International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3509

(12/2019)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Cloud Computing

Cloud computing – Functional architecture for data storage federation

Recommendation ITU-T Y.3509

International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	**Y.3500–Y.3999**
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

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

Recommendation ITU-T Y.3509

Cloud computing – Functional architecture for data storage federation

Summary

Recommendation ITU-T Y.3509 specifies the data storage federation (DSF) functions based on DSF logical components identified in Recommendation ITU-T Y.3505, the DSF functional architecture and its reference points. This Recommendation also provides relationships between the DSF functional architecture and the cloud computing reference architecture defined in Recommendation ITU-T Y.3502.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3509	2019-12-14	13	11.1002/1000/14135

Keywords

Cloud computing, cloud storage, data storage federation, functional architecture, reference point.

* 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 received notice of intellectual property, protected by patents, 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 TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3509

Cloud computing – Functional architecture for data storage federation

1 Scope

This Recommendation provides functional architecture for data storage federation (DSF). It specifies the detailed DSF functions and DSF functional architecture based on functional requirements defined in [ITU-T Y.3505].

This Recommendation defines the following:

– DSF functions;

– DSF functional architecture and reference points.

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 Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture*.

[ITU-T Y.3505] Recommendation ITU-T Y.3505 (2018), *Cloud computing – Overview and functional requirements for data storage federation*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

3.1.2 cloud service user [ITU-T Y.3500]: Natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services.

NOTE – Examples of such entities include devices and applications.

3.1.3 data storage federation (DSF) [ITU-T Y.3505]: A processing to provide a single virtual volume from the multiple heterogeneous data storages using storage virtualization.

NOTE – In this Recommendation, heterogeneous storage refers to DSF local storage.

3.1.4 DSF local storage [ITU-T Y.3505]: A physical storage to be integrated.

NOTE – DSF local storage includes on-premises storage such as main memory, non-volatile memory express (NVMe), solid state disk, hard disk drive, serial attached small computer system interface (SCSI), Internet SCSI storage and network-attached storage, object-based storage device, intelligent storage device, etc. and cloud storage with different management units such as block, object and file.

3.1.5 storage virtualization [ITU-T Y.3505]: An abstraction of storage resource to provide logical storage.

NOTE – The abstraction includes consolidating the different type of storages into a virtual storage pool as well as dividing a virtual storage pool into a single virtual volume.

3.1.6 virtual storage pool [ITU-T Y.3505]: A logical storage by integration of DSF local storage.

3.1.7 single virtual volume [ITU-T Y.3505]: A virtual storage unit provided in forms of a block device, disk, or object device.

NOTE – Disk and object device are considered as file and object-based storage in this Recommendation.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Program Interface

CRUD Create Read Update Delete

CSC Cloud Service Customer

CSP Cloud Service Provider

CSU Cloud Service User

CUA-F Customer Access Function

DFM-F Data Fragment Function

DME-F Data Manipulation Enhancement Function

DM-FS DSF data Manipulation Functions

DMP Data Manipulation Provider

DOC-F Data Operation with write buffer and read Cache Function

DSC-F DSF local Storage Connection Function

DSF Data Storage Federation

DS-FS DSF local Storage Functions

ENC-F Encryption/decryption, compression/decompression Function

FTP File Transfer Protocol

I/O Input/Output

iSCSI internet Small Computer System Interface

NAS Network Attached Storage

NFS Network File System

NVMe Non-Volatile Memory express

POL-F Policy management of data storage and data manipulation Function

PP-FS Provision and Policy management Functions

PRO-F Provision of single virtual volume and virtual storage pool Function

RAM Random Access Memory

SAN Storage Attached Network

SC-FS Single virtual volume Connection Functions

SCSI Small Computer System Interface

SFP Storage Federation Provider

SFTP Secure File Transfer Protocol

SSH Secure Shell

SSD Solid State Drive

STS-F Storage Structuring Function

SVI-F Single Virtual volume Interface Function

VSP-F Virtual Storage Pool management Function

5 Conventions

None.

6 DSF functions

Figure 6-1 shows data storage federation (DSF) functions derived from the DSF requirements and DSF logical components defined in [ITU-T Y.3505].

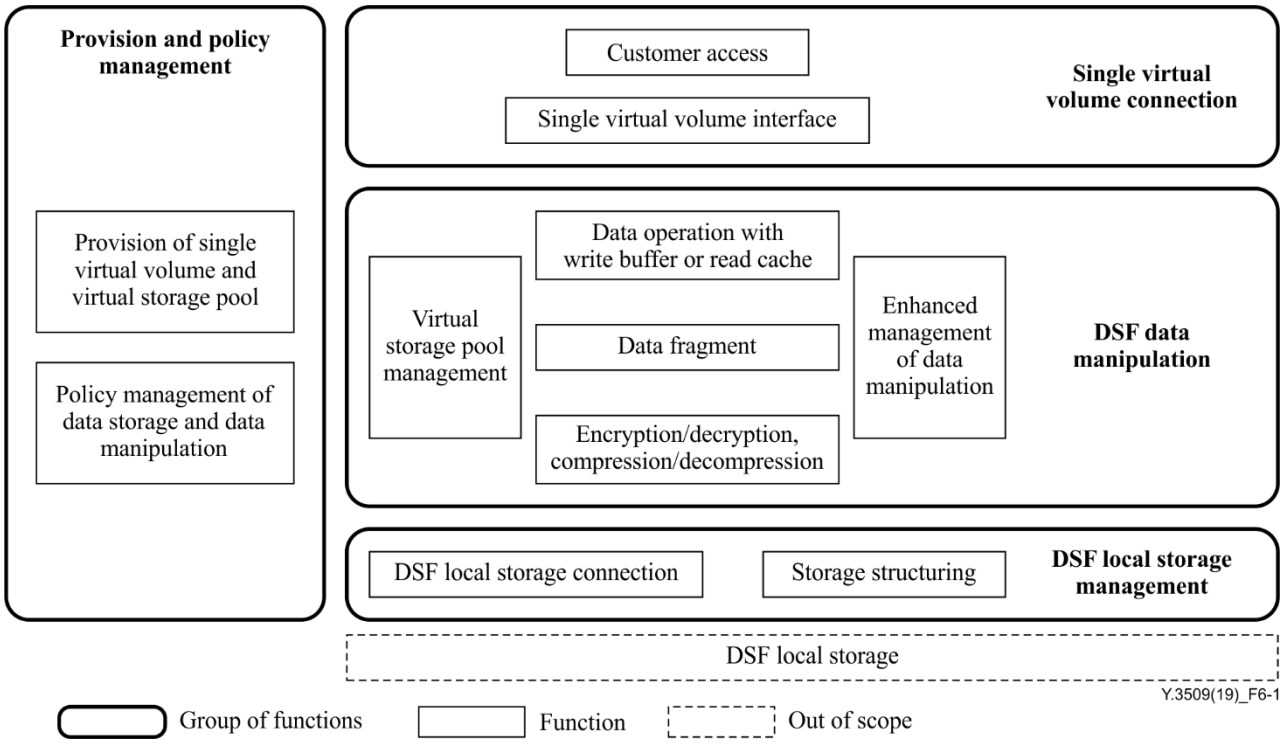

Figure 6-1 – DSF functions

NOTE 1 – Appendix I provides details regarding the relationships between the DSF requirements and DSF logical components defined in [ITU-T Y.3505] and the DSF functions defined in this clause.

NOTE 2 – Appendix II describes the relationships between DSF functions and functional components of the cloud computing reference architecture [ITU-T Y.3502].

In the remaining parts of this Recommendation, the term "cloud service user" (and its acronym "CSU") corresponds to "DSF service customer" as used in Recommendation [ITU-T Y.3505].

6.1 Single virtual volume connection

The single virtual volume connection functions include:

– customer access (see clause 6.1.1); and

– single virtual volume interface (see clause 6.1.2).

