



Security Guide | PUBLIC

Document Version: 2020.0 – 2020-10-07

# Security Guide

# Content

<b>1</b>	<b>Before You Start. . . . .</b>	<b>4</b>
1.1	About This Document. . . . .	4
1.2	Target Audience. . . . .	5
1.3	What's New in This Document. . . . .	6
1.4	Additional Information. . . . .	6
1.5	Document Abbreviations. . . . .	7
1.6	Why is Security Necessary?. . . . .	7
<b>2</b>	<b>Technical System Landscape. . . . .</b>	<b>9</b>
2.1	SAP CC Architecture. . . . .	9
2.2	Configurations and Catalogue. . . . .	10
<b>3</b>	<b>Security Aspects of Cockpit and Apache Tomcat Server. . . . .</b>	<b>11</b>
3.1	Security Aspects of Cockpit. . . . .	11
3.2	Security Aspects of Apache Tomcat Server. . . . .	11
<b>4</b>	<b>Security Aspects of Data, Data Flow and Processes. . . . .</b>	<b>13</b>
4.1	Security during provisioning requests. . . . .	13
4.2	Security during charging requests. . . . .	14
<b>5</b>	<b>User Administration and Authentication. . . . .</b>	<b>16</b>
5.1	User Management and Authentication. . . . .	16
	User Management Tools. . . . .	16
	Security Profiles. . . . .	17
	Password Management Policy. . . . .	18
	Required Users. . . . .	19
5.2	Integration into Single Sign-On Environments. . . . .	22
	SAML Sender Vouches with Certificates. . . . .	22
	User Management. . . . .	24
<b>6</b>	<b>Authorizations. . . . .</b>	<b>25</b>
6.1	Standard Roles. . . . .	25
6.2	Roles and Authorizations. . . . .	26
6.3	Critical Combinations. . . . .	31
6.4	Master Data Access Restriction. . . . .	31
<b>7</b>	<b>Network and Communication Security. . . . .</b>	<b>33</b>
7.1	Communication Channel Security. . . . .	33
	SOAP over HTTP. . . . .	34

	REST over HTTP. . . . .	43
	XML over HTTP (HTTP Communication Interface - HCI). . . . .	46
	JSON over HTTP. . . . .	51
	Packets over TCP/IP. . . . .	51
	RFC over TCP/IP. . . . .	52
	Messages over UDP. . . . .	55
	Java Database Connectivity. . . . .	56
7.2	Network Security. . . . .	56
<b>8</b>	<b>Data Storage Security. . . . .</b>	<b>60</b>
<b>9</b>	<b>Data Protection and Privacy. . . . .</b>	<b>61</b>
<b>10</b>	<b>Security-Relevant Logging and Tracing. . . . .</b>	<b>62</b>

# 1 Before You Start

[About This Document \[page 4\]](#)

[Target Audience \[page 5\]](#)

[What's New in This Document \[page 6\]](#)

[Additional Information \[page 6\]](#)

[Document Abbreviations \[page 7\]](#)

[Why is Security Necessary? \[page 7\]](#)

## 1.1 About This Document

### → Remember

The commands used in this guide have been tested in the different scenarios with the dedicated tools. However, using these tools is not mandatory: other tools are available according to your preferences. In this case, the commands may differ.

The Security Guide provides an overview of the security-relevant information that applies to SAP Convergent Charging, referred to as SAP CC within 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.
<a href="#">Technical System Landscape [page 9]</a>	This section provides an overview of the technical components and communication paths that are used by SAP CC.

Section Title	Content Description
<a href="#">Security Aspects of Data, Data Flow and Processes [page 13]</a>	This section provides an overview of the security aspects within SAP CC through data flows related to the 2 main processes of the solution.
<a href="#">User Administration and Authentication [page 16]</a>	This section provides an overview of the user and authentication management.
<a href="#">Authorizations [page 25]</a>	This section provides an overview of the authorization concepts related to SAP CC.
<a href="#">Network and Communication Security [page 33]</a>	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.
<a href="#">Data Storage Security [page 60]</a>	This section provides an overview of any critical data that is used by SAP CC and the security mechanisms that apply.
<a href="#">Data Protection and Privacy [page 61]</a>	This section provides information about the management of personal data
<a href="#">Security-Relevant Logging and Tracing [page 62]</a>	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.

## 1.2 Target Audience

This guide is intended for the following audiences:

- Security Experts
- Security Auditors
- Application and System Administratorss
- Support Specialist (SAP SE, Local Support Team)s

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.

## 1.3 What's New in This Document

### What's New in FPS 0 ?

SAP Convergent Charging 2020 provides you with the following modifications of this documentation:

- New app in **Cockpit** dedicated to the pricing configuration: [Manage Rate Plans](#)

## 1.4 Additional Information

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

Content	Quick Link
SAP CC documentation	<a href="https://help.sap.com/cc50">help.sap.com/cc50</a>
	<b>i Note</b> SAP CC is part of the SAP solution SAP Billing based on SAP Business Suite or SAP S/4 HANA. Consult the central solution information at the following address: <a href="https://cx.sap.com/fr/products/billing">https://cx.sap.com/fr/products/billing</a>
Related SAP notes	<a href="https://support.sap.com/notes">support.sap.com/notes</a> Please consult in particular the following SAP Notes: <ul style="list-style-type: none"><li>• <a href="#">1394093</a> (Collective Security Note)</li><li>• <a href="#">1702364</a> (Convergent Charging Integration with Convergent Invoicing)</li></ul>
SAP Solution Manager	<a href="http://support.sap.com/solutionmanager">http://support.sap.com/solutionmanager</a>

## 1.5 Document Abbreviations

Abbreviation	Meaning
A2A	Application To Application
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	Relational Database Management System
RFC	Remote Function Call
SAML	Security Assertion Markup Language
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSL	Secure Socket 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

## 1.6 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.

## **Meeting Your Own Security Requirements: Security Policy**

Your security requirements are not limited to SAP Convergent Charging, but apply to your entire system landscape. Therefore, we recommend establishing a security policy that reflects the security issues that apply at a company-wide level. Your security policy should cover aspects such as:

- User authentication
- Authorizations
- Data integrity
- Data Storage Security
- Data Protection and Privacy
- Auditing
- Logging

Once you have established your security policy, use this guide to implement and enforce security for SAP Convergent Charging.



