Security Guide
SAP Convergent Charging
Document Version: 1.6 – 2015-04-17

CUSTOMER

SAP Convergent Charging 4.0

Typographic Conventions

Type Style	Description
Example	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Textual cross-references to other documents.
Example	Emphasized words or expressions.
`EXAMPLE`	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
`Example`	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example`	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE`	Keys on the keyboard, for example, `F2` or `ENTER`.

Document History

 Caution

Before you start the implementation or audit of SAP Convergent Charging software component, make sure you have the latest version of this document. You can find the latest version in SAP Service Marketplace at the following location: https://service.sap.com/securityguide → SAP Business Suite Applications → SAP CC.

Version	Date	Change
1.0	August 2013	Initial version
1.1	February 2014	First maintenance version (4.0 SP03)
1.2	April 2014	Second maintenance version (4.0 SP04)
1.3	July 2014	Third maintenance version (4.0 SP05)
1.4	October 2014	Fourth maintenance version (4.0 SP06)
1.5	January 2015	Fifth maintenance version (4.0 SP07)
1.6	April 2015	Sixth maintenance version (4.0 SP08)

Table of Contents

1 Introduction

1.1 Target Audience

- Security consultants
- Security auditors
- System administrators
- Support specialists

This document is not included as part of the Installation Guides, Configuration Guides, Technical Operation Manuals, or Upgrade Guides. Such guides are only relevant for a certain phase of the software life cycle, whereas the Security Guides provide information that is relevant for all life cycle phases.

1.2 Why Is Security Necessary?

With the increasing use of distributed systems and the Internet for managing business data, the demands on security are also on the rise. When using a distributed system, you need to be sure that your data and processes support your business needs without allowing unauthorized access to critical information. User errors, negligence, or attempted manipulation on your system should not result in loss of information or processing time. These demands on security apply likewise to SAP Convergent Charging . To assist you in securing SAP Convergent Charging, we provide this Security Guide.

1.3 About this Document

The Security Guide provides an overview of the security-relevant information that applies to SAP Convergent Charging, referred to as SAP CC in this guide.

The Security Guide contains the following main sections:

Section Title	Content Description
Before You Start	This section contains information about why security is necessary, how to use this document and references to other Security Guides that build the foundation for this Security Guide.
Technical System Landscape	This section provides an overview of the technical components and communication paths that are used by SAP CC.
Security Aspects of Data, Data Flow and Processes	This section provides an overview of the security aspects within SAP CC through data flows related to the 2 main processes of the solution.
User Administration and Authentication	This section provides an overview of the user and authentication management.

Section Title	Content Description
Authorizations	This section provides an overview of the authorization concepts related to SAP CC.
Network and Communication Security	This section provides an overview of the communication paths used by SAP CC and the security mechanisms that apply. It also includes our recommendations for the network topology to restrict access at the network level.
Data Storage Security	This section provides an overview of any critical data that is used by SAP CC and the security mechanisms that apply.
Security-Relevant Logging and Tracing	This section provides an overview of the trace and log files that contain security-relevant information, for example, so you can reproduce activities if a security breach occurs.
Copyrights	This section provides references to further information.

1.4 What's New in this Document

1.4.1 What’s New in SP08

As of SP08, SAP Convergent Charging provides you with the following feature:

- A new web service named “Activation” has been added to the dispatcher instance. This web service provides an operation named “ChargingContractActivate” which gives the possibility to activate a charging contract stored in SAP CC, including all the associated charging contracts in case a parent/linked relationship exists

1.4.2 What’s New in SP07

As of SP07, SAP Convergent Charging provides you with the following feature:

- The algorithm used for hashing passwords is SHA-256. 128-bit random salt is used for prefixing the passwords before hashing.

1.5 Document Abbreviations

The table below shows the list of abbreviations used throughout this document:

Abbreviation	Meaning
A2A	Application To Application

Abbreviation	Meaning
ACL	Access Control List
API	Application Programming Interface
BART	Batch Acquisition and Rating Toolset
CCR	Credit Control Request
CDR	Call Detail Record or more generally Consumption Detail Record
HCI	Http Communication Interface
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secured
JSE	Java platform, Standard Edition
OS	Operating System
RDBMS	Relationship Data Base Management System
RFC	Remote Function Call
SAML	Security Assertion Markup Language
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSL	Secure Sockets Layer
SSO	Single Sign-On
STS	Security Token System
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security
WS	Web Services
WSS	Web Services Security
WSDL	Web Services Description Language
XML	eXtended Markup Language

2 Before You Start

2.1 Fundamental Guides

For a complete list of the available SAP Security Guides, see SAP Service Marketplace at the following location: http://service.sap.com/securityguide.

For a complete list of the available Guides and Online Helps related to the SAP Convergent Charging 4.0 solution, see SAP Support Portal at the following location: http://service.sap.com/instguidescc →SAP CC 4.0

The following technical documentation is available in the Core Server SDK:

- System Parameter Reference
- Database Reference
- Error Code Reference
- Java Core API Reference (Javadoc)
- Web Services SOAP Specifications
- User Interfaces

2.2 Important SAP Notes

For more information about the content of the current SAP Convergent Charging software release, please consult the following SAP Notes on the SAP Support Portal at the following location: http://service.sap.com/securitynotes.

SAP Note	Title	Comment
1394093	Collective Security Note	
1702364	Convergent Charging Integration with Convergent Invoicing	

2.3 Additional Information

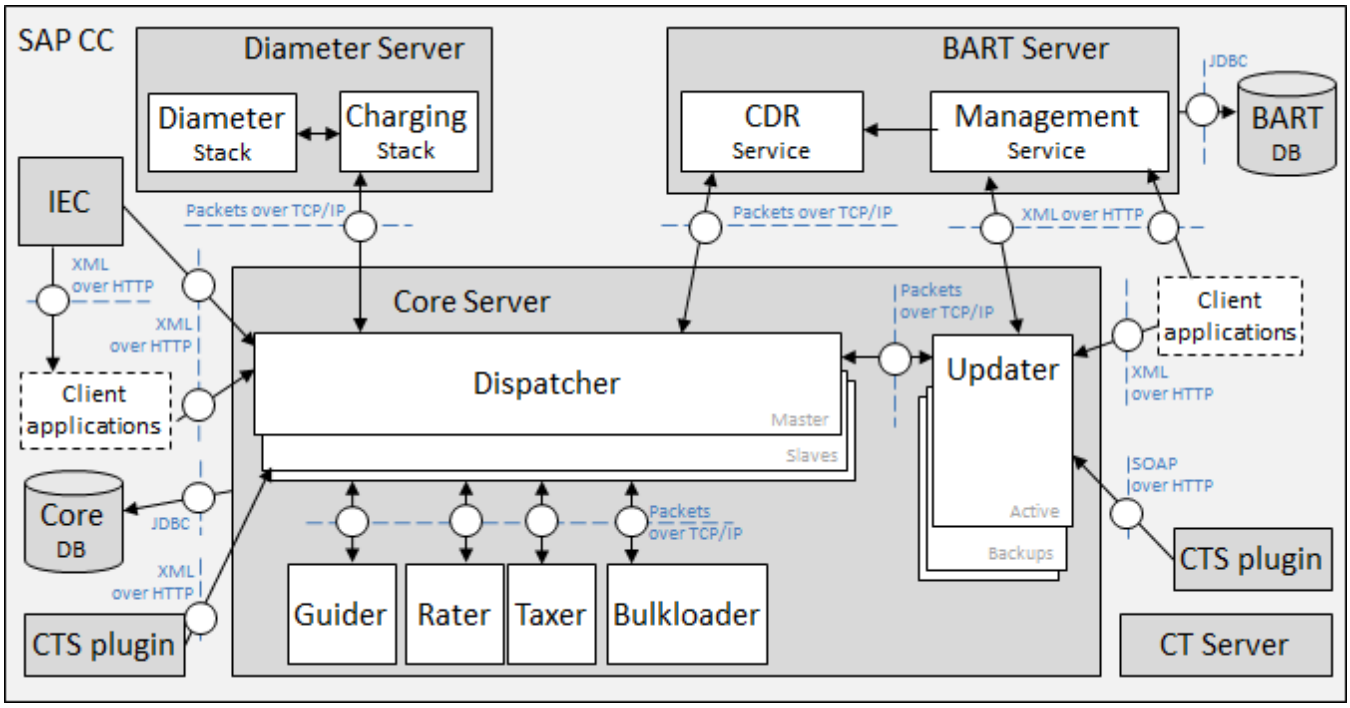
For more information about specific topics, see the quick links as shown in the table below:

Content	Quick Link on SAP Service Marketplace
Security	https://service.sap.com/security
Related SAP notes	https://service.sap.com/notes
Released platforms	https://service.sap.com/platforms
SAP Solution Manager	https://service.sap.com/solutionmanager

3 Technical System Landscape

3.1 SAP CC Architecture

Built upon a modular 3-tier client/server architecture, SAP CC implements the concept of services through multiple servers and/or server instances execution. The figure below shows an overview of the SAP CC technical system landscape:



As described above, SAP CC architecture relies on multiple components:

- **SAP CC Core Server**, made up with a set of server instances acting as business services:
  - Dispatchers, used to distribute the clients' requests to the adequate server instance
  - Updaters, used to manage business objects and provide up-to-date information to other server instances
  - Guiders, dedicated to rating services guiding
  - Raters, dedicated to all rating services
  - Taxers, dedicated to real-time calculation of United States telco taxes
  - Bulkloaders, used to load charged items files in a third-party billing system using a bulk mode
- **SAP CC BART Server**, a rating injector dedicated to batch rating and charging operations
- **SAP CC Diameter Server**, used to translate incoming Diameter CCR messages into SAP CC Core Server comprehensible events
- **SAP CC IEC**, used to consolidate and schedule data transfers between SAP CC and third-party systems

- **SAP CC Communications Taxing Server**, used to manage calculation and reporting of U.S Telco taxes in accordance with the BillSoft EZTax system
- **SAP CC client applications**, which give the possibility to administer and manage server instances and business objects through:
  - Console applications, mainly used for configuration and administration purposes
  - Desktop applications, dedicated to business purposes and providing user-friendly graphical interfaces
  - A Core Server component of another SAP CC system (when using the Catalog Transport feature)

These components have been specifically designed to ensure the stability and performance of the global platform during pricing, rating and charging operations. They communicate together through different communication channels described in the Network and Communication section of this document.