6.1.1 Customer access

The customer access function supports the following:

– Registering the cloud service user's (CSU) information;

NOTE 1 – Examples of CSU's information for configuring storage is as shown below:

- Data storage service name;
- Cloud storage and interworking information (CSU name, password, cloud storage connection endpoint information);
- On-premises storage connection information;
- Data storage specification (size, caching, tier, encryption and other data storage policies);
- Cloud storage name;
- Types of single virtual volume such as file storage such as direct-attached storage (DAS) and network-attached storage (NAS), object storage such as a storage area network (SAN) connecting to a working server for applications or databases, and block storage e.g., [b-Ceph], [b-Swift], and [b-Lustre];
- Access mechanisms.

NOTE 2 – Once registration of CSU's information is completed, the CSU can access the DSF service and request the allocation and capability of storage such as single virtual volume and DSF local storage.

– Enabling interactions between the DSF service and the CSU for both storage operations and data operations.

NOTE 3 – A single virtual volume is created through storage operations while the CSU's data is stored and managed through data operations.

6.1.2 Single virtual volume interface

The single virtual volume interface function supports the following:

– Provisioning interfaces between a CSU and a single virtual volume according to the type of storage requested by the CSU;

– Selecting CSU's data access mechanisms and setting the related parameters;

NOTE – Examples of data access mechanisms are [b-iSCSI] for block storage, [b-NFS], [b-SSH], [b-SFTP], [b-FTP] for file storage and APIs of [b-Ceph], [b-Swift], and [b-Lustre] for object storage.

– Interfacing with CSU's web application or client software used to access a single virtual volume.

6.2 DSF data manipulation

The DSF data manipulation functions include:

– virtual storage pool management (see clause 6.2.1);

– data operations with write buffer and read cache (see clause 6.2.2);

– data fragmentation (see clause 6.2.3);
– encryption/decryption and compression/decompression (see clause 6.2.4);
– enhanced management for data manipulation (see clause 6.2.5).

6.2.1 Virtual storage pool management

The virtual storage pool management function supports the following:

– Configuring virtual storage pool using storage management metadata and virtual storage pool information;

NOTE 1 – Storage management metadata (see [ITU-T Y.3505]) is a description required to perform storage operations. This metadata includes elements such as the location of DSF local storage, read/write speed, storage capacity, API for customer data operation, etc.

NOTE 2 – Examples of virtual storage pool information include:

- size of virtual storage pool;
- the number of DSF local storage used by CSU;
- the type of DSF local storage (e.g., on premise or cloud storage).

– Connecting to DSF local storage according to the storage types selected by CSU;

NOTE 3 – Types of DSF local storage include on premise storage, cloud storage, etc.

– Creating virtual storage pools;

NOTE 4 – Creating a virtual storage pool means creating the associated storage volume and interfacing with DSF local storage.

– Referring to the DSF global registry to securely write and read data in the selected DSF local storage;
– Activating write buffer and read cache depending on CSU's selection regarding the usage of write buffer and read cache when virtual storage pool is configured;
– Transmitting the sizes of write buffer and read cache;
– Executing storage operations;
– Managing connections among separated virtual storage pools.

NOTE 5 – In this case, a proxy interface (see [ITU-T Y.3505]) can be used by the virtual storage pool management function to establish connections among separate virtual storage pools and to manage the network used for transmitting data to the DSF local storage.

6.2.2 Data operation with write buffer or read cache

The data operation with write buffer or read cache function supports the following:

– Buffering data during write operations;

NOTE 1 – Since DSF local storage can be connected with different I/O storage speeds, a write buffer is used to overcome differences in I/O storage speeds and to get faster data operation.

– Caching data during read operations;

NOTE 2 – Caching data allows lower latency data operations.

– Transmitting data in the write buffer to DSF local storage periodically;

NOTE 3 – When the write buffer is full or depending on policies for data manipulation, the data is transmitted from the write buffer to DSF local storage.

– Overwriting buffered data with new CSU's data;
– Searching data in read cache;

NOTE 4 – The objective of read cache is to improve response times of read data operations.

– Accessing to DSF global registry to search for data operation metadata;

– Storing data from DSF local storage to read cache and deleting data from read cache after a given period of time;

NOTE 5 – The period of time to keep data in read cache depends on defined caching policies or on caching mechanisms themselves.

– Adjusting and limiting read cache and write buffer sizes according to CSU requests;

NOTE 6 – The read cache and write buffer sizes are adjusted within the physical limitations specified by the DSF service provider.

– Accessing to DSF global registry for storing data operation metadata.

6.2.3 Data fragmentation

The data fragmentation function supports the following:

– Receiving DSF local storage information and data operation metadata for fragmentation;

NOTE 1 – DSF local storage information refer to credentials, access mechanisms, endpoints, storage performance and storage capacity.

NOTE 2 – Data operation metadata, see [ITU-T Y.3505], includes data operation metadata for fragmentation which provides information about the fragment size, the number of fragments, the number of parity bits, the number of fragments per storage, etc.

– Setting maximum and minimum fragment sizes;

NOTE 3 – Maximum and minimum fragment sizes depend on I/O bandwidth, storage capacity, cache usage, etc.

NOTE 4 – A too large fragment maximum size may lead to heavy copying to DSF local storage while a too small minimum fragment size may lead to missing cache hits.

– Selecting a fragment size according to maximum and minimum fragment sizes;

– Receiving data from write buffer for further fragmentation;

– Moving fragmented data to DSF local storage;

NOTE 5 – Moving fragmented data refers to the transmission of fragmented data for encryption, compression, or direct transmission to DSF local storage depending on policy of data manipulation. Policy of data manipulation includes fragmentation policy (see [ITU-T Y.3505]).

– Transmitting data from DSF local storage to the read cache;

NOTE 6 – When reading data, the data fragmentation function usually transmits frequently used data to the read cache.

– Reflecting policy of data manipulation.

6.2.4 Encryption/decryption and compression/decompression

The encryption/decryption and compression/decompression function supports the following:

– Encrypting data according to CSU's requests;

NOTE 1 – The encryption process is going on until data is stored in the DSF local storage which is connected to the virtual storage pool.

– Protecting data using high-performance encryption and decryption mechanisms;

NOTE 2 – All data stored in DSF local storage is provided with block encryption, such as [b-AES], [b-DES] or [b-SEED].

– Applying encryption algorithms to data according to CSU's requests;

NOTE 3 – A CSU can request that multiple encryption algorithms be applied to the data depending upon the different DSF local storage used to store the data (e.g., on-premises storage and public cloud storage).

– Using encryption key tables for key management;

NOTE 4 – The encrypted data, key tables and the related metadata (data operation metadata and storage management metadata) are saved separately in different DSF local storage.

NOTE 5 – For example, if the encrypted data is stored in on-premises storage then the key and related metadata is stored in cloud storage or other available types of storage.

– Authorizing access to encryption key tables;
– Compressing data stored in DSF local storage;
– Applying compression algorithms according to CSU's requests;
– Decrypting data in accordance with encryption algorithms requested by CSUs;
– Decompressing data in accordance with compression algorithms requested by CSUs.

6.2.5 Enhanced management for data manipulation

The enhanced management for data manipulation function supports the following:

– Replicating data fragments for distribution to DSF local storage;

NOTE 1 – Replicated data fragments are distributed to DSF local storage for high availability reasons.

NOTE 2 – In case of fast replication, data de-duplication is performed.

– Maintaining latest (most up-to-date) data between replicated data fragments and original data;
– Determining distribution of replicated data fragments according to DSF local storage information;

NOTE 3 – Replicated data fragments are not recommended to be distributed to low performance DSF local storage.

– Backing up and recovering DSF local storage using snapshots;
– Migrating DSF local storage;

NOTE 4 – Migration is the process of moving data from a source DSF local storage to a target DSF local storage. Migration is useful when a DSF local storage is experiencing low performances or its available capacity is becoming low.

– Backing up DSF global registry for high availability;

NOTE 5 – Backing up the DSF global registry provides a secondary DSF global registry to be used during failover. Using this secondary DSF global registry, the primary DSF global registry can be recovered in case of failover.