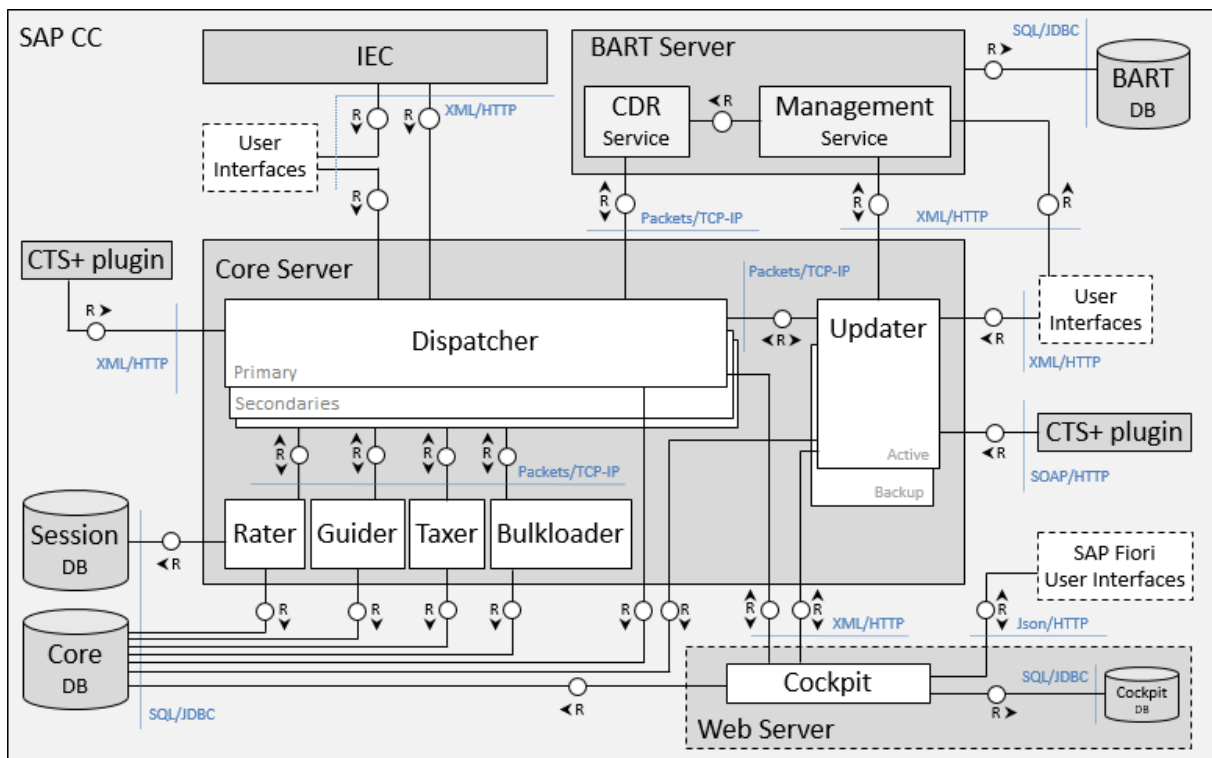
## 2 Technical System Landscape

[SAP CC Architecture \[page 9\]](#)

[Configurations and Catalogue \[page 10\]](#)

### 2.1 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 system landscape:



As described above, the 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 Import/Export Connector**, used to consolidate and schedule data transfers between SAP CC and third-party systems
- **SAP CC Cockpit**, running within a web server and provided applications that give the possibility to manage the SAP CC Core Server system and business objects quickly and efficiently
- **SAP CC user interfaces**, 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 rating (dynamic pricing) and charging operations. They communicate through different communication channels such as:


- [SOAP over HTTP \[page 34\]](#), used for Web Services operations
- [XML over HTTP \(HTTP Communication Interface - HCI\) \[page 46\]](#), based on XML proprietary messages
- [JSON over HTTP \[page 51\]](#), used for communication between the SAP Fiori user interfaces and the Cockpit element
- [Java Database Connectivity \[page 56\]](#), used for communication with databases
- And so on

For further information about these communication channels, refer to the [Network and Communication Security \[page 33\]](#) section of this document.

### **i 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.

## **2.2 Configurations and Catalogue**

For a complete list of the supported platforms, see SAP Support Portal at the following location: [support.sap.com/pam](https://support.sap.com/pam) .

## 3 Security Aspects of Cockpit and Apache Tomcat Server

[Security Aspects of Cockpit \[page 11\]](#)

[Security Aspects of Apache Tomcat Server \[page 11\]](#)

### 3.1 Security Aspects of Cockpit

Cockpit is a Web application (.war) based on the SAP Fiori/SAP UI5 infrastructure which is designed for supporting your security requirements.

Moreover, all the security measures related to the Web contents and to the Java scripts delivered by Cockpit, have been implemented within the Cockpit application.

However, the Apache Tomcat Server that is recommended and used for running Cockpit, is not shipped with SAP Convergent Charging and must be installed/deployed/secured by the IT administrator within an MZ area (that corresponds to the same secured area of your landscape than the one used to install the Core Server system).

If Cockpit is accessible from the Internet, please note that the individual user used to administrate Cockpit is subject to the Password Management Policy, described in the [Password Management Policy \[page 18\]](#) dedicated section afterwards. In particular, this user can be locked after a given number of failed logon attempts, a situation that may occur in case the login has been stolen or unveiled, and improperly used by a person with dubious intentions.

#### **i** Note

You install and deploy a secured Tomcat Server for each Cockpit application you want to secure. For further information, refer to the [SAP CC 2020 Installation and Maintenance Guide](#) documentation.

