ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T F.743.24 (02/2024)

SERIES F: Non-telephone telecommunication services

Multimedia services

Scenarios and requirements for distributed ledger technology (DLT) in video surveillance system interworking

ITU-T F-SERIES RECOMMENDATIONS

Non-telephone telecommunication services

TELEGRAPH SERVICE	F.1-F.109
Operating methods for the international public telegram service	F.1-F.19
The gentex network	F.20-F.29
Message switching	F.30-F.39
The international telemessage service	F.40-F.58
The international telex service	F.59-F.89
Statistics and publications on international telegraph services	F.90-F.99
Scheduled and leased communication services	F.100-F.104
Phototelegraph service	F.105-F.109
MOBILE SERVICE	F.110-F.159
Mobile services and multidestination satellite services	F.110-F.159
TELEMATIC SERVICES	F.160-F.399
Public facsimile service	F.160-F.199
Teletex service	F.200-F.299
Videotex service	F.300-F.349
General provisions for telematic services	F.350-F.399
MESSAGE HANDLING SERVICES	F.400-F.499
DIRECTORY SERVICES	F.500-F.549
DOCUMENT COMMUNICATION	F.550-F.599
Document communication	F.550-F.579
Programming communication interfaces	F.580-F.599
DATA TRANSMISSION SERVICES	F.600-F.699
MULTIMEDIA SERVICES	**F.700-F.799**
ISDN SERVICES	F.800-F.849
UNIVERSAL PERSONAL TELECOMMUNICATION	F.850-F.899
ACCESSIBILITY AND HUMAN FACTORS	F.900-F.999

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

Recommendation ITU-T F.743.24

Scenarios and requirements for distributed ledger technology (DLT) in video surveillance system interworking

Summary

Recommendation ITU-T F.743.24 provides an overview of video surveillance system interworking (VSSI) based on distributed ledger technology (DLT), for which it specifies application scenarios and capability requirements to realize interoperability, high reliability and high efficiency of VSSI identity authentication and authorization.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T F.743.24	2024-02-13	16	11.1002/1000/15846

Keywords

DLT, requirements, scenarios, video surveillance.

* To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

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

Recommendation ITU-T F.743.24

Scenarios and requirements for distributed ledger technology (DLT) in video surveillance system interworking

1 Scope

This Recommendation specifies application scenarios and requirements for distributed ledger technology (DLT) in video surveillance system interworking (VSSI), based on the requirements and architectures specified in [ITU-T F.743], [ITU-T H.626] and [ITU-T H.626.1], which includes:

1) overview;

2) scenarios, including registration, authentication and authorization, request and sharing;

3) requirements, including basic and advanced.

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 F.743] Recommendation ITU-T F.743 (2019), *Requirements and service description for video surveillance.*

[ITU-T F.751.0] Recommendation ITU-T F.751.0 (2020), *Requirements for distributed ledger systems.*

[ITU-T F.751.2] Recommendation ITU-T F.751.2 (2020), *Reference framework for distributed ledger technologies.*

[ITU-T H.626] Recommendation ITU-T H.626 (2019), *Architectural requirements for video surveillance system.*

[ITU-T H.626.1] Recommendation ITU-T H.626.1 (2013), *Architecture for mobile visual surveillance*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 customer unit [ITU-T F.743]: A device located at the customer part of a video surveillance system and used to present multimedia information (such as audio, video, image, alarm signal, etc.) to the end user.

3.1.2 distributed ledger [b-ITU-T X.1400]: A type of ledger that is shared, replicated, and synchronized in a distributed and decentralized manner.

3.1.3 distributed ledger technology (DLT) [b-ITU-T X.1400]: Technology that enables the operation and use of distributed ledgers.

3.1.4 premises unit [ITU-T F.743]: A device located at the remote part of a video surveillance system and used to capture multimedia information (such as audio, video, image, alarm signal, etc.) from a surveilled object.

3.1.5 video surveillance system [ITU-T H.626]: A telecommunication service focusing on video (including audio and image) application technology, which is used to remotely capture multimedia (such as audio, video, image, alarm signals, etc.) and present them to the end user in a user-friendly manner, based on a managed broadband network with ensured quality, security and reliability.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 video surveillance system interworking platform: A series of devices and subsystems located at the centred part of the interworking video surveillance systems. The platform is used to integrate the capabilities of different video surveillance systems and enable the resource and data sharing of different video surveillance systems.

NOTE – Definition based on [b-ITU-T F.743.3]; "video" replaces "visual".

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BVSSI	DLT in Video Surveillance System Interworking
CU	Customer Unit
DLT	Distributed Ledger Technology
ID	Identifier
IPU	Intelligent Premises Unit
ISP	Internet Service Provider
MCU	Mobile Customer Unit
MSU	Media Storage Unit
PU	Premises Unit
SC	Smart Contract
SHA	Secure Hash Algorithm
VS	Video Surveillance
VSS	Video Surveillance System
VSSI	Video Surveillance System Interworking

5 Convention

In this Recommendation:

– The phrase "is required" indicates a requirement that must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

– The phrase "is recommended" indicates a requirement that is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

– The phrase "can optionally" indicates an optional requirement that 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