Applying error correction mechanisms to data;

NOTE 6 – Error correction is used to prevent data losses during data transmission. Examples of error correction mechanisms include cyclic redundancy code, checksum, cryptographic hash function, or forward error correction.

– Maintaining latest (most up-to-date) data location information in the DSF global registry for data transparency;

NOTE 7 – Data transparency refers to: a) the ability to access and work with data no matter where data is located, and b) the assurance that data being reported is accurate and is coming from the trusted source.

Preventing data leakage when processing sensitive data;

NOTE 8 – Sensitive data refers to e.g., financial information, health information and personal identification data.

NOTE 9 – In order to protect sensitive data, data operations are performed in a secure region.

NOTE 10 – A secure region is a logical area (e.g., in RAM, NVMe or SSD) accessed only through a secure interface such as an application program interface (API), or a secure gateway.

NOTE 11 – Processing sensitive data in a secure region consists of:

- copying encrypted sensitive data from DSF local storage to a secure region (through a secure gateway or API);
- decrypting the encrypted sensitive data in the secure region;
- processing CSU's requested data operations in the secure region;
- returning the data operation results to the CSU from the secure region.

– Restoring data for automatic storage fail-over;

NOTE 12 – The processing of automatic storage fail-over includes:

- monitoring and detecting newly added storage from DSF local storage information;
- validating the connection between virtual storage pools and newly added storage;
- connecting newly added storage to a virtual storage pool;
- providing existing data operation metadata and information about the global DSF registry to newly added virtual storage pool.

– Applying policies for performance enhancement.

NOTE 13 – These policies are applied for replication, backup, snapshots, migration, error correction, data protection, and disk fail-over, etc.

6.3 DSF local storage management

DSF local storage management functions provide the following:

– DSF local storage connection (see clause 6.3.1);

– Storage structuring (see clause 6.3.2).

6.3.1 DSF local storage connection

The DSF local storage connection function supports the following:

– Collecting DSF local storage information to manage DSF local storage;

– Connecting and disconnecting DSF local storage to/from virtual storage pool based on DSF local storage information;

– Interpreting and translating CSU's requested operations to the data operations of DSF local storage;

– Maintaining the sessions for connecting to DSF local storage;

– Monitoring the sessions and DSF local storage information for ensuring seamless data transmission;

– Establishing secure connections to DSF local storage by hiding communication channel information to CSUs;

NOTE 1 – Examples of channel information include protocol, address and port number.

– Establishing multiple accesses in parallel to DSF local storage for high availability;

NOTE 2 – The use of multiple parallel accesses helps compensating different transmission speeds between on premise and DSF local storage.

– Managing the proxy interface used to connect DSF local storage to virtual storage pool.

NOTE 3 – The proxy interface manages garbage collection, virtual storage pool connection control, data locking management, etc.

6.3.2 Storage structuring

The storage structuring function supports the following:

– Determining storage-tiers based on the performance, capacity, and the policy for data storage;

NOTE 1 – The storage-tiers in [ITU-T Y.3505] are hierarchically organized storages to improve access to data.

NOTE 2 – For example, frequently accessed data is stored in the high-speed storage such as RAM based disk or SSD for caching.

– Monitoring the performance of write buffer, read cache, and DSF local storage;

NOTE 3 – The transmission speed, capacity, read/write speed, etc. are monitored.

– Configuring hierarchical storage structure by using heterogeneous storage;

– Applying policy for data storage according to storage types.

NOTE 4 – Policy for data storage in [ITU-T Y.3505] includes policy for storage tiering.

NOTE 5 – Storage types related with tiering include location-based storage, time-based storage, and content addressable storage (CAS). Examples of typical use of these storage types include location-based storage for write buffer, time-based storage for DSF local storage and CAS for read cache.

6.4 Provision and policy management

The provision and policy management functions provide the following:

– policy management of data storage and data manipulation (see clause 6.4.1);

– provision of single virtual volume and virtual storage pool (see clause 6.4.2).

6.4.1 Policy management of data storage and data manipulation

The policy management of data storage and data manipulation function supports the following:

– Managing policies including administering related policy rules;

NOTE – Managed policies include policy for data storage and policy of data manipulation (see [ITU-T Y.3505]).

– Transmitting policies to DSF functions for further enforcement;

6.4.2 Provision of single virtual volume and virtual storage pool

The provision of single virtual volume and virtual storage pool function supports the following;

– Receiving and validating storage management metadata and virtual storage pool information;

– Configuring and provisioning virtual storage pools;

– Configuring and provisioning single virtual volumes in virtual storage pools;

– Creating DSF global registry;

NOTE 1 – The DSF global registry is a registry that stores and provides precise information of CSU's data including data name, data location and data size. The DSF global registry supports high speed data access to search data name, data location, etc.

– Performing fail-over of the DSF global registry;

NOTE 2 – For fail-over, secondary DSF global registry is necessary. Secondary DSF global registry is used for recovery when the primary DSF global registry is no longer operational.

– Managing data operation metadata and storage management metadata.

7 DSF functional architecture

Figure 7-1 shows the DSF functional architecture.