> **Note**
>
> According to your needs, the implemented business scenario can differ. As a consequence, multiple technical system landscapes exist for SAP CC. From a security point of view, the chosen system landscape leads to specific security-related issues which must be addressed during setup and configuration steps.

For more information about the technical system landscape, see the Quick Links as shown in the table below:

Topic	Guide / Tool	Quick Link on SAP Service Marketplace
Business Scenario	SAP for Telecommunications Master Guide	https://service.sap.com/instguides
Compatibility and System Requirements: • Platform Overview • Landscape Catalogue • SAP CC Core Server and Instance Deployment	SAP CC Installation Guide	https://service.sap.com/instguidescc
Technical System Landscape	SAP CC Solution Operations Guide	https://service.sap.com/instguidescc

3.2 Configurations and Catalogue

For a complete list of the supported platforms, see SAP Service Marketplace at the following location: https://service.sap.com/pam.

4 Security Aspects of Data, Data Flow and Processes

The SAP Convergent Charging solution gives the possibility to execute multiple processes which:

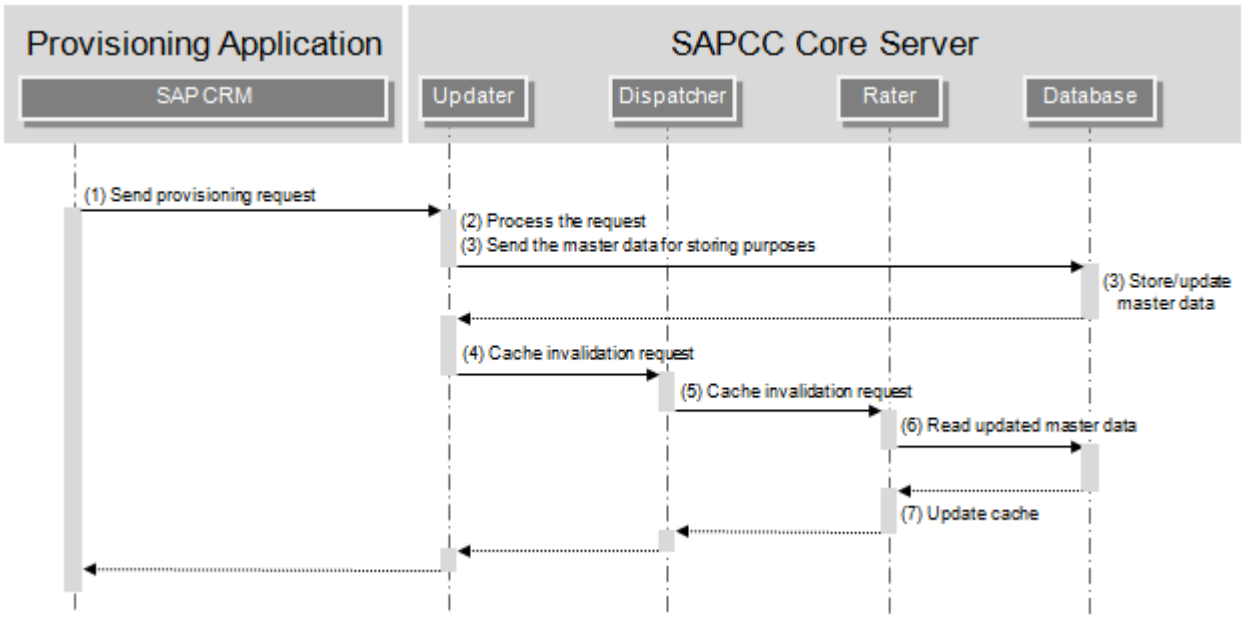
- Deal with internal and/or external data
- Communicate with internal and/or external components through data transfers

The two figures below show an overview of the data flows related to the following processes, with the associated security measures:

- **Customer provisioning**, used to manage customers' subscriptions and access provisioning
- **Usage Rating and Subscriber Account Charging**, dedicated to external and internal events rating using rating trees to compute these events and determine an amount

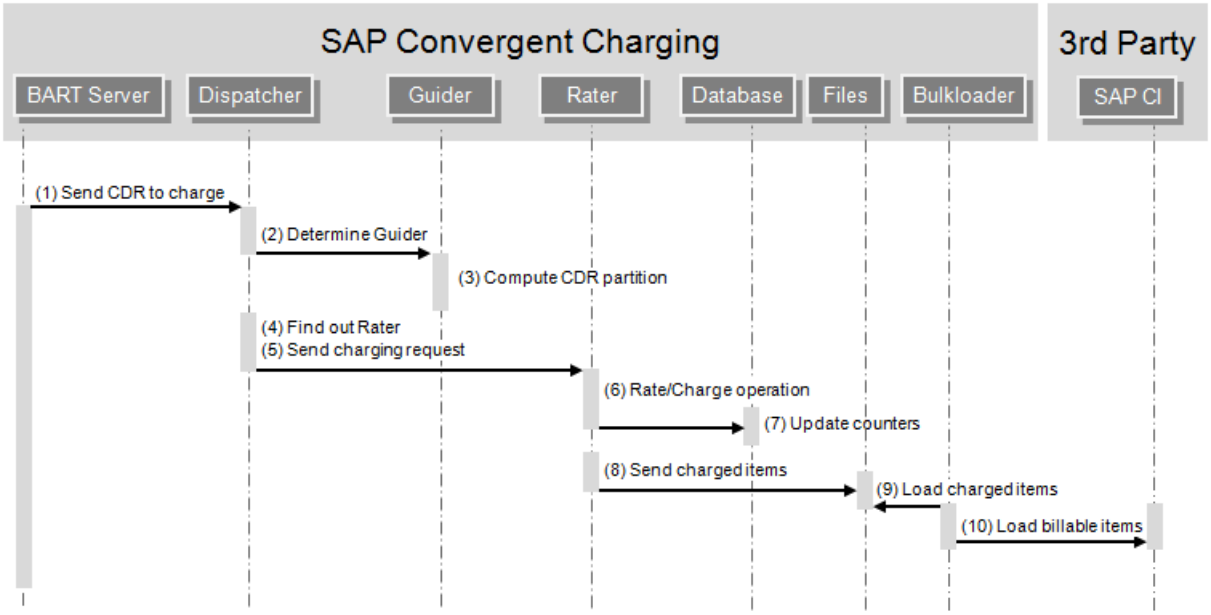
> **Note**
>
> For further information about these 2 processes, refer to the SAP Convergent Charging Application Help documentation.

4.1 Security during provisioning requests



Step	Description	Security Measure
1	A third party system like a CRM sends a request to create/change/cancel a SAP CC master data.	The third party system is authenticated with a login/password mechanism. Communication protocol : HTTPS
2	The request is processed by the Updater server instance.	Not applicable
3	The Updater server instance stores/updates the master data in the adequate database	Communication protocol: JDBC
4,5	The Updater server instance informs the Rater server instances that cached data must be updated	Communication protocol: TCP/IP
6,7	The Rater server instance updates its cached data with the new/updated master data	Communication protocol: JDBC

4.2 Security during charging requests



Step	Description	Security Measure
1	An injector sends a request to SAP Convergent Charging in order to charge a given chargeable item. This injector can be: • The SAP CC BART Server • The SAP CC Diameter Server • A network element able to generate such external events	
2	The Dispatcher server instance delegates the partition computation to a Guider server instance	

Step	Description	Security Measure
3	The Guider server instance computes the partition identifier	Not applicable
4	According to the determined partition identifier, the Dispatcher server instance finds out the Rater server instance in charge of the user who generated the chargeable item	Not applicable
5	The Dispatcher server instance delegates the chargeable item to the determined Rater server instance for charging purposes	
6	The Rater server instance rates the chargeable item and charges the user account(s) related to its service usage	Not applicable
7	The Rater server instance updates the counters and account balances to make them persistent	
8	The Rater server instance writes the charged items into files	Accesses to the files are limited using specific OS ACLs
9	The Bulkloader server instance reads the charged items files	
10	The Bulkloader server instance creates the billable items from the loaded charged items and sends them into SAP Convergent Invoicing	

5 User Administration and Authentication

SAP Convergent Charging does not use the user management and authentication mechanisms provided with the SAP platforms.

5.1 User Management

User management within SAP Convergent Charging uses proprietary mechanisms: user data, user roles, tools, user types and password policies. For an overview of these mechanisms, refer to the adequate section below. In addition, a list of the standard users required for operating the SAP CC systems is provided.

5.1.1 User Management Tools

The table below shows the different tools which can be used to manage and administrate users within SAP CC:

Tool	Activity	Description
Core Tool	User data management	SAP CC user creation, modification, and deletion
	User management	User lock and unlock
Admin+	System configuration	User password policy management
	User management	User work session control and management

User data is stored in the Core database by the SAP CC Core Server. There is no data replication.

If another component of SAP CC 4.0 requires user authentication services, it must connect to the SAP CC Core Server system or to an intermediate server. The Core Server system then manages the authentication and answers to the authorization request.

> **Note**
>
> For further information about the tasks and procedures related to user management, refer to the SAP Convergent Charging Configuration Guide documentation.

5.1.2 User Types

It is often necessary to specify different security policies for different types of users.
For example, your policy may specify that:

- Individual users performing interactive asks have to change their passwords on a regular basis and the storage of their password in the database must be secured
- Users under which background processing jobs run must not change their password and the storage of their password in the database can be less secured in order to get better performances when calling CC APIs

> **Note**
>
> Individual users often choose passwords they can easily remember. Those passwords can be vulnerable and their storage in the database must thus be as secured as possible. On the contrary, passwords used for systems securing do not have to be remembered, and shall thus be as strong as possible.