### 3.2 Security Aspects of Apache Tomcat Server

To ensure a high level of security, the Cockpit application natively:


- Manages Cross-Site Request Forgery (CSRF) vulnerabilities to prevents cross-site attacks
- Sets the `X-XSS-Protection` flag of the HTTP<sup>1</sup> responses headers to `1; mode=block` in order to enables XSS filtering and sanitize pages in case a cross-site scripting attack is detected
- Sets the `X-Frame-Options` flag of the HTTP responses headers to `SAMEORIGIN` in order to avoid click-jacking attacks

- Sets the `X-Content-Type-Options` flag of the HTTP responses headers to `nosniff` in order to avoid MIME-type sniffing attacks
- Sets the `HTTPOnly` flag for cookies used to store the session IDs

In addition, SAP SE recommends that you consider the following security measures for the Cockpit application and the configuration of its Apache Tomcat Server:

- To fully prevent cross-site attacks, activate the Cross-Origin Resource Sharing (CORS) Tomcat filter
- To protect the communication channels, activate the support of SSL/TLS in Tomcat in order to:
  - Run the Cockpit application in a secured mode within the user's browser
  - Secure communications between the Cockpit application and the Core Server system

For further information, refer to the [Securing Communications with Cockpit and Tomcat Server](#) procedure available in the [SAP CC 2020 Installation and Maintenance Guide](#) documentation and to the Apache Tomcat Server documentation.

Complete these security recommendations by defining and applying additional security measures based on your experience or global security policy. In particular, please ensure that your browser respects the Content Security Policy (CSP) implemented by the Apache Tomcat Server. For further information, refer to the dedicated documentation reference available on the following address: <https://content-security-policy.com>.

---

<sup>1</sup> HyperText Transfer Protocol

## 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 figures in the two next topics 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

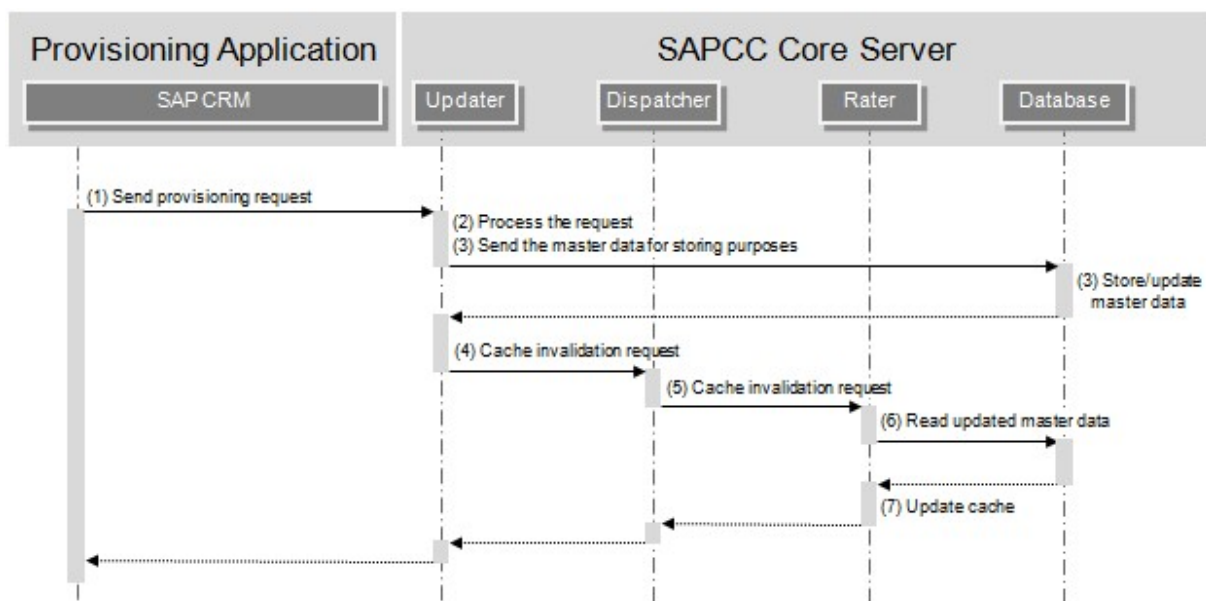
### i Note

For further information about these 2 processes, refer to the [SAP CC 2020 Application Help](#) documentation.

[Security during provisioning requests \[page 13\]](#)

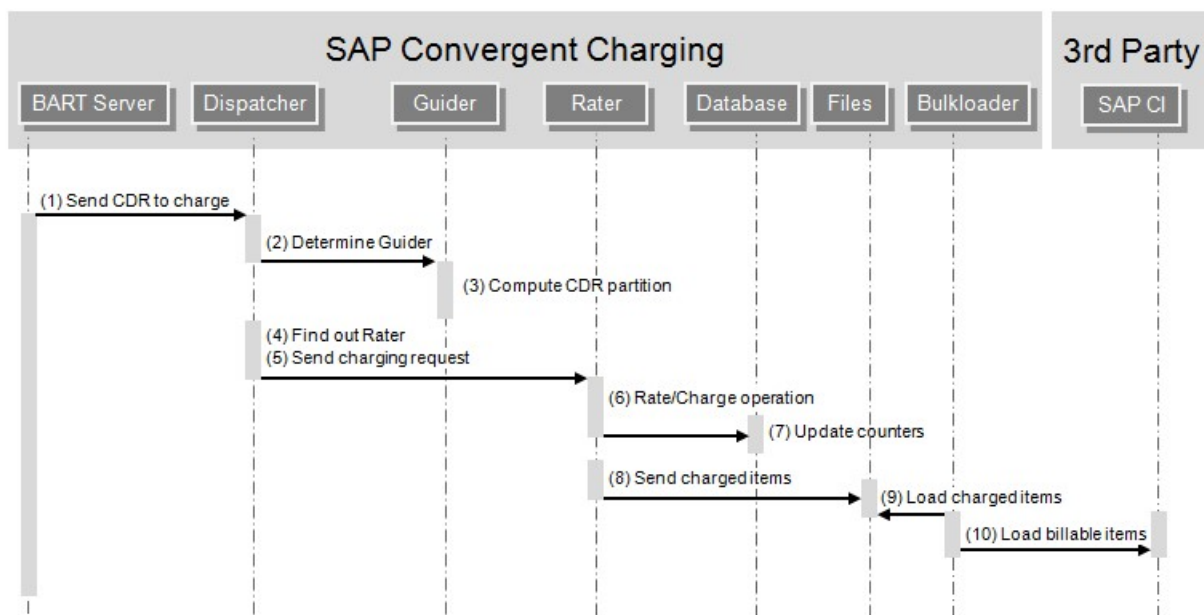
[Security during charging requests \[page 14\]](#)