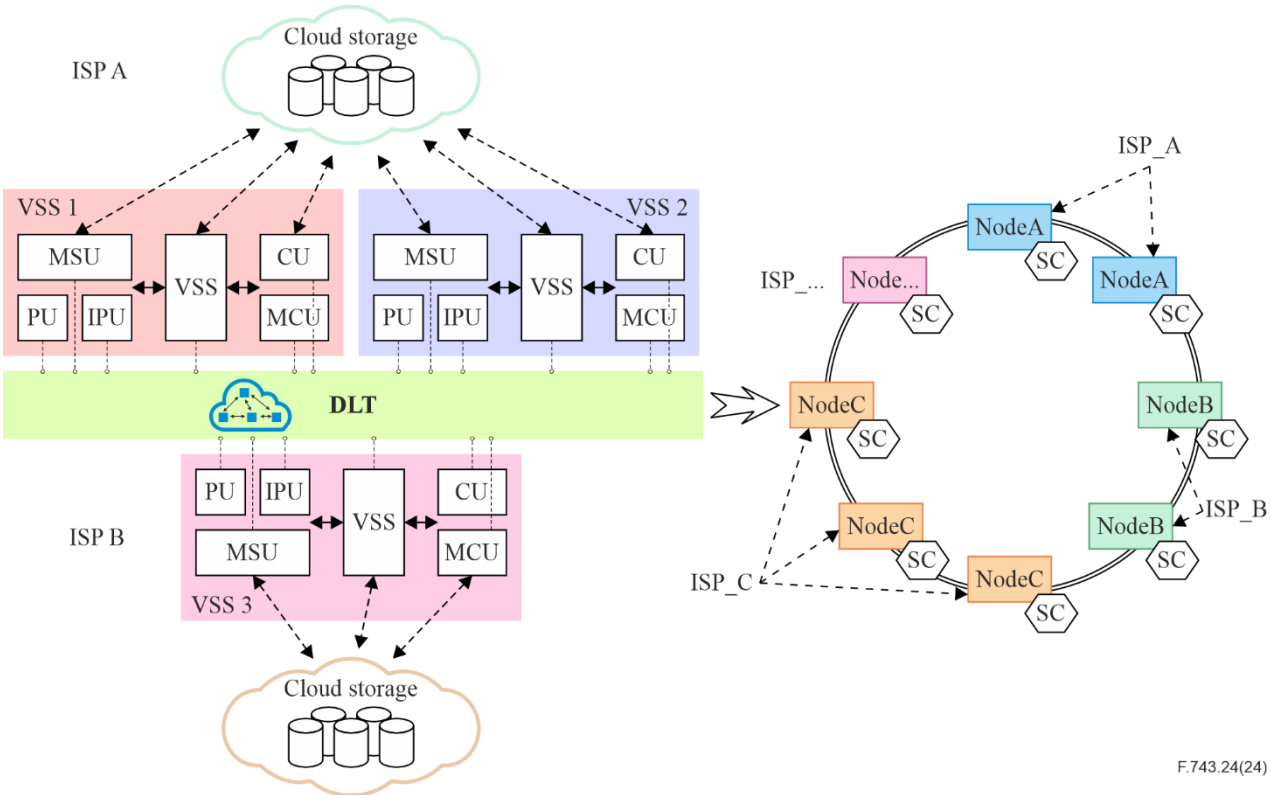
by the network operator or service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

6 Overview of DLT in video surveillance system interworking

This Recommendation specifies scenarios and requirements for DLT [ITU-T F.751.0] in VSSI. VSSI is a new model for enabling users to have ubiquitous, convenient and on-demand network access to a shared pool of configurable storage resources, which can be rapidly provisioned and released with minimal management effort or service-provider interaction.

DLT enables operation and use by providing a verifiable, append-only chained data structure of transactions, through allowing the data to be stored and updated in distributed way. DLT is essentially a decentralized architecture that no longer relies on a centralized authority. The transactions are approved by nodes and recorded in time-stamped blocks, where each block is identified by a cryptographic hash and chained to preceding blocks in chronological order. In some ways, DLT can establish an irrefutable database (DB), which uses a consensus mechanism to maintain the integrity, security, tamper-proofing and peep-proofing of the data recorded on the blocks.

In video surveillance systems (VSSs), three key components work together: the VSS itself; DLT; and cloud storage. DLT plays a crucial role in identifying users, hardware equipment and multimedia data (like videos, audio and images) within the VSS. It accomplishes this through a network of nodes equipped with smart contracts (SCs) [ITU-T F.751.2]. Whenever a new entity (e.g., customer unit (CU), premises unit (PU)) joins the VSS and generates multimedia content, it receives a unique, globally recognizable identifier (ID), as shown in Figure 1. Such functions as ID management, identity authentication, rights management and video data authenticity verification are realized through SCs on the ID chain, which is the DLT system in VSSI. Based on a unified global ID, interoperability of VSSs across systems and operators can be realized.



IPU: intelligent premises unit; MSU: media storage unit

Figure 1 – DLT in video surveillance system interworking

7 General framework of DLT in video surveillance system interworking

7.1 Ecosystem and roles

DLT in video surveillance system interworking (BVSSI) is the system that supports users of their VSS and devices of their VSS to share the video resource for others as business demands.

This clause describes a VSSI environment, with roles and sub-roles. It also specifies necessary activities for roles performed based on DLT.

The BVSSI environment includes the following roles.

– Video resource provider: Provide a video surveillance (VS) resource, whose main activities include resource identity, resource debugging, making sharing regular and an open-resource application programming interface.

– Video resource user: The end user or platform to obtain the resource or results, or services from a provider. The activities include requesting and obtaining the resource.

– VS platform: A PU or CU terminal and DB of user and provider. The activities include equipment registration, and resource authentication and authorization.

The BVSSI ecosystem includes the following sub-role.

– DLT infrastructure provider: DLT infrastructure construction, including consensus algorithm design and SCs. The main activities include node admittance, node classification, anomaly detection and node status monitoring.

7.2 General framework of DLT in video surveillance system interworking

The general framework of DLT in VSSI involves multiple roles, which work together to promote VSSI based on DLT, as shown in Figure 2.

In order interactively to share video data resources, a provider needs to classify them into general and privacy. Resources are then shared with a data requester based on DLT infrastructure, In which process, it is required that privacy data be stored in a local DB by the provider to sufficiently protect information from disclosure, a shared certificate into DLT infrastructure to trade be recorded, and general data be stored in the DLT infrastructure for sharing, which could involve verification of user information, including data provider and requester, as well as the user VSS device.

