International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.3504
(06/2016)

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

Cloud Computing

Functional architecture for Desktop as a Service

Recommendation ITU-T Y.3504

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND 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

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

Recommendation ITU-T Y.3504

Functional architecture for Desktop as a Service

Summary

Recommendation ITU-T Y.3504 describes Desktop as a Service (DaaS) functions and functional architecture for DaaS. This Recommendation also describes the relationship between the DaaS functional architecture and the cloud computing reference architecture.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3504	2016-06-13	13	11.1002/1000/12889

Keywords

DaaS functional architecture, DaaS functions, Desktop as a Service, virtual desktop.

---

* 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/11.1002/1000/11 830-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.3504

Functional architecture for Desktop as a Service

1 Scope

This Recommendation provides functional architecture for desktop as a service (DaaS) to specify the detailed functions and their relationships based on the general and functional requirements of [ITU-T Y.3503]. It addresses the following subjects:

– DaaS functions;

– DaaS functional architecture;

– mapping DaaS functional architecture to the cloud computing reference architecture.

2 References

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

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

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

[ITU-T Y.3503] Recommendation ITU-T Y.3503 (2014), *Requirements for desktop as a service*.

[ITU-T Y.3510] Recommendation ITU-T Y.3510 (2016), *Cloud computing infrastructure requirements*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

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

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

3.1.3 DaaS client [ITU-T Y.3503]: A physical device and associated software running on the device that collectively enable a cloud service user to access Desktop as a Service (DaaS).

3.1.4 Desktop as a Service [ITU-T Y.3503]: A cloud service category in which the capabilities provided to the cloud service customer are the ability to build, configure, manage, store, execute, and deliver users' desktop functions remotely.

NOTE – Examples of end user's desktop functions can include desktop interface functions for applications, data access functions for multimedia data, and control functions for input/output (I/O) devices.

3.1.5 hypervisor [ITU-T Y.3510]: A type of system software that allows multiple operating systems to share a single hardware host.

3.1.6 virtual desktop [ITU-T Y.3503]: An environment for accessing end user's desktop functions remotely.

3.1.7 virtual machine [b-DMTF OVF]: The complete environment that supports the execution of guest software.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CCM-F	Client Connection Management Function
CN-F	Connection Negotiation Function
CPC-F	Client Peripheral Connection Function
CPU	Central Processing Unit
CSC	Cloud Service Customer
CS-FS	Client Support Functions
CSP	Cloud Service Provider
CSU	Cloud Service User
DaaS	Desktop as a Service
DB	Database
DPP-F	Delivery Protocol Processing Function
FC	Functional Component
GPU	Graphic Processing Unit
HA-F	High Availability for DaaS Function
H/W	Hardware
IAM-F	Infrastructure Access Management Function
ID	Identification
I/O	Input/Output
IP	Internet Protocol
MAC	Media Access Control
MC-F	Monitoring and Controlling virtual desktop resource Function
OS	Operating System
OPM-F	Operational Policy Management for DaaS Function
PA-F	Provisioning and Allocation of virtual desktop Function
PE-F	Performance Enhancement for virtualization platform Function
PM-F	Power Management of virtual desktop resource Function
PV-F	Platform Virtualization Function
QoS	Quality of Service

RA-F   Resource Assignment Function

RAD-F   virtual desktop Resource Allocation and Distribution Function

SCUE-F   Service Continuity for User Environment Function

SC-F   Service Connection Function

UAM-F   User Access Management Function

UAPM-F   User Account and Profile Management Function

VDCD-FS   Virtual Desktop Connection and Delivery Functions

VDRM-FS   Virtual Desktop Resource Management Functions

VI-FS   Virtualization Infrastructure Functions

VM   Virtual Machine

5   Conventions

Throughout this Recommendation, the term "DaaS user" is to be understood as equivalent to "cloud service user (CSU)".

6   Relationship between DaaS logical components and DaaS functions

There are five DaaS logical components in Recommendation [ITU-T Y.3503]:

1)   DaaS client;

2)   connection manager;

3)   resource pool;

4)   virtualization infrastructure;

5)   virtual desktop delivery.

NOTE – The relationship between the DaaS logical components and the cloud computing reference architecture in [ITU-T Y.3502] is described in Appendix I.

In DaaS, a connection manager is configured to establish connections to a DaaS client and manage these connections. Virtual desktops in the virtualization infrastructure are provided to DaaS users through virtual desktop delivery. The resource pool is provisioned or configured to assign optimum resources to virtual desktops for the DaaS clients. These DaaS logical components are realized by the following DaaS functions:

–   **virtualization infrastructure support functions**: These functions support DaaS in terms of virtualization infrastructure with resource pool;

–   **virtual desktop connection and delivery functions**: These functions configure, provision, and deliver virtual desktops in connection manager and virtual desktop delivery;

–   **virtual desktop resource management functions**: These functions manage resources in resource pool for virtual desktops;

–   **DaaS client support functions**: These functions support DaaS from a DaaS client's perspective.

Table 6-1 shows the relationship between DaaS logical components in [ITU-T Y.3503] and DaaS functions in this Recommendation.

Table 6-1 – Relationship between DaaS logical components and DaaS functions

DaaS logical components [ITU-T Y.3503]	DaaS functions This Recommendation
Virtualization infrastructure	Virtualization infrastructure support (see clause 7.1)
Connection manager	Virtual desktop connection and delivery (see clause 7.2)
Virtual desktop delivery	
Resource pool	Virtual desktop resource management (see clause 7.3)
DaaS client	DaaS client support (see clause 7.4)

7 DaaS functions

7.1 Virtualization infrastructure support

Virtualization infrastructure support functions provide the abilities to:

– offer abstracting hardware resources (see clause 7.1.1);

– allocate resources to a virtual desktop resource assignment function (see clause 7.1.2);

– improve the performance in terms of a DaaS platform (see clause 7.1.3);

– supply the interfaces to access the virtualization infrastructure (see clause 7.1.4).

7.1.1 Platform virtualization

Providing a separate virtual desktop environment for each DaaS user is a main role of the platform virtualization function. This function:

– performs abstracting hardware resources in order to assign them to a virtual desktop efficiently;

   NOTE – Abstracting hardware resources has different approaches, e.g., operating-system-level virtualization and hypervisor which are configured to accommodate one or more virtual machines above hardware;

   • operating-system-level virtualization is a virtualization method where the input/output (I/O) management part of a base operating system (OS) allows for multiple isolated user space instances, instead of just one. Such instances may look like a virtual desktop environment from the point of view of its DaaS users. (E.g., container based approach);

   • a hypervisor is a type of system software that allows multiple OSs to share a single hardware host [ITU-T Y.3510]. It is classified into two types depending on the installation on a host machine. In the one type, hypervisors are installed and run directly on the host machine's hardware like an OS. The other type is described such a way that hypervisors are installed on an existing operating system OS of the host machine and run just as other applications do.

– coordinates invocations on central processing unit (CPU), memory, disk, network and other resources through the platform OS. Since the platform OS takes care of all the hardware, this function supports the hardware compatibility;

– consolidates multiple platforms into the pool of physically separated hardware resources;

– isolates virtual desktops not to affect the operation of a platform itself or any other virtual desktops;

– constructs the multiple systems for DaaS such as server, storage and network to serve different DaaS users.

7.1.2   Resource assignment

The resource assignment function:

–   allocates the software and hardware resources to a virtual desktop;

      NOTE 1 – Software resources include OS image, disk image, applications, templates and profile, etc. Hardware resources include all hardware in virtualization infrastructure such as CPU, memory, storage which is the separated space to store a user's own data and network, etc.

–   provides resource interfaces to assign the hardware resources to a virtual desktop;

      NOTE 2 – Resource interface includes virtual or physical device driver, virtual I/O interface and API etc.

–   operates when creating virtual desktops and operates when a DaaS user requests resource changes. All resources for DaaS are managed through resource pooling. These pooled resources are prepared and managed to be provided quickly from the pre-configured environment to a DaaS user.

7.1.3   Performance enhancement for virtualization platform

The performance enhancement for virtualization platform function:

–   utilizes graphic processing acceleration which uses rendering resources in both a DaaS platform and a DaaS client simultaneously;

      NOTE 1 – Rendering resources include CPU, graphic processing unit (GPU) and software resources for rendering, etc. To reduce the delays in delivering high-definition display, graphic processing acceleration also adopts hardware-based compression and decompression units in a DaaS platform and a DaaS client, respectively. A DaaS platform can be also configured with vGPU.

–   employs in-memory virtual desktop which is created, stored and managed on main memory to provide high-speed processing to a DaaS user. This virtual desktop environment, in main memory, is backed up when a DaaS platform is turned off and restored from backup storage with non-volatile characteristics when a DaaS platform is turned on due to the volatile characteristics of memory. In order for virtual desktop environments to be managed on small-size memory, the de-duplicated image is adopted;

      NOTE 2 – the de-duplicated image in the main memory is converted to a read/write command which is transferred in blocks to the actual read/write command on the accessible main memory address.

–   uses caching which is used to increase the loading rate of the virtual desktop environment at the creation step of the virtual desktop. One pre-configured virtual desktop environment (especially, OS or disk image) on shared storage is converted into copy-on-write file format stored in a memory cache and allocated to the virtual desktop;

–   optimizes the delivery protocol from the created multiple paths for different DaaS user's services to improve network performance.

7.1.4   Infrastructure access management

There are three ways to access virtualization infrastructure in DaaS:

1)   access for the resource allocation by provisioning;

2)   access for virtual desktop over delivery protocol by a DaaS client;

3)   access for the management of DaaS platforms by administrators.

