International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2902

(11/2008)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Next Generation Networks – Carrier grade open environment

Carrier grade open environment components

Recommendation ITU-T Y.2902

ITU-T

ITU International Telecommunication Union

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

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
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Future networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	**Y.2900–Y.2999**

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

Recommendation ITU-T Y.2902

Carrier grade open environment components

Summary

Recommendation ITU-T Y.2902 describes carrier grade open environment (CGOE) components, assigned to specific categories of the CGOE reference model, which may be used in commercial off-the-shelf components, suitable for implementation in next generation networks (NGNs). The characteristics of each individual CGOE component are presented in the following new annexes:

– Annex A: The Diameter client CGOE component.

– Annex B: The Diameter server CGOE component.

– Annex C: The FTP client CGOE component.

– Annex D: The FTP server CGOE component.

Source

This edition of Recommendation ITU-T Y.2902 includes the amendments approved on 29 June 2008 by ITU-T Study Group 13 (2005-2008) and the amendments approved on 13 November 2008 by ITU-T Study Group 13 (2009-2012) under Recommendation ITU-T A.8 procedures.

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/.

CONTENTS

Page

Recommendation ITU-T Y.2902

Carrier grade open environment components

1 Scope

This Recommendation provides a set of carrier grade open environment (CGOE) components, each of which can be related to a CGOE category identified in the CGOE model that is defined in [ITU-T Y.2901]. These CGOE components are intended for use by vendors to assist them in developing commercial off-the-shelf (COTS) components. It is recognized that CGOE components will continue to be identified on a going forward basis and annexes will be added to capture these additions. Additionally, to ensure that a consistent approach is used in the generation of future annexes, a framework for the specification of new CGOE components is provided.

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.2901] Recommendation ITU-T Y.2901 (2006), *The carrier grade open environment reference model*.
<http://www.itu.int/rec/T-REC-Y.2901>

[IETF RFC 854] IETF RFC 854 (1983), *Telnet Protocol Specification*.
<http://www.ietf.org/rfc/rfc854.txt>

[IETF RFC 855] IETF RFC 855 (1983), *Telnet Option Specifications*.
<http://www.ietf.org/rfc/rfc855.txt>

[IETF RFC 959] IETF RFC 959 (1985), *File Transfer Protocol (FTP)*.
<http://www.ietf.org/rfc/rfc959.txt>

[IETF RFC 2228] IETF RFC 2228 (1997), *FTP Security Extensions*.
<http://www.ietf.org/rfc/rfc2228.txt>

[IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.
<http://www.ietf.org/rfc/rfc2246.txt>

[IETF RFC 2401] IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*.
<http://www.ietf.org/rfc/rfc2401.txt>

[IETF RFC 2640] IETF RFC 2640 (1999), *Internationalization of the File Transfer Protocol*.
<http://www.ietf.org/rfc/rfc2640.txt>

[IETF RFC 2773] IETF RFC 2773 (2000), *Encryption using KEA and SKIPJACK*.
<http://www.ietf.org/rfc/rfc2773.txt>

[IETF RFC 3659] IETF RFC 3659 (2007), *Extensions to FTP*.
<http://www.ietf.org/rfc/rfc3659.txt>

[IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol*.
<http://www.ietf.org/rfc/rfc3588.txt>

[IETF RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol*. <http://www.ietf.org/rfc/rfc4301.txt>

[IETF RFC 4346] IETF RFC 4346 (2006), *The Transport Layer Security (TLS) Protocol Version 1.1*. <http://www.ietf.org/rfc/rfc4346.txt>

[IETF RFC 4960] IETF RFC 4960 (2007), *Stream Control Transmission Protocol*. <http://www.ietf.org/rfc/rfc4960.txt>

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 agent [b-ITU-T Q.1290]: An entity acting on behalf of another.

NOTE – In client server systems, an agent is the part of the system that performs information preparation and exchange on behalf of a client or server application

3.1.2 application [ITU-T Y.2901]: An application is a piece of software answering a set of user's requirements using telecommunication network services via an IT system.

3.1.3 carrier grade [ITU-T Y.2901]: Colloquially, a "carrier grade" implementation of a solution, building block, or a COTS component exhibits particular qualities beyond regular information technology (IT) reliability, availability, serviceability and manageability (RASM) features enabling its mission-critical use in a service provider's offering.

NOTE – COTS component can be called "carrier grade" with respect to a particular building block if it meets all of the necessary and sufficient non-fuctional requirements of a COTS category for such a building block.

3.1.4 CGOE category [ITU-T Y.2901]: A unit of description of the CGOE reference model. It comprises one or more CGOE components.

NOTE – This method of abstraction keeps the size of the framework manageable and understandable. It avoids being too specific or leaning towards the needs of a certain building block. For example, the alarm management category consists of several components, e.g., alarm generation and alarm clearance.

3.1.5 CGOE component [ITU-T Y.2901]: A CGOE component is an abstract description of technical tasks, interfaces and properties.

3.1.6 CGOE reference model [ITU-T Y.2901]: A model that organizes the CGOE categories.

NOTE 1 – Each category is intended to be independent in the sense that it does not require the existence of the categories above it; however, to produce carrier grade functionality, functions may be needed from more than one category.

NOTE 2 – Multiple categories are logically grouped and referred to as the server hardware and the operating platform.

3.1.7 COTS component [ITU-T Y.2901]: A hardware or a software component instantiation of one or more CGOE components.

NOTE 1 – Existing or new components may instantiate CGOE components.

NOTE 2 – The following are examples of components: database system, operating system and management middleware.

3.1.8 component instance [ITU-T Y.2901]: A component instance is a specific representation of a component, which satisfies the specific needs of building a specific building block.

NOTE – Technology providers develop component instances. During the engineering process within the solution providers, instances are chosen according to the requirements and integrated to eventually stage the entire building block. Examples of component instances: Linux, management middleware for Q3-access.

3.1.9 Diameter [ITU-T Y.2901]: An IETF protocol that may be used to provide an authentication, authorization and accounting (AAA) framework for applications.

3.1.10 framework [ITU-T Y.2901]: A framework is an environment that provides a partial solution, usually automating a particularly tedious or difficult part of an application project.

3.1.11 functional requirements [ITU-T Y.2901]: The set of interfaces, capabilities and features, developed with respect to a service architecture associated with a building block.

3.1.12 middleware [ITU-T Y.2901]: The mediating entity between two information elements. Such an element can be, for example, an application, infrastructure component or another mediating entity.

3.1.13 non-functional requirements [ITU-T Y.2901]: A list of features that a building block must provide in order to ensure certain behaviour within the service architecture.

NOTE – This list mostly represents requirements to allow for smooth operations and lifecycle management.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 Diameter agent: A Diameter agent is a Diameter component that provides either relay, proxy, redirect or translation services.

3.2.2 Diameter client: A Diameter client is a device at the edge of the network that performs access control.

3.2.3 Diameter peer: A Diameter peer is a Diameter component to which a given Diameter component has a direct transport connection.

3.2.4 Diameter server: A Diameter server handles authentication, authorization and accounting requests.

NOTE – A Diameter server shall support Diameter applications in addition to the base protocol.

3.2.5 non-functional property: A property that does not relate to the function performed by a device or component, e.g., scalability and availability.

3.2.6 proxy: A system authorized to work on behalf of another system including responding to protocol requests.

3.2.7 proxy agent: An agent that acts as a proxy.

NOTE – In addition to forwarding requests and responses, proxy agents may make policy decisions relating to resource usage and provisioning. This would typically be accomplished by tracking the state of network access server devices. While proxies typically do not respond to client requests prior to receiving a response from the server, they may originate reject messages in cases where policies are violated. As a result, proxies need to understand the semantics of the messages passing through them, and may not support all Diameter applications.

3.2.8 relay agent: An agent that performs a relay function.

NOTE – Relay agents forward requests and responses based on routing-related attribute value pairs (AVPs) and realm routing table entries. Relays do not make policy decisions and thus, they do not examine or alter non-routing AVPs. Consequently relay agents never originate messages, do not need to understand the semantics of messages or non-routing AVPs, and are expected to be capable of handling all Diameter application or message types. As relays make decisions based solely on information in routing AVPs and realm forwarding tables, they do not keep state on network access server resource usage or sessions in progress.