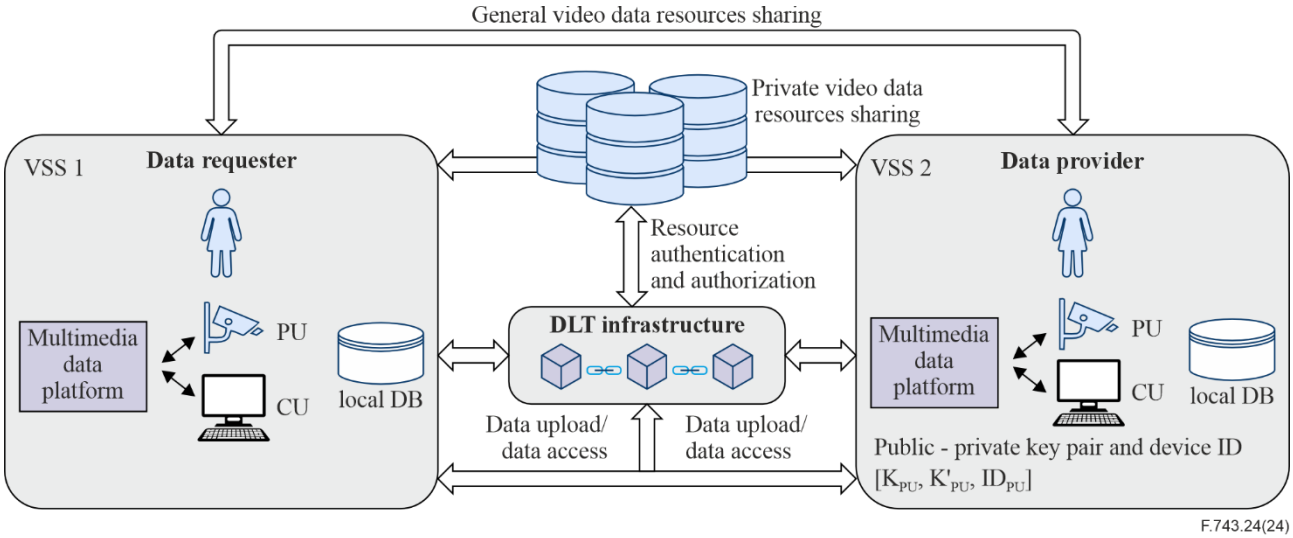


Figure 2 – General framework of DLT in video surveillance system interworking

7.3 General flow of DLT in video surveillance system interworking

Based on the general framework, the general flow of DLT in VSSI includes five steps: registration in VSSI; authentication and authorization; request for surveillance video data; video resource upload to the DLT and verification; and video data resource sharing.

7.3.1 Registration in VSSI

Users register their VSS and associated devices in the DLT to prepare for BVSSI. The registration includes registration of user and equipment, the typical detailed flow is described in clause I.1.

– User registration: users register their information in the DLT infrastructure, generating user identification, user public key and user private key. Considering the different capabilities, users can be divided into providers and requesters of data.

– Equipment registration: users register their VSS devices, generating their identification and public and private keys.

7.3.2 Authentication and authorization

A data provider receives an encryption authorization request massage sent by a data requester. The encryption authorization request message consists of information about the device identification, as well as the public and private device keys of the data requester, who has encrypted it using the public key of the data provider.

The data provider uses its device private key to decrypt the massage and get the device identification and device public key of data requester, and then authenticates the information by DLT.

The typical detailed flow is described in clause I.2.

7.3.3 Request the surveillance video data

After authentication and authorization by DLT, the data requester requests the resource; the data provider sends its public and private device keys to the data requester to access VSS.

The typical detailed flow is described in clause I.3.

7.3.4 Video data resource upload to the DLT and verification

The data provider divides video data into general and privacy. Privacy data is stored in a local DB and general data is uploaded to the DLT infrastructure.

The system generates the video resource ID and resource hash information, uploads them to the DLT infrastructure and verifies the uploaded information.

The typical detailed flow is described in clause I.4.

7.3.5 Video data resource sharing

Sharing video data resources has two different scenarios: general and private.

– In the general video data resources sharing scenario, the data owner uploads the video to cloud storage and sets the SC for access rules, and the data requester obtains video resources from the cloud storage via DLT.

– The private video data resources sharing scenario, which is suitable for extremely confidential data, is not suitable for uploading video to cloud storage. Due to their high privacy, the data owner stores video data in a local private DB. When there is a sharing demand, the data owner actively sends out a private transaction request for the specified target object. The result of the encryption of the private data includes an encrypted file and hash value; hash value is used to verify whether the encrypted file has been tampered with by the data requester.

The typical detailed flow is described in clause I.5.

8 Requirements for DLT in video surveillance system interworking

8.1 Basic requirements for DLT in video surveillance system interworking

8.1.1 User identification and authentication requirements

Req UIAR-1: It is required to provide user identity management and authentication capabilities within VSSI to ensure mutual access and resource sharing among different users.

Req UIAR-2: It is required to provide a capability of identity authentication and management, including generating public-private key pairs for users.

8.1.2 System requirements

Req SyR-1: It is required to provide a capability to VSS for publishing network resources, including video data resource.

Req SyR-2: It is required to provide a capability to write or read data from ledger precisely used for resource registration and history traceability.

Req SyR-3: It is recommended to provide the ability to repair faulty nodes and realize the reconstruction of shared resource services.

Req SyR-4: It is recommended to provide a node redundancy strategy to ensure DLT node availability.

Req SyR-5: It is required to provide a capability of node control that can detect bad DLT nodes in time and disable them.

Req SyR-6: It is recommended to provide a capability of an effective transmission of video data resource to ensure the upload and download of video data resources between VSSIs.

Req SyR-7: It is required to provide a capability of VS equipment management and record VS equipment information in the VSS, such as hardware serial numbers and device IDs.

Req SyR-8: It is required to provide a capability of reliable public-private key pair management to achieve the identity authentication necessary for interaction with different VSSs.

Req SyR-9: It is required to provide a secure device interaction interface through which the platform can ensure the management of different PUs in the VSS and the scheduling of VS resource.

Req SyR-10: It is required to provide SC security audits and keep audit records.

Req SyR-11: It is required to provide a capability to manage sharing resources information and VSS information, including resources requirements, resources status and VSS registration status.

8.1.3 Service requirements

Req SeR-1: It is required to provide the video data resource catalogue to the video data resource requester.

Req SeR-2: It is required to provide the ability to manage identity and authentication using SCs to reduce the time cost for users to obtain authentication. The system can satisfy the permission of the user to obtain encrypted video data through the simplest process.

Req SeR-3: It is required to provide the capability to record video monitoring resources, including video resource uploading and sharing, and record the video resource sharing process.

Req SeR-4: It is required to provide the capability to manage SCs and maintain the life cycle of SCs for resource sharing permission authorization to share video data resources among different VSSs.