Infrastructure access management function:

–   grants access to the virtualization infrastructure after confirming the access authority;

–   connects to the virtualization infrastructure through the interface of resource, which is allocated according to the user account and cloud service customer (CSC) type;

NOTE – Virtualization infrastructure for DaaS utilizes various cloud infrastructures from different cloud service providers (CSPs) or an individual platform owned by one CSP. Interface in this function refers to both cases.

– transmits operating commands on the virtual desktop to access the selected resources;

– maintains, changes and deletes the access authority of infrastructure which has already been established from a user request;

– applies to the separated access authorities of each resource in the infrastructure individually.

7.2 Virtual desktop connection and delivery

Virtual desktop connection and delivery functions:

– perform a delivery protocol (see 7.2.1 delivery protocol processing function);

– connect virtual desktops for a DaaS user (see 7.2.2 client connection management function);

– validate a DaaS user with user authentication (7.2.3 user access management function);

– establish a virtual desktop for a DaaS user (7.2.4 provisioning and allocation function).

7.2.1 Delivery protocol processing

The delivery protocol processing function:

– provides the communication channels through the network for exchanging information between the DaaS client and the DaaS platform;

NOTE 1 – Examples of exchanged information by the delivery protocol processing function are virtual desktop's display, video and audio data, events of input devices (e.g., mouse, keyboard), and events of other DaaS client peripherals.

– transmits virtual desktop environments to the DaaS client after the coordination process performed by the client connection management function (see clause 7.2.2) and the connection to the virtual desktop by the DaaS client with the virtual desktop access information;

NOTE 2 – Virtual desktop access information includes the information for connecting virtual desktop such as internet protocol (IP) address, URI, port number of the DaaS platform, port number of assigned virtual desktop, and password for secure connection.

– redirects virtual desktop's graphic display to a DaaS client;

– provides the compressed display to decrease the network bandwidth for high resolution and dimension display data;

– transmits video/audio data encoded and decoded with standard codec for each applicable video/audio content;

– determines connection negotiation results based on monitoring information received from the connection negotiation function (see clause 7.4.2) and the monitoring and controlling virtual desktop resource function (see clause 7.3.1);

NOTE 3 – Connection negotiation result includes screen resolution, compression rate of video and audio, transmission rate of display, and kind of video and audio codec.

– uses standard security protocols in order to protect the content exchanged between a DaaS client and a DaaS platform.

7.2.2 Client connection management

The client connection management function:

– establishes a connection to a DaaS client after DaaS user's authentication related with the user access management function (see clause 7.2.3);

–   identifies CSC types (e.g., allocated user, pooled user, multi-virtual machine (VM) user) which were previously assigned from CSU's account information;

NOTE 1 – The allocated user uses its own allocated virtual desktop persistently and has its own permanent virtual desktop by adopting a pre-set method and a manual method.

NOTE 2 – The pooled user has a non-persistent virtual desktop for one-time use only. When the user terminal, divided as the pooled user is logged off from the operation server, the virtual desktop used by the user terminal is deleted. When the user terminal accesses the operation server again, a new virtual desktop is allocated to the user terminal. The operation server does not store a personal profile of the user when the access of the user terminal of the pooled user is released.

NOTE 3 – The multi-VM user is allowed to use multiple virtual desktops.

NOTE 4 – CSU's account information is registered by an administrator at the portal of a DaaS platform or the administrator's terminal to approve a DaaS user's prior permission. This information includes CSC type, user name, e-mail, telephone number, social security number and employee identification (ID), etc. This information can be maintained and provided using database (DB), active directory, or lightweight directory access protocol.

–   identifies the user profile managed by the user profile management function (see clause 7.3.2) if a DaaS user has already been registered;

–   coordinates with different virtualization infrastructures according to a delivery protocol, in some cases the client connection needs to be customized according to dedicated infrastructure;

–   sends virtual desktop access information and/or other formats like a customized access connector software, access connection plugins in a browser to a DaaS client to proceed with client connection;

–   performs connection monitoring for any type and reconnection with the connection monitoring if a DaaS client is disconnected; it also guarantees both security and quality of service (QoS) of the delivered DaaS service based on the connection;

–   validates the license of the user's applications of virtual desktops.

7.2.3   User access management

The user access management function:

–   validates a DaaS user with CSU's access information in logon procedure;

NOTE 1 – CSU's access information is registered at the portal of a DaaS platform or a DaaS user's terminal. This information includes ID, password, and other check items for authority. This information can be used in login procedure.

NOTE 2 – For a DaaS user who accesses DaaS for the first time, an administrator prepares CSU's access information for the DaaS user's logon procedure in advance in the user account and profile management function (see clause 7.3.2).

–   accesses the user account and profile management function (see clause 7.3.2) for each DaaS client according to CSC types, the information may be used to authorize access, establish connections with DaaS-specific protocol/connection;

–   notifies the result of a client connection to a DaaS client to give guides to access a DaaS platform and requests the client connection to the client connection management function (see clause 7.2.2) after validating a DaaS user, the access can be achieved through a dedicated connector software or through a web browser and plugin supporting DaaS-specific protocol;

–   supports differentiated permissions according to CSC types;

NOTE 3 – The permissions are classified into authority of administration, resource access, and service access.

– supports secure access through a security protocol (such as secure shell or transport layer security) and technical access depending on the type of DaaS client such as the dedicated software, general-purpose web browser;

– maintains logs such as the date and time of the user log-on and log-off, the type of DaaS client, the location of the DaaS client, and the service usage, etc.

7.2.4 Provisioning and allocation of virtual desktop

The provisioning and allocation function:

– prepares hardware and software resources for a virtual desktop corresponding with CSU's account information, load-balancing or allocation policy;

– configures a DaaS platform with a virtual desktop delivery protocol and resource pool for virtual desktop environments;

   NOTE 1 – This function involves the following processes:

   • the provision for a DaaS client configured to receive the allocation of a virtual desktop;

   • the provision for a connection manager to control a type of a virtual desktop to be allocated according to CSU's account and access information;

   • the provision for a DaaS Platform to be selected among platforms in the datacentre or server farm on which the virtual desktop is allocated.

– configures a pre-configured virtual desktop environment (such as an OS image and a user disk image) and stores it to share for convenience and speed of the configuration;

– installs and updates software in a pre-configured virtual desktop environment as well as a DaaS platform;

– deploys a DaaS platform which scales up, down, and out including redundancy;

   NOTE 2 – If a heterogeneous virtualization infrastructure is adopted, this function deploys it and prepares a new pre-configured environment compared with the previous user environment.

– determines operating status of a DaaS platform and a virtual desktop according to CSC type;

   NOTE 3 – Based on the operating status, this function assigns a previously allocated virtual desktop, a temporary allocated virtual desktop, or a newly created virtual desktop on the optimum DaaS platform according to CSU's account information.

   NOTE 4 – The optimum DaaS platform has best-efforts performance from the monitoring of server power or performance among DaaS platforms.

– identifies CSC type and service catalogue.

7.3 Virtual desktop resource management

Virtual desktop resource management functions:

– monitor and control states of virtual desktop resources (see clause 7.3.1 monitoring and controlling virtual desktop resource function);

– manage user accounts and profiles in terms of administrators and DaaS users (see clause 7.3.2 user account and profile management function);

– offer a virtual desktop and other resources to a DaaS user in a timely manner (see clause 7.3.3 virtual desktop resource allocation and distribution function);

– establish operational policy (see clause 7.3.4 operational policy management for DaaS function);

– offer high availability (see clause 7.3.5 high availability for DaaS function);

– supply management of power consumption (see clause 7.3.6 power management of virtual desktop resource function).

7.3.1 Monitoring and controlling virtual desktop resource

In the monitoring and controlling virtual desktop resource function, monitored and controlled targets for DaaS are mainly virtualization infrastructure and virtual desktops. Monitoring information is classified into static and run-time data.

NOTE 1 – The exchanged monitoring information is communicated through a protocol between a monitoring target and virtualization infrastructure. A software agent or daemon activated in virtualization infrastructure is used to gather monitoring information which is stored as a form of database or other file formats. This database is normally accessible by other functions.

The monitoring and controlling virtual desktop resource function:

– monitors the information of virtualization infrastructure to gather by event processing during running DaaS;

  NOTE 2 – The monitoring information of virtualization infrastructure is as follows:

  • basic information of virtualization infrastructure: machine's host name, machine type;

  • hardware (H/W) resource for virtualization infrastructure: total memory space, the number of CPUs, total storage space, machine's IP address, media access control (MAC) address, the availability for performance enhancement, estimated power;

  • virtualization related resource: hypervisor information, the number of currently running virtual desktops, the supported maximum number of virtual desktops, supported OSs.

– monitors the information for each virtual desktop to gather by event processing;

  NOTE 3 – The monitoring information of virtual desktops is as follows:

  • basic information of a virtual desktop: virtual desktop ID, OS type, hypervisor type, current status;

  • H/W resource for virtual desktop: assigned memory space, the assigned number of CPUs, assigned storage space, virtual desktop's IP address, virtual desktop's MAC address, accessible port number, performance enhancement factor.

– monitors the run-time information of virtualization infrastructure and virtual desktop. This monitoring information is dynamically monitored at run-time and usually checked periodically;

  NOTE 4 – The run-time information includes CPU utilization, memory utilization, storage utilization, network utilization, etc.

– performs the controls by a DaaS user and an administrator.

  NOTE 5 – Following are the controls at both sides:

  • DaaS user's controls: virtual desktop state controls such as on, create, reset, pause, resume, and off:

    – on/off: turn on or turn off a virtual desktop;

    – create: make a new virtual desktop;

    – reset: reboot the OS of a virtual desktop;

    – pause/resume: pause the OS maintaining a connection and resume the OS from a pause status;

    – delete: elimination of a virtual desktop.