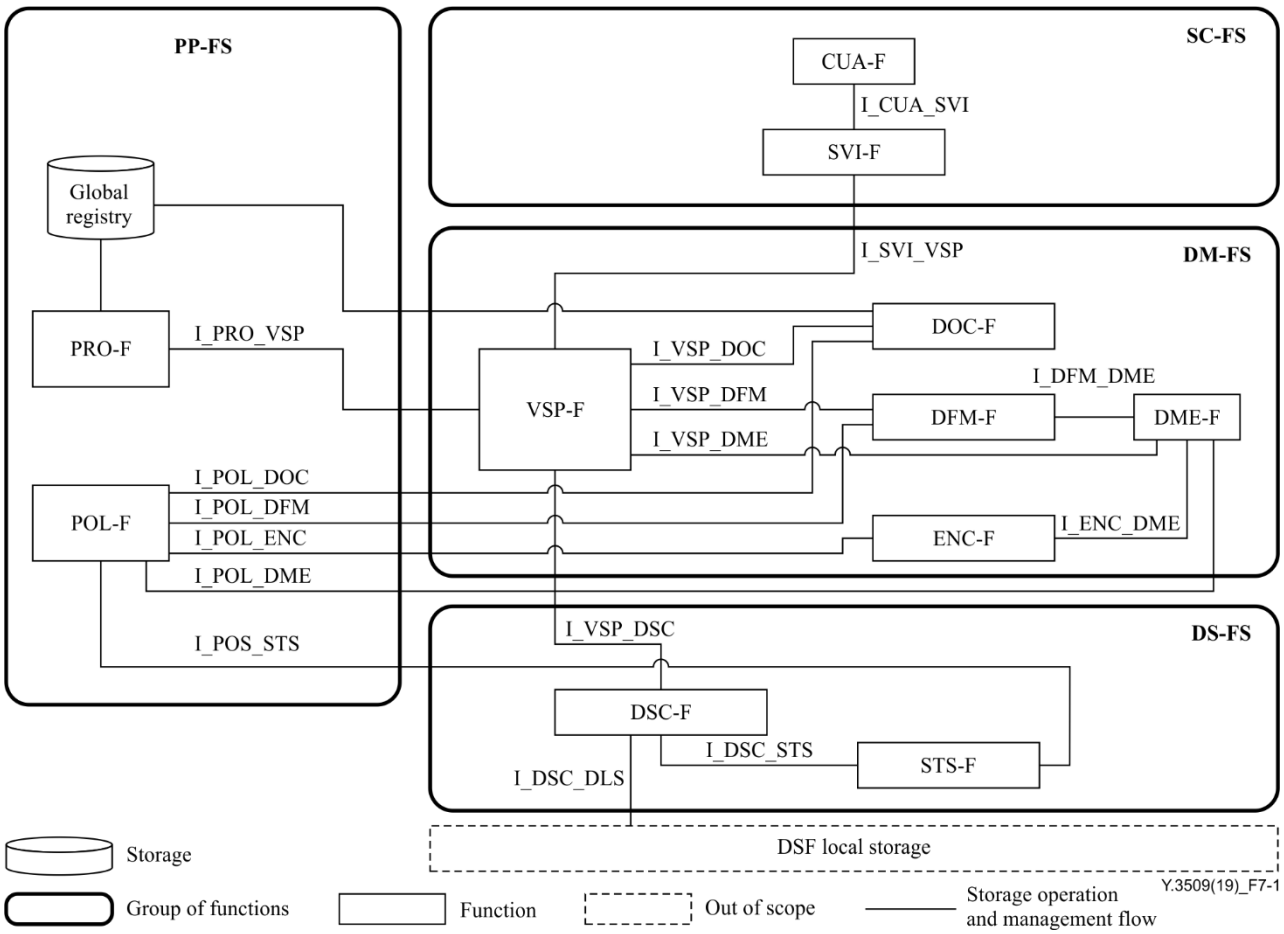

Figure 7-1 – DSF functional architecture

7.1 Single virtual volume connection functions

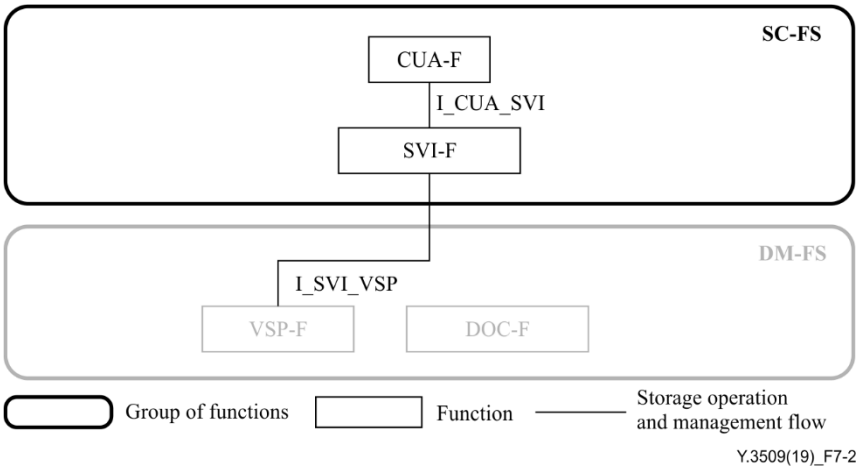

Figure 7-2 – SC-FS and related reference points

The single virtual volume connection functions (SC-FS) consist of two functions: customer access function (CUA-F) and single virtual volume interface function (SVI-F) as shown in Figure 7-2.

The SC-FS interacts with the DSF data manipulation functions (DM-FS).

7.1.1 Customer access function

The customer access function (CUA-F) (see clause 6.1.1) sends the CSU's information to the single virtual volume interface function (SVI-F), and sends the request for allocation of storage to the virtual storage pool management function (VSP-F).

7.1.2 Single virtual volume interface function

The single virtual volume interface function (SVI-F) (see clause 6.1.2) sends storage management metadata and virtual storage pool information to VSP-F for configuring interfaces between a CSU and a single virtual volume, and receives the parameters which are related to selected data access mechanism from CAU-F.

7.2 DSF data manipulation functions

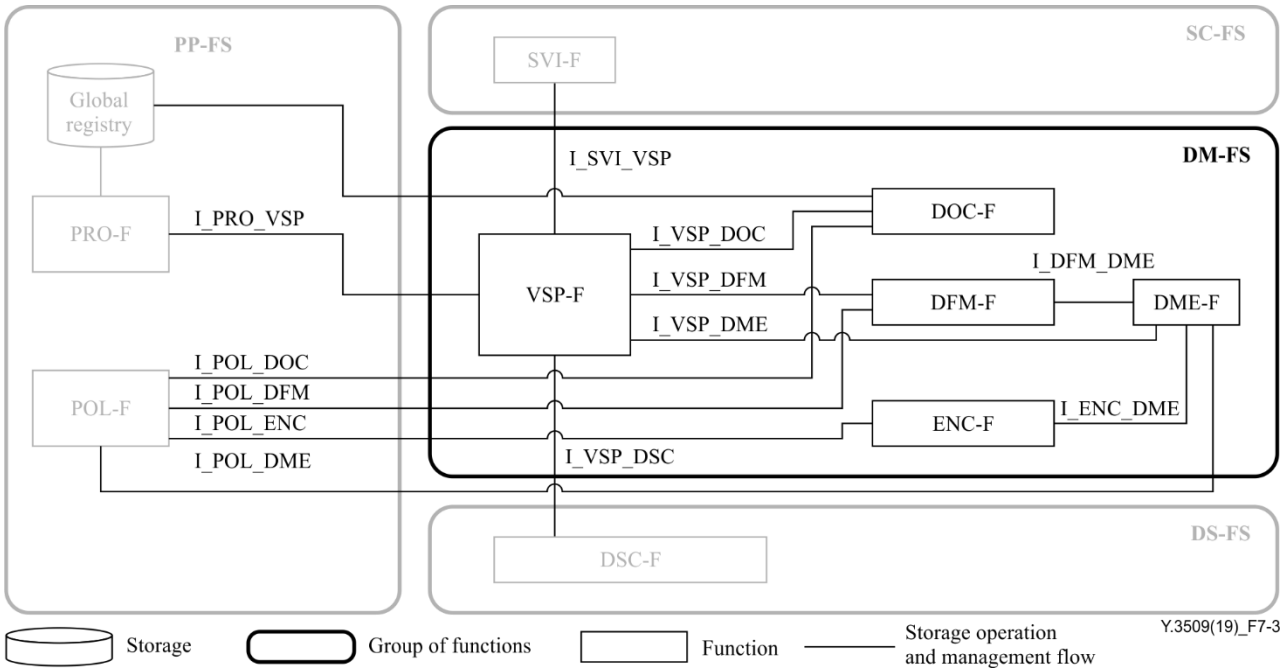

Figure 7-3 – DM-FS and related reference points

The DSF local storage management functions (DM-FS) consist of five functions: virtual storage pool management function (VSP-F), data operation with write buffer or read cache function (DOC-F), data fragment function (DFM-F), encryption/decryption, compression/decompression function (ENC-F), and data manipulation enhancement function (DME-F) as shown in Figure 7-3.

The DM-FS interacts with the single virtual volume connection functions (SC-FS), the DSF local storage management functions (DS-FS), and the provision and policy management functions (PP-FS).

7.2.1 Data operation with write buffer or read cache function

The data operation with write buffer or read cache function (DOC-F) (see clause 6.2.2) receives maximum and minimum sizes of write buffer or read cache from VSP-F. DOC-F receives policy of data manipulation from POL-F.

7.2.2 Encryption/decryption and compression/decompression function

The encryption/decryption and compression/decompression function (ENC-F) (see clause 6.2.4) receives policy of data manipulation related to compression/decompression and encryption/decryption from POL-F.

7.2.3 Data fragmentation function

The data fragmentation function (DFM-F) (see clause 6.2.3) receives DSF local storage information, virtual storage pool information and selected fragment size for fragmentation from VSP-F. DFM-F receives policy of fragmentation from POL-F.

7.2.4 Virtual storage pool management function

The virtual storage pool management function (VSP-F) (see clause 6.2.1) interacts with other DSF functions as follows:

– VSP-F receives storage management metadata and virtual storage pool information for creating single virtual volume and a virtual storage pool from SVI-F;

– VSP-F receives DSF local storage information from DCS-F and forwards DSF local storage information for selecting DSF local storage by CSU to SVI-F;

– VSP-F sends DSF local storage information for distribution of replicated fragments and fail-over to DME-F;

– VSP-F receives storage management metadata in DSF global registry from PRO-F;

– VSP-F sends the sizes of write buffer and read cache to DSC-F.