Req SeR-5: It is required to provide that SC version control be provided to ensure that the version of the SC invoked in the video data resource sharing transaction is explicit.

Req SeR-6: It is required to provide distinct VS resource sharing conditions to data requesters.

Req SeR-7: It is required to provide the capability to generate the temporary public-private key pair for VSS user authorization safely, and provide temporary permissions for the interaction between CUs and PUs of different VSSs. The data owner has the right to manage the sharing rights of the video data resources generated by the PU of its own VSS, including the setting of conditions such as usage period, usable range and permission.

Req SeR-8: It is required to provide the transaction desensitization mechanism, realize the privacy protection of video data resource sharing transaction, reduce the density of transaction information and prevent illegal attackers from using transaction information for cluster analysis.

Req SeR-9: It is required to provide the capability to ensure the interaction between CUs and PUs between different VSSs, such as being able to implement the data sharing request task of requester to a PU under VSS of the provider according to the temporary public-private key pair of device authorization.

Req SeR-10: It is required to provide a general transmission regulation for VS resource sharing between different VSSs.

Req SeR-11: It is required to provide a secure resource monitoring and resource encryption mechanism to ensure the data protection and security of video data resources.

Req SeR-12: It is required to provide a capability to support the general video data resources sharing, and the shared data needs to be encrypted.

Req SeR-13: It is required to provide the ability to share private video data that is stored in the local private DB. The transaction request needs to include the target node ID, encrypted video data and its hash, and private transaction parameters. The private transaction parameter identifies the sharing transaction as a private transaction, and specifies the relevant node that can participate in the private video data sharing transaction.

Req SeR-14: It is required to provide the ability to share private data, and only the relevant nodes in the private transaction parameters can participate in the transaction.

Req SeR-15: It is required to provide the ability to identify whether the shared data has been tampered with. It can be judged by comparing whether the data hash in the node is consistent with that stored in the DLT.

8.2 Advanced video surveillance system interworking based on DLT

Req ABVSSI-1: It is recommended to provide an efficient and flexible consensus mechanism to ensure that incremental data synchronization and ledger updates are consistent.

Req ABVSSI-2: It is required to provide an oversight strategy for the consensus process to ensure that the consensus history is auditable, regulated and immutable.

Req ABVSSI-3: It is required to provide the ability to share data across chains to provide video data access to users under different platforms.

Req ABVSSI-4: It is required to provide the ability for cross-platform consistency to ensure a unified interface for different data uploads.

Req ABVSSI -5: It is required to provide the ability to provide the availability of data. Data shared by different systems need to be completely available.

Req ABVSSI-6: It is recommended to provide the ability to provide high-speed transmission and communication in order to support secure sharing and transmission of encrypted video data in BVSSI.

Req ABVSSI-7: It is required to provide a user information collection notification policy if collection is necessary to ensure that the content and purpose of the collection of personal information are clear to users.

Req ABVSSI-8: It is required to provide a scalable storage mechanism and trusted node deployment hardware facilities, combine cloud storage and DLT to achieve massive resource data storage and sharing, and ensure the sustainability of ledger synchronization.

Req ABVSSI-9: It required to provide a video data scheduling mechanism to ensure a more efficient sharing strategy for VS data with different usage frequencies.

Req ABVSSI-10: It is recommended to provide an optional encryption mechanism to ensure that VS data owners perform data encryption operations according to their own needs.

Req ABVSSI-11: It is required to provide a capability of pricing principle to realize the transaction of video data assets and value transfer of video data elements.

Appendix I

Scenarios and use cases of video surveillance system interworking based on DLT

(This appendix does not form an integral part of this Recommendation.)

I.1 Registration in VSSI

Alice registers her VSS and the devices of her VSS through an Internet service provider (ISP) to the DLT, to prepare for BVSSI.

NOTE – The ISP is responsible for providing access authentication and network access services for users. Here, users can access a BVSSI network through ISP authentication.

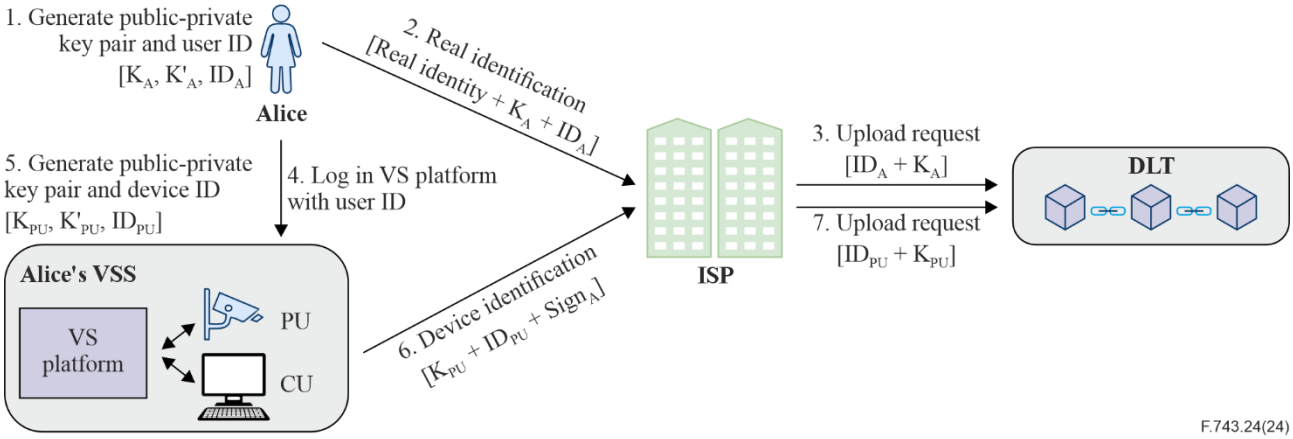


Figure I.1 – Registration workflow in BVSSI

I.1.1 User registration

Step 1: Alice adopts an asymmetric encryption algorithm to generate a public-private key pair and a user ID. The public key ($K_{pub\ of\ Alice}$) is a tool used by other users to verify the signature of text sent by Alice. The private key ($K_{pri\ of\ Alice}$) is a tool for Alice to make a digital signature and is stored by Alice. The user ID (ID_{Alice}) is Alice's identity in VSS.