  • administrator's controls: virtual desktop state controls, resource modification (CPU change, memory change, storage change, adding/deleting USB, network selection etc.), virtual desktop migration.

7.3.2 User account and profile management

CSU's accounts are separated into two types as follows:

1) administrative account for an administrator who has the authority to control and manage a system;

2)   general user account combined with CSC types such as service level, the type of virtual desktop, the authority of resource utilization, and the virtual desktop persistence user or not. See [ITU-T Y.3503].

The user account and profile management function:

–   classifies each CSC type and clarifies the service catalogue since different DaaS users have their own accounts and profiles;

–   manages CSU's accounts and profiles to guarantee correct access to their resources;

–   maintains CSU's account information and provides it to the user access management function (see clause 7.2.3);

–   maintains types of profiles such as virtual desktop user profile and virtual desktop hardware profile in order to build and maintain DaaS user's individual virtual desktop environments;

NOTE 1 – Virtual desktop user profile consists of desktop preferences and the CSU's application settings, etc.

NOTE 2 – Virtual desktop hardware profile includes the specific hardware configuration information to be allocated to a DaaS user and the information for booting-up procedure, etc.

NOTE 3 – Since virtual desktop hardware profile depends on physical hardware in virtualization infrastructure, the physical hardware information from hypervisor or platform is collected and stored.

–   generates profiles from CSU's account information or the pre-configured virtual desktop environment (such as virtual desktop user profile or template). These generated profiles are bound to CSU's accounts and are reflected in a corresponding virtual desktop;

–   saves profiles whenever they are changed;

NOTE 4 – For a particular CSC type (such as non-persistence), this function does not save the profile. In this case, this function provides new profiles whenever a DaaS user connects a virtual desktop.

–   prepares and provides new virtual desktop user profiles and hardware profiles by comparing physical hardware information with the pre-configured environment.

7.3.3   Virtual desktop resource allocation and distribution

The virtual desktop resource allocation and distribution function is manually accessed by an administrator or dynamically operated by the operational policy management function (see clause 7.3.4). The virtual desktop resource allocation and distribution function:

–   receives the resource usage from the monitoring and controlling virtual desktop resource function (see clause 7.3.1) and provides an administrator or a resource scheduler with the analysis of resource usage statically or dynamically;

NOTE – This analysis includes the resource usage state, resource usage pattern, and modification history, etc. A resource scheduler requests the resource distribution to virtualization infrastructure based on the analysis of resource usage.

–   determines resources to be allocated to or released from a virtual desktop, respectively, through the interface of the resource assignment function (see clause 7.1.2);

–   provides the interfaces to allocate and distribute the resources for the pre-configured virtual desktop environment when a virtual desktop is created or changed;

–   applies the operational policy dynamically or manually from the operational policy management function (see clause 7.3.4);

–   allocates and distributes resources dynamically to a virtual desktop according to the operational policy (such as setting the threshold of resource usage) when its resources are insufficient or overloaded;

–   modifies or reallocates resources to satisfy the performance of a virtual desktop from a DaaS user's request.

7.3.4 Operational policy management for DaaS

The operational policy management for DaaS function:

– establishes DaaS user's group policies according to CSC types and user accounts;

  NOTE 1 – These polices are reflected in the individual user account related with a virtual desktop user profile and a pre-configured environment.

– establishes a group policy to apply to the virtualization infrastructure or virtual desktops which use the same operational policy;

  NOTE 2 – If a DaaS user utilizes similar applications, tasks and usage patterns, they are grouped and assigned to the same virtualization infrastructure with sharing resources.

  NOTE 3 – A DaaS user's usage pattern is the information about a DaaS user's average usage of resources (e.g., CPU, memory, network and disk) from the monitoring information for a certain period. The virtualization infrastructure with DaaS user's similar tasks and usage patterns can improve performance by the caching process to provide a virtual desktop when the virtual desktop performs the similar tasks running on it.

– establishes a policy of the limitation or the arbitration for resource usage to prohibit the performance degradation from the assignment of excessive resources;

  NOTE 4 – In order to satisfy different DaaS user's requirements, different operational policies are reflected in each resource (such as an application policy, a network plolicy, other resource policies).

– requests the reallocation of insufficient resources, when some resources are needed more for some CSC types;

  NOTE 5 – During this process, this function detects which resources are dominantly used from a DaaS user's usage pattern according to a DaaS user's tasks.

– provides a policy to assign the DaaS platforms on which a virtual desktop is running;

  NOTE 6 – This function considers the physical distance on the network from a DaaS user to a DaaS platform and sets the policy on the shortest path. Otherwise, this function considers power consumption or utilization of the platform according to the weighted resource usage or the number of virtual desktops operated in one platform and sets the policy on the lowest utilization rate or the fewest number of virtual desktops. Also, if DaaS users perform similar tasks and requests specific virtual desktop by CSC type, this function considers the allocation of the pre-classified groups.

– gathers information on the platform power consumption or utilization according to the weighted resource usage from the power management function (see clause 7.3.6);

  NOTE 7 – The weighted resource usage mean which resources are heavily used as usual; the platform power consumption is estimated by the sum of these usages.

– performs the scheduling from the policies about a DaaS user's usage pattern and power consumption in virtualization infrastructure;

– sends a policy to the allocation function (see clause 7.2.4) to select the virtualization infrastructure to operate a virtual desktop;

– establishes a backup policy which covers types and frequency of backing up the virtual desktop enviorment to prepare for a system disaster;

– provides user interfaces for established policies which are established and applied dynamically or manually by the administrator.

7.3.5 High availability for DaaS

For high availability, DaaS adopts platform clustering which includes connection manger and virtualization infrastructure to maintain the seamless DaaS user's connection in a failure occurrence situation. The high availability for DaaS function:

– detects a system failure by confirming states among DaaS platforms;

–　　ensures DaaS users have a stable running environment in terms of delivery and operation of virtual desktops;

–　　sets up the redundancy for the client connection management function (see clause 7.2.2) to perform failover with minimum downtime and connection continuity;

NOTE 1 – The redundancy for the client connection management function (see clause 7.2.2) includes the duplication by active-active form or active-standby form. In order not to lose the DaaS user's connection, CSU's account and access information (such as DB, license or active directory) are duplicated or mirrored.

–　　configures the failover to redundancy for virtualization infrastructure;

NOTE 2 – The redundancy for virtualization infrastructure (such as the redundant server on active state for virtual desktop environments) is configured to perform failover for minimizing downtime. It helps to allocate a virtual desktop by load balancing or migrating a virtual desktop to the activated server to a DaaS client when the failure occurs on the server to which the virtual desktop is allocated, by providing a service without the loss of the user environment.

–　　saves the user's environment during a certain time and backs up and restores it on a local disk or on shared storage, thus preventing the loss of the user environment.

7.3.6　Power management of virtual desktop resource

The power management of virtual desktop resources function manages the power consumption of a DaaS platform with virtual desktop resources. This function:

–　　monitors the power consumption and the related performance factors of a virtual desktop and each resource in a DaaS platform;

–　　calculates the variation of power consumption and performance of a virtual desktop or a DaaS platform by collecting monitoring information;

–　　supports other functions for the provisioning and allocation of virtual desktop function (see clause 7.2.4) or the operational policy management for DaaS function (see clause 7.3.4).

7.4　Client support

Client support function:

–　　establishes a connection for a virtual desktop on the client side (see clause 7.4.1 service connection function);

–　　supports the optimized user interaction on a DaaS client (see clause 7.4.2 connection negotiation function);

–　　handles peripherals on a DaaS client (see clause 7.4.3 client peripheral connection function);

–　　guarantees that the virtual desktop service remains turned on (see clause 7.4.4 service continuity for user environment).

7.4.1　Service connection

The service connection function supports a DaaS client to establish a connection for virtual desktop service. This function:

–　　transmits CSU's access information to the user access management function (see clause 7.2.3) to verify a DaaS user;

–　　exchanges virtual desktop access information with the client connection management function (see clause 7.2.2) after user authentication;

–　　supports various types of DaaS clients such as personal computer, laptop computer, tablet computer, and thin client to access a virtual desktop;

–　　periodically sends the connection state of the DaaS client to the client connection management function (see clause 7.2.2) to monitor the client state for the preservation of the

client connection. In case of a temporarily unavailable connection, the DaaS client notifies the connection state to a DaaS user;

– transmits the DaaS user's requests (i.e., additional resource, resources cancelling, and additional virtual desktop service) to the client connection management function (see clause 7.2.2);

– maintains a standard security connection to protect the content exchanged between a DaaS client and a DaaS platform.

7.4.2 Connection negotiation

The connection negotiation function considers two main factors for DaaS: network performance (e.g., network bandwidth or traffic information) between a DaaS client and a DaaS platform; and the client state of a DaaS client. Based on these two main factors, it supports the optimized user interaction on the DaaS client.

The connection negotiation function:

– gathers network performance information and the client state, and transmits them to a DaaS platform through a network;

NOTE 1 – The client state consists of static and dynamic information of a DaaS client such as specification of display, usage and specification of hardware resources (i.e., CPU, GPU, and memory), and user interaction methods supported on a DaaS client.

NOTE 2 – The static information is collected at the initial connection between a DaaS client and a DaaS platform after user verification. The dynamic information is collected periodically when the client is connected to the DaaS platform to use a virtual desktop service.

– allows a DaaS client to display with best-efforts resolution for client without delay;

– receives the negotiation results from a DaaS platform after the completion of a negotiation;

– reflects the negotiation results in a DaaS client.