3.2.9 redirect agent: An agent that performs a redirect function.

NOTE – Rather than forwarding requests and responses between clients and servers, redirect agents refer clients to servers and allow them to communicate directly. Since redirect agents do not sit in the forwarding path after a redirect function has been invoked, they cannot alter any AVPs transiting between clients and servers. Redirect agents do not originate messages and are capable of handling any message type, although they may be configured only to redirect messages of certain types. Redirect agents do not keep state with respect to sessions or network access server resources.

3.2.10 translation agent: A translation agent is a stateful Diameter component that performs protocol translation between Diameter and another AAA protocol, such as RADIUS.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA Authentication, Authorization and Accounting

AVP Attribute Value Pair

CGOE Carrier Grade Open Environment

COTS Commercial Off-The-Shelf

FTP File Transfer Protocol

HTTP HyperText Transfer Protocol

IPSec IP Security

NASREQ Network Access Server Requirements

OAM&P Operations, Administration, Maintenance and Provisioning

RADIUS Remote Authentication Dial In User Service

RASM Reliability, Availability, Serviceability and Manageability

SCTP Stream Control Transmission Protocol

SIP Session Initiation Protocol

TACACS Terminal Access Controller Access Control System

TLS Transport Layer Security

UML Unified Modelling Language

5 Conventions

In this Recommendation:

– End-to-end security refers to the security between two Diameter nodes, possibly communicating through Diameter agents.

– Transport connection is used to refer to a TCP or SCTP connection existing directly between two Diameter peers.

5.1 Terms

This Recommendation uses a number of terms and it is important that the relationship between these terms is clearly understood. The CGOE reference model in [ITU-T Y.2901] defines CGOE categories. Each CGOE category will be comprised of one or more CGOE components defined in this Recommendation. Each COTS component will be comprised of one or more CGOE components. Usually a CGOE category is not equivalent to a COTS component.

5.2 CGOE component diagrams

This Recommendation uses the following CGOE component diagram conventions.

5.2.1 Unified modelling language

The unified modelling language (UML) as defined by the object management group (OMG) for CGOE component diagrams is used. UML is a visual modelling language using views, modelling elements and diagrams to model systems of various kinds.

– The UML version used is specification version 2.0.

– A very circumscribed set of modelling elements and diagrams are used. The intent is that complicated modelling tools are not a prerequisite for this application of UML.

– Other modelling elements and diagrams *may* be used as desired to show other aspects of components and their environment.

– Terms shown in ***bold italic*** type are used in the way they are used and defined in the UML specification.

5.2.2 Key modelling elements

– The ***component*** – This modelling element represents a CGOE component (the tabs on the side are intended to suggest a "pluggable" element). The component name is placed on the inside of the component. Components ***implement*** or export interfaces.

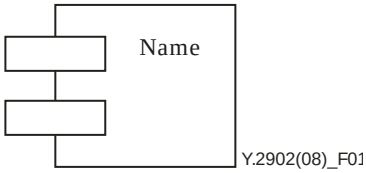

Figure 1 – Component

– The ***interface*** – An interface is a well-defined means of accessing a logical grouping of functional behaviour. Interfaces are *freestanding* objects that are not *necessarily* associated with *specific* components: multiple components can implement the same interface. Each interface is named and the name is placed near the interface. Interfaces that are exported by a component are referred to as primary interfaces. Interfaces that are imported by a component are referred to as secondary interfaces.

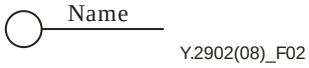

Figure 2 – Interface

– The ***dependency*** – A dependency element represents a relationship between two modelling elements. In the CGOE, this dependency relationship is (generally) unnamed and represents a "uses" relationship between components and interfaces.

Figure 3 – Dependency

– The ***category*** – The CGOE uses a ***stereotype*** of the UML ***package*** modelling element to represent the CGOE categories used in the CGOE model (which is indicated by the "<<Category>>" marking). The name of the category is placed inside the category modelling element. The tabbed shape of the package symbol is intended to suggest a file folder.

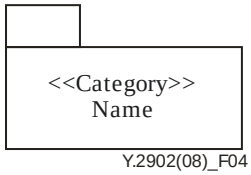

Figure 4 – Category

– The ***note*** – The note element is used to convey plain-text information of any kind that is not otherwise conveyed by the UML elements in the diagram.

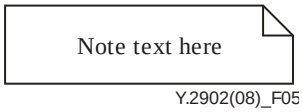

Figure 5 – Note

5.2.3 Use of modelling elements

- Modelling elements should only be used when they serve an explanatory purpose in the environment where they are used. For example, it is not necessary to use the category element unless its use somehow explains something in the context of the diagram.
- Over cluttered diagrams can confuse rather than educate. Consider breaking large diagrams into smaller pieces.
- Names can be left off elements when the meaning of the diagram is not harmed by doing so. For example, it is common practice to leave the name off "generic" components when showing how an arbitrary component fits into a scenario with specific ones.

5.2.4 Diagrams

The CGOE uses component diagrams to describe relationships between components and scenarios of component use. For example:

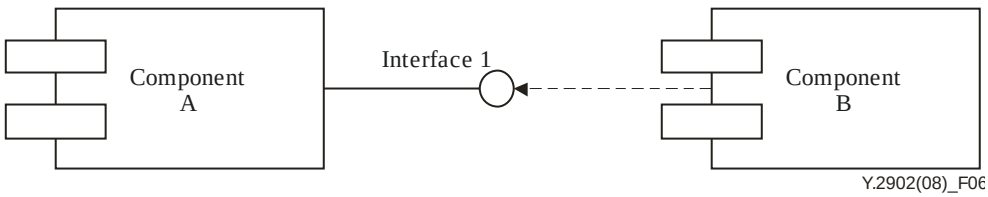

Figure 6 – Relationship (Example)

Figure 6 shows that component A implements (or exports) interface 1 and that component B uses (or imports) this interface.

– Components can implement multiple interfaces and use multiple interfaces.

– Different components can implement the same interface.

A more extensive figure that shows all the modelling elements described above is shown in Figure 7:

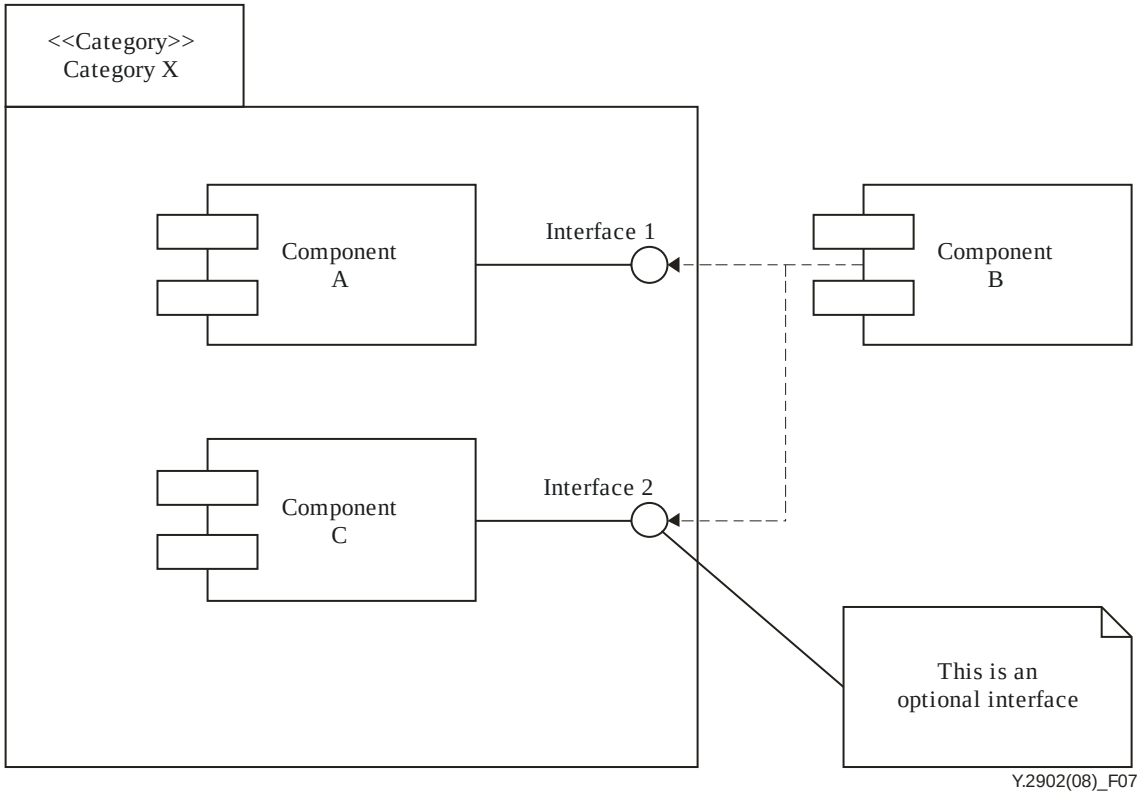

Figure 7 – Relationships (example)

Figure 7 shows that components A and C are part of CGOE category "X" and implement interfaces 1 and 2, respectively. Interface 2 is noted as being "optional" (this example is for didactic purposes only and no meaning is ascribed here to the term "optional"). Component B uses interfaces 1 and 2.