### 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 request is authenticated with the logon and password mechanism.  Communication protocol: HTTPS <sup>2</sup>
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 <sup>3</sup>
4,5	The updater server instance informs the rater server instances that cached data must be updated	Communication protocol: TCP/IP <sup>4</sup>
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



<sup>2</sup> HyperText Transfer Protocol Secured

<sup>3</sup> Java Database Connectivity

<sup>4</sup> Transmission Control Protocol / Internet Protocol

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: <ul style="list-style-type: none"> <li>• The BART Server</li> <li>• A network element able to generate such external events</li> </ul>	
2	The dispatcher server instance delegates the partition computation to a guider server instance	
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 ACL <sup>5</sup> s
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	

<sup>5</sup> Access Control List

## 5 User Administration and Authentication

### i Note

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

[User Management and Authentication \[page 16\]](#)

[Integration into Single Sign-On Environments \[page 22\]](#)

### 5.1 User Management and Authentication

User management within SAP Convergent Charging uses proprietary mechanisms and tools to manage users' data, roles, 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.

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 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.

#### 5.1.1 User Management Tools

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

Tool	Activity	Description
<a href="#">Core Tool</a>	User data management	SAP CC user creation, modification, and deletion
	User management	User lock and unlock
<a href="#">Admin+</a>	System configuration	Definition of the user password policy
	User management	<ul style="list-style-type: none"><li>• User work session control and management</li><li>• User isolation</li></ul>
<a href="#">Cockpit</a>	System configuration	Definition of the user password policy
<a href="#">SCIM</a> <sup>6</sup>	User data management	SAP CC user creation and deletion by external systems

<sup>6</sup> System for Cross-domain Identity Management



### i Note

For further information about the tasks and procedures related to user management, refer to the [SAP CC 2020 Tuning Guide](#) documentation.

## 5.1.2 Security Profiles

According to business requirements, it is often necessary to define different security policies for the users of your system, such as:

- The validity, the rollover policy or the complexity of the users' passwords
- The encryption level of these passwords
- The scope of accessible elements for each type of user

To handle such situation, SAP Convergent Charging handles security profiles that are associated to 2 different types of users:

- Individual users, whose passwords are encrypted and must be regularly changed
- Service users, whose passwords are less secured (for performance reasons) and never expire

### i 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
- SAP CC also gives the possibility to control work sessions of individual users in order to limit the simultaneous connections to a given graphical user interface. For further information about this concept, refer to the [SAP CC 2020 Tuning Guide](#) documentation.

Usually, individual users correspond to users able to log on to the different user interfaces (desktop applications and command-line tools, and Web applications), whereas service users are used for low-level operations such as Web Services operations, OS accesses, communication with third-party applications, and so on.

Before SAP CC 4.1 SP 1, both service users and individual users were allowed to execute Web Services and HCI<sup>7</sup> operations, and launch the SAP CC user interfaces.

As of SAP CC 4.1 SP 1, the management of users within SAP Convergent Charging has evolved. A new system parameter named [USER\\_ISOLATION\\_ENABLED](#) has been introduced in order to specify whether service users must be isolated from individual users, or not. Isolating users guarantees that:

- Web Services operations can only be executed specifying a service user
- HCI operations can only be executed specifying an individual user
- User interfaces can only be launched specifying an individual user

---

<sup>7</sup> Http Communication Interface

## 5.1.3 Password Management Policy

In addition to the security profiles, SAP CC 2020 gives you the possibility to configure and apply a security policy for managing the user passwords (which are prefixed with a 128-bit random salt and then hashed using an SHA-256 algorithm).

Passwords are case sensitive.

### **i** Note

When the password management policy is enabled, every individual user whose password has been modified will have to modify again this password, by himself at the next logon to a SAP CC user interface.

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, and must not contain the user name (user ID) that is the logon.
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 values "uppercase", "lowercase", "digit" and "special".
Password Failed Logon Limit	This setting gives the possibility to specify the maximum number of failed logon 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 (related to individual users only). 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.
User Account Locking Policy	This setting gives the possibility to specify a maximum number of days between two logons. Users whose last logon timestamp exceeds this period of time must be locked.
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.

## i Note

For further information about user management, role assignment and password policy specificities, refer to the [SAP CC 2020 Tuning 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 the appropriate roles:

- **SAP CC super administrator and emergency user** (identifier: "admin")  
Created at installation time by the SAP installer, this individual user represents the default user granted 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 SAP Note [1890952](#).

- **SAP CC landscape administrator(s)**  
Created during the post-installation phase, these individual users must be granted the "Administrator" role.
- **SAP CC user administrator(s)**  
Created during the post-installation phase, these individual users must be granted the "User Administrator" role.
- **SAP CC Cockpit administrator**  
Created during the post-installation phase, this individual user must be granted the "Administrator" or "Remote Support" roles.
- **SAP CC Cockpit power user(s)**  
Created during the post-installation phase, this individual user must be granted the "Marketing" role.
- **SAP CC Cockpit user(s) for Processing Chargeable Items**  
Created during the post-installation phase, this service user must be granted the "Message Charging Client" role. Enables Cockpit users to use the Process a Chargeable Item app.

- **SAP CC power user(s)**  
Created during the post-installation phase, these individual users must be granted the "CSR<sup>8</sup>" or "Marketing" roles.
- **SAP CC user(s) for data provisioning**  
Optionally created during the post-installation phase, these service users must be granted the "Customer Sales Representative" role in order to create and maintain SAP CC data in: subscriber accounts, provider contracts, subscriptions and price tables (for example, a service user for the communication with a CRM<sup>9</sup> system).
- **SAP CC user(s) for users provisioning**  
Optionally created during the post-installation phase, this service user must be granted the "User Administrator" role in order to allow the use of the SCIM<sup>10</sup> API<sup>11</sup>.
- **SAP CC user(s) for catalog transport**  
Optionally created during the post-installation phase, these service users must be granted 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 the "Batch Rating Administrator" role in order to connect to the BART user interfaces (BART+ and BART Tool).
- **SAP CC BART Server service user(s)**  
Created after installing Core Server and before installing BART Server, these service users must be granted the roles "Process Manager" and "Message Charging Client".
- **SAP CC Diameter Server service user(s)**  
Created after installing Core Server and before installing Diameter Server, these service users must be granted the "Message Charging Client" role.
- **SAP CC Core Server service user(s)**  
Created during the post-installation phase, these service users must be granted the "Process Manager" role.
- **SAP CC Remote Support User(s)**  
Optionally created during the post-installation phase, these individual users must be granted the "Remote Support" role. These users can be used for remote support access to SAP CC.