Step 2: Alice sends her real identity (such as identity card), public key and user ID to ISP for real identity identification.

Step 3: ISP authenticates Alice's real identity. If the authentication is successful, Alice's public key and user ID are signed by the ISP and form a record. Then the record is uploaded to DLT as a transaction.

I.1.2 Equipment registration

Step 4: Alice logs in to the VS platform of her VSS with user ID to control her PUs and CUs in intra-system and inter-system interaction.

Step 5: Before joining VSS, PUs and CUs newly purchased by Alice also need to generate public-private key pairs (the private key can be mixed by the hardware serial number and the password set by the user) and device IDs. The private key is stored by Alice.

Step 6: Device IDs and public key record are sent to the ISP after being signed by Alice with her private key.

Step 7: The ISP verifies the signature of the received record. If the verification is successful, the ISP uploads the device IDs and the corresponding public key to DLT.

I.2 Authentication and authorization

Bob owns a VSS consisting of multiple CUs and mobile customer units (MCUs). Alice's and Bob's VSSs have been registered on DLT. Bob wants to access the data of PU1 in Alice's VSS with his CU, so he needs Alice's authorization first.

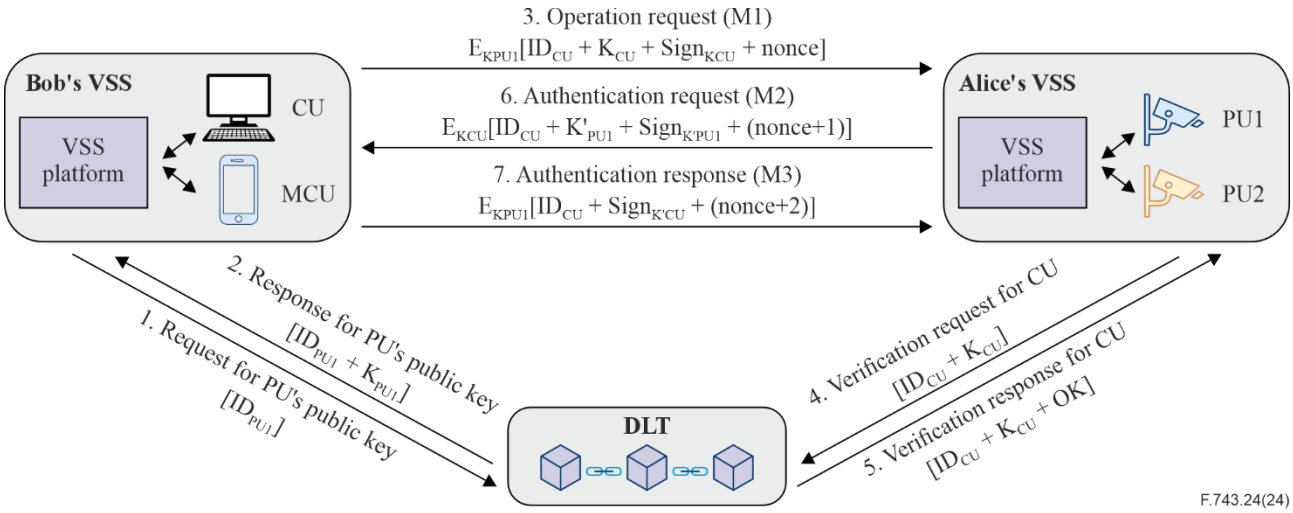


Figure I.2 – Authentication and authorization workflow in BVSSI

Step 1: First, Bob's VSS searches for the public key of Alice's PU1 ($K_{pub\ of\ PU1}$) on DLT, according to the ID of PU1 (ID_{PU1}).

Step 2: DLT receives a legitimate query request from Bob's VSS. The corresponding public key of PU1 ($K_{pub\ of\ PU1}$), which is generated by PU1 during the registration, is then queried in DLT ledger according to the received ID_{PU1}. If it exists, the $K_{pub\ of\ PU1}$ is returned to Bob's VSS.

Step 3: When Bob's VSS receives the public key of Alice's PU1 ($K_{pub\ of\ PU1}$), it initiates an authorization session with Alice's VSS. Bob's VSS sends a cryptographic authorization request message (M1) to Alice's VSS, including ID_{CU}, the public key of CU ($K_{pub\ of\ CU}$), a signature encrypted by the private key of CU ($K_{pri\ of\ CU}$), and a nonce used for maintaining the response sequence of message. Bob's VSS encrypts the first message (M1) with the public key of PU1 ($K_{pub\ of\ PU1}$) and sends the cipher text to Alice's VSS.

Step 4: Alice's VSS decrypts M1 with $K_{pri\ of\ PU1}$ after receiving it, and obtains ID_{CU} and $K_{pub\ of\ CU}$. Alice's VSS then verifies the authenticity of the message through signature and $K_{pub\ of\ CU}$. If the message is legitimate, Alice's VSS sends a verification request to DLT to verify the ID_{CU} and its corresponding $K_{pub\ of\ CU}$ further.

Step 5: DLT receives a legitimate verification request from Alice's VSS. It queries and verifies the $K_{pub\ of\ CU}$ in DLT ledger according to the ID_{CU}, and then returns the verification result to Alice's VSS.

Step 6: If the verification of CU's information is successful, Alice's VSS generates a temporary public-private key pair ($K'_{pub\ of\ PU1}$, $K'_{pri\ of\ PU1}$) for this authorization of Bob's CU to access Alice's PU1.

NOTE – The temporary key pair is generated based on the root key pair of the PU1 ($K_{pub\ of\ PU1}$, $K_{pri\ of\ PU1}$) and is only valid in this authorization. Its lifecycle is controlled by Alice's VSS. In addition, the $K_{pri\ of\ PU1}$ cannot be obtained through this temporary key pair.

Step 7: Alice's VSS continues the authorization session, and sends an identity verification request message (M2) to Bob's VSS, consisting of ID_{PU1}, $K'_{pub\ of\ PU1}$, a signature encrypted by $K'_{pri\ of\ PU1}$, and nonce+1 which is used for maintaining the response sequence of the message. Alice's VSS encrypts the entire message with $K_{pub\ of\ CU}$ and sends the cipher text to Bob's VSS.