7.4.3 Client peripheral connection

The client peripheral connection function:

– recognizes peripherals on a DaaS client when they are connected to the DaaS client;

– sends a connection request event to a DaaS platform according to the type of DaaS client;

NOTE 1 – When this function requests the connection of the peripheral, the DaaS platform executes a device driver on a virtual desktop to operate the client peripheral remotely on a DaaS client.

– transmits the control events (such as attachment and detachment) and data for the client peripherals to a DaaS platform through a delivery protocol;

– disconnects the peripheral on a DaaS client safely.

NOTE 2 – When a DaaS user want to disconnect a peripheral on the assigned virtual desktop, this function disconnects the peripheral on the virtual desktop through the removal control event of the peripheral on the DaaS platform.

7.4.4 Service continuity for user environment

The service continuity for user environment function provides a DaaS client with a reconnection to provide for the continuity of service against the network failure or any faults of a DaaS platform. This function:

– requests a reconnection to the client connection management function (see clause 7.2.2) in case of a connection failure in order to maintain continuous virtual desktop service;

– reconnects a virtual desktop running on a DaaS client with an available DaaS platform;

– saves the DaaS user states of the virtual desktop on the DaaS client;

NOTE – The DaaS user state includes data, working environments for a DaaS user, etc.

–   synchronizes the saved user states of the virtual desktop on the DaaS client with user states of the virtual desktop on the DaaS platform when the DaaS client is reconnected to the DaaS platform.

7.5   Relationships among DaaS functions

Figure 7.1 depicts the summary of the relationships among the DaaS functions described in clause 7.1 through 7.4. Each link between two functions has related information.
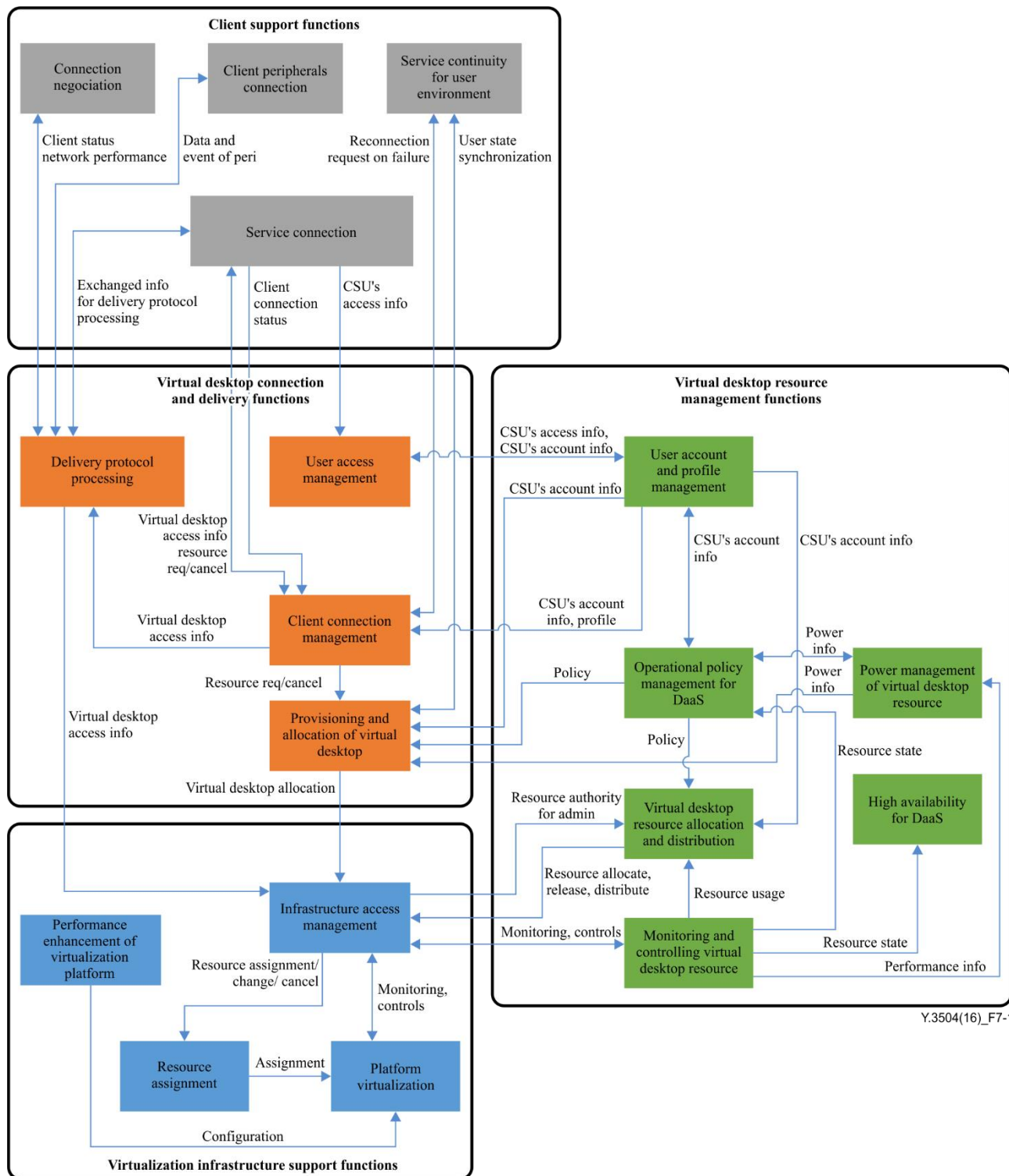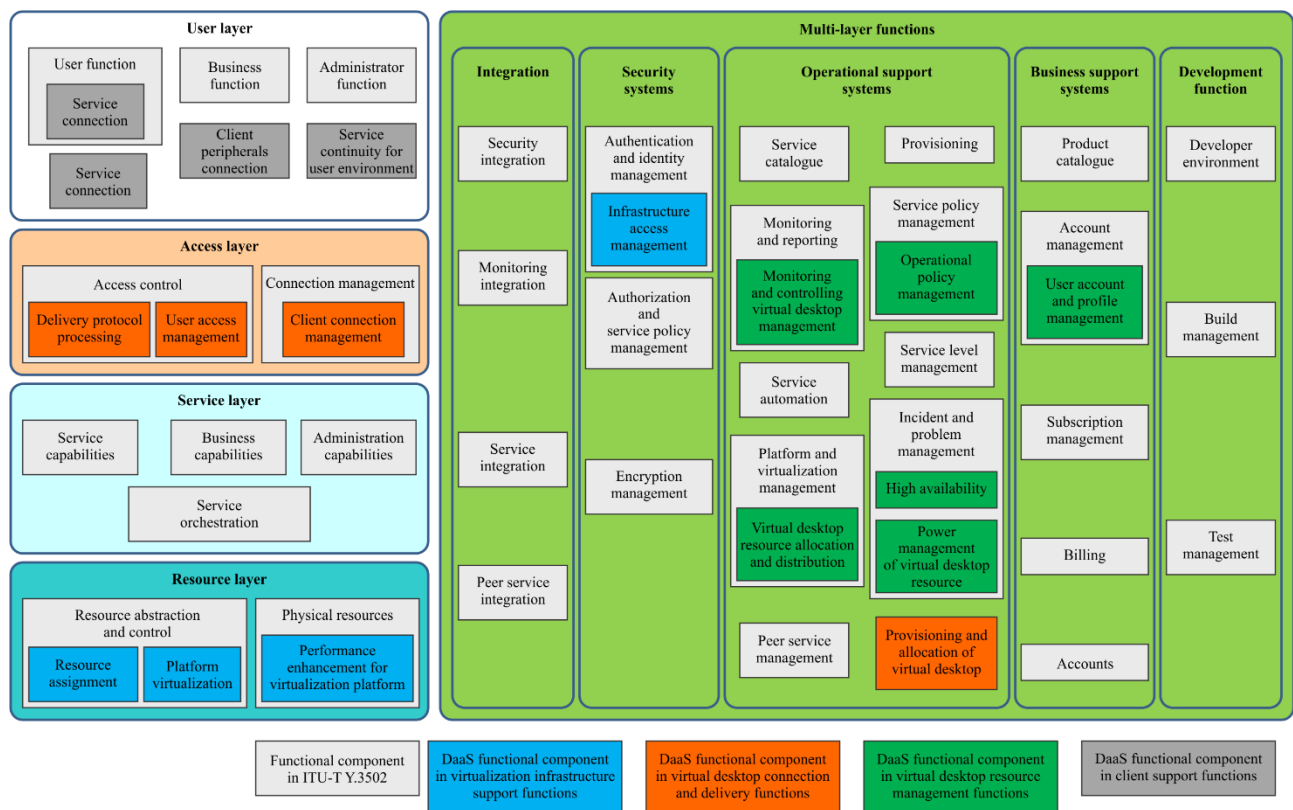

Figure 7-1 – Relationships among DaaS functions

8 Relationships between DaaS functions and functional components of cloud computing reference architecture

Figure 8-1 shows the mapping between the DaaS functions in clause 7 and the functional components in [ITU-T Y.3502].