## i Note

- SAP CC user names are case sensitive. If the system landscape includes an SQL Server RDBMS<sup>12</sup>, consult the [SAP CC 2020 Installation and Maintenance Guide](#) documentation
- For further information about the authorization concept and the role definitions, refer to the dedicated [Roles and Authorizations \[page 26\]](#) section of this document

<sup>8</sup> Customer Service Representative

<sup>9</sup> Customer Relationship Management

<sup>10</sup> System for Cross-domain Identity Management

<sup>11</sup> Application Programming Interface

<sup>12</sup> Relational Database Management System

## 5.1.4.2 Third-Party Users

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

- **SAP system administrator(s)** (identifier: "sapadm" or "<system\_ID>adm", e.g. "cc4adm")  
Created at installation time by the SAP installer, 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 the SAP installer, this individual user concerns the operating system of the SAP CC solution for Microsoft Windows platforms only.
- **SAP CC administrator of the Core Database**  
This individual user concerns the RDBMS<sup>13</sup> which hosts the SAP CC Core Database.
- **SAP CC Cockpit user for the Core Database**  
Optionally created during the post-installation phase, this service user must be granted a read access to database views pointing on the `FILE_METADATA` and `FILE_METADATA_PATH` tables.
- **SAP CC user for the Core Database** (e.g. "DBUser")  
Created at installation time by the SAP installer, this service user concerns the RDBMS which hosts the SAP CC Core Database.
- **SAP CC administrator of the BART Database**  
Created when the BART Server component is deployed, this individual user concerns the RDBMS which hosts the SAP CC BART Database.
- **SAP CC user for the BART Database** (e.g. "DBUser")  
Created at installation time by the SAP installer (when the BART Server component is deployed), this service user concerns the RDBMS which hosts the SAP CC BART Database.
- **SAP CC user for web services**  
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 the adequate roles, and associated to a given pricing catalog.
- **SAP CC user for SAP System Landscape Directory**  
This service user concerns the SAP 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`

### i Note

For further information about the communications performed through the RFC<sup>14</sup> over TCP/IP<sup>15</sup> communication channel, refer the [dedicated section \[page 52\]](#) afterwards.

- **SAP CC JCo user for communications with SAP CRM**

<sup>13</sup> Relational Database Management System

<sup>14</sup> Remote Function Call

<sup>15</sup> Transmission Control Protocol / Internet Protocol

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.

#### **i Note**

For further information about the communications performed through the RFC over TCP/IP communication channel, refer the [dedicated section \[page 52\]](#) afterwards.

- **SAP CC user for SAP Solution Manager**

Granted 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.

- **OS user of the Tomcat Server dedicated to SAP CC Cockpit**

This individual or service user runs the Tomcat Server where the Cockpit user interface is deployed. The user account relates to the operating system of Tomcat host. This OS<sup>16</sup> user owns the Tomcat process or service. The user is associated to the configuration of the installed Web applications. For further information, refer to the [SAP CC 2020 Installation and Maintenance Guide](#) documentation.

## **5.2 Integration into Single Sign-On Environments**

In addition to the default Username Token security profile, SAP Convergent Charging also supports an A2A<sup>17</sup> SSO<sup>18</sup> mechanism to authenticate users consuming Web Services. This SSO mechanism only concerns the SOAP<sup>19</sup> over HTTP<sup>20</sup> communication channel and is based on the SAML Token security profile which consists in transporting an SAML<sup>21</sup> token (generated by a client application acting as a STS<sup>22</sup>) into the header of SOAP messages.

#### **i Note**

- SAP Convergent Charging supports the 1.1 and 2.0 versions of the SAML standard
- 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 CC 2020 System Parameter Reference](#) documentation.

### **5.2.1 SAML Sender Vouches with Certificates**

When the SSO<sup>23</sup> mechanism is activated, integrity of SOAP<sup>24</sup> messages is protected using the SAML<sup>25</sup> Sender Vouches authentication method. This method relies on the use of a certificate, provided by the client