7.2.5 Data manipulation enhancement function

The data manipulation enhancement function (DME-F) (see clause 6.2.5) receives policy for performance enhancement from POL-F to reflect CSU's policy about performance. DME-F receives data operation metadata for fragmentation from DFM-F. DME-F sends policy of performance enhancement for applying sensitive data encryption/decryption and compression/decompression to ENC-F.

7.3 DSF local storage management functions

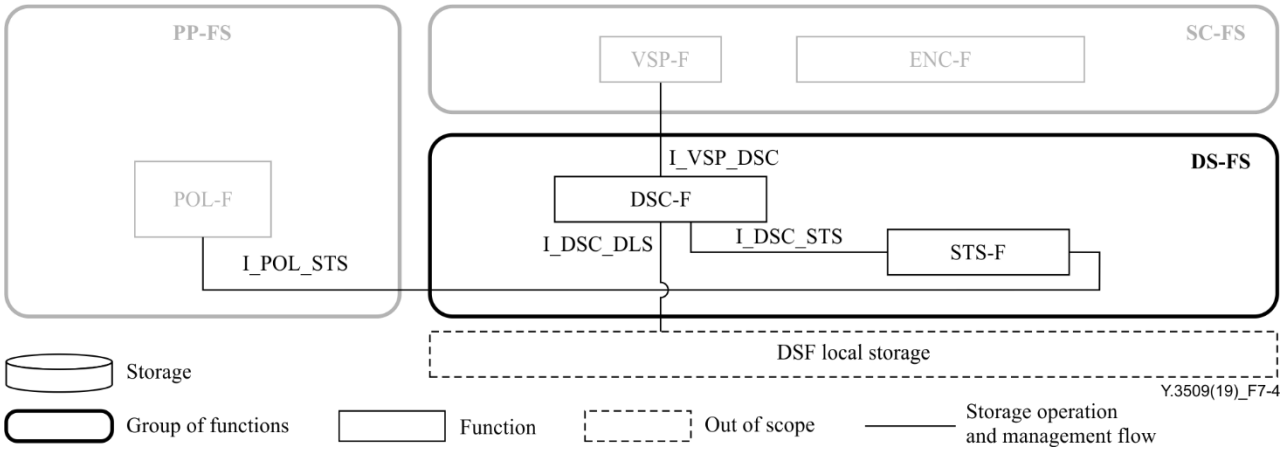

Figure 7-4 – DS-FS and related reference points

The DSF local storage management functions (DS-FS) consist of two functions: DSF local storage connection functions (DSC-F) and storage structuring function (STS-F) as shown in Figure 7-4.

The DS-FS interacts with the DSF data manipulation functions (DM-FS), the provision and policy management functions (PP-FS), and DSF local storage.

7.3.1 DSF local storage connection function

The DSF local storage connection function (DSC-F) (see clause 6.3.1) receives DSF local storage information from DSF local storage. DSC-F sends DSF local storage information to VSP-F and to STS-F.

7.3.2 Storage structuring function

The storage structuring function (STS-F) (see clause 6.3.2) receives policy of storage tier from POL-F. STS-F receives DSF local storage information from DSC-F.

7.4 Provision and policy management functions

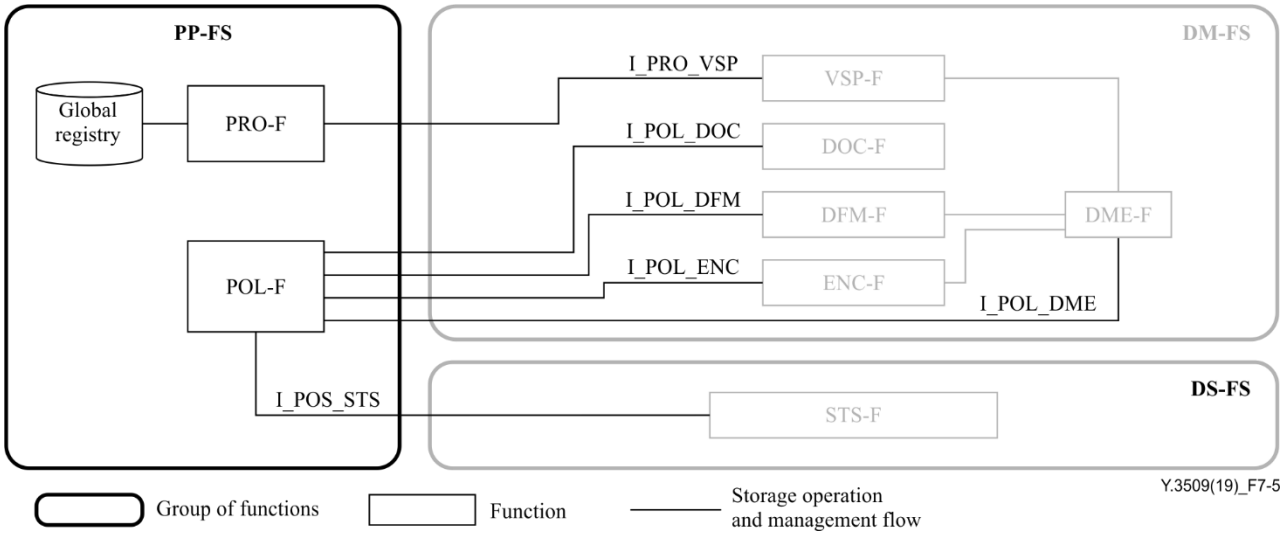

Figure 7-5 – PP-FS and related reference points

The provision and policy management functions (PP-FS) consist of two functions: provision of single virtual volume and virtual storage pool (PRO-F), and policy management of data storage and data manipulation (POL-F) as shown in Figure 7-5.

The PP-FS interacts with DSF data manipulation functions (DM-FS) and DSF local storage management functions (DS-FS).

7.4.1 Provision of single virtual volume and virtual storage pool function

The provision of single virtual volume and virtual storage pool function (PRO-F) (see clause 6.4.2) receives storage management metadata for validating the metadata and virtual storage pool from VSP-F. PRO-F receives data operation metadata for creating single virtual volume from VSP-F.

7.4.2 Policy management of data storage and data manipulation function

The policy management of data storage and data manipulation function (POL-F) (see clause 6.4.1) sends following policies:

– policy of data manipulation for acceleration of data operation to DOC-F;
– policy of data manipulation to DFM-F for efficiency of data storing;
– policy of data manipulation for protection and compression of data to ENC-F;
– policy for performance enhancement to DME-F;
– policy of storage tier to STS-F.

8 DSF reference points

This clause describes the reference points among DSF functions.

8.1 Reference point between SC-FS and DM-FS

The reference point between SC-FS and DM-FS is as follows:

I_SVI_VSP reference point between VSI-F and VSP-F. Storage management metadata and virtual storage pool information are exchanged through this reference point.

8.2 Reference point between DM-FS and DS-FS

The reference point between DM-FS and DS-FS is as follows:

I_VSP_DSC reference point between VSP-F and DSC-F. DSF local storage information for configuring virtual storage pool is registered through this reference point.

8.3 Reference points between PP-FS and DM-FS

The reference points between PP-FS and DM-FS are as follows:

I_PRO_VSP reference point between PRO-F and VSP-F. Storage management metadata for configuring virtual storage pool and data operation metadata for allocating single virtual volume are delivered through this reference point.

I_POL_DOC reference point between POL-F and DOC-F. Through this reference point, POL-F sends policy of data manipulation for read cache and write buffer of data.

I_POL_DFM reference point between POL_F and DFM-F. Through this reference point, POL-F sends policy of data manipulation for efficiency of data storing.

I_POL_ENC reference point between POL-F and ENC-F. Through this reference point, POL-F sends policy of data manipulation for protection and compression of data.

I_POL_DME reference point between POL-F and DME-F. Through this reference point, POL-F sends policy for performance enhancement for high availability of data and data storage.

8.4 Reference point between PP-FS and DS-FS

The reference point between PP-FS and DS-FS is as follows:

I_POL_STS reference point between POL-F and STS-F. Through this reference point, POL-F sends policy of storage tier for performance enhancement of data access and usage.