Figure 8-1 – Mapping between DaaS functions and functional components of cloud computing reference architecture

Among the 18 DaaS functions identified in clause 7, 14 of these can be mapped to functional components in [ITU-T Y.3502]. These mappings, in terms of the layering framework, are as follows:

- User layer:
  - user function: service connection function (see clause 7.4.1)
- Access layer:
  - access control functional component: delivery protocol processing function (see clause 7.2.1), user access management function (see clause 7.2.3)
  - connection management functional component: client connection management function (see clause 7.2.2)
- Resource layer:
  - resource abstraction and control functional component: resource assignment function (see clause 7.1.2), platform virtualization function (see clause 7.1.1)
  - physical resources functional component: performance enhancement for virtualization platform function (see clause 7.1.3)
- Multi-layer functions:
  - security systems functional component-authentication and identity management: infrastructure access management function (see clause 7.1.4)

- operational support systems functional component-monitoring and reporting: monitoring and controlling virtual desktop resource function (see clause 7.3.1)
- operational support systems functional component-service policy management: operational policy management for DaaS function (see clause 7.3.4)
- operational support systems functional component-platform and virtualisation management: virtual desktop resource allocation and distribution function (see clause 7.3.3)
- operational support systems functional component-incident and problem management: high availability for DaaS function (see clause 7.3.5), power management of virtual desktop resource function (see clause 7.3.6)
- business support systems functional component-account management: user account and profile management function (see clause 7.3.2)

There are four DaaS functions that are not mapped to any functional components in [ITU-T Y.3502]; they can be located in the layering framework as follows:

– User layer:
  - connection negotiation function (see clause 7.4.2), client peripheral connection function (see clause 7.4.3), service continuity for user environment function (see clause 7.4.4)

– Multi-layer functions:
  - operational support systems functional compoenent: provisioning and allocation of virtual desktop function (see clause 7.2.4)

The detailed mapping is in Appendix II.

Since there are no reference points among functional components in [ITU-T Y.3502], it is necessary to adopt the grouping of DaaS functions in order to specify their reference points for convenience. Clause 9 explains the reference points based on four groups of DaaS functions as in Figure 7-1, i.e., client support functions, virtual desktop connection and delivery functions, virtual desktop resource management functions, and virtualization infrastructure functions.

9 DaaS functional architecture

9.1 Client support functions

The client support functions (CS-FS) have four functions including: connection negotiation function (CN-F), client peripheral connection function (CPC-F), service connection function (SC-F), and service continuity for user environment function (SCUE-F) as shown in Figure 9-1. The CS-FS interfaces with only the virtual desktop connection and delivery functions (VDCD-FS).
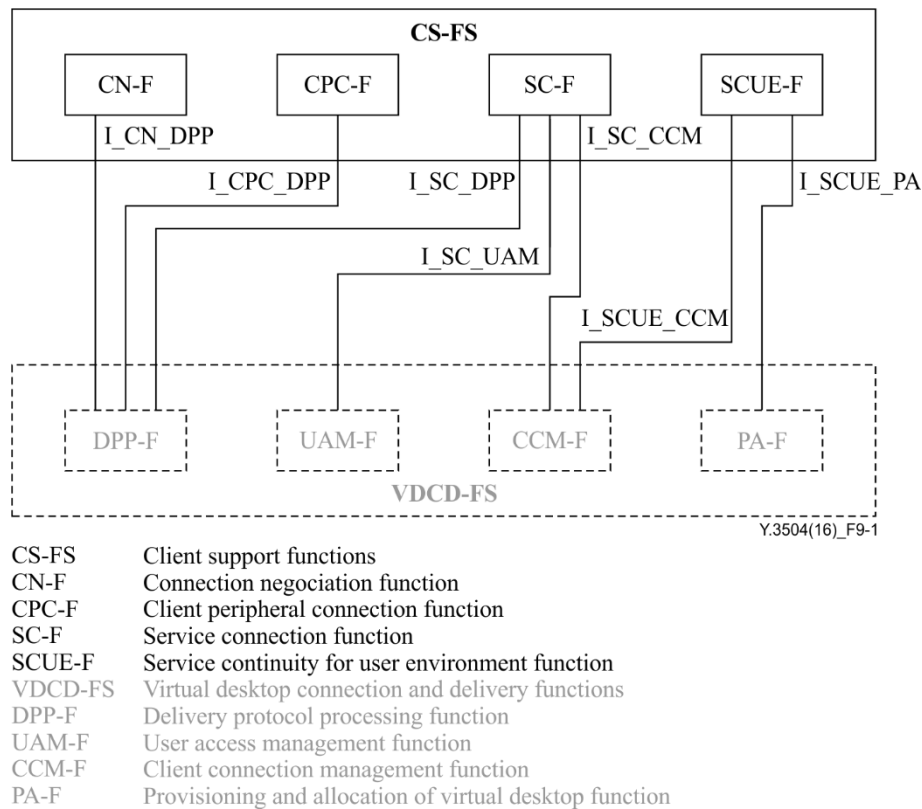
CS-FS — Client support functions
CN-F — Connection negociation function
CPC-F — Client peripheral connection function
SC-F — Service connection function
SCUE-F — Service continuity for user environment function
VDCD-FS — Virtual desktop connection and delivery functions
DPP-F — Delivery protocol processing function
UAM-F — User access management function
CCM-F — Client connection management function
PA-F — Provisioning and allocation of virtual desktop function

Figure 9-1 – Functions and reference points in CS-FS

9.1.1 Service connection function

The SC-F connects a virtual desktop in the CS-FS while the user access management function (UAM-F) and client connection management function (CCM-F) are the counterparts to the same operations in the VDCD-FS. The SC-F sends CSU's access information to the UAM-F through I_SC_UAM to perform user authentication. The SC-F exchanges the virtual desktop access information with the CCM-F through I_SC_CCM to connect a virtual desktop. In addition, the SC-F delivers the DaaS client's connection state and additional resource request/cancellation to the delivery protocol processing function (DPP-F) though I_SC_DPP. Detailed functional description for the SC-F is specified in clause 7.4.1.

9.1.2 Connection negotiation function

The CN-F provides the CS-FS with the user interaction by using negotiation results. The CN-F gathers network performance information and the DaaS client state, and delivers them to the VDCD-FS through I_CN_DPP. Consequently, the CN-F also receives the negotiation result from the DPP-F in the VDCD-FS thorough I_CN_DPP. Detailed functional description for the CN-F is specified in clause 7.4.2.

9.1.3 Client peripheral connection function

The CPC-F handles DaaS client's peripherals on a DaaS client. When the CPC-F recognizes the peripherals, all sorts of peripheral events (e.g., a connection and control events) are sent to the VDCD-FS though I_CPC_DPP. A detailed functional description for the CPC-F is specified in clause 7.4.3.
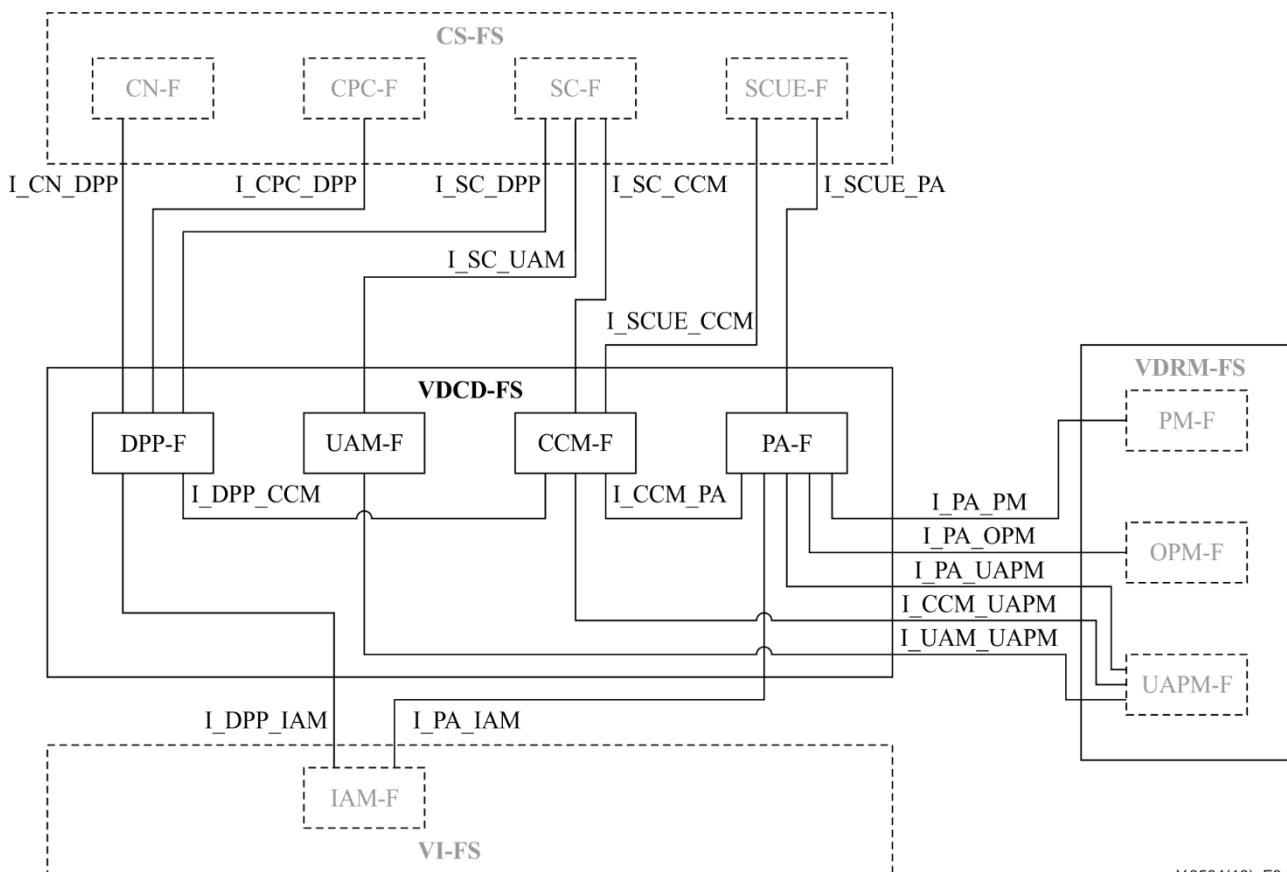
9.1.4 Service continuity for user environment function

The SCUE-F maintains the same user environment even on abnormal network state. When the network is disconnected, the SCUE-F requests the reconnection to the CCM-F through I_SCUE_CCM. And, the SCUE-F synchronizes the DaaS user's states between the CS-FS and the

provisioning and allocation of virtual desktop function (PA-F) through I_SCUE_PA. A detailed functional description for the SCUE-F is specified in clause 7.4.4.