6 CGOE components

This Recommendation defines CGOE components which align with the categories of the CGOE reference model. Each CGOE component is defined by:

- A category which ties it to the CGOE reference model.
- Programmatic interfaces used and exported.

  (These interfaces typically reference existing standards or, should it be impossible to identify an interface standard because none exists, they identify gaps in the set of relevant existing standards.)
- Internal functional properties which describe what a component *does* beyond that which the interfaces describe. These properties may also be the subject of standards or gaps in standards.
- Non-functional properties. These are properties that are expected to be documented by the provider of a component instance (see definitions).

NOTE – To foster the CGOE operating environment and to limit the number of types of interfaces that must be supported by CGOE components, an attempt is made to limit the number of interface types to be supported when there is a set of different interfaces that could be used.

In some instances, it will be determined that standards do not exist for a particular interface type. In those instances, it may be appropriate to initiate a work item within the ITU-T to develop the standard for this interface or to identify this specification shortcoming to another standards development organization.

As the number of CGOE components will increase over time, this Recommendation has been structured to allow addition of defined CGOE components without requiring the need to re-approve the entire Recommendation when a new CGOE component is to be added. In that regard, each CGOE component that is presented will be added as an annex to this Recommendation. Thus, on a going forward basis, an unlimited number of CGOE components may be added to this Recommendation. This Recommendation also provides the methodology that should be followed when identifying and adding new CGOE components.

7 CGOE framework

The CGOE framework can be viewed at several levels of scale or detail. At the least detailed level, Figure 8 categorizes the technology usage and basic functions.

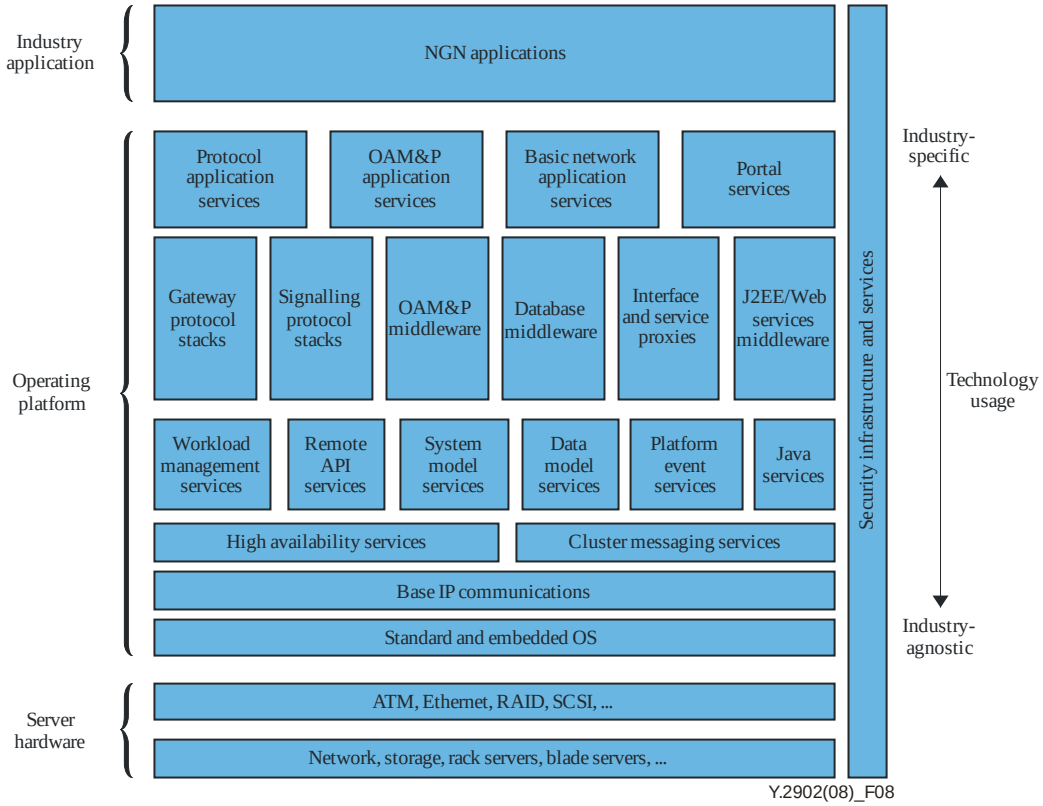

Figure 8 – Carrier grade open environment reference model

At an intermediate level, Figure 9 illustrates how a subset of CGOE components could be presented using an interface-oriented view of the CGOE categories and collecting the CGOE components into categories. At this level only the major interfaces (which fall into the first category defined above) are exposed and the interfaces used by components within a category are hidden, as well as the interfaces that allow interaction with the operating system. The illustration also does not present the external non-programmatic interfaces (like protocols). The network of interfaces to these CGOE components defines the relationships between the components. Further, when a particular CGOE component is selected, e.g., logging, all other CGOE components out of the CGOE reference model should use the interfaces exported by this component, as appropriate.

Also the CGOE reference model may be used to engage other ITU-T Study Groups or other standards development organizations on gaps in their specifications for standards and interfaces and to stimulate creation of a comprehensive eco-system of COTS components that satisfy NGN services.

This intermediate level of definition can be used to navigate the CGOE. For example, consider the "OAM&P middleware" component:

– It uses the "requests" interface of the "HTTP" component. The detailed HTTP component description contains the programmatic interface, the external interactions, etc.

– It abstracts the variety of access mechanisms (HTTP, FTP, SNMP) and presents a "query" interface to other CGOE components and to the application. The detailed OAM&P middleware component description explains how this is done.

This Recommendation is a (mostly) *technology-independent* example use of the CGOE framework. The programmatic interfaces could be expressed in any computer language, e.g., JAVA or C++. The detailed component descriptions reference standards for specific instances of these interfaces.