To handle such situations, two different types of users exist:

- **Individual users**, which correspond to users able to log on to the different user interfaces (desktop and console applications) according to their associated roles
- **Service users**, which correspond to users used for low-level operations such as services querying, communication protocols, background tasks, OS accesses, and so on

> **Note**
>
> For individual users, SAP CC can control user work sessions to limit the simultaneous connections to a given graphical user interface. For further information about this concept, refer to the SAP Convergent Charging Configuration Guide documentation.

5.1.3 Password Management Policy

SAP CC 4.0 gives you the possibility to configure and apply a security policy for managing the user passwords.

As of SAP CC 4.0 SP07, the algorithm used for hashing passwords is SHA-256. 128-bit random salt is used for prefixing the passwords before hashing.

The table below shows the possible settings for defining your password policy:

Processing Mode	Description
Password Mandatory	Enable or disable the password management policy. By default, passwords are mandatory.
Password Different from Login	This setting gives the possibility to specify that passwords must not contain the login (user name). It is automatically activated if the “Password Mandatory” setting is enabled.
Password Minimum Length	This setting gives the possibility to specify a minimum length for passwords. It is thus highly linked to the “Password Complexity” setting described below.
Password Complexity	This setting gives the possibility to specify the type of characters that must be present at least once in the password. It is possible to force the use of upper case letters, lower case letters, digits and special characters. Parameter format: It consists of a comma separated list that can contain the

Processing Mode	Description
	values “uppercase”, “lowercase”, “digit” and “special”.
Password Failed Login Limit	This setting gives the possibility to specify the maximum number of failed login attempts which are allowed for both individual and service users. When this number is reached, the user is locked and cannot be used anymore until an administrator unlocks it.
Password Duration Limit	This setting gives the possibility to specify the expiration time (in days) for passwords. When this period is reached, concerned passwords are expired and must be changed.
Password Change Delay	This setting gives the possibility to specify the number of days until which a password cannot be modified.
Password Reuse Delay	This setting gives the possibility to specify the number of days until which a password cannot be reused.
Password Reuse Cycle	This setting gives the possibility to specify the number of password modifications which must be done until which an already used password can be used again.
Force Password Modification at Next Logon	This setting gives the possibility to specify that a user must change his password when connecting to any tool of the SAP Convergent Charging solution or when using an API directly.
User Account Locking Policy	This setting gives the possibility to specify a maximum number of days between 2 logins. Users whose last login timestamp exceeds this period of time must be locked.
Apply Password Expiration and Locking Policy	This setting gives the possibility to enable or disable the expiration and locking setting for a given user.
Password Hash Rounds	This setting gives the possibility to specify the number of rounds of the SHA-256 algorithm that must be applied for hashing passwords to be stored in the database. **Caution** As this number of rounds is applied each time Web Services or HCI are used, it has an impact on the performance. By default, at installation, the value is set to 10,000 rounds for both individual and service users, but we recommend using a lower value for service users such as 1,000 or even 100 to reduce the impact on performances.

Note

For further information about user management, role assignment and password policy specificities, refer to the SAP Convergent Charging Configuration Guide documentation.

5.1.4 Required Users

To install and run the SAP Convergent Charging solution, multiple users are required.
These users are considered as:

- Standard users, which represent the users that must be created to start and run the different deployed components of the solution
- Third parties users, which represent the users required by the different third party systems used in conjunction with the solution, such as databases and operating systems

5.1.4.1 Standard Users

The following standard users must be manually created during the post-installation phase and granted with the appropriate roles:

- **SAP CC super administrator and emergency user** (identifier: “admin”)
  Created at installation time by SAPinst, this individual and service user represents the default user granted with all the available roles. This user is named “admin” and is associated to a default “admin” password, which must be changed for security reasons. During the post-installation phase, it is highly recommended to create all the necessary users in SAP Convergent Charging and then delete this user.

  
  Caution

  Note that it is possible to recreate or reset this user in case of emergency situation. For further information about the emergency recovery procedure, refer to the SAP Convergent Charging Configuration Guide available on the SAP Service Marketplace portal.

- **SAP CC landscape administrator(s)**
  Created during the post-installation phase, this individual user must be granted with the “Administrator” role.
- **SAP CC user administrator(s)**
  Created during the post-installation phase, these individual users must be granted with the “User Administrator” role.
- **SAP CC power user (s)**
  Created during the post-installation phase, these individual users must be granted with the “CSR” or “Marketing” roles.
- **SAP CC user(s) for data provisioning**
  Optionally created during the post-installation phase, these service users must be granted with the “Customer Sales Representative” role in order to create and maintain SAP CC data in: subscriber accounts, provider contracts, subscriptions and price tables. Ex.: a service user for the communication with a CRM system.
- **SAP CC user(s) for catalog transport**
  Optionally created during the post-installation phase, these service users must be granted with the “Administrator” role and must not be associated to a catalog. These users can be used by other SAP CC systems (including the SAP CC CTS plugin) when configuring transport destinations as part of catalog transport operations to the current SAP CC system.

- **SAP CC BART Server individual user(s)**
  Created during the post-installation phase (when the BART Server component is deployed), these individual users must be granted with the "Batch Rating Administrator" role in order to connect to the BART user interfaces (BART+ Tool and BART Tool).
- **SAP CC Core Server and BART Server service user(s)**
  Created during the post-installation phase, these service users must be granted with the "Process Manager" role, and should not be concerned by the password management policy to avoid runtime problems such as password expiration or user locking.
- **SAP CC Remote Support User(s)**
  Optionally created during the post-installation phase, these individual users must be granted with the "Remote Support" role. These users can be used for remote support access to SAP CC.

> **Note**
>
> For further information about the authorization concept and the role definitions, refer to the next chapter of this document.

5.1.4.2 Third Parties Users

The following third parties users must be created in the relevant third party systems during the pre-installation phase and granted with the appropriate rights or roles:

- **SAP system administrator(s)** (identifier: "sapadm" or "<system_ID>adm", e.g. "cc4adm")
  Created at installation time by SAPinst, this individual user concerns the operating system of the SAP CC solution.
- **SAP service user for a system** (identifier: SAPService<SYSTEM_ID>", e.g. "SAPServiceCC4")
  Created at installation time by SAPinst, this individual user concerns the operating system of the SAP CC solution for Microsoft Windows platforms only.
- **SAP CC Core Database administrator**
  This individual user concerns the RDBMS which hosts the SAP CC Core database.
- **SAP CC Core database user** (e.g. "DBUser")
  Created at installation time by SAPinst, this service user concerns the RDBMS which hosts the SAP CC Core database.
- **SAP CC BART database administrator**
  Created when the BART Server component is deployed, this individual user concerns the RDBMS which hosts the SAP CC BART database.
- **SAP CC BART database user** (e.g. "DBUser")
  Created at installation time by SAPinst (when the BART Server component is deployed), this service user concerns the RDBMS which hosts the SAP CC BART database.
- **SAP CC web service user**
  This service user must be used by any third party application which needs to execute operations in SAP CC using the available Web Services technical interface. It must correspond to an SAP CC user granted with the adequate roles, and associated to a given pricing catalog.

- **SAP CC SLD user**
  This service user concerns the System Landscape Directory for Netweaver system, and should be created before the installation of the SAP CC solution.
- **SAP CC JCo user for communications with SAP ERP (*)**
  This service user is used to communicate with an SAP ERP/FI-CA system in an integrated SAP Solution scenario with SAP Convergent Invoicing. This user should be created in each SAP ERP system before the installation of the SAP CC software component. This user must have the following attributes:
  - User Type: "C Communications Data"
  - Profile with authorization objects: F_KKBIXBIT, F_KKBIXCON, S_TABU_DIS, and S_RFC
- **SAP CC JCo user for communications with SAP CRM (*)**
  This service user is used to communicate with an SAP CRM system in an integrated SAP Solution scenario. It should be created in each SAP CRM system before the installation of the SAP CC software component.
- **SAP CC Solution Manager user**
  Granted with no role, this technical user concerns the SAP Solution Manager system, and must be created when enabling the Customer Usage Measurement mechanism within SAP CC.

> **Note**
>
> For further information about the communications performed through the RFC over TCP/IP communication channel, refer the “Communication Destinations” section afterwards.

5.2 Integration into Single Sign-On Environments

In addition to the default Username Token security profile, the SAP Convergent Charging software also supports an A2A SSO mechanism to authenticate users consuming Web Services. This SSO mechanism only concerns the SOAP over HTTP communication channel, and is based on the SAML Token security profile which consists in transporting an SAML token (generated by a client application acting as a STS) into the header of SOAP messages.

> **Note**
>
> The SSO mechanism can be activated or deactivated using the "WS_SSO_ENABLED" administration parameter. When activated, both Username Token and SAML Token security profiles are available to transport information related to users consuming Web Services. For backward compatibility purposes, it is possible to deactivate the SSO mechanism, and provide information related to users by only using the Username Token security profile, For further information about this administration parameter, refer to the SAP Convergent Charging Parameter Reference documentation.