9.2 Virtual desktop connection and delivery functions

The VDCD-FS comprise DPP-F, UAM-F, CCM-F, and PA-F as shown in Figure 9-2. The VDCD-FS have three interfaces with other functional groups such as CS-FS, virtual desktop resource management functions (VDRM-FS), and virtualization infrastructure functions (VI-FS).

VDCD-FS	Virtual desktop connection and delivery functions	VDRM-FS	Virtual desktop resource management functions
DPP-F	Delivery protocol processing function	PM-F	Power management of virtual desktop resource function
UAM-F	User access management function	OPM-F	Operational policy management for DaaS function
CCM-F	Client connection management function	UAPM-F	User account and profile management function
PA-F	Provisioning and allocation of virtual desktop function	VI-SF	Virtualization infrastructure functions
CS-FS	Client support functions	IAM-F	Infrastructure access management function
CN-F	Connection negociation function		
CPC-F	Client peripheral connection function		
SC-F	Service connection function		
SCUE-F	Service continuity for user environment function		

Figure 9-2 – Functions and reference points in VDCD-FS

9.2.1 Delivery protocol processing function

The DPP-F delivers the exchanged information to the SC-F through I_SC_DPP. The DPP-F communicates to the CN-F and the CPC-F to perform the connection negotiation and peripheral event through I_CN_DP and ICP_DP, respectively. Virtual desktop access information from the CCM_F on I_DP_CCM is forwarded to VI-FS through I_DPP_IAM. A detailed functional description for the DPP-F is specified in clause 7.2.1.

9.2.2 User access management function

For user authentication, the UAM-F validates a DaaS user with CSU's access information through I_SC_UAM and connects the user account and profile management function (UAPM-F) through

I_UAM_UAPM with CSU's access information and CSU's account information. A detailed functional description for the UAM-F is specified in clause 7.2.3.
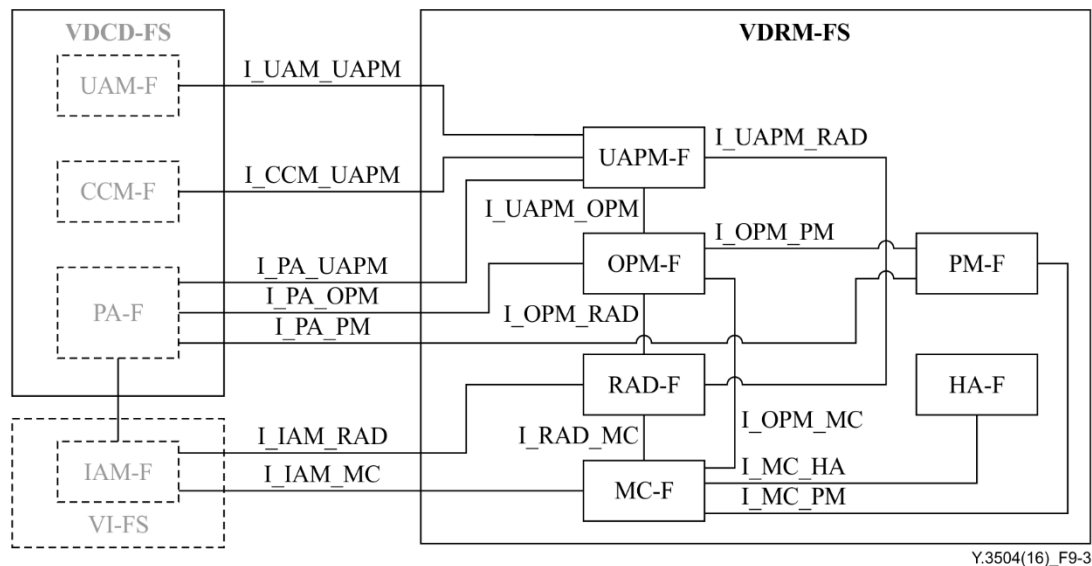
9.2.3 Client connection management function

The CCM-F delivers and verifies virtual desktop access information to CS-FS through I_SC_CCM. Virtual desktop access information from the SC-F is transferred to the DPP-F through I_DP_CCM. The CCM-F also uses I_CCM_UAPM to refer to CSC types and profiles from the UAPM-F. A resource request/cancellation is delivered by I_SC_CCM and transferred to PA-F thorough I_CCM_PA. Additionally, the CCM-F receives the client connection state from the SC-F through I_SC_CCM to monitor virtual desktop connection and reconnection requests from the SCUE-F through I_SCUE_CCM against network failure. A detailed functional description for the CCM-F is specified in clause 7.2.2.

9.2.4 Provisioning and allocation of virtual desktop function

In order to configure the pre-configured virtual desktop environment or create new virtual desktops, the PA-F uses I_PA_PM, I_PA_OPM, and I_PA_UAPM to get power performance information, policies, and CSU's account information, respectively. After configuration of a virtual desktop, the PA-F allocates the virtual desktop using VI-FS through I_PA_IAM. The PA-F also synchronizes the DaaS user's state with the SCUE-F through I_SCUE_PA. Detailed functional description for the PA-F is specified in clause 7.2.4.

9.3 Virtual desktop resource management functions

The VDRM-FS are composed of monitoring and controlling virtual desktop resource function (MC-F), UAPM-F, virtual desktop resource allocation and distribution function (RAD-F) and operational policy management for DaaS function (OPM-F). VDRM-FS also includes high availability for DaaS function (HA-F) and power management of virtual desktop resource function (PM-F) for more effective management. Figure 9-3 shows VDRM-FS with two interconnections of VDCD-FS and VI-FS.

Y.3504(16)_F9-3

VDCD-FS	Virtual desktop connection and delivery functions	VDRM-FS	Virtual desktop resource management functions
UAM-F	User access management function	UAPM-F	User account and profile management function
CCM-F	Client connection management function	OPM-F	Operational policy management for DaaS function
PA-F	Provisioning and allocation of virtual desktop function	RAD-F	Virtual desktop resource allocation and distribution function
VI-FS	Virtualization infrastructure functions	MC-F	Monitoring and controlling virtual desktop resource function
IAM-F	Infrastructure access management function	PM-F	Power management of virtual desktop resource function
		HA-F	High availability for DaaS function

Figure 9-3 – Functions and reference points in VDRM-FS

9.3.1   Monitoring and controlling virtual desktop resource

The MC-F has the connection with virtualization infrastructure through I_IAM_MC to receive monitoring information or send the control commands from or to the infrastructure access management function (IAM-F). The MC-F is connected with the HA-F through I_MC_HA and with the OPM-F through I_OPM_PM for the resource state. The MC-F also sends monitoring information of resources and resource usages to the PM-F and RAD-F with I_MC_PM and I_OPM_MC, respectively. Detailed functional description for the MC-F is specified in clause 7.3.1.

9.3.2   User account and profile management

The UAPM-F creates CSU's account with CSU's access information through I_UAM_UAPM. The UAPM-F has two more reference points I_CCM_UAPM and I_PA_UAPM for authentication with CSU's account information and for the pre-configured environments and profiles, respectively. When RAD-F allocates and distributes resources, the UAPM-F provides CSU's account information on I_UAPM_RAD or I_UAPM_OPM. Detailed functional description for the UAPM-F is specified in clause 7.3.2.

9.3.3   Virtual desktop resource allocation and distribution

The RAD-F has a reference point of MC-F through I_RAD_MC with monitoring information to analyse resource usage. I_IAM_RAD enables the RAD_F to approach IAM-F and resource assignment function (RA-F) for resource assignment. A detailed functional description for the RAD-F is specified in clause 7.3.3.

9.3.4   Operational policy management for DaaS

The OPM-F has two reference points I_OPM_PM and I_OPM_MC to receive the performance or resource usage which is used to establish the policies. These policies are applied to PA-F with I_PA_OPM. A detailed functional description for the OPM-F is specified in clause 7.3.4.

### 9.3.5   High availability for DaaS

The HA-F has only the reference point with the MC-F through I_MC_HA in order to monitor the resource state for establishing the related policies. A detailed functional description for the HA-F is specified in clause 7.3.5.

9.3.6   Power management of virtual desktop resource

The PM-F collects performance information from the MC-F through I_MC_PM and transfers the power related information to the PA-F through I_PA_PM for efficient provisioning. A detailed functional description for the PM-F is specified in clause 7.3.6.