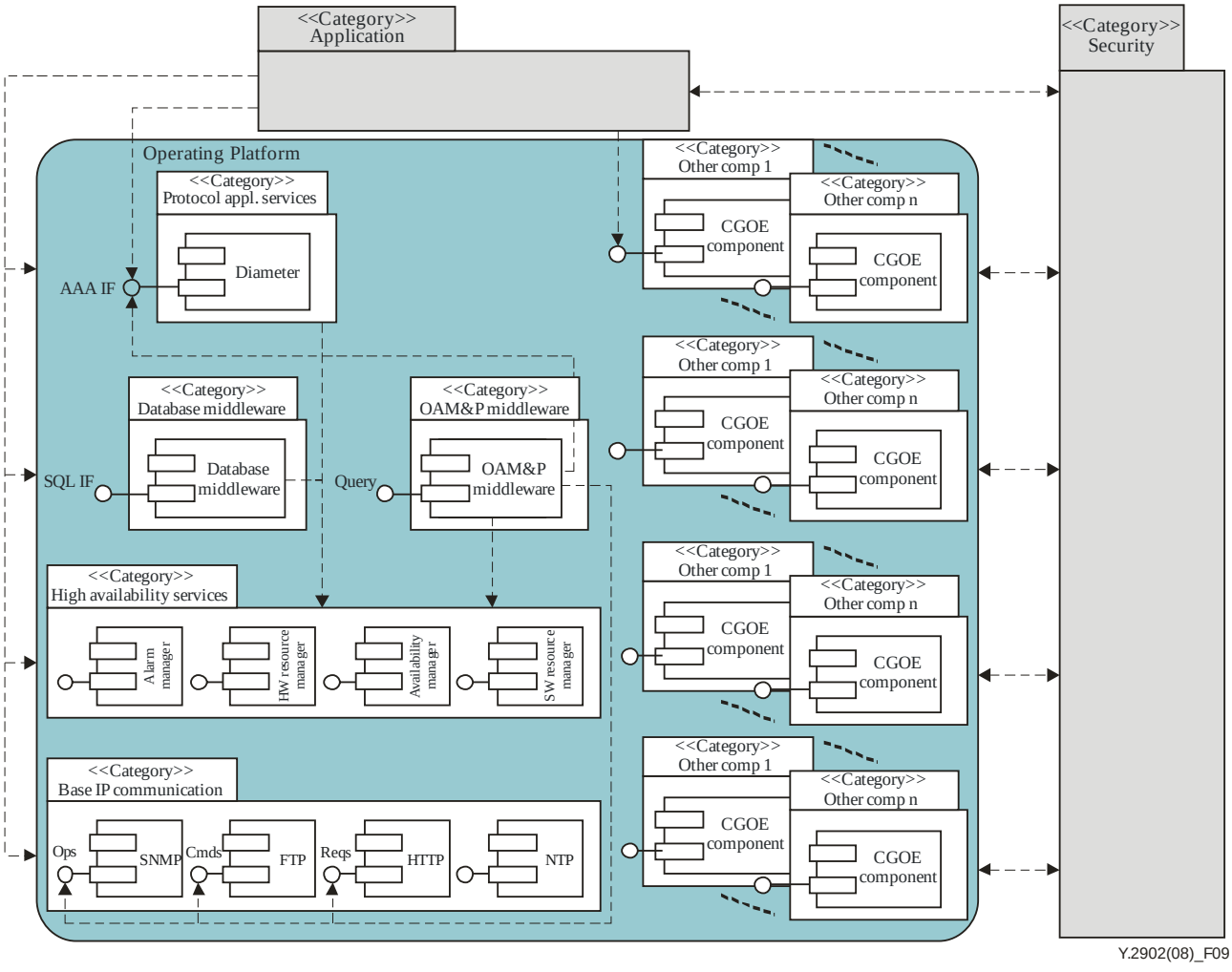

Figure 9 – Example usage of the CGOE component framework

At the most detailed level, each individual component can be examined and each interface, functional property and non-functional property exposed.

8 Security considerations

Although there is no security consideration detailed here, each associated annex will contain the necessary security considerations.

Annex A

The Diameter client CGOE component

(This annex forms an integral part of this Recommendation)

A.1 Scope

This annex specifies the Diameter client CGOE component.

The Diameter base protocol may be used to provide an authentication, authorization and accounting (AAA) framework for applications. A Diameter server CGOE component operating in conjunction with a Diameter client CGOE component can be used to provide an AAA facility.

A.2 References

See clause 2.

A.3 Definitions

See clause 3

A.4 Abbreviations and acronyms

See clause 4.

A.5 Conventions

This annex uses the CGOE component diagram conventions detailed in clause 5.

A.6 The Diameter client CGOE component

A.6.1 General

A technology-independent description of the Diameter client CGOE component is in Figure A.1.

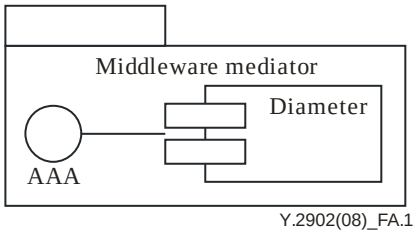

Figure A.1 – Technology-independent view

The primary purpose of Diameter is to offer the capability for authentication, authorization and accounting.

The Diameter has a client-server architecture. A principle description is in Figure A.2.

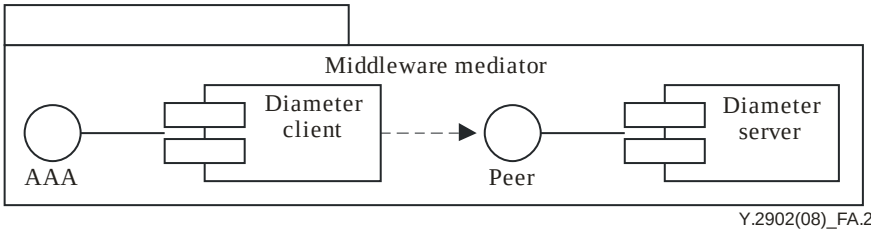

Figure A.2 – Diameter client-server architecture

This annex focuses on the client component of the Diameter component. However, while most of the description holds also for the server CGOE component of Diameter, it is outside the scope of this annex and is the subject of Annex B.

A.6.2 Relationship with other CGOE components

A CGOE compliant Diameter client component may make use of other interfaces as shown in Figure A.3. These are secondary interfaces which are described in the CGOE documentation for each component. Each of these secondary interfaces will have one or more technology-specific instances.

The CGOE component Diameter client is used by the CGOE component OAM&P middleware. Diameter is an optional interface which may be present or not to the OAM&P middleware.

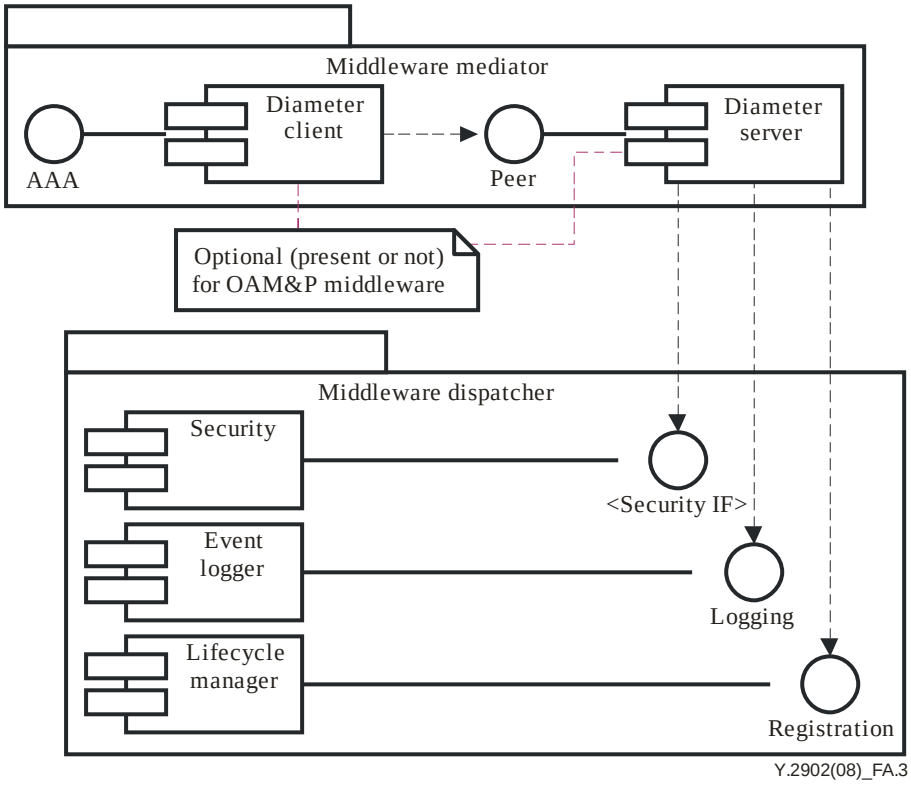

Figure A.3 – Diameter client-server architecture with secondary interfaces of the client side

A.6.3 Internal functional properties

A.6.3.1 Diameter relay function

The CGOE Diameter client component shall be capable of performing the Diameter relay function. A Diameter relay agent that performs the relay function shall be protocol transparent and thus shall

transparently support the Diameter base protocol, which includes accounting and all Diameter applications.