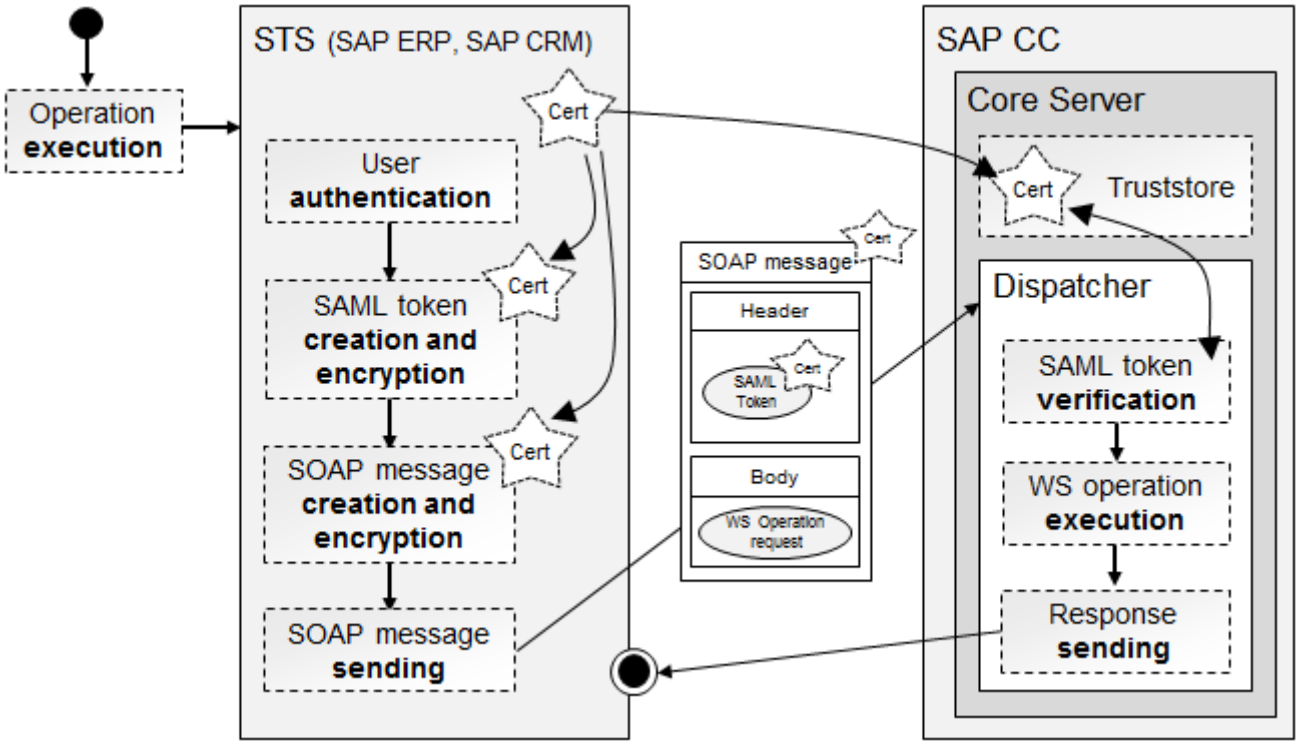
5.2.1 SAML Sender Vouches with Certificates

When the SSO mechanism is activated, integrity of SOAP messages is protected using the SAML Sender Vouches authentication method. This method relies on the use of a certificate, provided by the client application (acting as a STS) and attesting the identity of the user requesting the execution of a Web Service. This certificate is used:

- To encrypt the SAML token generated by the client application
- To encrypt some elements of the SOAP message (such as the web service operation request)
- By the SAP CC WS server to trust the client application and retrieve the information of the SOAP message

When a user executes an operation using a client application (acting as a STS), it is first authenticated by the client application. In case of positive authentication, an SAML token is created and encrypted using the certificate of the STS. This token is then inserted in the header of the SOAP message sent to SAP CC using the SOAP over HTTP communication channel. When SAP CC receives the SOAP message, it checks the identity of the STS by using the certificate registered in its truststore. In case of positive identification, SAP CC verifies the SAML token, executes the requested operation, and finally returns the response to the client application.

The following schema summarizes these interactions between a user, a STS and SAP CC:



Notes

- The certificates of every client application acting as a STS must be imported into the truststore of the SAP Convergent Charging solution. To import such certificates, it is necessary to use the "certentry" target of the Setup Tool in order to link the concerned certificates to the "sts" service type. For further information about the Setup Tool and its available targets, refer to the SAP Convergent Charging User Interfaces documentation

- The SAP Convergent Charging solution only supports the SAML Sender Vouches authentication method. **The SAML Holder-Of-Key authentication method is not supported**

5.2.2 User management

As described in the User Administration and Authentication section above, the SAP Convergent Charging solution manages a proprietary list of owners, granted with specific roles and authorizations. When using SSO to execute an operation of a given Web Service, it is thus necessary to ensure that the client application (acting as a STS) transports the identity of a user which is known by SAP CC and granted with the adequate role in order to execute the operation.

> **Note**
>
> No dedicated mechanism is available to replicate users into SAP CC. **It is thus highly recommended to ensure that all the users whose identity is sent by the client application (acting as a STS) using SSO are created in SAP CC before executing an operation of a Web Service.**

6 Authorizations

The authorization concept of SAP CC is based on:

- Configured roles which provide authorizations to perform certain operations. Every SAP user can be associated to one or more roles which correspond to predefined levels of authorization
- Data access restrictions which constrain an SAP CC user to work with the master data objects of the same owner. The available operations depend on the role(s) granted to the user

6.1 Standard Roles

Standard roles are configured by default in the system with the relevant authorizations.
The table below shows the standard roles that are defined for the SAP CC users (individual or service):

Role	Description
Administrator	This role gives the possibility to perform administration actions such as user creation, system configuration, change lists transport operations, batch operations execution, and so on. As a consequence, this role must be carefully used and modified. **Note** To ensure a global coherency, users granted with the "Administrator" role cannot be updated by users granted with lower roles
Batch Rating Administrator	This role gives the possibility to connect to the BART user interfaces (BART+ and BART Tool) and thus perform all actions related to batch operations.
Connector Administrator	This role concerns the IEC optional standalone element of the SAP Convergent Charging solution. It gives the possibility to execute scenarios using the remote mode of the IEC, both from the CAT Tool user interface or from the IEC command-line tool.
Customer Sales Representative	This role gives the possibility to entirely manage data related to the business agreements' domain (provider contract, subscriptions, subscriber accounts), and display additional catalog objects such as charges, charge plans, offers, and so on.
Marketing	This role gives the possibility to entirely manage data related to the catalog' domain, such as charges, refill logic, charge plans and refill plans, offers, and so on.
Process Manager	This role gives the possibility to use web services in order to execute business and technical operations such as subscription and/or provider contract activation, charged item bulk loading, and so on.
User Administrator	This role gives the possibility to perform actions related to the "users" domain, such as users' creation/deletion, password modification and roles allocation.
Remote Support	This role gives read-only rights on the data and configuration of SAP CC and does not

Role	Description
	allow performing any changes. This role also gives the possibility to access to the windows dedicated to the Data Auditing feature available in the Core Tool user interface.

> **Note**
>
> The roles which are available in SAP CC can be assigned to new or existing SAP Users using the File → New (or Open) → User menu of the Core Tool user interface. For further information about Core Tool, refer to the SAP Convergent Charging Online Help documentation

6.2 Roles and Authorizations

According to the roles, different actions can be performed on technical and business objects (master data, business data). The table below shows these authorizations:

	Adm.	User Adm.	Batch Rating Adm.	CSR	Market.	Connector Adm.	Process Manager	Remote Support
Allowance event class			RO	RO	RW			RO
Allowance interface			RO	RO	RW			RO
Allowance logic			RO	RO	RW			RO
Allowance plan			RO	RO	RW			RO
Audit mngt	RW						RW	RO
Accesses mngt			RO	RW				RO
Batch rating groups mngt			RW	RO	RW			RO
Billable item mapping mngt			RO	RO	RW			RO
Catalog mngt	RO	RO	RO	RO	RW			RO
CDR mngt			RW					RO
Chargeable item packages mngt			RO	RO	RW			RO
Charges mngt			RO	RO	RW			RO
Charge plans mngt			RO	RO	RW			RO
Charged item class mngt			RO	RO	RW			RO
Counter dictionary mngt			RO	RO	RW			RO
Customer management area	RW			RO	RO			RO
Spending status descriptions mngt			RO	RO	RW			RO
Currencies mngt	RO	RW	RO	RO	RW			RO
Mapping table class mngt			RO	RO	RW			RO
Mapping table mngt			RO	RW	RW			RO
Monitoring plans mngt			RO	RO	RW			RO
Object change logs								RO

	Adm.	User Adm.	Batch Rating Adm.	CSR	Market.	Connector Adm.	Process Manager	Remote Support
Object snapshots								RO
Offers mngt			RO	RO	RW			RO
Pricing macros mngt			RO	RO	RW			RO
Provider contracts mngt			RO	RW				RO
Public holidays mngt					RW			RO
Range table class mngt			RO	RO	RW			RO
Range table mngt			RO	RW	RW			RO
Rating sessions mngt			RW				RW	RO
Refill item classes mngt			RO	RO	RW			RO
Refill logic mngt			RO	RO	RW			RO
Refill plans mngt			RO	RO	RW			RO
Refill record classes mngt			RO	RO	RW			RO
Scenarios mngt (CAT, IEC)						RW		RO
Subscriber accounts mngt				RW				RO
Subscriber mapping table mngt			RO	RW				Ro
Subscriber range table mngt			RO	RW				RO
Subscriptions mngt			RO	RW				RO
Tier tables mngt			RO	RO	RW			RO
Translation tables mngt			RO	RO	RW			RO
Change list mngt	RW				RW			RO
Transport request mngt	RW				RW			RO
Users and Roles mngt	RW	RW						RO
Administration								
Bulk operations	RW				RW			
Administration operations *	RW	RW	RO	RO	RO	RO	RW	
Metrics management	RW						RW	RO
Rerating management	RW		RW					RO
Solution configuration	RW	RO	RO	RO	RO	RO	RO	RO
Web Services								
Catalog Management								
Charge plan class display			RO	RO	RO			RO
Refill plan class browsing			RO	RO	RO			RO
Monitoring plan class display			RO	RO	RO			RO
Mapping table mngt			RO	RW	RW			RO
Range table mngt			RO	RW	RW			RO
Subscriber Account Management								
Subscriber accounts mngt			RO	RW				RO

	Adm.	User Adm.	Batch Rating Adm.	CSR	Market.	Connector Adm.	Process Manager	Remote Support
External accounts mngt			RO	RW				RO
Prepaid accounts mngt			RO	RW				RO
Subscriber Mapping Table Management								
Subscriber mapping tables				RW				RO
Subscriber Range Table Management								
Subscriber range tables				RW				RO
Charging Contract Management								
Charging contract mngt				RW				RO
Refill Management								
Prepaid account retrieval				RO				RO
Prepaid account refill				RW				
Business Job Management								
Rating sessions launch	EX						EX	
Charging contracts bulk activation	EX						EX	
Subscriptions bulk activation	EX						EX	
Charged items load	EX						EX	
Job status read	RO						RO	RO
Chargeable Items Charging								
Chargeable items charging							EX	
Chargeable Items Rerating								
Charging contract locking							EX	
Charging contract unlocking							EX	
Dependent charging contract finding							RO	
Charging contract restoration point finding							RO	
Charging contract restoration							EX	
Chargeable item recharging							EX	
Recharging process preparation							EX	
Activation								
Charging contract activation	EX						EX	
Allowance Management								
Find allowances				RO				RO

	Adm.	User Adm.	Batch Rating Adm.	CSR	Market.	Connector Adm.	Process Manager	Remote Support
Transport of Catalog Data								
Change list applying	EX							

RO: Read Only mode, RW: Read Write mode, EX: Execution mode

* No role can access to all the administration operations (a given role can only access to a part of the operations).