8.5 Reference point between DS-FS and DSF local storage

The reference point between DS-FS and DSF local storage is as follows:

I_DSC_DLS reference point between DSC-F and DSF local storage. DSC-F gathers DSF local storage information for checking connection status through this reference point.

8.6 Reference point within SC-FS

The reference point within SC-FS is as follows:

I_CUA_SVI reference point between CUA-F and SVI-F. CUA-F sends information for configuring single virtual volume through this reference point.

8.7 Reference points within DM-FS

The reference points within DM-FS are as follows:

I_VSP_DOC reference point between VSP-F and DOC-F. VSP-F sends the sizes of write buffer and read cache through this reference point.

I_DFM_DME reference point between DFM-F and DME-F. Through this reference point, DFM-F sends data operation metadata for fragmentation in order to replicate data.

I_VSP_DFM reference point between VSP-F and DFM-F. Through this reference point, VSP-F sends DSF local storage information and virtual storage pool information.

I_VSP_DME reference point between VSP-F and DME-F. Through this reference point, DSF local storage information for distribution of replicated fragments and fail-over is sent.

I_ENC_DME reference point between ENC-F and DME-F. Through this reference point, DME-F transfers policy of performance enhancement for sensitive data encryption/decryption and compression/decompression.

8.8 Reference point within DS-FS

The reference point within DS-FS is as follows:

I_DSC_STS reference point between DSC-F and STS-F. DSF local storage information for multiple access and monitoring is exchanged through this reference point.

9 Security considerations

Security considerations related to DSF are categorized as follows:

– DSF security functions related to CSUs

CSP (i.e., DSF service provider) provides various access mechanisms for a CSU to access CSU's storage and single virtual volume for a CSU to create, read, update, and delete data (see clause 6.1). Therefore, it is necessary for CSP to consider:

- identity and access management (IAM), authentication, authorization, transaction audit, and interface security defined in [b-ITU-T X.1601];
- security controls in transmit stage, and use stage defined in [b-ITU-T X.1641].

– Security functions of DSF architecture

The CSU's data is encrypted, fragmented, distributed, and stored in DSF local storage. The fragmented data is encrypted and then transferred to DSF local storage (see clause 6.2). Therefore, it is necessary for CSP to consider:

- data isolation, protection and privacy protection defined in [b-ITU-T X.1601];
- security controls in create stage, storage stage, migrate stage, destroy stage, and backup and restore stage defined in [b-ITU-T X.1641].

– Interface related security functions of DSF architecture

Virtual storage pool is built by consolidating DSF local storage and administered by policy (see clause 6.3). Logical components are configured and controlled by policy, and DSF local storage is provisioned and single virtual volume is provided to a CSU with interface (see clause 6.4). Therefore, it is necessary for the CSP to consider:

- interface related security, operational security, service security assessment and audit defined in [b-ITU-T X.1601];
- security controls in transmit stage, storage stage, and use stage defined in [b-ITU-T X.1641].

Appendix I

Relationships between DSF functional requirements, DSF logical components, and DSF functions

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

DSF logical components are described in clause 6.3 of [ITU-T Y.3505]. Table I.1 shows key features of these logical components for deriving DSF functions.

Table I.1 – Logical component and summarized features by keyword

Logical component in [ITU-T Y.3505]	Summarized key features from [ITU-T Y.3505]
Storage connection	• Customer access for single virtual volume • The interface of single virtual volume • The protocols or I/O interfaces for customer access (including acceleration for protocol and I/O)
Data manipulation	• The management of virtual storage pool (including configuration virtual storage pool and performing storage operation) • The data operation with write buffer or read cache • The enhanced management for data manipulation (snapshots, fast replication, and distributed transaction logs, enhancement of the read and write response time)
Data distribution and storing	• Data fragmentation to distribute and store data (including optimization of writing data to DSF local storage) • Encryption/decryption and compression/decompression
DSF local storage management	• Connections and management to DSF local storage • Storage structuring with tiering
Provisioning and policy management	• Configurations and controls of logical components • Policy management of data storage and data manipulation • Provision of single virtual volume and virtual storage pool

The analysis of the relationships between the DSF requirements, DSF logical components, and DSF functions is shown in Table I.2.

Table I.2 – The relationships between DSF requirements, DSF logical components, and DSF functions

DSF functional requirement in [ITU-T Y.3505]		Related in [ITU-T Y.3505]	Related logical component in [ITU-T Y.3505]	Related DSF functions
A. Storage connection requirement	(1) It is required that CSP:SFP provide an interface to connect DSF local storage	Connections and management to DSF local storage	DSF local storage management	DSF local storage connection (6.3.1)
	(2) It is required that CSP:SFP provide a user interface for CSC:CSU to use a single virtual volume	Customer access for single virtual volume	Storage connection	Customer access (6.1.1)
	(3) It is recommended that CSP:SFP support the change of CSC:CSU's access mechanism according to the storage type of single virtual volume	The protocols or I/O interfaces for customer access	Storage connection	Single virtual volume interface (6.1.2)
	(4) It is required that CSP:DMP provide translation between data operation and corresponding interface of DSF local storage	Connections and management to DSF local storage	DSF local storage management	DSF local storage connection (6.3.1)
	(5) It is recommended that CSP:SFP provide secure access mechanism to use single virtual volume for CSC:CSU	The protocols or I/O interfaces for customer access	Storage connection	Single virtual volume interface (6.1.2)
	(6) It is required that CSP:DMP provide the registration of the CSC:CSU's requirements	Customer access for single virtual volume	Storage connection	Customer access (6.1.1)
	(7) It is required that CSP:SFP provide the seamless connection of DSF local storage interface to communicate with DSF local storage	Connections and management to DSF local storage	DSF local storage management	DSF local storage connection (6.3.1)
B. Data manipulation requirements	(1) It is required that CSP:DMP provide the execution of CSC:CSU's CRUD data operation	The data operation with write buffer or read cache	Data manipulation	Data operation with write buffer or read cache (6.2.2)
	(2) It is required that CSP:DMP provide search data operation from CSC:CSU's data using query to global registry	The data operation with write buffer or read cache	Data manipulation	Data operation with write buffer or read cache (6.2.2)
	(3) It is recommended that CSP:DMP provide sharing data operation by updating of sharing status of DSF data in global registry after checking sharing status of DSF data	The data operation with write buffer or read cache	Data manipulation	Data operation with write buffer or read cache (6.2.2)

Table I.2 – The relationships between DSF requirements, DSF logical components, and DSF functions

DSF functional requirement in [ITU-T Y.3505]		Related in [ITU-T Y.3505]	Related logical component in [ITU-T Y.3505]	Related DSF functions
	(4) It is recommended that CSP:DMP provide the capacity saving of data storage using de-duplication of DSF data	Encryption/decryption and compression/ decompression	Data distribution and storing	Encryption/decryption and compression/ decompression (6.2.4)
	(5) It is recommended CSP:DMP provide DSF data encryption/decryption for data transfer to DSF local storage	Encryption/decryption and compression/ decompression	Data distribution and storing	Encryption/decryption and compression/ decompression (6.2.4)
	(6) It is required CSP:DMP provide data recovery of CSC:CSU from system failure	The enhanced management for data manipulation	Data manipulation	Enhanced management for data manipulation (6.2.5)
	(7) It is recommended that CSP:DMP provide DSF data migration to available DSF local storage for resilience and cost efficiency of the storage space	The enhanced management for data manipulation	Data manipulation and DSF local storage management	Enhanced management for data manipulation (6.2.5)
	(8) It is required that the CSP:DMP provide the validation of DSF data on data operation to check the data integrity	The enhanced management for data manipulation	Data manipulation	Enhanced management for data manipulation (6.2.5)
	(9) It is required that CSP:DMP support CSC:CSU's data consistency for replicated DSF data	The enhanced management for data manipulation	Data manipulation	Enhanced management for data manipulation (6.2.5)
	(10) It is required that CSP:DMP support CSC:CSU's data transparency	The enhanced management for data manipulation	Data manipulation	Enhanced management for data manipulation (6.2.5)
C. Storage federation requirements	(1) It is recommended that CSP:SFP provide the performance information of DSF local storage from storage management metadata	Data fragmentation to distribute and store data (including optimization of writing data to DSF local storage)	Data distribution and storing, DSF local storage management	Data fragmentation for distribution (6.2.3)
	(2) It is recommended that CSP:SFP provide virtual storage pool optimization considering the performance of DSF local storage	Data fragmentation to distribute and store data (including optimization of writing data to DSF local storage)	Data distribution and storing	Data fragmentation for distribution (6.2.3)