Standards:

– [IETF RFC 3588].

A.6.3.2 Diameter redirect agent function

The CGOE Diameter client component shall be capable of performing the Diameter redirect agent function. A Diameter redirect agent that performs the redirect function shall be protocol transparent and thus shall transparently support the Diameter base protocol, which includes accounting and all Diameter applications.

Standards:

– [IETF RFC 3588].

A.6.3.3 Proxy capability of the Diameter client

Diameter proxies must support the Diameter base protocol, which includes accounting. Additionally, they must fully support each Diameter application that is needed to implement proxied services.

Standards:

– [IETF RFC 3588].

A.6.3.4 Translation agent

A translation agent is a stateful Diameter node that performs protocol translation between Diameter and another AAA protocol. The CGOE Diameter client component may be capable of performing the translation agent function between:

– Diameter and RADIUS

  Standards:

  • [IETF RFC 3588].
  • [b-IETF RFC 2865].
  • [b-IETF RFC 2868].
  • [b-IETF RFC 3575].

– Diameter and TACACS

  Standards:

  • [IETF RFC 3588].
  • [b-IETF RFC 1492].

A.6.4 Non-functional properties

A.6.4.1 Transport failure detection

– This property measures the occurrence of Diameter message failures during transport. Detection of such failures will minimize the occurrence of messages sent to unavailable agents, resulting in unnecessary delays, and will provide for better failover performance.

– Unit of measure: Not applicable.

A.6.4.2 Recovery

– This property measures the behaviour of the components after an outage condition has been restored.

– Unit of measure: Yes/partly/no.

A.6.5 Interfaces

A.6.5.1 Diameter client-IF-01 <Applications>

The AAA application interface is the primary interface of a Diameter client CGOE component and it supports the interface to authentication, authorization and accounting applications. When the base Diameter protocol is in use for authentication and authorization, it is always extended for a particular application. For example, two Diameter applications are defined: NASREQ and mobile IPv4. These applications are not part of the Diameter client CGOE component.

Standards:

– [IETF RFC 3588].

A.6.5.2 Diameter client-IF-02 <Peer>

The peer interface is the basic connection interface offered by the Diameter client CGOE component. For connections to a peer CGOE Diameter component, when the communications channel is not contained within a trusted environment, this interface shall connect to an IPSec or TLS CGOE component. At a minimum, a Diameter node SHOULD have an established connection with two peers per realm, known as the primary and secondary peers.

– Diameter client-IF-02 <IPSec peer>

  Standards:

  • [IETF RFC 2401].
  • [IETF RFC 3588].

– Diameter client-IF-02 <TLS peer>

  Standards:

  • [IETF RFC 4346].
  • [IETF RFC 3588].

A.6.5.3 Diameter client-IF-03 <Logging>

The logging interface is a secondary interface of the Diameter client CGOE component and provides the capability to log any transaction in relation to the Diameter client CGOE component.

Standards:

– GAP (possible solution, the logging component of the specific middleware can be used).

A.6.5.4 Diameter client-IF-04 <Security: End-to-End >

The security IF is a secondary interface of the Diameter client CGOE component. End-to-end security refers to security between two Diameter nodes, possibly communicating through Diameter agents. It should be noted that TLS and IPSec provide hop-by-hop security or security across only a transport connection. Thus, when Diameter relays or proxies are involved, hop-by-hop security does not fully protect the Diameter session. This security interface protects the Diameter communications path from the originating Diameter component to the terminating Diameter component.

Standards:

– [IETF RFC 3588].

– GAP (possible solution, IETF work in progress on end-to-end security).

A.6.5.5 Diameter client-IF-05 <Stream Control Transmission Protocol>

The Diameter client CGOE component provides a number of interfaces. For those instances where the interface requires a transport capability, the interface may use TCP over IP or SCTP over IP.

This interface provides mechanisms to transfer Diameter messages over the Internet Protocol using the stream control transmission protocol.

Standards:

– [IETF RFC 3588].

– [IETF RFC 4960].

A.6.5.6 Diameter client-IF-06 <Transmission Control Protocol>

The Diameter client CGOE component provides a number of interfaces. For those instances where the interface requires a transport capability, the interface may use TCP over IP or SCTP over IP. This interface provides mechanisms to transfer Diameter messages over the Internet protocol using the transmission control protocol.

Standards:

– [IETF RFC 3588].

– [IETF RFC 4960].

A.6.6 Relationship with Internet Assigned Numbers Authority

Each Diameter application must have an Internet Assigned Numbers Authority (IANA) assigned application identifier. Implementations must only use Diameter applications for which an IANA assigned application identifier has been obtained.

Standards:

– [b-IETF RFC 3692].

A.7 Security

The Diameter client CGOE component will communicate with other CGOE components through its primary and secondary interfaces. In some cases, these inter CGOE component links will occur in fully trusted environments, while in other cases this will not be true. As a result, the Diameter client CGOE component shall be able to make use of standard transmission links and transmission links that are protected through the use of TLS or IPSec.

The Diameter protocol shall not pass through an untrusted environment without the benefit of a security mechanism, viz TLS or IPSec.

Annex B

The Diameter server CGOE component

(This annex forms an integral part of this Recommendation)

B.1 Scope

This annex specifies the Diameter server CGOE component.

The Diameter base protocol can be used to provide an authentication, authorization and accounting (AAA) framework for applications. A Diameter server CGOE component operating in conjunction with a Diameter client CGOE component can be used to provide an AAA facility.

B.2 References

See clause 2.

B.3 Definitions

See clause 3.

B.4 Abbreviations and acronyms

See clause 4.

B.5 Conventions

This annex uses the CGOE component diagram conventions detailed in clause 5.

B.6 The Diameter server CGOE component

B.6.1 General

A technology-independent description of the Diameter server CGOE component is in Figure B.1.

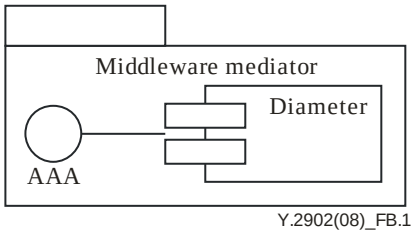

Figure B.1 – Technology-independent view

The primary purpose of Diameter is to offer the capability for authentication, authorization and accounting.

The Diameter has a client-server architecture. A principle description is in Figure B.2.

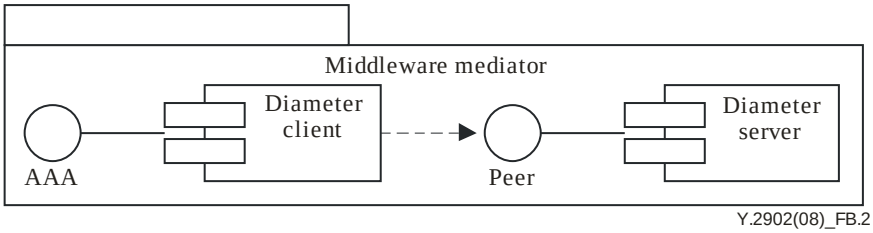

Figure B.2 – Diameter client-server architecture

This annex focuses on the server component of Diameter. However, while most of the description holds also for the client CGOE component of Diameter, it is outside the scope of this annex and is the subject of Annex A.

B.6.2 Relationship with other CGOE components

A CGOE compliant Diameter server component may make use of other interfaces as shown in Figure B.3. These are secondary interfaces which are described in the CGOE documentation for each component. Each of these secondary interfaces will have one or more technology-specific instances.

The CGOE component Diameter server is used by the CGOE component OAM&P middleware. Diameter is an optional interface which may be present or not to the OAM&P middleware.