6.3 Critical Combinations

It is technically possible to grant a user with multiple roles. This situation is considered as a critical role combination and can lead to involuntary operations such as data deletion.

> **Caution**
>
> SAP SE highly recommends that you create multiple SAP users with different roles instead of a single user with multiple roles.

6.4 Master Data Access Restriction

You can associate an SAP CC user to a particular pricing catalog of a service provider.
The user can only access to:

- Master data belonging to this pricing catalog, which correspond to:
  - Charges
  - Charge plans
  - Charged item classes
  - Offers
  - Mapping table classes
  - Mapping tables
  - Range table classes
  - Range tables
  - Tier tables
  - Translation tables
  - Pricing macros
  - Refill item classes
  - Refill logic
  - Refill plans
  - Refill record classes
  - Monitoring plans

- Allowance event classes
- Allowance logic
- Allowance plans

- Master data related to the end customers of this service provider (catalog's owner), which correspond to:
  - Subscriber accounts
  - Subscriber mapping tables
  - Subscriber range tables
  - Subscriptions
  - Provider contracts

> **Note**
>
> The restriction does not apply to the business data such as billable item mapping, public holidays, counter name dictionary, and currencies.

7 Network and Communication Security

The network infrastructure plays an important role in protecting your system. Your network needs to support the communication that is required for your business without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both operating system and application levels) or network attack such as eavesdropping. If users cannot log on to your application or database servers at the operating system or database layer then there is no way for intruders to compromise the machines and gain access to the backend system's database or files. Additionally, if users are not able to connect to the server LAN, they cannot exploit well-known bugs and security holes in network services on the server machines.

The network topology for SAP CC relies on typical client/server architecture, with additional specificities described in the following sections:

- **Communication Channel Security**
  This section describes the communication paths and protocols used by SAP CC.
- **Network Security**
  This section describes the recommended network topology for SAP CC. It shows the appropriate network segments for the various client and server components and where to use firewalls for access protection. It also includes a list of the ports needed to operate SAP CC.
- **Communication Destinations**
  This section describes the information needed for the various communication paths, such as which users are used for which communications.

7.1 Communication Channel Security

The communication between deployed components of SAP CC relies on 5 different protocols:

- HTTP
  - Used to transport SOAP messages (Web Services technical interface)
  - Used to transport proprietary XML messages (HTTP Communication Interface)
- TCP/IP, used to transport proprietary TCP Packets, either internally between server instances or externally between the deployed components
- UDP, used to transport messages dedicated to network discovery purposes
- JDBC, used to communicate with running RDBMS
- Diameter, used to communicate with network elements

The communication between the deployed components of SAP CC can be secured in order to fit the security policy of your landscape. To secure the different communication channels, refer to the "Securing SAP CC" procedure available in the SAP Convergent Charging Application Help documentation.

Caution

When securing components of SAPCC, it is highly recommended to ensure that the data remains encrypted whatever the communication channel is used. Mixing encrypted and unencrypted communication channels is not recommended.

7.1.1 SOAP over HTTP

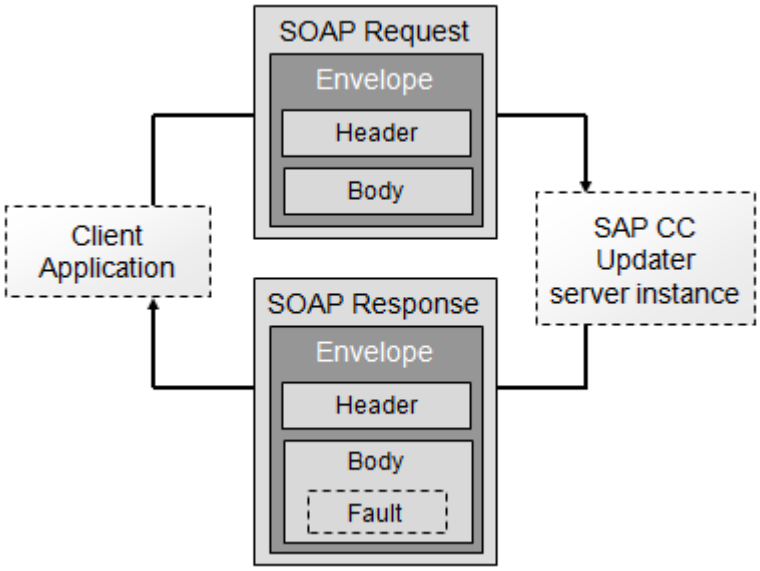
SAP CC provides a Web Services technical interface based on SOAP and HTTP standards. This interface gives the possibility for the SAP CRM or ERP systems to consume web services and thus execute specific operations.

To communicate with the published web services, client applications send SOAP messages to the Updater server instance using the HTTP protocol. These messages have an XML format, and contain the following elements:

- An **envelope**, which defines an XML document as a SOAP message and represents its root
- A **header**, which contains application-specific related to the SOAP message. It gives the possibility to specify all additional information which could be necessary to execute the request, such as:
  - Authentication information
  - Payment information
  - Request processing rules
  - Metadata related to the message
  - SOAP extensions
  - SAP passport
  - And so on
- A **body**, which contains the actual SOAP message intended for the ultimate endpoint of a message. This body section of a request message must contain:
  - The name of the targeted method
  - All mandatory and/or optional parameters related to the targeted method

    Note

    The body section of a response message can contain:
    - A simple answer
    - A new method call
    - A detailed error message, which is itself an XML element (named “Fault”) made up with sub elements providing information about the error



7.1.1.1 Web Service Security (WS-Security)

SAP CC does not implement the whole specifications of the OASIS standard named Web Service Security (in its 1.0 version). The security of SAP CC web services relies on the following security profiles:

- **SAML Token**, when the SSO mechanism is activated. For further information about SSO, refer to the adequate section below
- **Username Token**, which consists in sending the following information into the header of SOAP messages:
  - A **username**, which must correspond to an existing user of SAP CC, granted with the adequate roles and authorizations related to the execution of web services operations
  - A **password**, which is sent in clear text

> **Caution**
>
> When using the Username Token security profile, passwords are transported in a clear text format. **It is thus highly recommended to activate the encryption of HTTP connections when using the Username Token security profile.**

> **Notes**
>
> - The Username Token security profile is available for backward compatibility reasons
> - The encryption of the HTTP connections used during the execution of web services is automatically activated if the encryption is activated for the HCI communications.

Example 1

The following XML code represents a skeleton of a SOAP request sent by a client application to the SAP CC Updater server instance, using the Username Token security profile:

```
<?xml version="1.0"?>
<soapenv:Envelope ...>

   <soapenv:Header>
      <wsse:Security ... >
         <wsse:UsernameToken ... >
            <wsse:Username>USERNAME</wsse:Username>
            <wsse:Password ... >PASSWORD</wsse:Password>
         </wsse:UsernameToken>
      </wsse:Security>
   </soapenv:Header>

   <soapenv:Body>
     <soap:Fault>
     ...
     </soap:Fault>
   </soapenv:Body>

</soapenv:Envelope>
```

Example 2

The following XML code represents a skeleton of a SOAP request sent by a client application to the SAP CC Updater server instance, using the SAML Token security profile:

```
<?xml version="1.0"?>
<soapenv:Envelope ... >

   <soapenv:Header>
      <wsse:Security ... >
         <wsse:BinarySecurityToken ... />
         <saml:Assertion ...>
            ...
            <saml:AuthenticationStatement ... >
               <saml:Subject>
                  <saml:NameIdentifier ... >USERNAME</saml:NameIdentifier>
                  <saml:SubjectConfirmation>
                      <saml:ConfirmationMethod>
                          urn:oasis:names:tc:SAML:1.0:cm:sender-vouches
                      </saml:ConfirmationMethod>
                  </saml:SubjectConfirmation>
               </saml:Subject>
            </saml:AuthenticationStatement>
         </saml:Assertion>
      </wsse:Security>
   </soapenv:Header>

   <soapenv:Body>
     <soap:Fault>
     ...
```

```
      </soap:Fault>
    </soapenv:Body>

</soapenv:Envelope>
```

Note

The Fault element is a WSS standard element which exists in case of failed authentication. This element contains a reason and an associated message which provide information about the failure.

7.1.1.2 Channel Encryption

To increase the security level of communications relying on XML SOAP messages, it is possible to use HTTPs, which corresponds to the secured version of the HTTP protocol. This protocol represents a combination of the HTTP with the SSL/TLS protocols used to provide encryption and secure identification between network elements. HTTPS connections are often used for sensitive transactions in corporate information systems and are based on certificate authorities that users can rely on.

The secured version of HTTP is activated by default to secure the SAP CC XML requests and responses. For further information, refer to the "Securing SAP CC" procedure available in the SAP Convergent Charging Application Help documentation.