---

<sup>16</sup> Operating System

<sup>17</sup> Application To Application

<sup>18</sup> Single Sign-On

<sup>19</sup> Simple Object Access Protocol

<sup>20</sup> HyperText Transfer Protocol

<sup>21</sup> Security Assertion Markup Language

<sup>22</sup> Security Token System

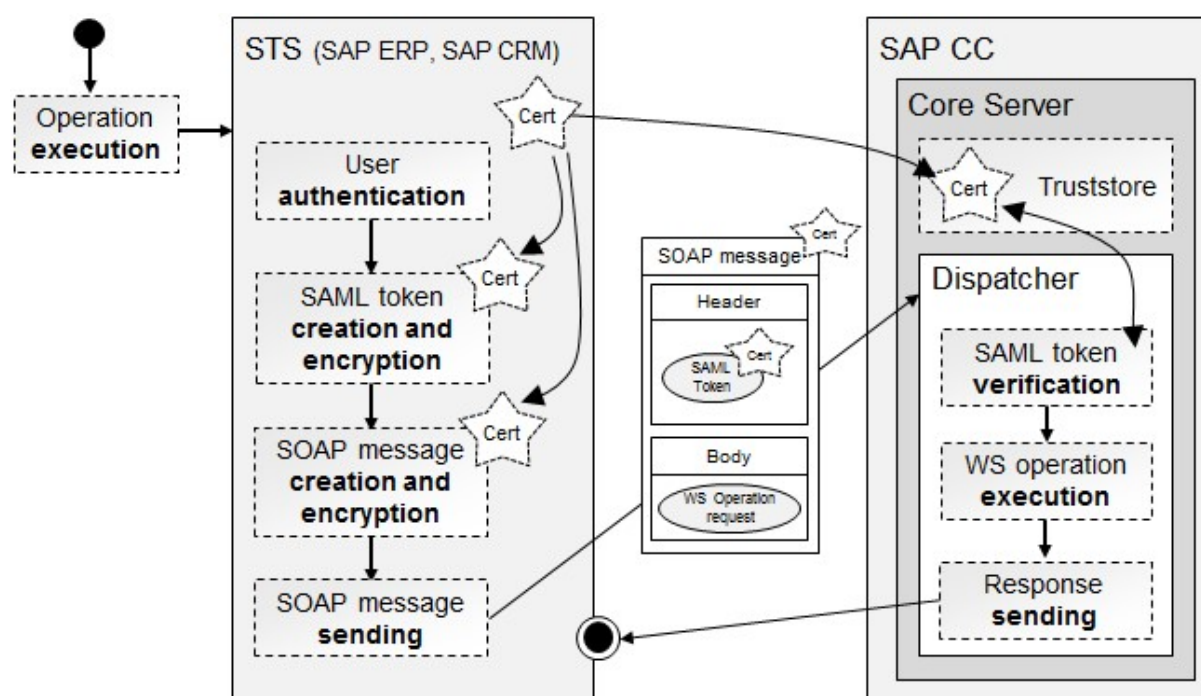
application (acting as a STS<sup>26</sup>) and attesting the identity of the user requesting the execution of a Web Service. This certificate is used:

- 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 WS server of SAP CC 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 \[page 34\]](#) 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 result, SAP CC:

- Verifies the signature of the SAML token
- Verifies the identity of the user specified within the SAML token
- Checks the roles granted to this user

When all these conditions are fulfilled, SAP CC executes the requested operation, and finally returns the response to the client application.



### Note

- The certificates of every client application acting as a STS must be imported into the truststore of SAP Convergent Charging. To import such certificates, it is necessary to use the "certentry" target of the [Setup Tool](#) user interface in order to link the concerned certificates to the "sts" service type. For further

<sup>23</sup> Single Sign-On

<sup>24</sup> Simple Object Access Protocol

<sup>25</sup> Security Assertion Markup Language

<sup>26</sup> Security Token System

information about Setup Tool and its available targets, refer to the [SAP CC 2020 Setup Tool](#) documentation

- SAP Convergent Charging 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 \[page 16\]](#) section above, SAP Convergent Charging manages a proprietary list of owners, granted specific roles and authorizations. When using SSO<sup>27</sup> to execute an operation of a given Web Service, it is thus necessary to ensure that the client application (acting as a STS<sup>28</sup>) transports the identity of a user which is known by SAP CC and granted the adequate role in order to execute the operation.

### i 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 within SAP CC before executing an operation of a Web Service.**

---

<sup>27</sup> Single Sign-On

<sup>28</sup> Security Token System



## 6 Authorizations

The authorization concept of SAP Convergent Charging is based on:

- Configured roles which provide authorizations to perform certain operations. Every SAP CC user can be associated to one or more roles which correspond to predefined levels of authorizations and permitted operations.
- 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

[Standard Roles \[page 25\]](#)

[Roles and Authorizations \[page 26\]](#)

[Critical Combinations \[page 31\]](#)

[Master Data Access Restriction \[page 31\]](#)

### 6.1 Standard Roles

Standard roles are configured by default in the system with the relevant authorizations and permitted operations.

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, <b>this role must be carefully used and modified.</b>
<div><div>i Note</div><div>To ensure a global coherency, users granted the "Administrator" role cannot be updated by users granted lower roles</div></div>	
Batch Rating Administrator	This role gives the possibility to connect to the BART user interfaces ( <a href="#">BART+</a> and <a href="#">BART Tool</a> ) and thus perform all actions related to batch operations.
Connector Administrator	This role concerns the IEC <sup>29</sup> 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 <a href="#">CAT Tool</a> 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.

<sup>29</sup> Import/Export Connector

Role	Description
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 allow performing any changes. This role also gives the possibility to access to the windows dedicated to the auditing functions available in the <a href="#">Core Tool</a> user interface to view object change logs and audited user operations.

### 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 CC 2020 Primary Help for Core Tool](#) 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 following tables shows these authorizations:

- [Operations](#) [page 26]
- [Administration](#) [page 28]
- [Web Services](#) [page 29]
- [Cockpit Apps](#) [page 30]

### Operations

	Adm.	User Adm.	Batch Rating Adm.	CSR <sup>30</sup>	Market.	Con- nector Adm.	Process Man- ager	Remote Support
Allowance event class			RO	RO	RW			RO
Allowance interface			RO	RO	RW			RO
Allowance logic			RO	RO	RW			RO

<sup>30</sup>

Customer Service Representative

	Adm.	User Adm.	Batch Rating Adm.	CSR <sup>30</sup>	Market.	Con- nector Adm.	Process Man- ager	Remote Support
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
Consumption item mapping mngt			RO	RO	RW			RO
Counter dictionary mngt			RO	RO	RW			RO
Customer management area	RW			RO	RO			RO
Currencies mngt	RO	RO	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
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

	Adm.	User Adm.	Batch Rating Adm.	CSR <sup>30</sup>	Market.	Con- nector Adm.	Process Man- ager	Remote Support
Spending status descriptions mngt			RO	RO	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

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

## Administration

	Adm.	User Adm.	Batch Rating Adm.	CSR	Market.	Con- nector Adm.	Process Man- ager	Remote Support
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

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).