Step 8: Bob's VSS decrypts M2 with $K_{pri\ of\ CU}$ after receiving it, and obtains the $K'_{pub\ of\ PU1}$ generated for this session. Bob's VSS then verifies the authenticity of the message through signature and $K_{pub\ of\ PU1}$. If the message is legitimate and authentic, Bob's VSS sends a response message (M3) to Alice's VSS. The response message includes ID_{CU}, a signature encrypted by $K_{pri\ of\ CU}$, and nonce+2 used to maintain the response sequence of messages. M3 is encrypted by $K'_{pub\ of\ PU1}$. Alice's VSS verifies the signature and nonce with $K_{pub\ of\ CU}$ after receiving and decrypting M3 using $K'_{pri\ of\ PU1}$.

If the verification is successful, bidirectional authentication is ended. The CU obtains the authorization of Alice's PU and prepares to establish the connection.

I.3 Request the surveillance video data in the cloud

Bob's VSS requests access authorization to video data stored by Alice's VSS in the cloud, which divided into three steps.

Step 1: Get a trusted identity on the DLT

Bob gets the public key of Alice's PU through the DLT, and then uses it to encrypt the identity information to initiate a video data request to Alice to access the cloud DB. Alice obtains Bob's CU public key through the block chain, as shown in flows 1 to 3 in Figure I.3.

Step 2: Authentication and authorization code issuing

Alice verifies Bob's identity by verifying the signature, and then sends Bob a cloud DB access authorization code. Alice's authorization code can include certain information, such as ID_{CU}, ID_{PU} and authorized access range, as shown in flows 4 and 5 in Figure I.3.

Step 3: Authorization code verification

Bob sends video data request to Alice's cloud DB through authorization code, and the cloud DB verifies the authorization code from Alice. If the authorization code is ok, then the whole request process ends, as shown in flows 6 to 8 in Figure I.3.

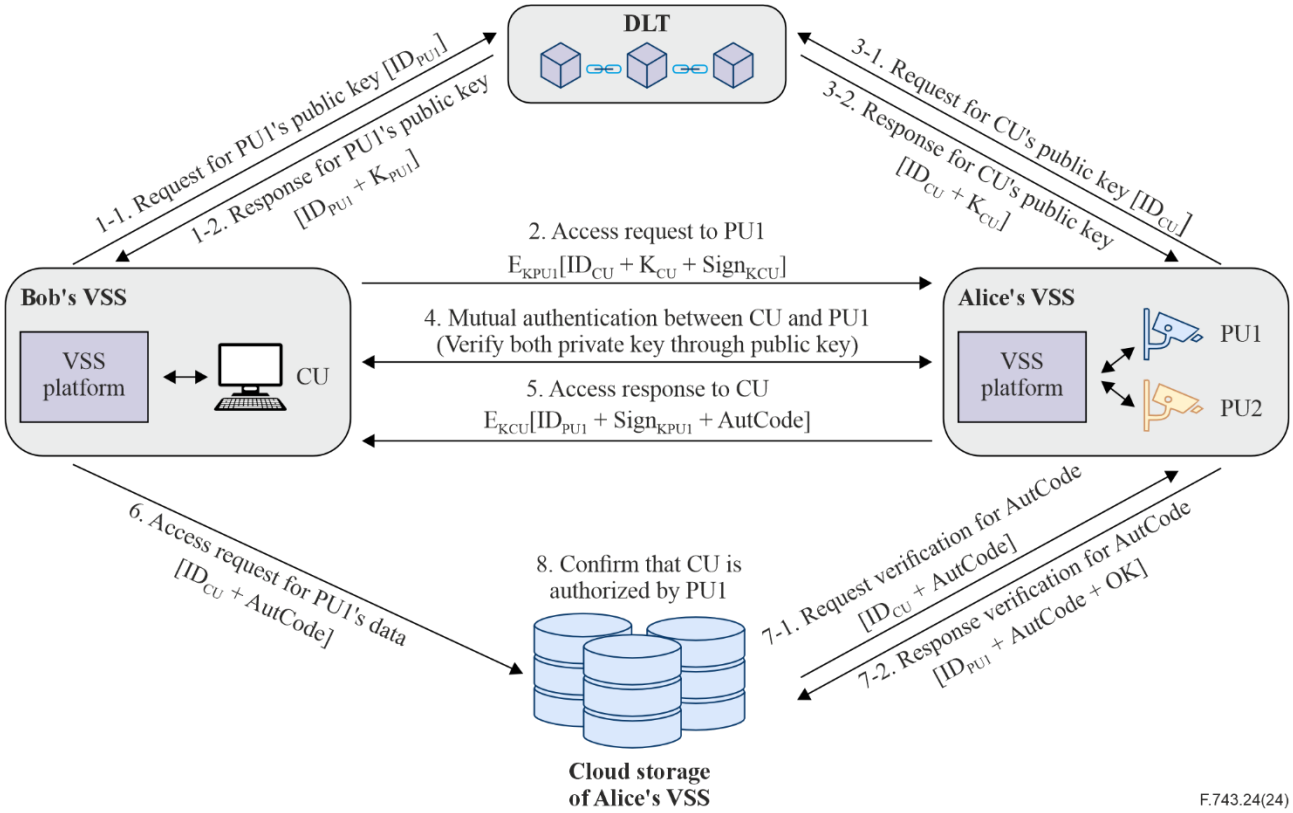


Figure I.3 – Request video data workflow in BVSSI

I.4 Video resource upload to the DLT and verification

Considering the authenticity requirement of the video resources which Bob's VSS downloads from the cloud storage by video resources ID, the following scenario based on the DLT can be considered.

Step 1: Video resource ID and resource hash information generation

The original video files recorded by Alice's VSS are generated encrypted video files through a symmetric key. Meanwhile, using a secure hash algorithm (SHA) series is used to map the encrypted video file to get a hash. In order to get the video resource ID, the multihash encoding (PU number + hash algorithm category + length of hash (number of bytes) + hash value) should then be generated to obtain the final video resource ID through hash mapping, as shown in flow 1 in Figure I.4.

Step 2: Uploading video resource ID and resource hash information to the DLT

Alice's VSS sends a video resource ID, encrypted video data, PU ID, resource hash information to cloud storage. The resource ID and resource hash information are then uploaded to the DLT by cloud storage server, appending the index value of the video resource stored in the cloud and these processes are recorded on the DLT, as shown in flows 2 to 4 in Figure I.4.

Step 3: Video information verification

When Bob's VSS CU downloads the video file (called data request in Figure I.4) from the cloud storage service provider, it searches the video resource by resource ID and index to download the video resource file. The CU then matches the hash value of the resource with that of the DLT to verify whether the video resource has been tampered with (called data response in Figure I.4) and these processes are also recorded on the DLT, as shown in flows 5 to 7 in Figure I.4.

NOTE – In this scenario, all interactions and transmissions are encrypted.

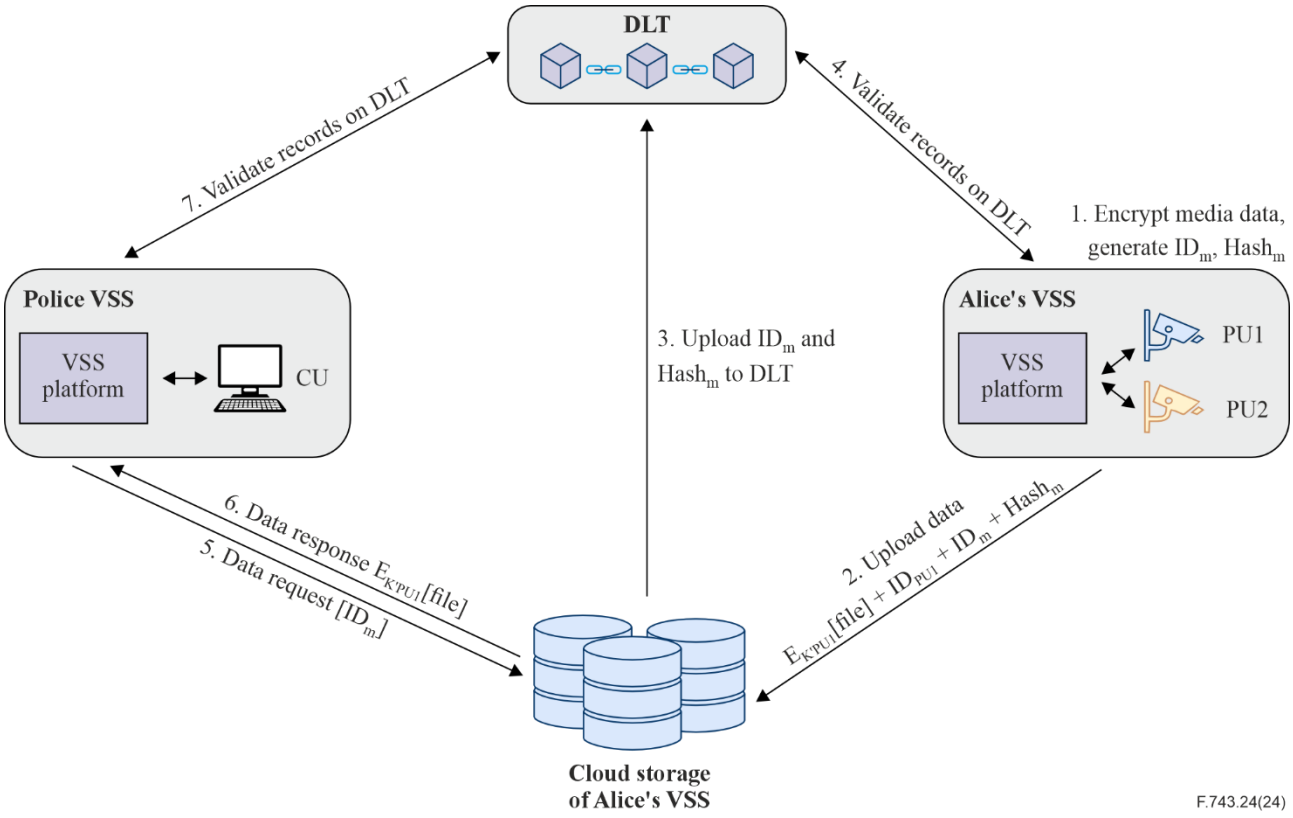


Figure I.4 – Information upload and verification workflow in BVSSI

I.5 Video data resources sharing

I.5.1 General video data resources sharing

See Figure I.5.

Based on the registration step, authentication and authorization, video data information uploading and video data resources can be shared between Alice's VSS and Bob's VSS.

In VSSI based on DLT, a video data resource can be shared automatically by SC in a trusted and secure fashion by public-private key pairs, traceable by data structure, etc.

Step 1: Sign the smart contract between Alice and Bob

During video resource upload to the DLT and verification, Alice (resource owner) has created a user SC, including usage period, usable range and permission. To obtain and use these resources, Bob (resource user) should sign this SC with his K_{pri}.

Step 2: Obtain the video data catalogue

After signing the SC, Bob obtains the data catalogue of Alice's VSS automatically, which can confirm the video data location, and sends a message to DLT, including ID_{Bob}, resource ID and PU number.

Step 3: Encrypt and decrypt video data

Alice's VSS encrypts the video data resource by Bob's K_{pub} and sends it by SC. Bob's VSS uses his own K_{pri} to decrypt the encrypted video data by his K_{pub}.

Step 4: Smart contract execution records are recorded on DLT

In video data resource sharing flow, all of SC execution records (including data-using records) are recorded on DLT to trace.