7.1.1.3 Known Limitations

The WSS freshness time period mechanism (materialized by the Created element of the UsernameToken element) is not taken into account in SAP CC, even if this SOAP message's creation timestamp is provided.

7.1.1.4 Endpoints

SAP CC provides several endpoints to access and implement Web Services and related operations available in the system landscape. Every endpoint represents a URI which respects the following format (case sensitive content):

http(s)://<INSTANCE_ADDRESS>:<INSTANCE_PORT_NB>/[v<WS_VERSION>/]<WS_TECH_NAME>

Where:

- **<INSTANCE_ADDRESS>** is the network address (DNS name or the IP address) of the host machine of the active Updater instance or Dispatcher instance of the SAP CC Core Server system
- **<INSTANCE_PORT_NB>** is the port number dedicated to the Web Services communications for the target instance
- **<WS_TECH_NAME>** is the technical name of the Web Service (process component)
- **<WS_VERSION>** is the version of the Web Service (optional, only required when accessions versions greater than 0). Each new version of a given Web Service is incremented by 1, which guarantees backward compatibility regarding the previous version.

SAP CC provides the following Web Services:

- Master Data for Product Modeling
  - **Catalog Management**, used to manage the commercial products through combinations of charge plan classes and refill plan classes, and partially manage the pricing catalog stored in SAP CC for a service provider
- Customer Master Data
  - **Subscriber Account Management**, used to configure and maintain master data related to the end customers' accounts and pricing information related to the business partners and business agreements
  - **Charging Contract Management** , used to configure and maintain master data related to end customers' contracts and pricing information stored in SAP CC
  - **Subscriber Mapping Table Management,** used to manage the subscriber mapping tables belonging to a subscriber account as part of the customer master data. Subscriber mapping tables are end customer data that can be shared between some of the charging contracts belonging to the same subscriber account
  - **Subscriber Range Table Management**, used to manage the subscriber range tables belonging to a subscriber account as part of the customer master data. Subscriber range tables are end customer data that can be shared between some of the charging contracts belonging to the same subscriber account
- Customer Data Migration
  - **Prepaid Account State Management**, used to manage the states of prepaid accounts in subscriber accounts which have been migrated to SAP Convergent Charging
  - **Charging Contract State Management**, used to manage the states of charging contracts which have been migrated to SAP Convergent Charging
- Business Processing
  - **Charging** , used to manage charging services of chargeable items
  - **Recharging**, used to manage recharging operations on chargeable items.
  - **Refilling** , used to manage refill services of prepaid accounts
  - **Activation**, used to activate a charging contract, including all the associated charging contracts in case a parent/linked relationship exists
  - **Allowance Management**, used to manage allowances associated to charging contracts
  - **Business Process Management**, used to manage business processes which can be triggered by an external application or system
- Restricted Services, which represent provided services and operations which can be used by other SAP applications, but not in an implementation project
  - **Data Export Management to SAP PSI**, used to export data (charge plans) to SAP Convergent Pricing Simulation (SAP PSI)
  - **Transport of Catalog Data**, used to transport catalog data from one SAP CC system to another

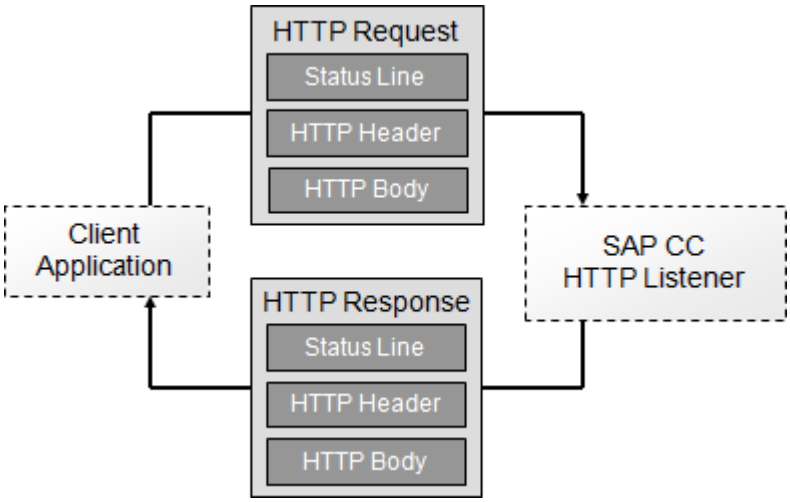
> **Note**
>
> For further information about the Web Services and their provided operations, refer to the SAP Convergent Charging SOAP Specifications documentation.

The following table summarizes the availability of the different Web Services:

Web Service	Technical Name	Hosted by	
		Dispatcher	Updater
Master Data for Product Modeling			
Catalog Management	/catalog		■
Customer Master Data			
Subscriber Account Management	/suacProvisioning		■
Charging Contract Management	/v2/contractProvisioning /v1/contractProvisioning /contractProvisioning		■
Subscriber Mapping Table Management	/subscriberMappingTableManagement		■
Subscriber Range Table Management	/subscriberRangeTableManagement		■
Customer Data Migration			
Prepaid Account State Management	/prepaidaccountstate		■
Charging Contract State Management	/contractstate		■
Business Processing			
Charging	/chargeableItemCharging	■	
Recharging	/recharging	■	
Refilling	/v1/refilling /refilling		■
Activation	/activation	■	
Allowance Management	/allowanceManagement	■	
Business Process Management	/rating		■
Restricted Services			
Data Export Management to SAP PSI	/IExporting		■
Transport of Catalog Data	/transport		■

7.1.2 XML over HTTP (HTTP Communication Interface - HCI)

SAP CC provides a proprietary communication interface (HCI) based on XML and HTTP standards. Client applications send XML proprietary messages to the deployed server instances using the HTTP protocol. HTTP requests and responses include a Status Line, a Header and a Body (which represents the real content of the HTTP request) separated by a Carriage Return (CR) followed by a Line Feed (LF).



7.1.2.1 HTTP request

The Status Line of a request consists in a token ended with a CRLF sequence and containing:

- A coding method (GET, POST, and so on depending on which method the addressed instance can deal with)
- The request URI (Universal Resource Identifier)
- The HTTP protocol version

> **Notes**
>
> - SAP CC only uses the POST method
> - SAP CC only uses the 1.1 version of the HTTP protocol (RFC 2616)

The Header part of a request contains the following information:

- **Host**: The host name and the port number used by the listener to receive incoming HTTP requests (format: <hostname>:<port>)
- **Content-Length**: The size (in bytes) of the HTTP request Body part
- **Content-Type**: A value which specifies that the message sent in the HTTP Body is XML-encoded (not URL-encoded). The value must be “text/xml”

The Body part of a request contains a XML stream commonly named “Message” or “XML message”. SAP CC XML messages are text-based and use the ISO 10646 character set in UTF-8 encoding (refer to the RFC 2279[21] for further details about this concept). Lines end with a CRLF sequence, but receivers should also be prepared to interpret CR and LF as line terminators separately. Text-based protocols make it easier to add optional parameters in a self-describing manner. Since the number of parameters and the frequency of commands are low, processing efficiency is not affected.

7.1.2.2 HTTP response

The Status Line of a response consists in a token ended with a CRLF sequence and containing:

- The HTTP protocol version
- A numeric status code:
  - 200 (Success), which means that the action was successfully received, read and accepted
  - 404 (Not Found), which means that the URI is erroneous
  - 500 (Internal Server Error), which means that a unidentified error occurred
  - 501 (Not Implemented), which means that a method different than POST has been used
- The textual signification of the numeric status code

The Header part of a response contains the following information:

- **Content-Type**: A value which specifies that the message sent in the HTTP Body is XML-encoded (not URL-encoded). The value must be “text/xml”
- **Content-Length**: The size (in bytes) of the HTTP response Body part
- **Connection status**: A “close” value which indicates that the connection will be closed after the completion of the response (the connection should not be considered as “persistent” after the current response is completed)

The Body part of a response is similar to the request Body part.
For further information about its content element, please refer above.

7.1.2.3 HCI envelope

HCI envelopes represent XML messages carried over the HTTP protocol inside the Body part of HTTP requests and responses. Each HCI envelope contains:

- A header
- A body

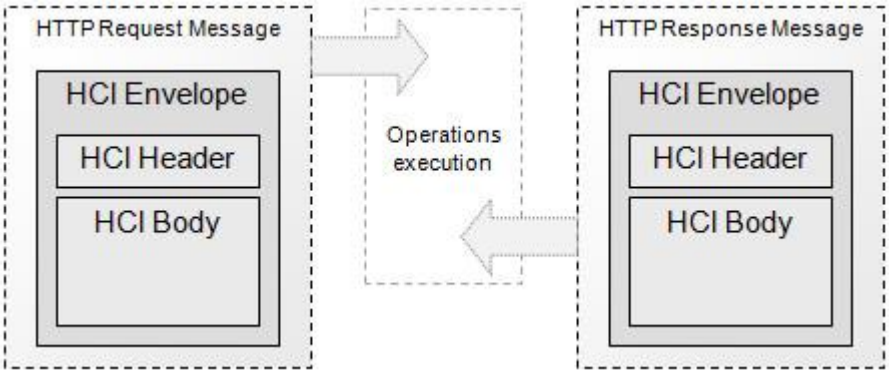
The following XML code represents a skeleton of a HCI envelope sent by a client application to the SAP CC Core server component:

```
<xs:element name="envelope">
 <xs:complexType>
  <xs:sequence>
    <xs:element ref="header" minOccurs="1" maxOccurs="1"/>
    <xs:element ref="body" minOccurs="1" maxOccurs="1"/>
  </xs:sequence>
 </xs:complexType>
</xs:element></soapenv:Envelope>
```

When a SAP CC HTTP listener receives an XML message, the following actions are performed:

- The different parts of the incoming XML message are analyzed
- The mandatory parts of this XML message are checked. If an error is detected, the message is rejected
- The identified HCI operations are executed

- A response XML message is sent back to the client



The Header part of a HCI envelope contains the following information:

- **Transaction type**: A value which specifies the strategy related to the HCI operations execution. Possible values are:

ALL	All or none of the operations are executed
FIRST-FAIL	All operations are executed and results committed into the database until the first fails
MOST	All operations are executed and valid results are committed into the database even if some of them failed
TRY	All operations are executed but results are rolled back. The database stays unchanged

- **Sender information**: Information related to the message sender (such as user name and clear password), used for authentication purpose to ensure that the sender is allowed to communicate with the listener (the sender is supposed to correspond to an existing user of SAP CC, granted with the adequate roles and authorizations)

```
<xs:element name="header">
 <xs:complexType>
  <xs:sequence>
    <xs:element
      ref="originator"
      minOccurs="1"
      maxOccurs="1"/>
</xs:sequence>
   <xs:attribute
      name="transaction"
      type="TransactionType"
      default="all"/>
 </xs:complexType>
</xs:element>
```

With the following substructures:

```
<xs:simpleType name="TransactionType">
  <xs:restriction base="xs:string">
    <xs:enumeration value="all"/>
    <xs:enumeration value="firstFail"/>
    <xs:enumeration value="most"/>
    <xs:enumeration value="try"/>
 </xs:restriction>
</xs:simpleType>
<xs:element name="originator">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="auth"/>
    </xs:sequence>
    <xs:attribute
        name="name"
        type="xs:string"/>
  </xs:complexType>
</xs:element>
<xs:element name="auth">
  <xs:complexType>
  <xs:attribute
      name="scheme"
      type="xs:string"
      default="simple"/>
```

	</xs:complexType> </xs:element>

The Body part of a HCI envelope contains the following information:

- **Operations** (only into HTTP request messages)
- **Results or Errors** (only into HTTP response messages)

The following XML code represents the Body part of a HCI envelope sent by a client application to the SAP CC Core server component:

```
<xs:element name="body">
  <xs:complexType>
    <xs:sequence>
      <xs:any minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
```

7.1.2.4 HCI operation

A HCI Operation is a set of instructions for actions such as creating, modifying or deleting data stored in a database. Every time a client application sends a HCI operation, the addressed listener executes it and sends back an HCI Operation Result. This operation result can be:

- A successful operation including an optional identifier
- An error describing the failed operation

Notes

- The same HCI envelope can include several HCI operations. When multiple operations must be executed, the returned HCI envelope includes the multiple related operation results (and associated error messages).
- A failed operation corresponds to an operation which returns an exception. Two types of exceptions can be considered:
  - Business exceptions, returned by business processes to indicate that an operation cannot be performed (for example, a cannotModifyException)
  - Server failure exceptions, which indicate that an issue occurred within SAP CC infrastructure (for example, a non-ready database, a locked resource, a HCI service violation, and so on)

Example 1

The following XML codes represent the HCI request and response related to a single HCI operation (creation of a subscriber account):

```
<envelope>
  <header ...> ... </header>
```

```
  <body> ...
     <createSubscriberAccount>
      <subscriberAccount code="FOO" vendor="BAR">
        . . .
      </subscriberAccount >
    </createSubscriberAccount>
</body>
</envelope>

<envelope>
    <header ...> ... </header>
    <body> ...
       <createSubscriberAccountResult reference="12345" code="FOO"/>
    </body>
</envelope>
```

Example 2

The following XML codes represent the HCI request and response related to multiple HCI operations (with a failure on the second operation, for example due to a wrong request's transaction type):

```
<envelope>
  <header ...> ... </header>
  <body> ...
     Operation1...
     Operation2...
     Operation3...
</body>
</envelope>

<envelope>
    <header ...> ... </header>
    <body> ...
       OperationResult1...
       ErrorFault2 (Operation2)...
       OperationResult3...
    </body>
</envelope>
```

7.1.2.5 Channel encryption

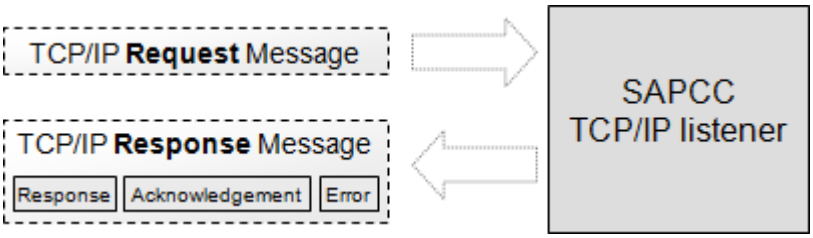
To increase the security level of communications relying on XML messages, it is possible to use HTTPs, which corresponds to the secured version of the HTTP protocol. This protocol represents a combination of the HTTP with the SSL/TLS protocols used to provide encryption and secure identification between network elements. HTTPS connections are often used for sensitive transactions in corporate information systems and are based on certificate authorities that users can rely on.

The secured version of HTTP is activated by default to secure the SAP CC XML requests and responses. For further information about the installation of the related certificates, refer to the "Securing SAP CC" procedure available in the SAP Convergent Charging Application Help documentation.

7.1.3 Packets over TCP/IP

To ensure better performances of the system during real-time charging operations, SAP CC uses proprietary packets which are transported over the TCP/IP protocol. These TCP/IP requests contain different information such as protocol version, length, type, topic, timeout, and so on. Each request waits for an expected response, which contains less information than the request, and can be:

- A normal response
- An acknowledgement to inform the client that the message has been received
- An error message if the request is not valid. This error message provides information about the reason of this error



Note

The Transmission Control Protocol / Internet Protocol (TCP/IP) is a suite of communication protocols used to connect different hosts over networks. These protocols define a standard for transmitting data over the World Wide Web.

TCP is considered as a transport method, particularly used when data coherence is required (because TCP ensures that data arrive intact and complete). The transported data are called “sockets” or “packets”, and the physical transport is ensured by the IP layer. The header prefixed to an IP packet contains not only source and destination addresses of the hosts, but source and destination addresses of the networks they reside in. Data transmitted using TCP/IP can be sent to multiple networks within an organization or around the globe via the Internet, the world's largest TCP/IP network. The terms "TCP/IP network" and "IP network" are thus synonymous.

7.1.3.1 Channel Encryption

As described above, communications relying on proprietary packets sent over TCP/IP both concern:

- Internal communications between server instances
- External communication between deployed components and/or client applications

To increase the security level of such communications, it is possible to secure these 2 communication interfaces. For further information, refer to the "Securing SAP CC" procedure available in the SAP Convergent Charging Application Help documentation.

> **Note**
>
> For performance reasons (as the encryption increases the size of the transported packets), it is not recommended to secure internal communication between server instances. Appropriate measures dedicated to the protection of network segments should be implemented instead.

7.1.3.2 Known Limitation

The size of the proprietary messages sent over TCP/IP cannot exceed 1 MB.

7.1.4 RFC over TCP/IP

SAP CC uses the standard SAP interface named Remote Function Call (RFC) to communicate over TCP/IP with the following SAP systems:

- SAP CRM
- SAP ERP

7.1.4.1 Channel Encryption

For security reasons, communications relying on RFC over TCP/IP are encrypted using the SAP Cryptographic Library.

> **Note**
>
> For general security information related to RFC over TCP/IP, refer to the RFC/ICF Security Guide on SAP Service Marketplace at https://service.sap.com/securityguide → SAP NetWeaver 7.0 Connectivity Security Guides → RFC/ICF Security Guide → RFC Scenarios → Communication Between SAP Systems and External (Non-SAP) Systems.

7.1.4.2 Communication Destinations

SAP CC uses the following RFC function modules, implemented by the different supported destinations:

- **BAPI_CURRENCY_GETLIST**, used to retrieve the list of currencies defined in the SAP ERP system
- **CRM_ISX_PPACC_ALERT_HANDLER**, used to transmit the business notifications about prepaid accounts (balance amount alert, account expiration alert) to SAP CRM

- **FKK_BIX_BIT_REVERSE_CC**, used to ask the appropriate SAP ERP/FI-CA system to cancel a billable item originally posted by SAP CC. This destination is only used in a rerating scenario based on BART Server
- **FKK_BIX_BIT_REVERSE_CHECK_CC**, used to check whether the rerating feature is supported by the ERP system that is responsible for canceling a set of billable items originally posted by SAP CC. This destination is only used in a rerating scenario based on BART Server (SAP CI and SAP ERP/FI-CA used as the billing system)
- **FKK_BIX_BITCAT_LIST_GET_SAPCC,** used to retrieve the list of billable item classes (released as productive) which have been created for SAP CC
- **FKK_BIX_BITCAT_STRUC_GET_API**, used to retrieve the technical definitions of a billable item class, such as the field names in the interface of the class
- **FKK_BIX_CITCAT_CC_PROXY_GET**, used to retrieve the technical definitions of a consumption item class (such as the field names in the interface of the class), and the expected mapping to be used by SAP CC
- **FKK_BIX_CITCAT_LIST_GET_SAPCC,** used to retrieve the list of consumption item classes (released as productive) which have been created for SAP CC
- **FKK_BIX_RERATE_SESSION**, used to manage a recharging session in SAP CC when the rerating operations are driven by SAP CI. This destination is only used in a rerating scenario based on SAP CI with the consumption item management function enabled
- **FKK_PREP_MESSAGE**, used to send notifications to SAP ERP when SAP CRM is not in the system landscape
- A dynamically allocated interface for the creation of consumption items (1 interface per consumption item class), named **/1FC/<name of CIT Class>_CIT_CREATE_PROXY**
- A dynamically allocated interface for the creation of billable items (1 interface per billable item class), named **/1FE/<name of BIT Class>_BIT_CREATE_API**

In addition to these RFC function, the SAP CC CT Server system implements the following RFC function modules, used by another SAP system, such as SAP CI:

- **RFC_CALCULATE_US_TELCOS_TAXES**, used to calculate the taxes relating to a transaction, with or without updating the tax journal
- **RFC_DETERMINE_LOCATION_CODE**, used to determine and return the location code of the taxing jurisdiction according to a given address
- **RFC_UPDATE_US_TELCOS_TAXES**, used to apply calculated taxes to a transaction by updating the tax journal. No tax is recalculated