9.4   Virtualization infrastructure functions

The VI-FS has four functions including performance enhancement for virtualization platform function (PE-F), IAM-F, RA-F, and platform virtualization function (PV-F) as shown in Figure 9-4. The VI-FS provide the interfaces with the other two function groups, VDCD-FS and VDRM-FS.
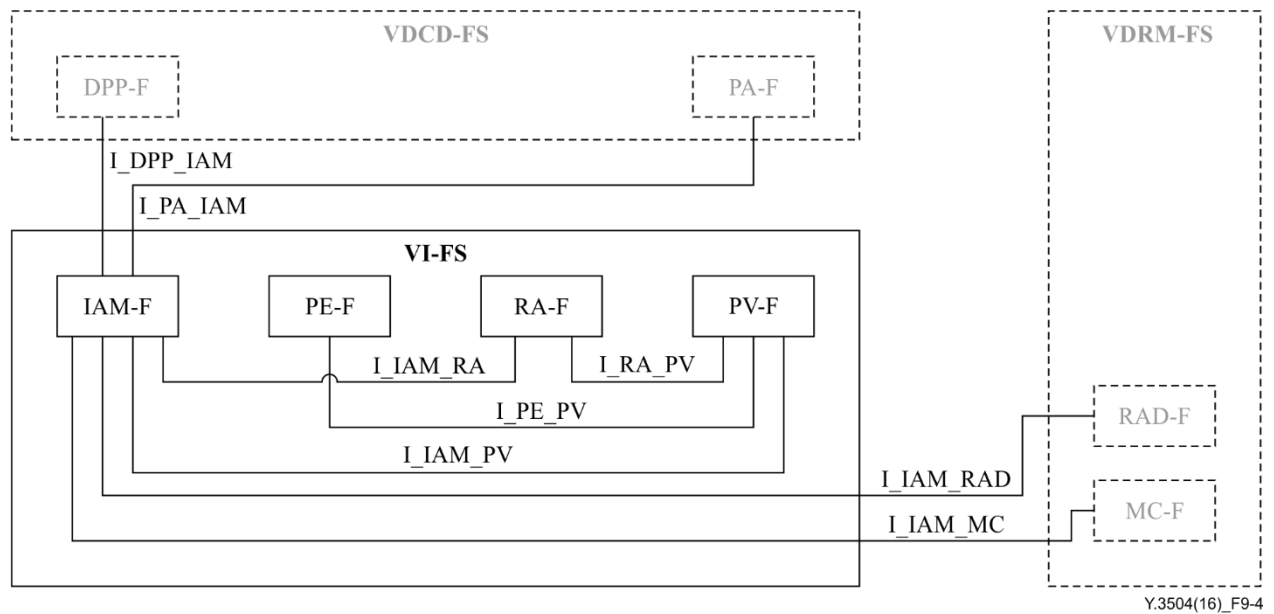
VI-FS   Virtualization infrastructure functions
IAM-F   Infrastructure access management function
PE-F   Performance enhancement for virtualization platform function
RA-F   Resource assignment function
PV-F   Platform virtualization function
VDCD-FS   Virtual desktop connection and delivery functions
DPP-F   Delivery protocol processing function
PA-F   Provioning and allocation of virtual desktop function

VDRM-FS   Virtual desktop resource management functions
RAD-F   Virtual desktop resource allocation and distribution function
MC-F   Monitoring and controlling virtual desktop resource function

Figure 9-4 – Functions and reference points in VI-FS

9.4.1 Infrastructure access management function

The IAM-F approves virtual desktop resource allocation through I_PA_IAM and the virtual desktop access through I_DPP_IAM. The IAM-F authorizes resource access from the administrator in order for the RAD-F to allocate, release, change and distribute resources through the I_IAM_RAD. The IAM-F also sends the request for resource assignment, change and cancellation from the RAD-F to the RA-F through I_ IAM _RA. Finally, the IAM-F delivers monitoring information and controls through the I_IAM_MC. A detailed functional description for the IAM-F is specified in clause 7.1.4.

9.4.2 Performance enhancement for virtualization platform function

The PE-F enhances the performance of virtualization platform and virtual desktop. The PE-F configures virtualization platform or infrastructure with the PV-F through the I_PE_PV. A detailed functional description for the PE-F is specified in clause 7.1.3.

9.4.3 Resource assignment function

The RA-F receives the resource assignment which is sent through the IAM-F during the creation of a virtual desktop. The RA-F assigns the resources to the virtual desktop on the PV-F through I_RA_PV according to the request from the IAM-F. According to the resource change from the IAM-F, the RA-F re-assigns the resources to the PV-F through the I_RA_PV. A detailed functional description for the RA-F is specified in clause 7.1.2.

9.4.4 Platform virtualization function

The PV-F configures the DaaS platform according to the PE-F. The PV-F transmits the monitoring information and receives controls through I_IAM_PV. A detailed functional description for the PV-F is specified in clause 7.1.1.

9.5 Reference points

9.5.1 Reference points between CS-FS and VDCD-FS

The reference points between CE-FS and VDCD-FS are summarized as follows:

I_CN_DPP   reference point between CN-F and DPP-F. The CN-F interacts with the DPP-F to handle connection negotiation through this reference point.

I_CPC_DPP   reference point between CPC-F and DPP-F. The CPC-F interfaces with the DPP-F to exchange the peripheral events through this reference point.

I_SC_DPP   reference point between SC-F and DPP-F. The SC-F requests or cancels additional resources through this reference point.

I_SC_UAM   reference point between SC-F and UAM-F. The SC-F inputs the user authentication information to the UAM-F through this reference point.

I_SC_CCM   reference point between SC-F and CCM-F. The SC-F and the CCM-F interact with each other to exchange virtual desktop access information through this reference point.

I_SCUE_CCM   reference point between SCUE-F and CCM-F. The SCUE-F requests a reconnection to the CCM-F in case of network failure, through this reference point.

I_SCUE_PA   reference point between SCUE-F and PA-F. The SCUE-F and PA-F perform the synchronization of a DaaS user's state through this reference point.

9.5.2 Reference points between VDCD-FS and VDRM-FS

I_UAM_UAPM   reference point between UAM-F and UAPM-F. CSU's access information, CSU's account information, and CSC types are transferred through this reference point.

I_CCM_UAPM   reference point between CCM-F and UAPM-F. CSC types and profiles are delivered from the UAPM-F to the CCM-F through this reference point.

I_PA_UAPM   reference point between PA-F and UAPM-F. CSU's account information is delivered from the UAPM-F to the PA-F through this reference point.

I_PA_OPM   reference point between PA-F and OPM-F. Operational policy information is delivered from the OPM-F to the PA-F through this reference point.

I_PA_PM   reference point between PA-F and PM-F. Power information is delivered from the PM-F to the PA-F through this reference point.

9.5.3 Reference points between VDCD-FS and VI-FS

I_DPP_IAM   reference point between DPP-F and IAM-F. Resource request/cancellation and virtual desktop access information are forwarded to IAM-F through this reference point.

I_PA_IAM   reference point between PA-F and IAM-F. The PA-F delivers virtual desktop allocation information to IAM-F through this reference point.

9.5.4 Reference points between VDRM-FS and VI-FS

I_IAM_RAD   reference point between IAM-F and RAD-F. The RAD-F accesses IAM-F to communicate with the RA-F.

I_IAM_MC   reference point between IAM-F and MC-F. The MC-F accesses IAM-F to communicate with PV-F.

9.5.5 Reference points within VDCD-FS

I_DPP_CCM   reference point between DPP-F and CCM-F. Virtual desktop access information from CCM-F is delivered to DPP-F through this reference point.

I_CCM_PA   reference point between CCM-F and PA-F. The CCM-F bypasses resource request/cancellation to the PA-F through this reference point.

9.5.6 Reference points within VDRM-FS

I_UAPM_OPM   reference point between UAPM-F and OPM-F. CSU's account information is communicated through this reference point.

I_UAPM_RAD   reference point between UAPM-F and RAD-F. CSU'S account information is sent from UAPM-F to RAD-F though this reference point.

I_OPM_PM   reference point between OPM-F and PM-F. The PM-F delivers the power performance to OPM-F to establish a policy through this reference point.

I_OPM_RAD   reference point between OPM-F and RAD-F. Operational policy information is delivered from the OPM-F to the RAD-F through this reference point.

I_OPM_MC   reference point between OPM-F and MC-F. The MC-F sends resource states to the OPM-F through this reference point.

I_RAD_MC   reference point between RAD-F and MC-F. The MC-F sends resource usage to the RAD-F through this reference point.

I_MC_HA   reference point between MC-F and HA-F. The MC-F sends resource states to the HA-F through this reference point.

I_MC_PM   reference point between MC-F and PM-F. The MC-F sends monitoring information to the PM-F through this reference point.

9.5.7 Reference points within VI-FS

I_IAM_RA   reference point between IAM-F and RA-F. The resource allocation and distribution is forwarded to the RA-F through this reference point.

I_PE_PV   reference point between PE-F and PV-F. The configuration to enhance the performance of virtualization platform is sent to the PV-F through this reference point.

I_RA_PV   reference point between RA-F and PV-F. The resource assignment is sent to the PV-F through this reference point.

I_IAM_PV   reference point between IAM-F and PV-F. The monitoring information and controls are transmitted through this reference point.

10 Security considerations

Security aspects for consideration within DaaS are addressed by security challenges for CSPs and CSCs, as described in [ITU-T X.1601]. In particular, [ITU-T X.1601] analyses security threats and challenges, and describes security capabilities that could mitigate these threats and meet security challenges.

It is recommended that relevant security requirements of [b-ITU-T Y.2201], [b-ITU-T Y.2701] and applicable ITU-T X-series, ITU-T Y-series and ITU-T M-series of Recommendations be taken into consideration, including access control, authentication, data confidentiality, data retention policy, network security, data integrity, availability and privacy.