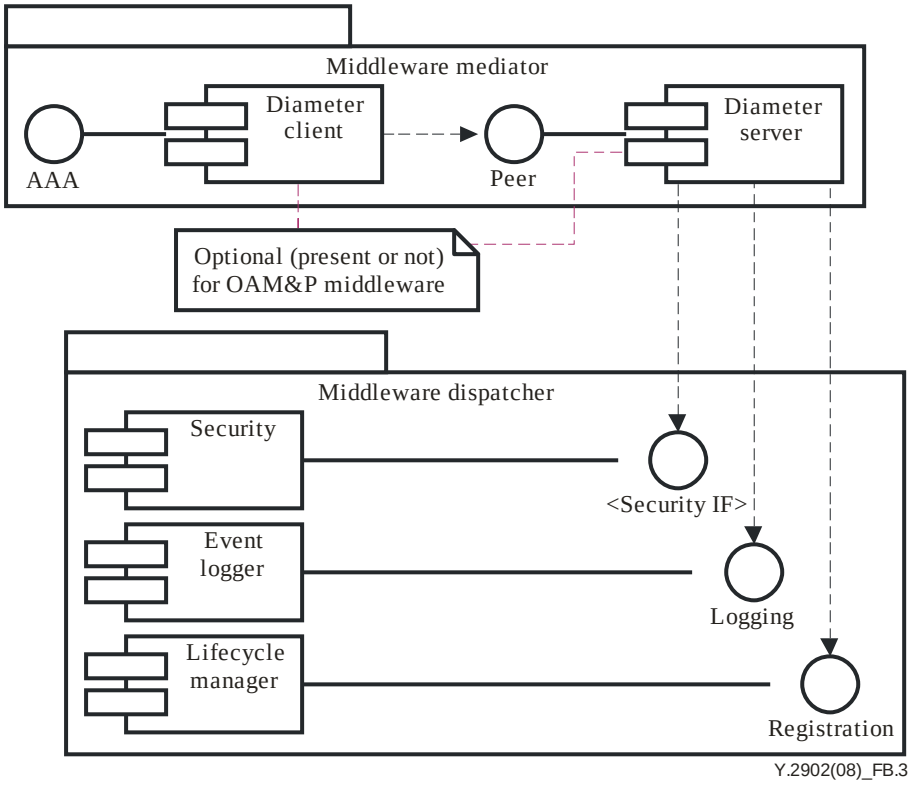

Figure B.3 – Diameter client-server architecture with secondary interfaces of the server side

B.6.3 Internal functional properties

B.6.3.1 Diameter relay function

The CGOE Diameter server component shall be capable of performing the Diameter relay function. A Diameter relay agent that performs the relay function shall be protocol transparent and thus shall

transparently support the Diameter base protocol, which includes accounting and all Diameter applications.

Standards:

– [IETF RFC 3588].

B.6.3.2 Diameter redirect agent function

The CGOE Diameter server component shall be capable of performing the Diameter redirect agent function. A Diameter redirect agent that performs the redirect function shall be protocol transparent and thus shall transparently support the Diameter base protocol, which includes accounting and all Diameter applications.

Standards:

– [IETF RFC 3588].

B.6.3.3 Proxy capability of the Diameter server

Diameter proxies must support the Diameter base protocol, which includes accounting. Additionally, they must fully support each Diameter application that is needed to implement proxied services.

Standards:

– [IETF RFC 3588].

B.6.3.4 Translation agent

A translation agent is a stateful Diameter node that performs protocol translation between Diameter and another AAA protocol. The CGOE Diameter server component may be capable of performing the translation agent function between:

– Diameter and RADIUS

  Standards:

  • [IETF RFC 3588].
  • [b-IETF RFC 2865].
  • [b-IETF RFC 2868].
  • [b-IETF RFC 3575].

– Diameter and TACACS

  Standards:

  • [IETF RFC 3588].
  • [b-IETF RFC 1492].

B.6.4 Non-functional properties

B.6.4.1 Transport failure detection

– This property measures the occurrence of Diameter message failures during transport. Detection of such failures will minimize the occurrence of messages sent to unavailable agents, resulting in unnecessary delays, and will provide for better failover performance.

– Unit of measure: Not applicable.

B.6.4.2 Recovery

– This property measures the behaviour of the components after an outage condition has been restored.

– Unit of measure: Yes/partly/no.

B.6.5 Interfaces

B.6.5.1 Diameter server-IF-01 <Applications>

The AAA application interface is the primary interface of a Diameter server CGOE component and it supports the interface to authentication, authorization and accounting applications. When the base Diameter protocol is in use for authentication and authorization, it is always extended for a particular application. For example, two Diameter applications are defined: NASREQ and mobile IPv4. These applications are not part of the Diameter server CGOE component.

Standard:

– [IETF RFC 3588].

B.6.5.2 Diameter server-IF-02 <Peer>

The peer interface is the basic connection interface offered by the Diameter server CGOE component. For connections to a peer CGOE Diameter component, when the communications channel is not contained within a trusted environment, this interface shall connect to an IPSec or TLS CGOE component. At a minimum, a Diameter node SHOULD have an established connection with two peers per realm, known as the primary and secondary peers.

– Diameter server-IF-02 <IPSec peer>

  Standards:

  • [IETF RFC 2401].
  • [IETF RFC 3588].

– Diameter server-IF-02 <TLS peer>

  Standards:

  • [IETF RFC 2246].
  • [IETF RFC 3588].

B.6.5.3 Diameter server-IF-03 <Logging>

The logging interface is a secondary interface of the Diameter server CGOE component and provides the capability to log any transaction in relation to the Diameter server CGOE component.

Standards:

– GAP (possible solution, the logging component of the specific middleware can be used).

B.6.5.4 Diameter server-IF-04 <Registration>

The registration interface is a secondary interface of the Diameter server CGOE component and is the interface used to connect to the CGOE component lifecycle manager.

Standards:

– GAP.

B.6.5.5 Diameter server-IF-05 <Security: End-to-End >

The security IF is a secondary interface of the Diameter server CGOE component. End-to-end security refers to security between two Diameter nodes, possibly communicating through Diameter agents. It should be noted that TLS and IPSec provide hop-by-hop security or security across only a transport connection. Thus, when Diameter relays or proxies are involved, hop-by-hop security does not fully protect the Diameter session. This security interface protects the Diameter communications path from the originating Diameter component to the terminating Diameter component.

Standards:

– [IETF RFC 3588].

– GAP (possible solution, IETF work in progress on end-to-end security).

B.6.5.6 Diameter server-IF-06 <Stream Control Transmission Protocol>

The Diameter server CGOE component provides a number of interfaces. For those instances where the interface requires a transport capability, the interface may use TCP over IP or SCTP over IP. This interface provides mechanisms to transfer Diameter messages over the Internet protocol using the stream control transmission protocol.

Standards:

– [IETF RFC 3588].

– [IETF RFC 4960].

B.6.5.7 Diameter server-IF-07 <Transmission Control Protocol>

The Diameter server CGOE component provides a number of interfaces. For those instances where the interface requires a transport capability, the interface may use TCP over IP or SCTP over IP. This interface provides mechanisms to transfer Diameter messages over the Internet protocol using the transmission control protocol.

Standards:

– [IETF RFC 3588].

– [IETF RFC 4960].

B.6.5.8 Relationship with Internet Assigned Numbers Authority

Each Diameter application must have an Internet Assigned Numbers Authority (IANA) assigned application identifier. Implementations must only use Diameter applications for which an IANA assigned application identifier has been obtained.

Standards:

– [b-IETF RFC 3692].

B.7 Security

The Diameter server CGOE component will communicate with other CGOE components through its primary and secondary interfaces. In some cases, these inter CGOE component links will occur in fully trusted environments, while in other cases this will not be true. As a result, the Diameter server CGOE component shall be able to make use of standard transmission links and transmission links that are protected through the use of TLS or IPSec.

The Diameter protocol shall not pass through an untrusted environment without the benefit of a security mechanism, viz TLS or IPSec.

Annex C

The FTP client CGOE component

(This annex forms an integral part of this Recommendation)

C.1 Scope

This annex specifies the FTP client CGOE component.

C.2 References

See clause 2.

C.3 Definitions

See clause 3.

C.4 Abbreviations

See clause 4.

C.5 Conventions

This annex uses the CGOE component diagram conventions detailed in clause 5.

C.6 The FTP client CGOE component

C.6.1 General

A file transfer protocol (FTP) is a component that operates as an interface. It allows and is used 1) to promote sharing of files (computer programs and/or data), 2) to encourage indirect or implicit (via programs) use of remote computers, 3) to shield a user from variations in file storage systems among hosts, and 4) to transfer data reliably and efficiently. FTP, though usable directly by a user at a terminal, is designed mainly for use by programs. The security of FTP can be increased by the use of FTP security extensions.