## Web Services

	Adm.	User Adm.	Batch Rating Adm.	CSR	Market.	Con- nector Adm.	Process Man- ager	Remote Support
<b>Catalog Management</b>								
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
<b>Subscriber Account Management</b>								
Subscriber accounts mngt			RO	RW				RO
External accounts mngt			RO	RW				RO
Prepaid accounts mngt			RO	RW				RO
<b>Subscriber Mapping Table Management</b>								
Subscriber mapping tables				RW				RO
<b>Subscriber Range Table Management</b>								
Subscriber range tables				RW				RO
<b>Charging Contract Management</b>								
Charging contract mngt				RW				RO
<b>Refill Management</b>								
Prepaid account retrieval				RO				RO
Prepaid account refill				RW				
<b>Business Job Management</b>								
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
<b>Chargeable Items Charging</b>								
Chargeable items charging							EX	
<b>Chargeable Items Rerating</b>								
Charging contract locking							EX	
Charging contract unlocking							EX	
Dependent charging contract finding							RO	

	Adm.	User Adm.	Batch Rating Adm.	CSR	Market.	Con- nector Adm.	Process Man- ager	Remote Support
Charging contract restoration point finding							RO	
Charging contract restoration							EX	
Chargeable item recharging							EX	
Recharging process preparation							EX	
<b>Activation</b>								
Charging contract activation	EX						EX	
<b>Allowance Management</b>								
Find allowances				RO				RO
<b>Transport of Catalog Data</b>								
Change list applying	EX							
<b>Echo</b>								
Echo	EX						EX	

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

## Cockpit Apps

	Adm.	User Adm.	Batch Rating Adm.	CSR	Market.	Con- nector Adm.	Process Man- ager	Remote Support
<b>Pricing Configuration</b>								
Manage Chargeable Item Classes					RW			RO
Manage Charged Item Classes					RW			RO
Manage Mapping Table Classes					RW			RO
Manage Mapping Tables					RW			RO
Manage Range Table Classes					RW			RO
Manage Range Tables					RW			RO
Manage Rate Plans					RW			RO
Process a Chargeable Item					RW			
<b>System Configuration</b>								
Manage SAP CC System Parameters	RW				RO			RO
<b>System Information</b>								
Analyze Item Files	RW				RO			RO

	Adm.	User Adm.	Batch Rating Adm.	CSR	Market.	Con- nector Adm.	Process Man- ager	Remote Support
Display System Status	RW				RO			RO
Display Usage Metrics	RW				RO			RO
Change list mngt	RW				RW			RO

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

## 6.3 Critical Combinations

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

### → Recommendation

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

## 6.4 Master Data Access Restriction

You can assign an SAP CC user to a given and unique pricing catalog of a service provider.

The user can only access to:

- Master data belonging to this pricing catalog, which correspond to the following pricing elements:
  - Charges
  - Charge plans
  - Charged item classes
  - Offers (former Data Model)
  - 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 (former Data Model)
  - Provider contracts

#### **i 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 systems. 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 back-end system's database or files. Additionally, if users are not able to connect to the server LAN<sup>31</sup>, they cannot exploit well-known bugs and security holes in network services on the server machines.

The network topology for SAP Convergent Charging (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.

[Communication Channel Security \[page 33\]](#)

[Network Security \[page 56\]](#)

## 7.1 Communication Channel Security

The communications between deployed components of SAP Convergent Charging (SAP CC) rely on the following protocols:

- HTTP<sup>32</sup>
  - Used to transport [SOAP \[page 34\]](#)<sup>33</sup> messages (Web Services technical interface)
  - Used to transport [REST \[page 43\]](#)<sup>34</sup> requests (Web Services technical interface)
  - Used to transport proprietary [XML \[page 46\]](#)<sup>35</sup> messages (HTTP Communication Interface, HCI)
  - Used to transport [JSON \[page 51\]](#)<sup>36</sup> messages between the SAP Fiori user interfaces and Cockpit

---

<sup>31</sup> Local Area Network

<sup>32</sup> HyperText Transfer Protocol

<sup>33</sup> Simple Object Access Protocol

<sup>34</sup> REpresentational State Transfer

<sup>35</sup> eXtended Markup Language

<sup>36</sup> JavaScript Object Notation

- TCP/IP<sup>37</sup>, used to transport proprietary TCP Packets, either internally between server instances or externally between the deployed components
- UDP<sup>38</sup>, used to transport messages dedicated to network discovery purposes
- JDBC<sup>39</sup>, used to communicate with running RDBMS<sup>40</sup>

The communication between the deployed components of SAP CC can be secured in order to fit the security policy of your SAP system landscape. To secure the different communication channels, refer to the [Securing SAP CC](#) procedure available in the [SAP CC 2020 Application Help](#) documentation.

### ⚠ Caution

When securing components of SAP CC (systems, backends, and user interfaces), 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.

[SOAP over HTTP \[page 34\]](#)

[REST over HTTP \[page 43\]](#)

[XML over HTTP \(HTTP Communication Interface - HCI\) \[page 46\]](#)

[JSON over HTTP \[page 51\]](#)

[Packets over TCP/IP \[page 51\]](#)

[RFC over TCP/IP \[page 52\]](#)

[Messages over UDP \[page 55\]](#)

[Java Database Connectivity \[page 56\]](#)

## 7.1.1 SOAP over HTTP

SAP Convergent Charging provides a **Web Services (WS) technical interface** based on SOAP<sup>41</sup> and HTTP<sup>42</sup> standards. This technical interface gives the possibility for the SAP CRM and SAP ERP systems to consume multiple web services and thus request specific operations in the connected SAP CC system.

To communicate with the published web services, client applications (or systems) send SOAP messages to the updater or dispatcher instance using the HTTP protocol. Several [endpoints \[page 40\]](#) are available.