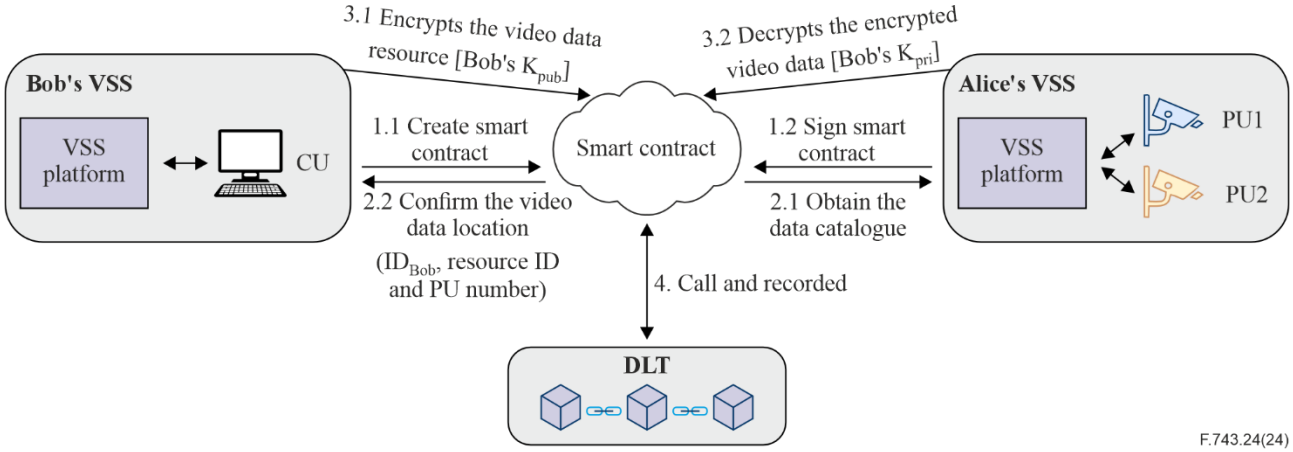


Figure I.5 – General video data resources sharing in BVSSI

I.5.2 Private video data resources sharing

See Figure I.6.

There is a private DB in each user's VSS. Similar to PU and CU, the private DB also has a public-private key pair and a device ID. The private key is stored by the user, and the public key and device ID are recorded in DLT.

For a private video resource that is extremely confidential, Alice stores it in her local private DB instead of uploading it to cloud storage. When there is a need to share the private video resource, Alice actively initiates a private transaction to a specific target object such as Bob, which process is divided into five steps.

Step 1: Alice's VSS requests the public key of Bob's private DB (K_{DB2}) on DLT, according to the ID of Bob's private database (ID_{DB2}), and DLT response for public key of Bob's private database [K_{DB2}, ID_{DB2}].

Step 2: Alice's VSS encrypts the private video resource that needs to be shared by the public key of Bob's private database (K_{DB2}). Meanwhile, Alice's VSS uses SHA series mapping on the encrypted video resource to get a hash ($Hash_v$). After that, in order to get the video resource ID, the multihash encoding (the number of Alice's private DB + hash algorithm category + length of hash (number of bytes) + hash value) should be generated to obtain the final video resource ID (ID_v) through hash mapping. Alice then uploads the resource ID (ID_v) and resource hash ($Hash_v$) information to the DLT.

Step 3: Alice initiates a private transaction request. The request contains the ID of Bob's private DB (ID_{DB2}), the ID of the resource (ID_v), the encrypted resource file (E_{KDB2} [file]), the hash value ($Hash_v$) and a private transaction parameter (PrivateParm{ID_{DB1}, ID_{DB2}}). The private transaction parameter identifies the transaction as private, and includes the relevant node IDs of the transaction, i.e., the IDs of Alice's (ID_{DB1}) and Bob's private databases (ID_{DB2}). Only the nodes in the parameters can participate in the transaction.

Step 4: Bob receives the private transaction request and compares whether his ID of private database (ID_{DB2}) belongs to the IDs in the private transaction parameters. If so, he participates in the transaction, otherwise not.

Step 5: Bob's VSS uses the private key of Bob's private DB to decrypt the video resource, obtains the resource and writes it into his own private DB. After then, Bob matches the hash value of the resource with that on the DLT to verify whether the video resource has been tampered with.

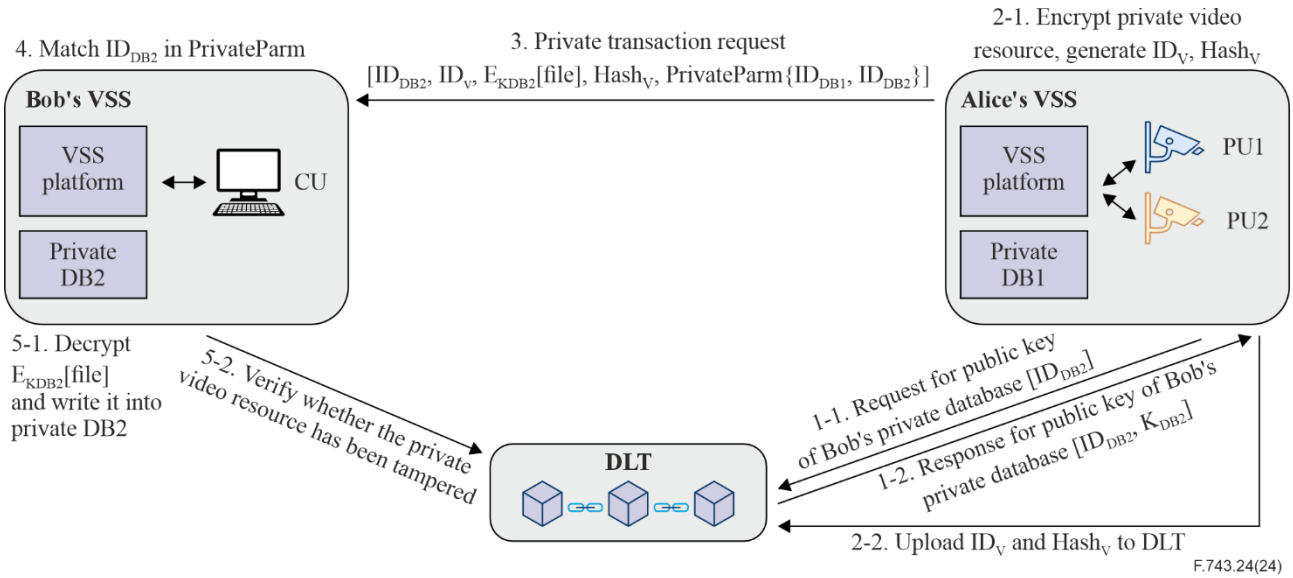


Figure I.6 – Private video data resources sharing in BVSSI

Bibliography

[b-ITU-T F.743.3] Recommendation ITU-T F.743.3 (2016), *Requirements for visual surveillance system interworking.*

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

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, 2024