The component FTP acts as a server, which provides a concrete communication facility.

A technology-independent description is in Figure C.1.

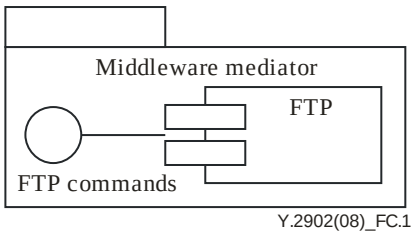

Figure C.1 – Technology-independent view

This shows that FTP offers the capability for communication based on commands. This is the primary interface for an FTP component.

FTP has a client-server architecture. A principle description is in Figure C.2.

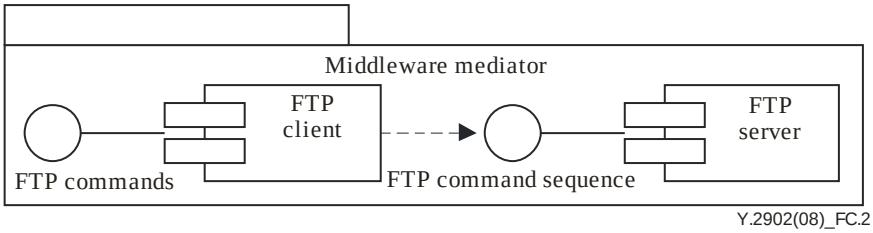

Figure C.2 – FTP client-server architecture

This annex focuses on the client part of the FTP component. However, most of the description holds also for the server part of the FTP component.

C.6.2 Relationship with other CGOE components

A CGOE-compliant FTP client component makes use of other interfaces as shown in Figure C.3. These are secondary interfaces which are described in the CGOE documentation for each component. Each of these secondary interfaces will have one or more technology-specific instances.

The CGOE component FTP client is used by the CGOE component OAM&P middleware. FTP is an optional interface which may be present or not to the OAM&P middleware.

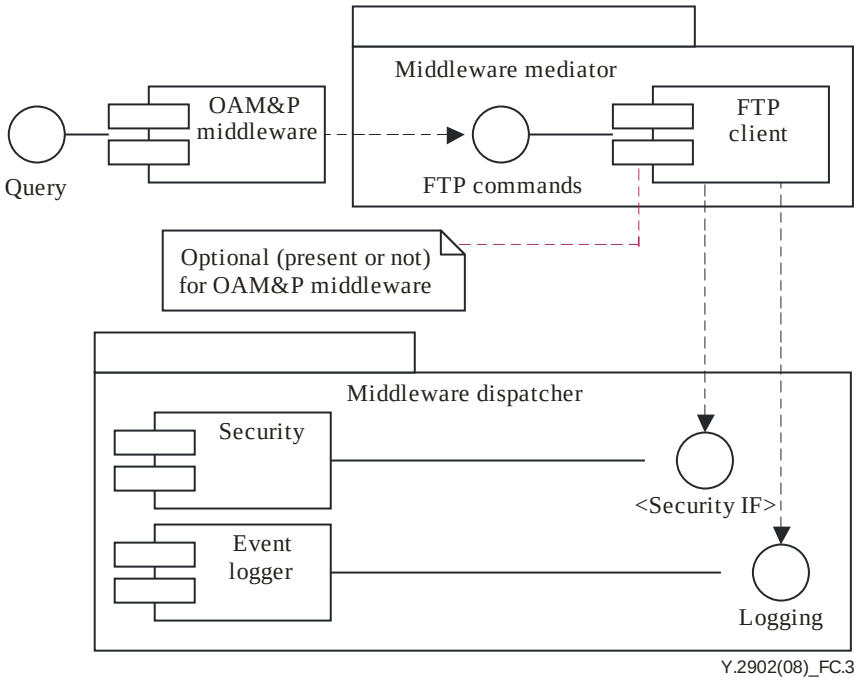

Figure C.3 – Secondary interfaces

C.6.3 Internal functional properties

C.6.3.1 Data connection

A data connection is used to transfer files.

Standards:

– [IETF RFC 959] updated by [IETF RFC 2228], [IETF RFC 2640], [IETF RFC 2773].

C.6.3.2 Tracing

Tracing deals with monitoring communication traffic for the purpose of error finding.

Standards:

– None.

C.6.4 Non-functional properties

This clause addresses non-functional properties which may be used to facilitate in the specification of non-functional requirements. However, non-functional requirements are outside the scope of this Recommendation.

C.6.4.1 Transaction performance

This property measures how many data can be transferred per second on a data connection.

Unit of measure: Bytes/second.

C.6.4.2 Modification of multitude data records

This property measures if a command of the interface operation supports modifying more than one data record.

Unit of measure: Yes/no.

C.6.4.3 Recovery

This property measures the behaviour of the components if there is no response or confirmation, e.g., due to a temporary outage.

Unit of measure: Yes/partly/no.

C.6.5 Interfaces

C.6.5.1 FTP client-IF-01 <FTP Commands>

Provides the communication commands.

NOTE – This also includes command sequences.

Standards:

– [IETF RFC 959] updated by [IETF RFC 2228], [IETF RFC 2640], [IETF RFC 2773].

C.6.5.2 FTP client-IF-02 <Logging>

Provides the capability to log any transaction in relation to the component FTP.

Standards:

– GAP (Possible solution: the logging component of the specific middleware can be used) [b-ETSI EN 300 444].

C.6.5.3 FTP client-IF-03 <Security IF>

The <Security IF> is the interface to the component security. Security also includes access control to files and directories.

Standards:

– GAP.

C.6.5.4 FTP client-IF-04 <Telnet>

The purpose of the TELNET protocol is to provide a fairly general, bidirectional, eight-bit byte oriented communications facility. A TELNET connection is a transmission control protocol (TCP) connection used to transmit data with interspersed TELNET control information.

Standards:

– [IETF RFC 854].

– [IETF RFC 855].

C.6.5.5 FTP client-IF-05 <File System>

Provides the capability to create, delete, read, write and modify files and directories. This includes also access rights.

Standards:

– [IETF RFC 854].

– [IETF RFC 855].

C.7 Security

Should security be required, consideration should be given to the use of the security extensions described in [IETF RFC 2228]. These extensions may be used to provide strong authentication, integrity and confidentiality on both the control and data channels.

Annex D

The FTP server CGOE component

(This annex forms an integral part of this Recommendation)

D.1 Scope

This annex specifies the FTP server CGOE component.

D.2 References

See clause 2.

D.3 Definitions

See clause 3.

D.4 Abbreviations

See clause 4.

D.5 Conventions

This annex uses the CGOE component diagram conventions detailed in clause 5.

D.6 The FTP server CGOE component

D.6.1 General

A file transfer protocol (FTP) is a component that operates as an interface. It allows and is used 1) to promote sharing of files (computer programs and/or data), 2) to encourage indirect or implicit (via programs) use of remote computers, 3) to shield a user from variations in file storage systems among hosts, and 4) to transfer data reliably and efficiently. FTP, though usable directly by a user at a terminal, is designed mainly for use by programs. The security of FTP can be increased by the use of FTP security extensions.

The component FTP acts as a server, which provides a concrete communication facility.

A technology-independent description is in Figure D.1.

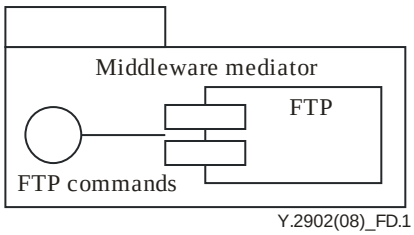

Figure D.1 – Technology-independent view

This shows that FTP offers the capability for communication based on commands. This is the primary interface for an FTP component.

FTP has a client-server architecture. A principle description is in Figure D.2.