Table I.2 – The relationships between DSF requirements, DSF logical components, and DSF functions

DSF functional requirement in [ITU-T Y.3505]		Related in [ITU-T Y.3505]	Related logical component in [ITU-T Y.3505]	Related DSF functions
	(3) It is recommended that CSP:SFP provide single virtual volume optimization based on CSC:CSU's purpose	The enhanced management for data manipulation (snapshots, fast replication, and distributed transaction logs, enhancement of the read and write response time)	Data manipulation	Enhanced management for data manipulation (6.2.5)
	(4) It is required that CSP:SFP provide the configuration of single virtual volume from CSC:CSU requests	Provision of single virtual volume and virtual storage pool	Provisioning and policy management, Storage connection	Provision of single virtual volume and virtual storage pool (6.4.3)
	(5) It is required that CSP:SFP provide a read/write cache to access data	The data operation with write buffer or read cache	Data manipulation	Data operation with write buffer or read cache (6.2.2)
	(6) It is recommended that CSP:SFP provide hierarchical cache management using cache multi-tiering	The data operation with write buffer or read cache	Data manipulation	Data operation with write buffer or read cache (6.2.2) Storage structuring (6.3.2)
	(7) It is required that CSP:SFP provide the backup of global registry for high availability	The enhanced management for data manipulation (snapshots, fast replication, and distributed transaction logs, enhancement of the read and write response time)	Data manipulation	Enhanced management for data manipulation (6.2.5)
	(8) It is recommended that CSP:SFP provide in-parallel access to DSF local storage	Connections and management to DSF local storage	DSF local storage management	DSF local storage connection (6.3.1)
	(9) It is required that CSP:SFP provide the registration of CSC:CSU's credential to DSF local storage	Connections and management to DSF local storage	DSF local storage management	DSF local storage connection (6.3.1)
	(10) It is recommended that CSP:SFP support monitoring the performance information of DSF local storage	Configurations and controls of logical components	Provisioning and policy management, DSF local storage management	Configurations and controls of logical components (6.4.1)

Table I.2 – The relationships between DSF requirements, DSF logical components, and DSF functions

DSF functional requirement in [ITU-T Y.3505]		Related in [ITU-T Y.3505]	Related logical component in [ITU-T Y.3505]	Related DSF functions
	(11) It is required that CSP:SFP provide the management of DSF local storage interface	Connections and management to DSF local storage. Configurations and controls of logical components	DSF local storage management, provisioning and policy management	DSF local storage connection (6.3.1) Configurations and controls of logical components (6.4.1)
	(12) It is recommended that CSP:SFP support to access the secured storage interface for DSF local storage	Connections and management to DSF local storage	DSF local storage management,	DSF local storage connection (6.3.1)
	(13) It is required that CSP:SFP provide the storage operation for DSF local storage	The management of virtual storage pool (including configuration virtual storage pool and performing storage operation)	Data manipulation, provisioning and policy management	Virtual storage pool Management (6.2.1)
	(14) It is required that CSP:SFP provide scaling of single virtual volume on CSC:CSU demand	The management of virtual storage pool (including configuration virtual storage pool and performing storage operation)	Data manipulation	Virtual storage pool management (6.2.1)
D. Metadata and policy management requirements	(1) It is recommended that CSP:SFP provide a configuration of single virtual volume by data storage policy for CSC:CSU	The management of virtual storage pool (including configuration virtual storage pool and performing storage operation). Policy management of data storage and data manipulation	Data manipulation, provisioning and policy management	Policy management of data storage and data manipulation (6.4.2)
	(2) It is recommended that CSP:SFP provide default data storage policies when policy is not configured	Policy management of data storage and data manipulation	Provisioning and policy management	Policy management of data storage and data manipulation (6.4.2)
	(3) It is recommended that CSP:DMP provide a transformation of DSF data by data manipulation policy	Policy management of data storage and data manipulation	Provisioning and policy management	Policy management of data storage and data manipulation (6.4.2)
	(4) It is recommended that CSP:DMP provide default data manipulation policy	Policy management of data storage and data manipulation	Provisioning and policy management	Policy management of data storage and data manipulation (6.4.2)
	(5) It is required that CSP:SFP provide global registry for customer data access	Policy management of data storage and data manipulation	Provisioning and policy management	Policy management of data storage and data manipulation (6.4.2)

Table I.2 – The relationships between DSF requirements, DSF logical components, and DSF functions

DSF functional requirement in [ITU-T Y.3505]		Related in [ITU-T Y.3505]	Related logical component in [ITU-T Y.3505]	Related DSF functions
	(6) It is required that CSP:SFP provide high-speed access of global registry	Policy management of data storage and data manipulation	Provisioning and policy management	Policy management of data storage and data manipulation (6.4.2)
	(7) It is required that CSP:DMP provide management of data operation metadata automatically according to execution of data operation	Policy management of data storage and data manipulation	Provisioning and policy management	Policy management of data storage and data manipulation (6.4.2)
	(8) It is required that CSP:SFP provide storage management metadata to communicate with DSF local storage	Policy management of data storage and data manipulation	Provisioning and policy management	Policy management of data storage and data manipulation (6.4.2)

Appendix II

Relationships between DSF functions and functional components of the cloud computing reference architecture

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

This appendix illustrates the relationship between DSF functions and functional components of the cloud computing reference architecture (CCRA) described in [ITU-T Y.3502].

DSF functions described in clause 6 are mapped to the functional components of the cloud computing reference architecture [ITU-T Y.3502] as shown in Figure II.1.