Notes

- These destinations and functions can be configured:
  - Using Setup Tool for the SAP CC Core Server system
  - Within the “ct.config” configuration file for the SAP CC Communications Taxing Server system
- For more information about the RFC function modules used by the integration between SAP CC and SAP Convergent Invoicing in SAP ERP/FI-CA, consult the documentation of SAP Contract Accounts Receivable and Payable with SAP ERP release 6.0 EhP7 at http://help.sap.com/fi-cax-607 → Application Help (English) → SAP Convergent Invoicing → Integration with Other Components and Products →Integration with SAP Convergent Charging

The following table summarizes the availability and use of the implemented functions:

Function	Implemented by			Used by
	SAP CRM	SAP ERP	SAP CC CT Server	SAP CC Core Server
BAPI_CURRENCY_GETLIST		■		■
CRM_ISX_PPACC_ALERT_HANDLER	■			■
FKK_BIX_BIT_REVERSE_CC		■		■
FKK_BIX_BIT_REVERSE_CHECK_CC		■		■
FKK_BIX_BITCAT_LIST_GET_SAPCC		■		■
FKK_BIX_BITCAT_STRUC_GET_API		■		■
FKK_BIX_CITCAT_CC_PROXY_GET		■		■
FKK_BIX_CITCAT_LIST_GET_SAPCC		■		■
FKK_BIX_RERATE_SESSION		■		■
FKK_PREP_MESSAGE		■		■
RFC_CALCULATE_US_TELCOS_TAXES			■	
RFC_DETERMINE_LOCATION_CODE			■	
RFC_UPDATE_US_TELCOS_TAXES			■	
/1FC/<name of CIT Class>_CIT_CREATE_PROXY		■		■
/1FE/<name of BIT Class>_BIT_CREATE_API		■		■

7.1.5 Messages over UDP

Client applications and deployed server instances send UDP messages over the network in order to retrieve information about the available Dispatchers. These UDP requests are proprietary messages multicast over a given SAP CC system.

7.1.5.1 UDP request

Discovery requests are sent to multicast UDP/IPv4 or IPv6 addresses. These requests contain:

- The identifier of the requesting client
- The required interface which needs to be contacted:
  - Internal, which is only provided and thus available into the server instances of the SAP CC Core Server
  - External, which is provided by client applications
- The name of the concerned SAP CC system which needs to be contacted and analyzed

7.1.5.2 UDP response

Discovery responses must be sent back within a configurable response time set by default to 2 seconds. These responses are sent by all alive Dispatchers using the same multicast address, and contain the following information:

- The name of the belonging SAP CC system
- The identifier of the replying Dispatcher (dispatcher#XXX)
- The following information when an internal interface has been required in the discovery request:
  - An “internal” flag
  - The internal address (IPv4 or IPv6) of the Dispatcher
  - The internal port of the Dispatcher
- The following information when an external interface has been required in the discovery request:
  - An “external” flag
  - The external address (IPv4 or IPv6) of the Dispatcher
  - The external port of the Dispatcher

> **Note**
>
> In case of protocol error or failure, a specific invalid message is sent back to inform about the concerned error.

7.1.5.3 Channel encryption

The Messages over UDP channel **does not support encryption**, for both security reasons (to prevent UDP flood attacks) and technical aspects (as the UDP service is not mandatory to run a SAP CC system and not natively supported by JSE). **It thus should not be used on a public network**, and appropriate measures should be taken in order to protect the network segments which use this type of connection

7.1.6 Java Database Connectivity

The Java Database Connectivity is a Java-based data access technology provided by Sun Microsystems, Inc.. This technology represents a Java API which:

- Defines how a client may access a database
- Provides methods for querying and updating data in a database
- Is oriented towards relational databases

> **Note**
>
> The SAP CC system uses the 2.0 implementation of JDBC to interact with both Core and BART databases.

7.1.6.1 Channel encryption

To increase the security level of communications relying on the JDBC channel, it is possible to encrypt the connections to the databases. For further information about the encryption of the databases connections, refer to the "Securing SAP CC" procedure available in the SAP Convergent Charging Application Help documentation.

7.1.7 Diameter

The Diameter protocol is an Authentication, Authorization and Accounting (AAA) protocol which is used by client applications such as the Diameter Server component for purposes such as credit-control. It is based on the RFC 3588 which defines a state machine able to maintain connections between peers and processing messages.

7.1.7.1 Channel encryption

To secure the communications with network elements and relying on the Diameter protocol, it is possible to encrypt the connections to the Diameter Server component and activate a secured version of the Diameter Stack. For further information about the encryption of the Diameter communications, refer to the "Securing SAP CC" procedure available in the SAP Convergent Charging Application Help documentation.

7.2 Network Security

As described in the Technical System Landscape section, the deployed SAP CC components communicate together using different protocols. Each protocol uses dedicated ports which are configured at the installation time. The table below shows the list of ports used throughout the SAP Convergent Charging solution:

Component	Description
SAP CC Core Server	
• Core database	The **SAP CC Core Server** uses a port to connect to the Core database. This port can be configured to fit specific environment configurations, and is set by default to: • 3<INSTANCE_NUMBER>15 for SAP HANA databases, where <INSTANCE_NUMBER> is the instance number of the SAP HANA database (e.g. 30015 for the instance number 00) • 5000 for Sybase ASE databases • 4464 for DB2 databases • 1433 for Microsoft SQL Server databases • 1521 for Oracle databases Note

Component	Description
	If the Oracle RAC mechanism is deployed, a port must be configured for each RAC instance
• Updater instance	The following ports must be configured for each deployed instance: • **HTTP**, used by client applications which communicate with the Core Server using HCI operations • **Web Services** (called WSPort in the instance map), used by client applications for master data distribution or replication purpose
• Dispatcher instance	The following ports must be configured for each deployed instance: • **HTTP**, used by client applications for administration purposes • **Messages**, used by client applications for business purposes (charging, rerating, and so on) • **Internal Messages**, used by the other deployed server instances for internal communication purposes (admin, multicast, and so on)
• Other instances	Raters, Guiders, Taxers, and Bulkloaders server instances are automatically configured with the Internal Messages port used by the Dispatcher server instances.
• SMD web service	The SMD web service uses the HTTP port of the Dispatcher server instance and thus does not need any specific configuration
SAP CC BART Server	
• BART database	A port must be configured to connect to this database
• BART server	The following ports must be configured: • **HTTP**, used by client applications for administration purposes • **Messages**, used by client applications for CDR acquisition purposes
SAP CC Diameter Server	
• Diameter server	The SAP CC Diameter server uses 2 different ports: • **HTTP Dispatcher**, which is used to communicate with the Dispatcher instance of the SAP CC Core Server component. This port must be configured and must obviously correspond to the port of an existing deployed Dispatcher (as the Diameter server does not implement any discovery mechanism) • **Diameter**, which corresponds to the default 3868 port of the Diameter protocol. This port is not configurable
SAP CC Communication Taxing Server	
• JCO destination	A port is automatically provided to the SAP CC Communication Taxing server when it registers to the SAP Gateway application server. This port is thus not configurable.
SAP CC optional elements	

Component	Description
• IEC	The IEC component uses a default 9002 listening port in remote mode for receiving operation request from the CAT Tool user interface. This port can be specified on startup using a “-port” argument in the command line.

Note

Messages, internal messages and Diameter are not encrypted. It thus should not be used on a public network, and appropriate measures should be taken in order to protect the network segments which use this kind of connections. As a consequence, it is highly recommended to implement typical network security rules such as:

- Firewall rules creation to control the traffic
- NAT rules use to reduce ports exposure
- And so on

8 Data Storage Security and Privacy

The SAP Convergent Charging solution does not implement any specific security mechanism to protect the Core and BART databases. The following typical standard rules have been applied to secure the connection with the RDBMS:

- Every connection URL used to connect to a given database requires a login and a password
- Connections to the SAP CC tools are controlled and limited by the USER_SESSION_VALIDITY_PERIOD and USER_SESSION_SESSION_LIMIT_PER_USER_AND_TOOL parameters. These parameters give the possibility to specify the number of simultaneous connections to a given tool for a given user. Technically, it is thus possible to authorize multiple simultaneous connections, but this behavior should not be implemented as possibly leading to errors. **It is highly recommended to create multiple user accounts to differentiate the connections**.

In addition to these security rules applied on RDBMS connections, the following rules have been implemented to ensure confidentiality regarding person-related data:

- Only passwords are encrypted to limit their readability. No other data recorded in the Core and BART databases are encrypted
- To ensure confidentiality, no feature or process provided by the SAP Convergent Charging solution requires filling in person-related data. As a consequence, no specific mechanism has been implemented to filter and/or remove such data

9 Security-Relevant Logging and Tracing

Logging and tracing are key functions for securing your SAP CC system landscape. Logs are important to monitor the security of your SAP CC systems and to track events if problems occur. Logs can be used to monitor the correct usage of the systems.

The logging and tracing functions of the SAP Convergent Charging solution give you the possibility to generate and record logs and traces for events affecting all components of SAP CC. To facilitate information requirements for different levels of troubleshooting, logs are recorded by categories and traces by domains. During runtime, you can change the severity thresholds of logs and traces that are output.

Each record includes the identifier of the SAP user who requested an operation.

A subcategory is dedicated to security-relevant information in the log messages related to the system processing or to the business processing (application level).

You can use your log viewer to filter this information.

Example

An SAP Convergent Charging user has been locked due to too many logon attempts with an incorrect password.

Note

SAP Convergent Charging does not generate any other security relevant information in the trace messages.

For more information about specific topics, see the quick links as shown in the table below:

Content	Quick Link on SAP Service Marketplace
Logging and Tracing Functions	SAP CC Application Help
Monitoring	Operations Guide
Troubleshooting	Operations Guide
System Configuration	Configuration Guide

www.sap.com/contactsap