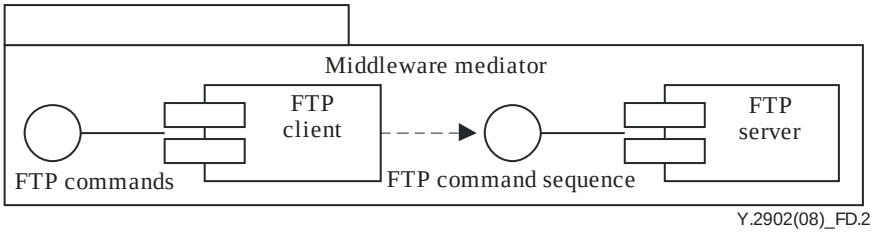

Figure D.2 – FTP client-server architecture

This annex focuses on the server part of the FTP component. However, most of the description holds also for the client part of the FTP component.

D.6.2 Relationship with other CGOE components

A CGOE-compliant FTP server component makes use of other interfaces as shown in Figure D.3. These are secondary interfaces which are described in the CGOE documentation for each component. Each of these secondary interfaces will have one or more technology-specific instances.

The CGOE component FTP server is used by the CGOE component OAM&P middleware. FTP is an optional interface which may be present or not to the OAM&P middleware.

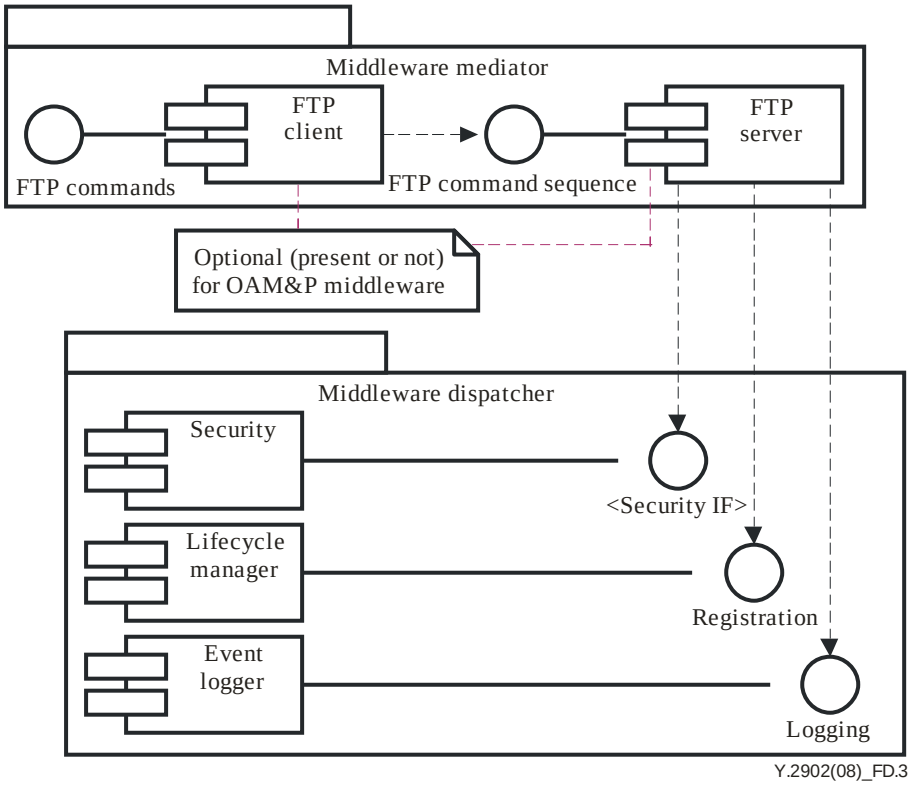

Figure D.3 – Secondary interfaces

D.6.3 Internal functional properties

D.6.3.1 Data connection

A data connection is used to transfer files.

Standards:

– [IETF RFC 959] updated by [IETF RFC 2228], [IETF RFC 2640], [IETF RFC 2773].

D.6.3.2 Tracing

Tracing deals with monitoring communication traffic for the purpose of error finding.

Standards:

– None.

D.6.4 Non-functional properties

This clause addresses non-functional properties which may be used to facilitate in the specification of non-functional requirements. However, non-functional requirements are outside the scope of this Recommendation.

D.6.4.1 Transaction performance

This property measures how many data can be transferred per second on a data connection

Unit of measure: Bytes/second.

D.6.4.2 Modification of multitude data records

This property measures if a command of the interface operation supports modifying more than one data record.

Unit of measure: Yes/no.

D.6.4.3 Recovery

This property measures the behaviour of the components if there is no response or confirmation, e.g., due to a temporary outage.

Unit of measure: Yes/partly/no.

D.6.5 Interfaces

D.6.5.1 FTP server-IF-01 <FTP Commands>

Provides the communication commands.

NOTE – This also includes command sequences.

Standards:

– [IETF RFC 959] updated by [IETF RFC 2228], [IETF RFC 2640], [IETF RFC 2773].

D.6.5.2 FTP server-IF-02 <Logging>

Provides the capability to log any transaction in relation to the component FTP.

Standards:

– GAP (possible solution the logging component of the specific middleware can be used).

D.6.5.3 FTP server-IF-03 <Security IF>

The <Security IF> is the interface to the component security. Security also includes access control to files and directories.

Standards:

– GAP.

D.6.5.4 FTP server-IF-04 <Registration>

Registration is the interface to the component lifecycle manager.

Standards:

– GAP.

D.6.5.5 FTP server-IF-05 <Telnet>

The purpose of the TELNET protocol is to provide a fairly general, bidirectional, eight-bit byte oriented communications facility. A TELNET connection is a transmission control protocol (TCP) connection used to transmit data with interspersed TELNET control information.

Standards:

– [IETF RFC 854].

– [IETF RFC 855].

D.6.5.6 FTP server-IF-06 <File System>

Provides the capability to create, delete, read, write and modify files and directories. This includes also access rights.

Standards:

– [IETF RFC 854].

– [IETF RFC 855].

D.7 Security

Should security be required, consideration should be given to the use of the security extensions described in [IETF RFC 2228]. These extensions may be used to provide strong authentication, integrity and confidentiality on both the control and data channels.

Bibliography

[b-ITU-T Q.1290] Recommendation ITU-T Q.1290 (1998), *Glossary of terms used in the definition of intelligent networks.*
<http://www.itu.int/rec/T-REC-Q.1290>

[b-ETSI EN 300 444] ETSI EN 300 444 (in force), Digital Enhanced Cordless Telecommunications (DECT) – Generic Access Profile (GAP)
<http://pda.etsi.org/pda/queryform.asp>

[b-ETSI TS 129 228] ETSI TS 129 228 (in force), *Digital cellular telecommunications system (Phase 2+);Universal Mobile Telecommunications System (UMTS);IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents.*
<http://pda.etsi.org/pda/queryform.asp>

[b-ETSI TS 129 229] ETSI TS 129 229 (in force), *Digital cellular telecommunications system (Phase 2+);Universal Mobile Telecommunications System (UMTS);Cx and Dx interfaces based on the Diameter protocol; Protocol details.*
<http://pda.etsi.org/pda/queryform.asp>

[b-ETSI TS 129 329] ETSI TS 129 329 (in force), *Digital cellular telecommunications system (Phase 2+);Universal Mobile Telecommunications System (UMTS); Sh interface based on the Diameter protocol; Protocol details.*
<http://pda.etsi.org/pda/queryform.asp>

[b-IETF RFC 1492] IETF RFC 1492 (1993), *An Access Control Protocol, Sometimes Called TACACS.*
<http://www.ietf.org/rfc/rfc1492.txt>

[b-IETF RFC 2865] IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS).*
<http://www.ietf.org/rfc/rfc2865.txt>

[b-IETF RFC 2868] IETF RFC 2868 (2000), *RADIUS Attributes for Tunnel Protocol Support.*
<http://www.ietf.org/rfc/rfc2868.txt>

[b-IETF RFC 3575] IETF RFC 3575 (2003), *IANA Considerations for RADIUS (Remote Authentication Dial In User Service).*
<http://www.ietf.org/rfc/rfc3575.txt>

[b-IETF RFC 3692] IETF RFC 3692 (2004), *Assigning Experimental and Testing Numbers Considered Useful.*
<http://www.ietf.org/rfc/rfc3692.txt>

[b-IETF RFC 5080] IETF RFC 5080 (2007), *Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes.*
<http://www.ietf.org/rfc/rfc5080.txt>

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	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
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**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2009