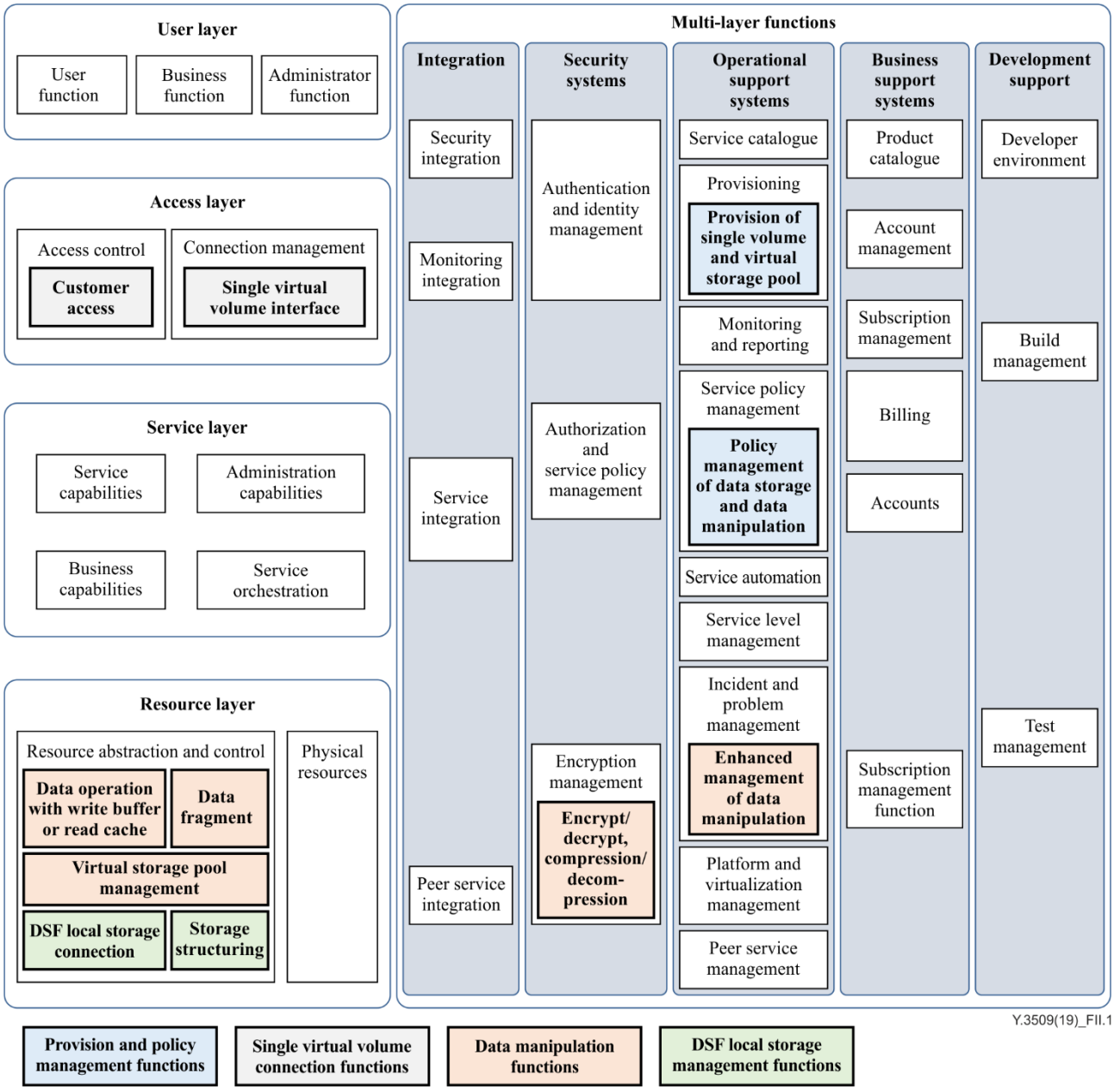

Figure II.1 – Relationship between DSF functions and functional components of the cloud computing reference architecture

Relationships between layers of the cloud computing reference architecture and DSF functions are as shown in Table II.1.

Table II.1 – Relationships between DSF functions and functional components of the cloud computing reference architecture (CCRA)

Relationships between cloud computing reference architecture and DSF functions	The related functions in this Recommendation
Access layer	• Customer access (see clause 6.1.1), and • Single virtual volume interface (see clause 6.1.2)
Resource layer	• Virtual storage pool management (see clause 6.2.1), • Data operation with write buffer or read cache (see clause 6.2.2), • Data fragmentation (see clause 6.2.3), • Encryption/decryption and compression/decompression (see clause 6.2.4), and • Enhanced management for data manipulation (see clause 6.2.5).
Resource layer	• DSF local storage connection (see clause 6.3.1), and • Storage structuring (see clause 6.3.2).
Multi-layer	• Policy management of data storage and data manipulation (see clause 6.4.1), and • Provision of single virtual volume and virtual storage pool (see clause 6.4.2).

Appendix III

Example of data flow in DSF functional architecture

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

The example of data flow in DSF functional architecture refers to the path through which data passes as shown in Figure III.1.

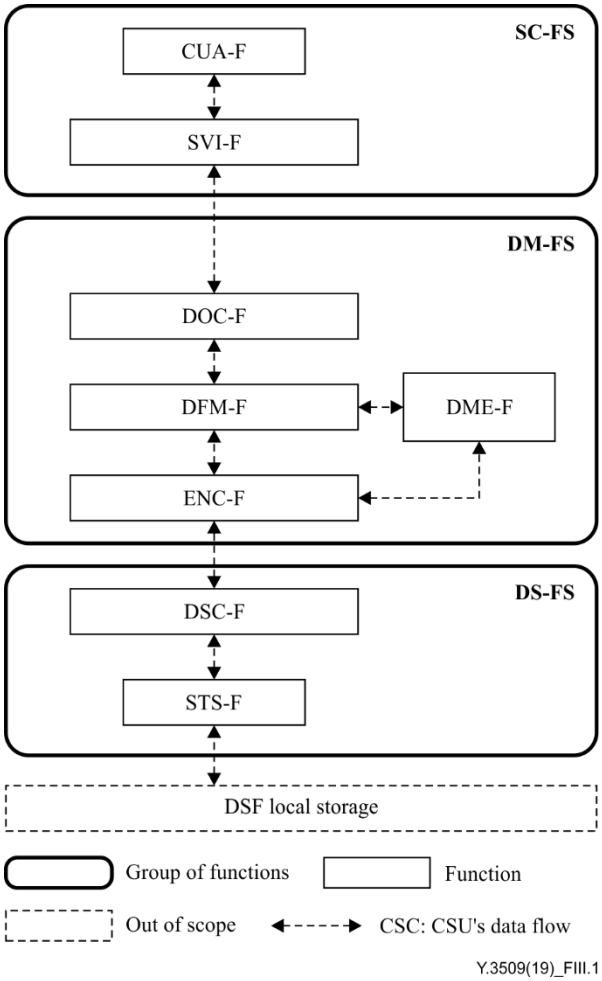

Figure III.1 – Example of data flow in DSF functional architecture

CSU's data is written in single virtual volume, which is allocated by SVI-F through CUA-F.

Then, the written data is buffered by DOC-F, data fragmented by DFM-F, and encrypted and compressed by ENC-F.

When CSU requests performance enhancement (such as data replication, backup, snapshots, migration, error correction, data protection, etc.), data is processed according to policy for performance enhancement by DME-F. Data is transferred to STS-F which tiers with hierarchical storage and then data is stored in DSF local storage.

SVI-F accesses DSF global registry to find the location of data, and DOC-F searches the data in read cache. When data is not available in read cache, DSC-F reads data from DSF local storage through STS-F. When data is encrypted/compressed, ENC-F decrypts/decompresses the data. When data is fragmented, DFM-F defragments the fragmented data.

Bibliography

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

[b-ITU-T X.1641] Recommendation ITU-T X.1641 (2016), *Guidelines for cloud service customer data security.*

[b-AES] Federal Information Processing Standards Publication (FIPS PUB), *Announcing the ADVANCED ENCRYPTION STANDARD (AES)*, Secretary of Commerce, United States National Institute of Standards and Technology (NIST), 2001.

[b-Ceph] SA Weil, SA Brandt, EL Miller, DDE Long and C Maltzahn (2006), *Ceph: A scalable, high-performance distributed file system*, Proc. OSDI.

[b-DES] Federal Information Processing Standards Publication (FIPS PUB), *Data encryption standard (DES)*, Department of Commerce, United States National Institute of Standards and Technology (NIST), 1999.

[b-FTP] IETF RFC 114 (1971), *A File Transfer Protocol*.

[b-iSCSI] IETF RFC 3270 (2004), *Internet Small Computer Systems Interface (iSCSI)*.

[b-Lustre] Corbet, Jonathon (2003). *Lustre 1.0 released*, Linux Weekly News.

[b-NFS] IETF RFC 1094 (1989), *NFS: Network File System Protocol Specification*.

[b-SCSI] IEEE Std 1394-1995, *IEEE Standard for a High-Performance Serial Bus*.

[b-SEED] RFC 4269, *The SEED Encryption Algorithm, Korea Internet and Security Agency (KISA)*, 2005.

[b-SFTP] IETF draft-ietf-secsh-filexfer-00.txt (2001), *SSH File Transfer Protocol*.

[b-SSH] IETF RFC 4253 (2006), *The Secure Shell (SSH) Transport Layer Protocol*.

[b-Swift] Openstack, *swift 2.19.1.dev136*, https://docs.openstack.org/swift/latest/LWN.net.

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

Printed in Switzerland
Geneva, 2020