Appendix I

Relationship between DaaS logical components and cloud computing reference architecture

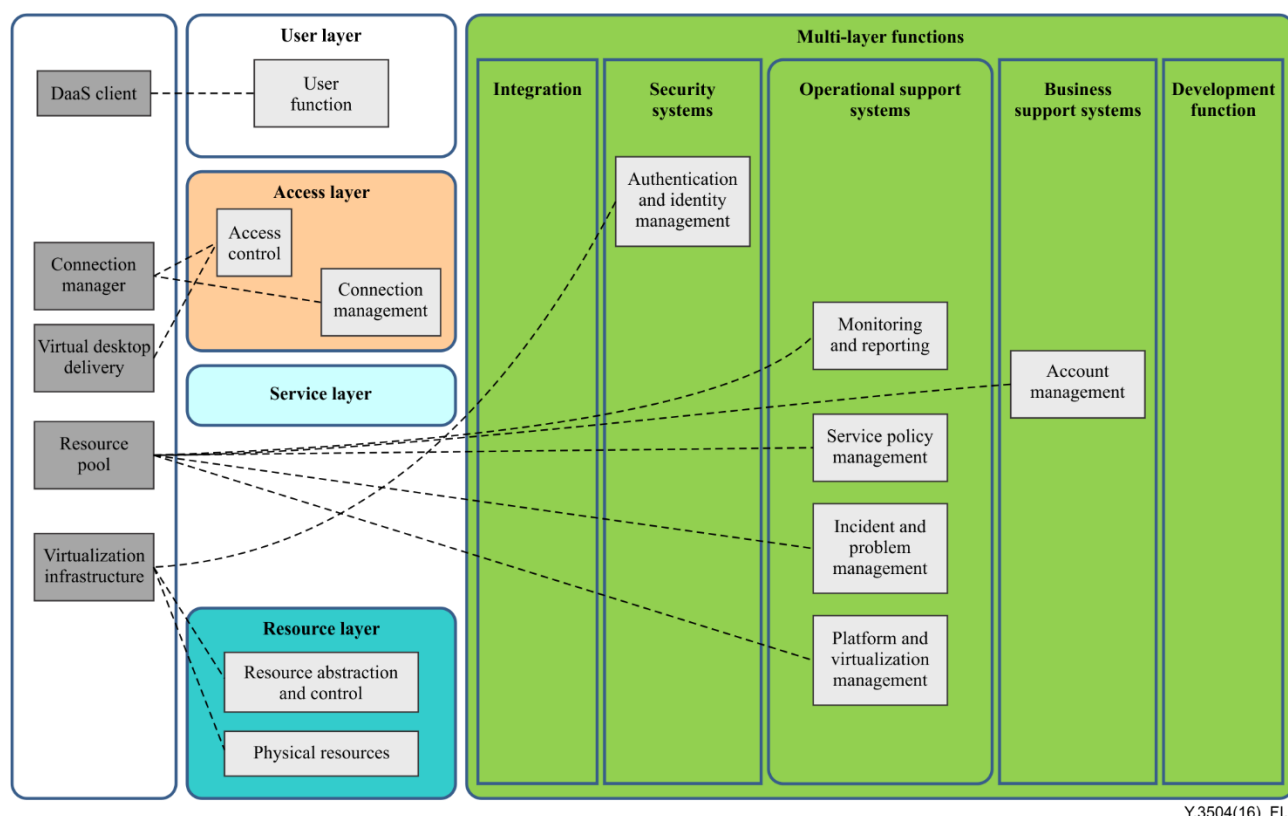*(This appendix does not form an integral part of this Recommendation.)*

This appendix provides the relationship between DaaS logical components [ITU-T Y.3503] and cloud computing reference architecture in [ITU-T Y.3502].

The relationship between DaaS logical components and cloud computing reference architecture can be done in two steps.

The first step is the mapping between DaaS logical components and DaaS functions in clause 6. Based on clause 6, each corresponding functions of DaaS for the DaaS logical components in [ITU-T Y.3503] is described in Table 6-1.

The second step is the mapping between DaaS functions and functional components of cloud computing reference architecture. This mapping is described in Figure 8-1.

Therefore, the possible mapping between DaaS logical components and functional components in cloud computing reference architecture is shown in Figure I.1.

Figure I.1 – Relationship between DaaS logical components and cloud computing reference architecture

Appendix II

Relationship between DaaS functions and functional components in cloud computing reference architecture

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

Table II.1 provides the relationship between DaaS functions in clause 7 and functional components of cloud computing reference architecture defined in [ITU-T Y.3502] by enumerating all the related functional components corresponding to DaaS functions. The term "related functional components" in this appendix means that the description of the functional component in [ITU-T Y.3502] is similar to that of the DaaS function but does not mean that the functional component in [ITU-T Y.3502] can replace or cover for the DaaS function.

Table II.1 – Relationship between Clause 7 DaaS functions and ITU-T Y.3502 reference architecture

DaaS functions	Keywords or simple descriptions	Related functional components (FCs) in [ITU-T Y.3502]	Notes
Platform virtualization	Virtualization	Resource layer-Resource abstraction and control	Resource abstraction and control FC includes software elements such as hypervisors, virtual machines, virtual data storage, and time-sharing. Platform and virtualization management FC provides the capabilities for virtualizing the use of those resources (e.g., by means of hypervisors).
Resource assignment	Resource assignment	Resource layer-Resource abstraction and control	Resource abstraction and control FC provides access to the physical computing resources through software abstraction.
Performance enhancement for virtualization platform	Performance enhancement	Resource layer-Physical resources	Physical resources include hardware resources, such as computers (CPU and memory), networks (routers, firewalls, switches, network links and network connectors, storage components (hard disks) and other physical computing infrastructure elements.
Delivery protocol processing	Delivery of virtual desktop	Access layer-Service access	Delivery of virtual desktop means access of service. Service object is a virtual desktop in DaaS.
Client connection management	Coordinating delivery protocol Connection monitoring, reconnections	Access layer-Connection management	Connection management FC provides enforcement of QoS policies regarding the traffic from and/or to the user layer. This is related with connection monitoring, reconnection on the DaaS side.
User access management	Validating a DaaS user Support secure access	Access layer-Access control	Validating a DaaS user and secure access are tightly associated with the access control FC and the authentication and identity management FC.

Table II.1 – Relationship between Clause 7 DaaS functions and ITU-T Y.3502 reference architecture

DaaS functions	Keywords or simple descriptions	Related functional components (FCs) in [ITU-T Y.3502]	Notes
Provisioning and allocation of virtual desktop	Preparing SW, HW resource Configure the pre-configured virtual desktop environment (OS, disk, profile image) Deploying DaaS platforms Selecting DaaS platform to assign virtual desktop	None	There is no FC specialized in virtual desktop matters as the provisioning function in [ITU-T Y.3502] is for service.
Infrastructure access management	Access I/F to infra (admin, DaaS user) Managing access authority	Security systems-Authorization and security policy management	This FC provides capabilities for the control and application of authorization for users to access specific capabilities or data. This FC is somewhat related with the infrastructure access management in that they cover authorization, but DaaS focuses on authority for resource access.
Monitoring and controlling virtual desktop resource	Monitoring infra and virtual desktop	Operational support systems-Monitoring and reporting	In the monitoring and reporting FC, the part of monitoring resources is similar to that on the DaaS side.
User account and profile management	Service catalogues CSU account info (CSC type name, id) Profile (HW configuration, SW)	Business support systems-Account management	Account management FC includes contracts, subscriptions, entitlements, and service pricing. This FC is partially related with UAPM-F in that it covers service catalogues, CSC type, and contracted HW/SW, but this does explain all of this function.
Virtual desktop resource allocation and distribution	Analysis of resource usage to admin Resource allocation, releasing Reallocating resources by a DaaS user request	Operational support systems-Platform and virtualization management	The resources are typically organized into resource pools with key characteristics: • standardized hardware componentry and configuration • readily expandable through the addition of new hardware capacity • automated shifting of resources as workload needs change • reduce and/or eliminate downtime through movement of workloads and data between resources • manage resource consumption based on goals
Operational policy	Group policy based on CSC types and user account	Operational support systems-	Policies can include business, technical, security, privacy and certification policies

**Table II.1 – Relationship between Clause 7 DaaS functions and
ITU-T Y.3502 reference architecture**

DaaS functions	Keywords or simple descriptions	Related functional components (FCs) in [ITU-T Y.3502]	Notes
management for DaaS	Resource reallocation policy DaaS platform allocation policy	Service policy management	that apply to cloud services and their usage by cloud service customers.
High availability for DaaS	Detecting failure Redundancy set up Backup and restore virtual desktop environment Load balance VM auto migration	Operational support systems-Incident and problem management	This FC is for capturing incident or problem reports and managing those reports through to resolution; the main role of the HA-F is to detect failure and manage it.
Power management of virtual desktop resource	Calculating power consumption	Operational support systems-Incident and problem management	Power management in DaaS is partly related with platform and virtualization management FC and incident and problem management in that the function can deal with workload matters and prepare the incident by exceptional power consumption.
Service connection	Supporting various type of DaaS clients DaaS client connection status info Additional resource request Security connection	User layer-User function	User function FC supports the service user to access and use cloud services. Service connection is responsible for the connection between a virtual desktop and a DaaS user on the client side, so this FC is related with the SC-F. However, this is not enough to cover specific operations of the function.
Connection negotiation	Gathering and delivering network performance info and client status info Receiving the negotiation result info	None	There is no specific FC to treat the connection negotiation on the client side.
Client peripheral connection	Peripheral connection Controlling event of peripheral	None	There is no specific FC to treat DaaS client's peripherals.
Service continuity for user environment	Reconnection Request on fault Off-line synchronization	None	There is no specific FC to treat DaaS client's connection on the client side.

Bibliography

[b-ITU-T Y.2201]   Recommendation ITU-T Y.2201 (2011), *Requirements and capabilities for ITU-T NGN*.

[b-ITU-T Y.2701]   Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

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

[b-DMTF OVF]   DMTF Standard DSP0243 Version 1.0.0 (2009), *Open virtualization format specification*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
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	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
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 and next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems