assurance for the DLT.
- It defines ten security assurance components encompassing security assurance and specifies criteria and guidelines for achieving each of the three levels of a security assurance component.

Selection of the appropriate LoSA based on a risk assessment of the transactions or services based on DLT			
Possible consequences of security failure	**Potential Protection impact by LoSA**		
	1	**2**	**3**
Inconvenience, distress or damage to standing or reputation	Low	Substantial	High
Financial loss or agency liability	Low	Substantial	High
Harm to the organization, its programs or public interests	N/A	Low/Substantial	High
Personal safety	N/A	Low	Substantial/High
Civil or criminal violations	Low	Low/Substantial	High

Criteria and guidelines for achieving 3 levels covering 10 security assurance components		
Level	**Description**	**data integrity, data confidentiality, credential management, identity proofing of users, entity authentication, access control, data obfuscation, consensus mechanism strength, smart contract and PII data protection**
LoSA1 – low	Minimal confidence in the respective security assurance component of DLT.	...
LoSA2 – medium	Some confidence in the respective security assurance component of DLT.	...
LoSA3 - high	High confidence in the respective security assurance component of DLT.	...

X.sc-dlt:Security controls for distributed ledger technology

Status: Under study

Introduction:

X.sc-dlt provides guidelines for organizational information security practices including the selection, implementation and management of controls on distributed ledger technologies.

TR.qs-dlt: Guidelines for quantum-safe DLT systems

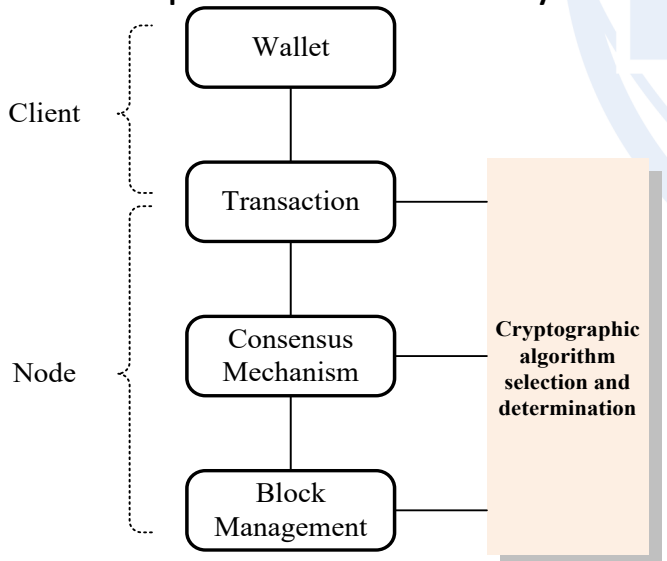
Status: Under study

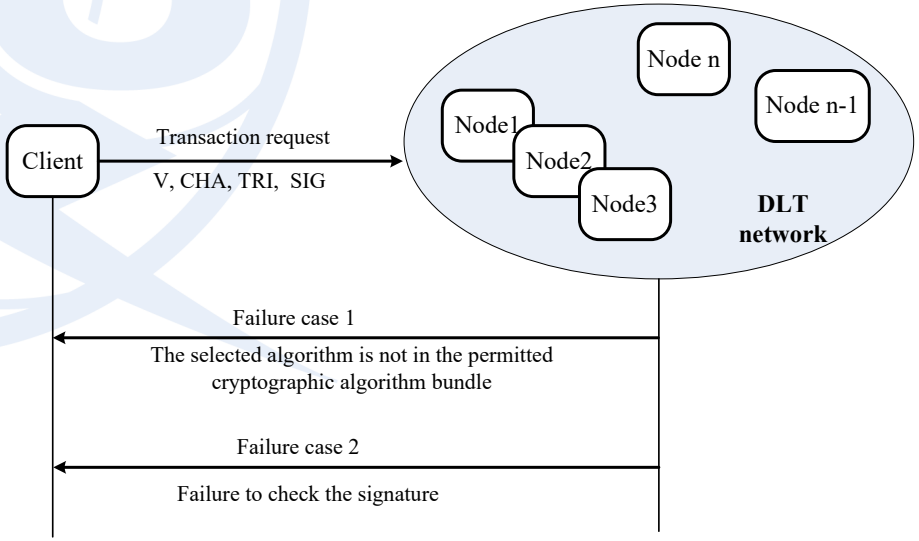
Introduction:

- TR.qs-dlt analyses impact of quantum computing on symmetric cryptographic algorithms, asymmetric cryptographic algorithms, hash algorithms and then the impact of quantum computing on permission-less and permissioned DLT system respectively.

	Permissionless DLT	**Permissioned DLT**
Account management	Affected but can be mitigated	Broken
Access control	Not applied	Broken
Transaction process	Affected but can be mitigated	Broken
Consensus mechanism	Most not affected, a small part broken	Most broken, a small part not affected.
Integrity protection of the ledger	Not affected	Not affected
Data confidentiality on the ledger	Affected but can be easily mitigated	Affected but can be easily mitigated
Message transmission	Not affected	broken

- TR.qs-dlt describes the requirements of a quantum-safe DLT systems including using quantum-safe cryptographic algorithms,supporting heterogeneous nodes and clients, Flexible deployment of cryptographic algorithms and gives the guidelines to build a quantum-safe DLT system.





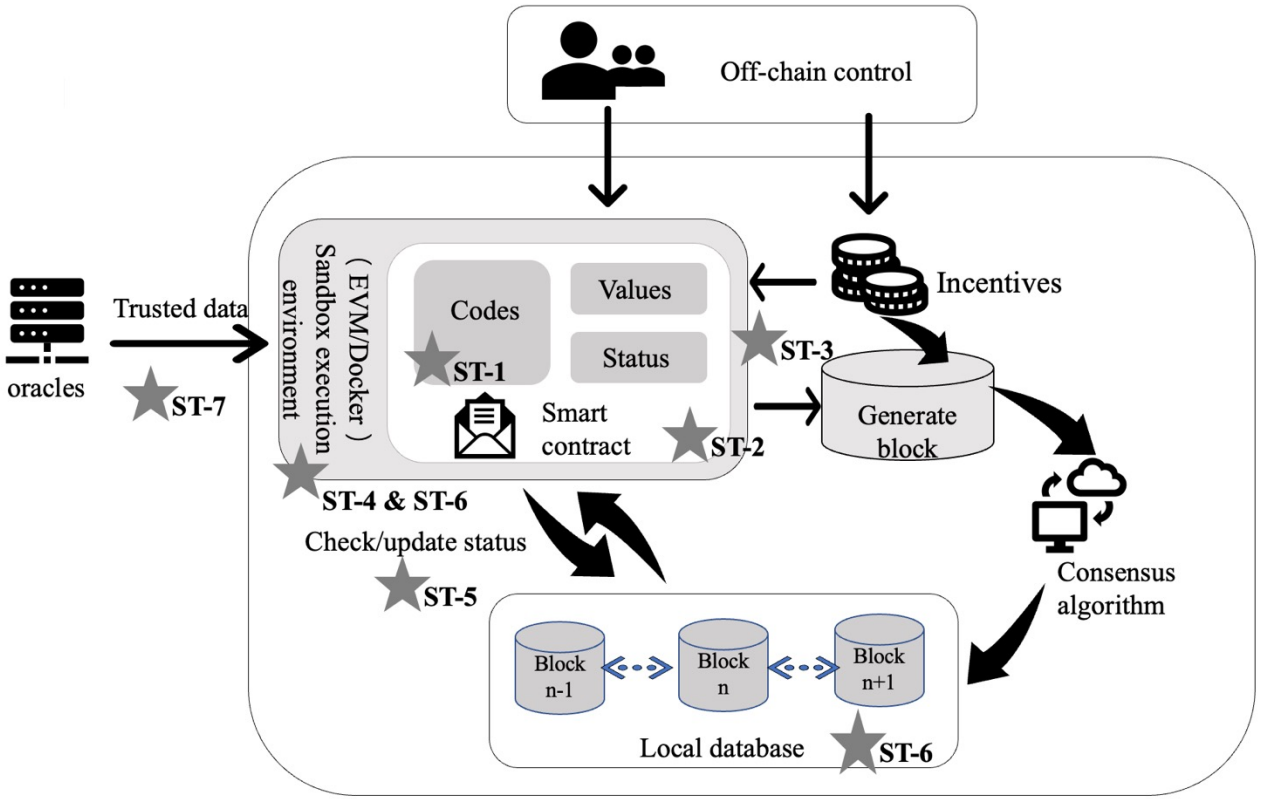
- TR.qs-dlt will discuss measures to migrate from a current DLT system using existing cryptographies to the quantum-safe DLT system using quantum-safe cryptographic algorithm.

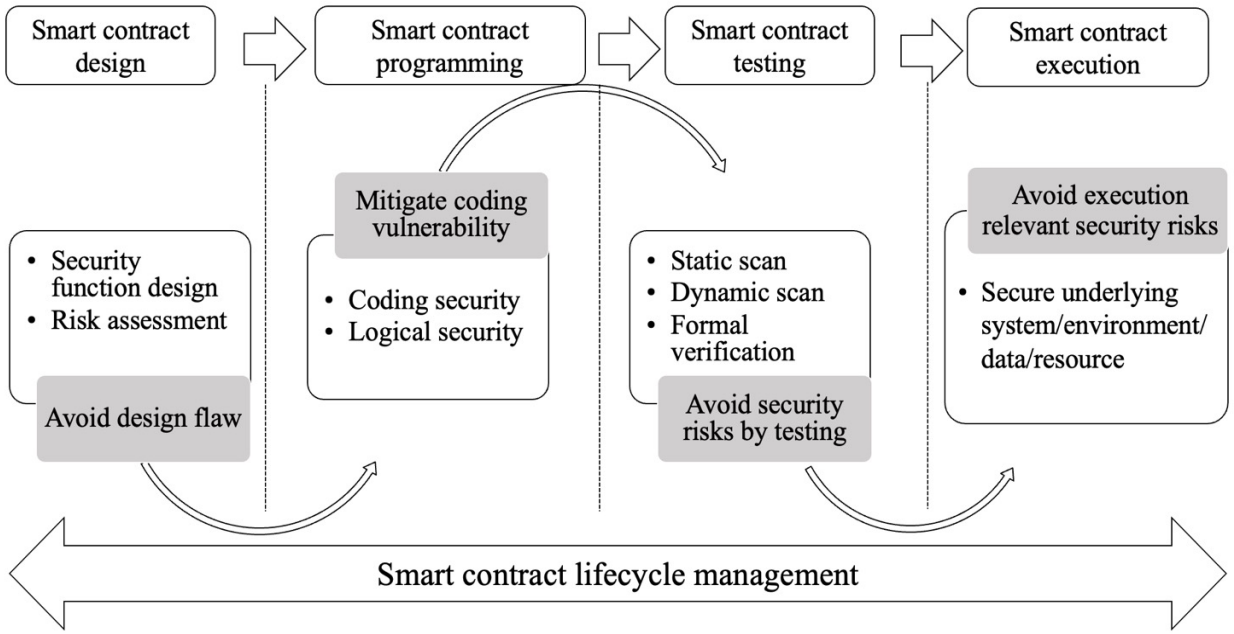
X.srscm-dlt: Security requirements for smart contract management based on the distributed ledger technology

Status: Under study

Introduction:

- X.srscm-dlt analyses the security threats and challenges of the smart contract in a DLT system.
- X.srscm-dlt specifies the security requirements to introduced through the whole smart contract lifecycle.





- Security protection of DLT
- **Security protection of DLT based applications**
- Using DLT for security

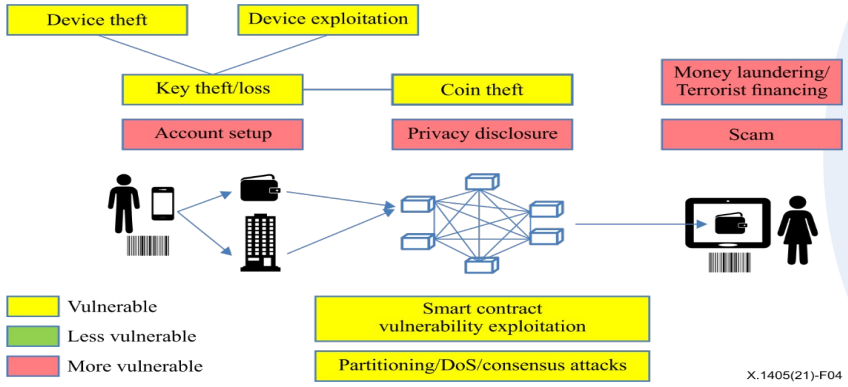
X.1405:Security threats and requirements for digital payment services based on distributed ledger technology

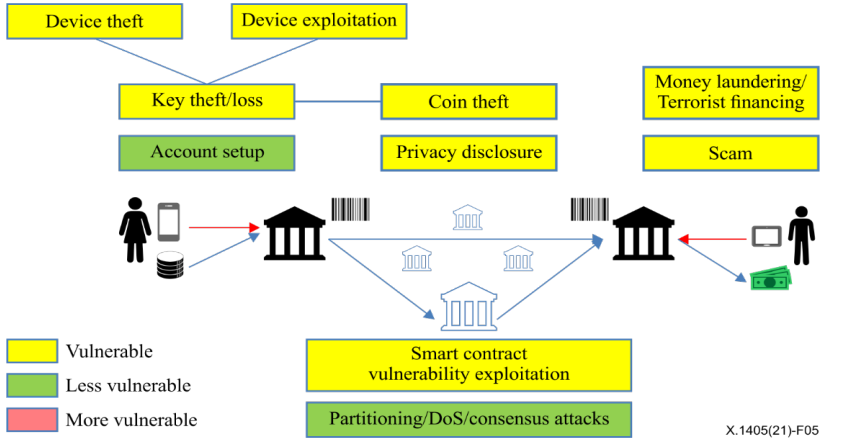
Status: Published on 2021-6

Introduction:

Digital payment services are used to transfer money from one account to another. Various digital financial services based on DLT are developed and operated in the real world.

X.1405 provides use cases analysis and the basic service model, Security threats and Security requirements





Threats	secure devices	secure nodes	Secure cryptographic	real name verification	Incident monitor response	Data confidentiality	Smart contract test	key manage	Different keys	Governing rules	user responsibility
Account set-up threats	√		√	√		√		√	√		√
Transaction threats	√		√		√	√	√	√	√	√	√
Scam					√			√			√
Systematic threats		√			√		√	√		√	
Money laundering / terrorist financing				√	√						
Insecure custodial and safekeeping services threats		√	√		√	√		√	√	√	√
Interoperability challenges	√	√	√		√	√	√	√	√	√	

X.1406:Security threats to online voting systems using distributed ledger technology

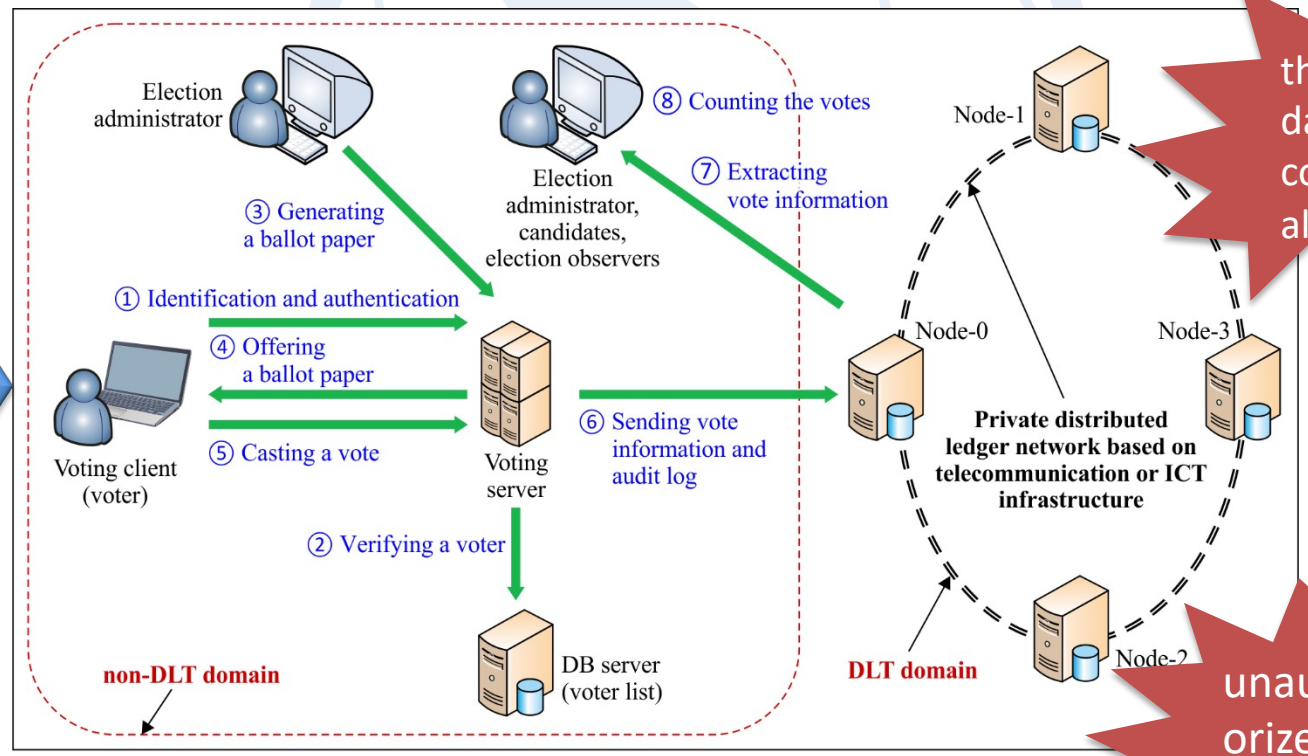
Status: Published on 2021-7

Introduction:

Many countries have implemented online voting systems using DLT based on telecommunication or ICT infrastructure.

X.1406 lists the required security considerarions of an online voting service and Potential security threats that could occur during the online voting service using DLT. .

1. data confidentiality
2. verifiability
3. robustness
4. receipt-free status
5. correctness
6. integrity
7. uniqueness;
8. voter authentication
9. coercion resistance
10. zero trust



threats to data confidentiality

threats to data integrity

threats to service availability

unauthorized access

malicious behaviour

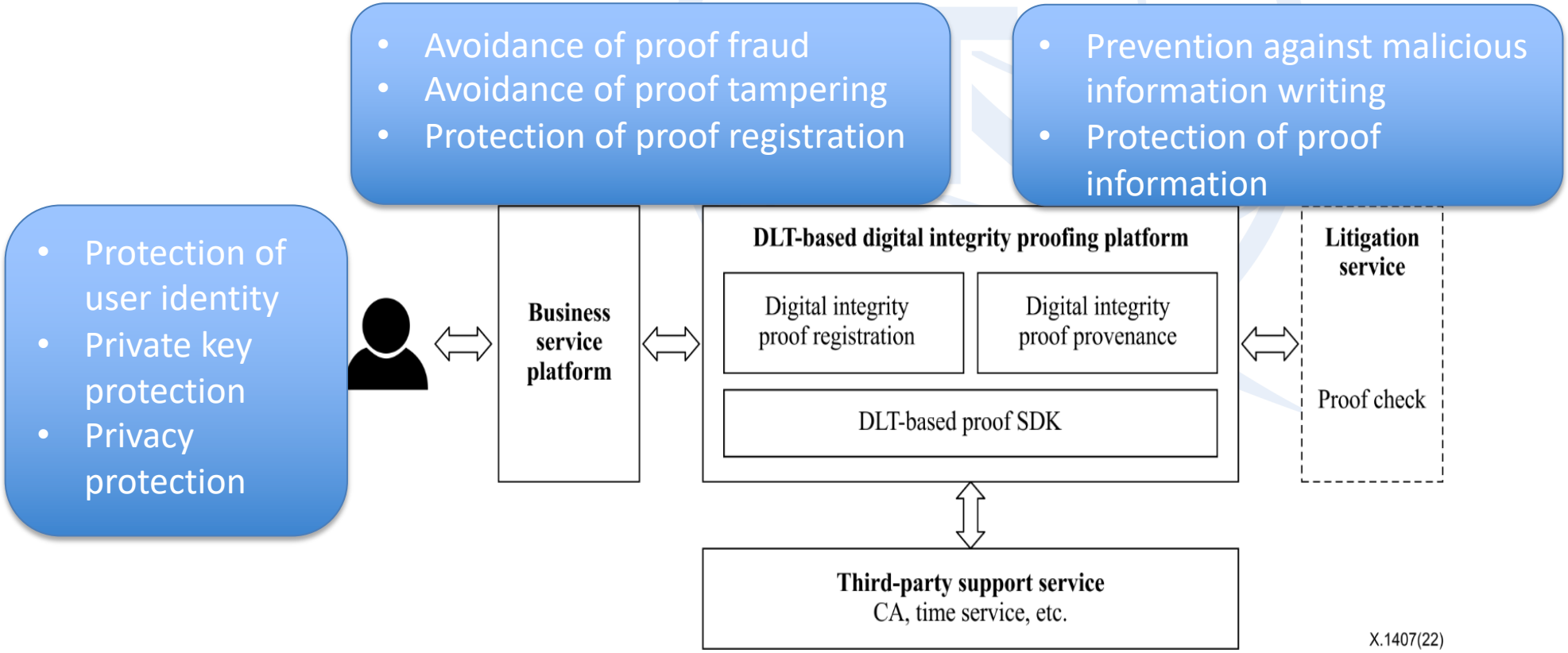
X.1407:Security requirements for digital integrity proofing service based on distributed ledger technology

Status: Published on 2022-1

Introduction:

The DLT-based digital integrity proofing platform provides services for distributing, querying, and tracking digital proof of the integrity of an entity using distributed ledger technologies.

- X.1407 specifies the security threats to user, proof registration, proof provenance.
- X.1407 specifies requirements for digital proofing of the integrity of an entity based on DLT.

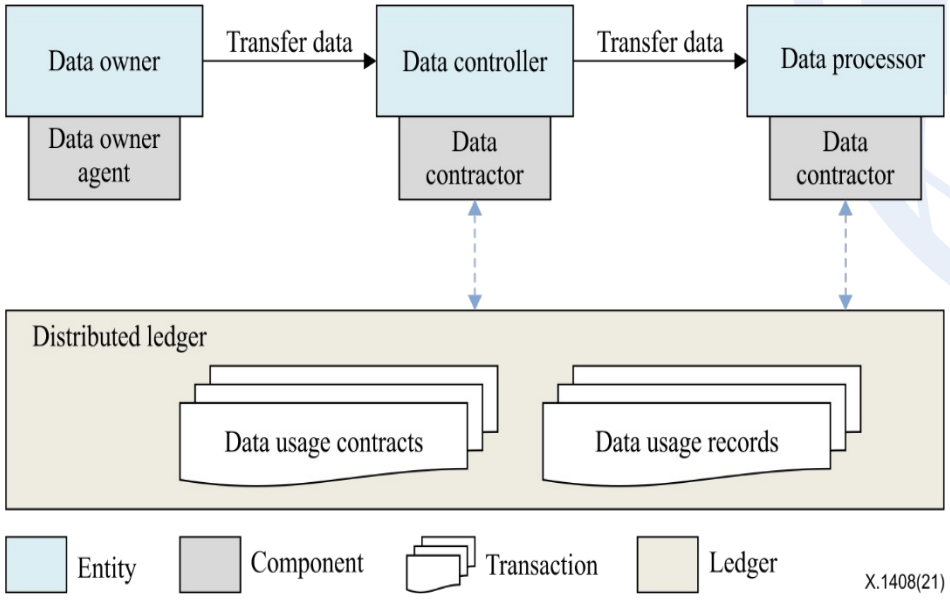


X.1408:Security threats and requirements for data access and sharing based on the distributed ledger technology

Status: Published on 2021-10

Introduction:

X.1408 specifies a reference model, security threats and security requirements to data access and sharing based on DLT.



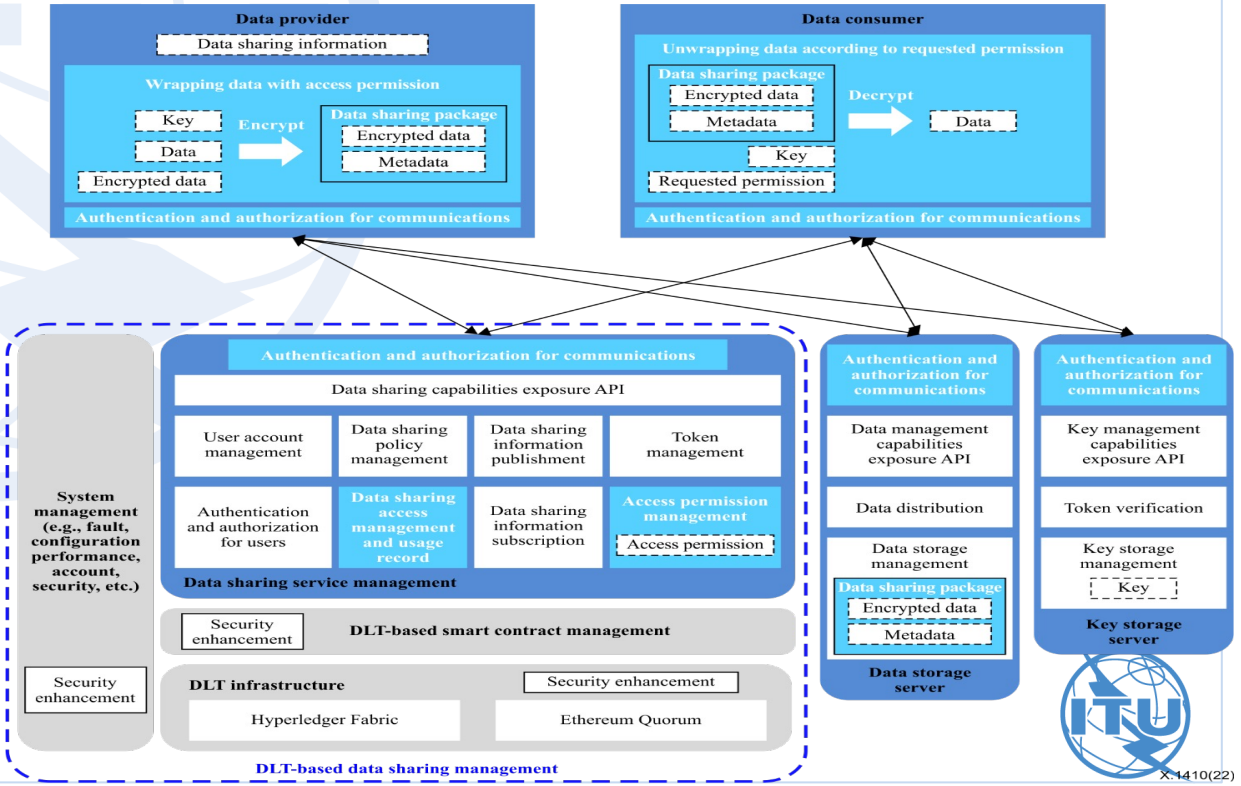
X.1410:Security architecture for data-sharing management based on distributed ledger technology

DLT can help enable trust and transparency on accountability and verifiability of data processing e.g., data provenance and usage tracking.

Status: determined, for TAP approval

Introduction:

X.1410 specifies a security architecture,interfaces and procedures of data-sharing management based on DLTs.



- Security protection of DLT
- Security protection of DLT based applications
- **Using DLT for security**

X.1403:Security guidelines for using distributed ledger technology for decentralized identity management

Status: Published on 2020-9

Introduction:

Identity systems based on DLT can be thought of as separate identity systems with different trust boundaries and cryptography keys. DLT acts as the identity trust vault and offers identity infrastructure services.

- X.1403 describes three continually evolving basic digital identity models from Centralized identity model, Federated identity model to Decentralized identity model.
- X.1403 provides overview of using DLT for the management of identity and data
- X.1403 discusses security threats of using DLT for decentralized identity management, guidance of the necessary controls.

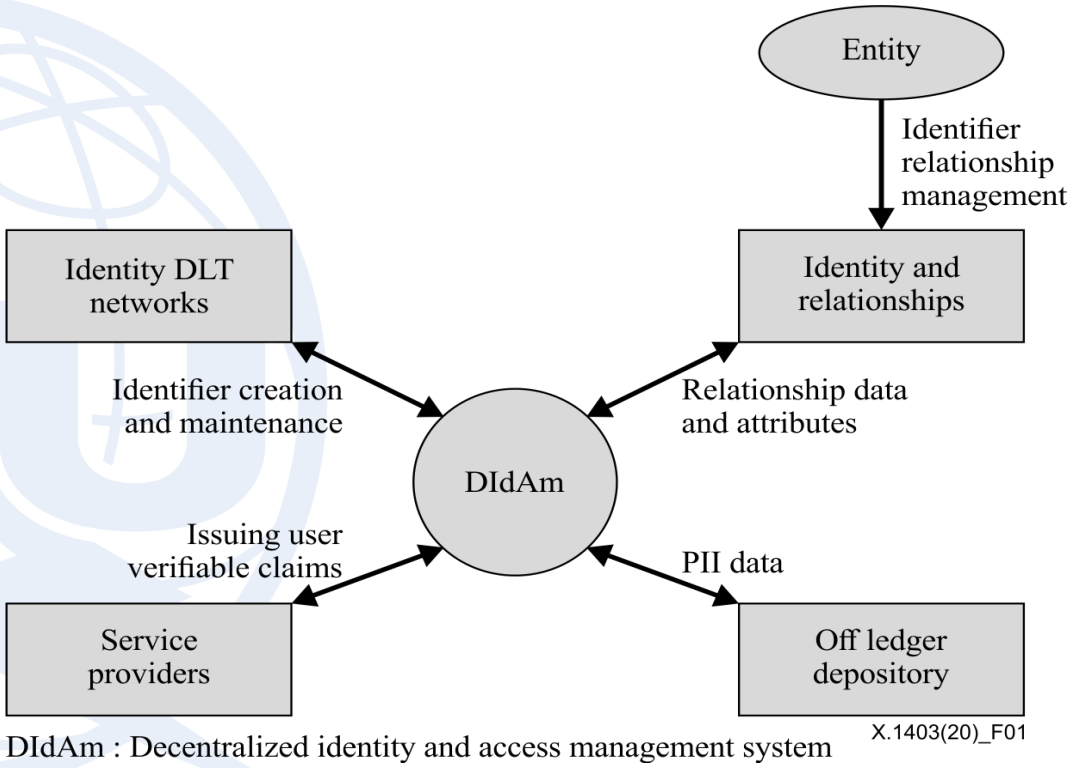


Figure -DIdAm framework

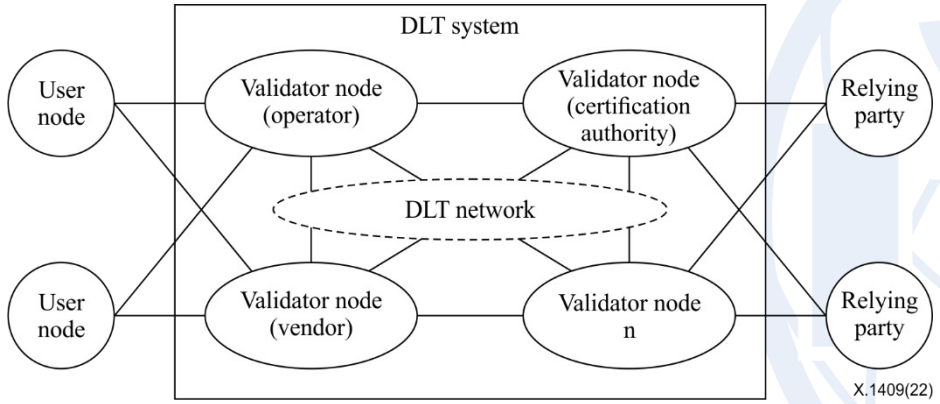
X.1409:Security services based on distributed ledger technology

Status: Published on 2022-7

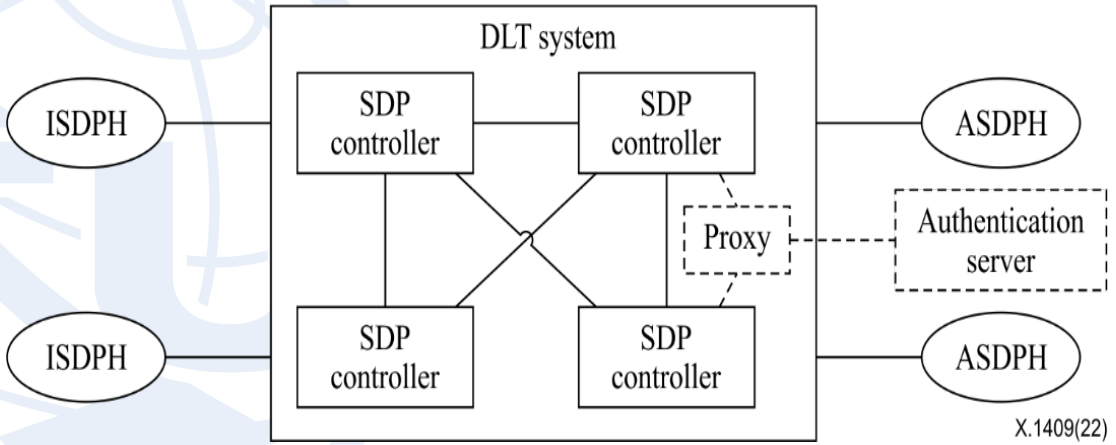
Summary:

X.1409 identifies aspects to be evaluated before delivering a security service based on DLT and provides four security services which could be delivered based on DLT:

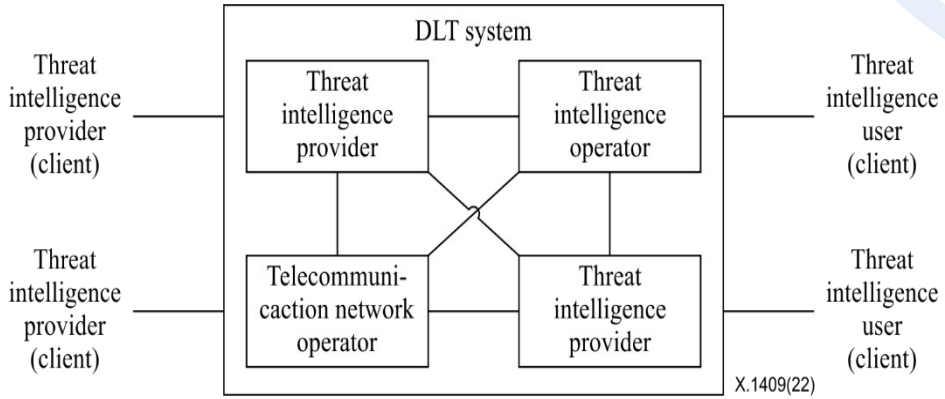
DLT-based public-key certificate management



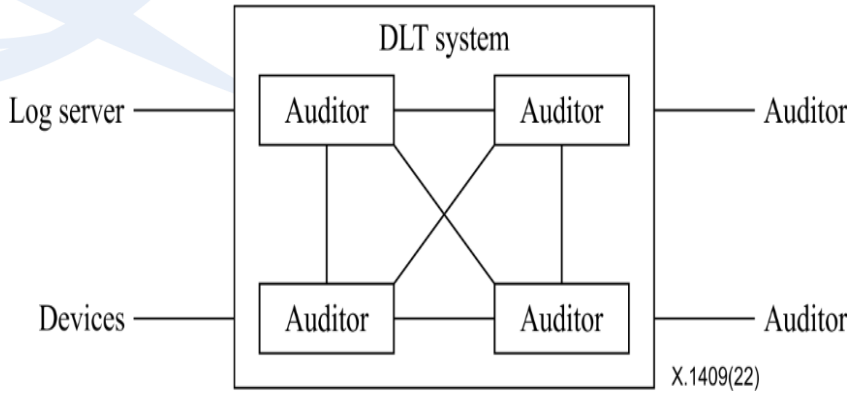
DLT-based software defined perimeter



DLT-based threat intelligence sharing



DLT-based security audit



Thanks!