These SOAP messages have an XML<sup>43</sup> 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 (depending on the selected authentication method)

<sup>37</sup> Transmission Control Protocol / Internet Protocol

<sup>38</sup> User Datagram Protocol

<sup>39</sup> Java Database Connectivity

<sup>40</sup> Relational Database Management System

<sup>41</sup> Simple Object Access Protocol

<sup>42</sup> HyperText Transfer Protocol

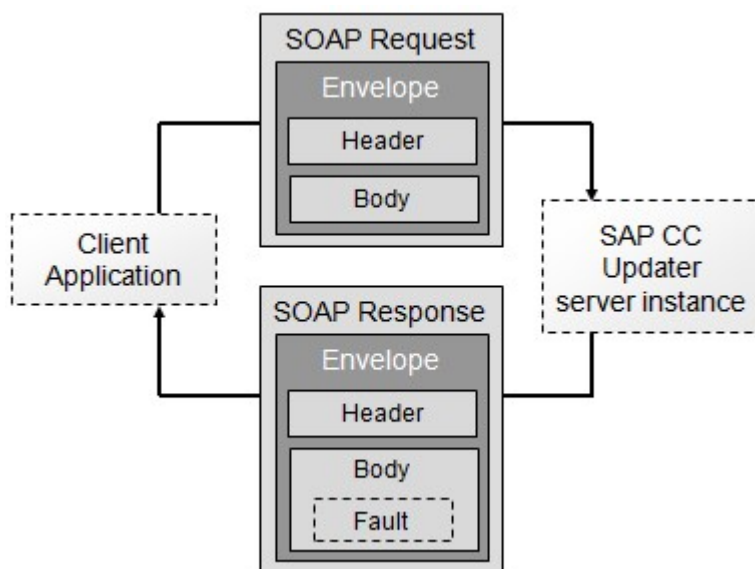
<sup>43</sup> eXtended Markup Language

- 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



See also: [SAP CC 2020 Web Services Documentation](#)

[Web Service Security \(WS-Security\) \[page 36\]](#)

[HTTP Basic Authentication \[page 39\]](#)

[Channel Encryption \[page 39\]](#)

[Channel Security \[page 40\]](#)

[Known Limitations \[page 40\]](#)

[Endpoints \[page 40\]](#)

## 7.1.1.1 Web Service Security (WS-Security)

Authentication at message level means that the authentication credentials of the WS consumer are transported in the SOAP header of the SOAP envelope with authentication token profiles. For this, you use the `wsse:Security` XML element.

SAP Convergent Charging (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<sup>44</sup> 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<sup>45</sup> messages:
  - A **username**, which must correspond to an existing user of SAP CC, granted 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 in the SAP CC system when using the "Username Token" security profile.**

### → Remember

The "Username Token" security profile is available for backward compatibility reasons.

### i Note

The encryption of the HTTP<sup>46</sup> connections used during the execution of web services is automatically activated if the encryption is activated for the HCI<sup>47</sup> communications.

### ❖ Example

The following XML<sup>48</sup> code represents a skeleton of a SOAP request sent by a client application to the updater 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>
```

<sup>44</sup> Single Sign-On

<sup>45</sup> Simple Object Access Protocol

<sup>46</sup> HyperText Transfer Protocol

<sup>47</sup> Http Communication Interface

<sup>48</sup> eXtended Markup Language

```

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

```

### ❖ Example

The following XML code represents a skeleton of a SOAP request sent by a client application to the updater 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>

```

### i Note

The `Fault` element is a WSS<sup>49</sup> standard element which exists in case of failed authentication. This element contains a reason and an associated message which provide information about the failure.

## 7.1.1.1.1 SAML Token

In the SOAP header, the `wsse:Security` XML element contains the `saml:Assertion` XML element and the expected nested XML elements.

### ❖ Example

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

<sup>49</sup> Web Services Security

```

<?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` XML element is a WSS<sup>50</sup> standard element that exists in case of failed authentication. This element contains a reason and an associated message that provide information about the failure.

## 7.1.1.1.2 Username Token

In the SOAP header, the `wsse:Security` XML element contains the `wsse:UsernameToken` XML element and the necessary nested XML elements (user logon and password).

### ❖ Example

The following XML<sup>51</sup> code represents a skeleton of a SOAP request sent by a client application to the updater 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>

```

<sup>50</sup> Web Services Security

<sup>51</sup> eXtended Markup Language

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

### i Note

The `Fault` XML element is a WSS<sup>52</sup> standard element that exists in case of failed authentication. This element contains a reason and an associated message that provide information about the failure.

## 7.1.1.2 HTTP Basic Authentication

SAP Convergent Charging (SAP CC) supports the HTTP basic authentication that lets external applications (or systems) make web service requests without providing a logon token. The HTTP basic authentication is based on the credentials (user ID/logon, password) for the SAP CC service user that sends a SOAP message. This authentication method uses standard fields in the HTTP header.

In the HTTP request message, the HTTP header must include the `Authorization` field and its value set to:

```
Authorization: Basic <USERID>:<PASSWORD>
```

The credentials must be encoded in Base64 as defined by RFC 2617.

### → Remember

User IDs that contain the `:` character cannot be used with the HTTP basic authentication.

### ⚠ Caution

When using the HTTP basic authentication, user IDs and passwords are insecurely transported in an base64-encoded text format. They are not encrypted.

**It is thus highly recommended to activate the encryption of HTTP connections in the SAP CC system when using this HTTP basic authentication.** See [Channel Encryption \[page 39\]](#).

## 7.1.1.3 Channel Encryption

To increase the security level of communications relying on SOAP messages, it is possible to use HTTPS<sup>53</sup>, which corresponds to the secured version of the HTTP<sup>54</sup> protocol. This protocol represents a combination of the HTTP with the SSL/TLS protocols used to provide encryption and secure identification between network

<sup>52</sup> Web Services Security

<sup>53</sup> HyperText Transfer Protocol Secured

<sup>54</sup> HyperText Transfer Protocol

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 XML requests and responses within SAP CC. For further information, refer to the [Securing SAP CC](#) procedure available in the [SAP CC 2020 Application Help](#) documentation.

## 7.1.1.4 Channel Security

Communications performed over the SOAP<sup>55</sup> over HTTP<sup>56</sup> communication channel rely on the Apache CXF third-party software that addresses various security topics such as WS-SecurityPolicy or SAML<sup>57</sup>.

Security relating to XML<sup>58</sup> parsing operations is only provided by the Woodstox StAX implementation, without any additional SAP CC-specific mechanism.

## 7.1.1.5 Known Limitations

The WSS<sup>59</sup> freshness time period mechanism (materialized by the `Created` element of the `UsernameToken` element) is optional. When a date is specified in the `Created` element, this date must be a valid date in the following range: ] D-5 minutes , D+1 minute [, where D corresponds to the server's current date.

### ❖ Example

Considering an incoming request processed by SAP CC at 2015-01-01T05:08:02Z (UTC), the `Created` element of the `UsernameToken` element must correspond to a date:

- Posterior to 2015-01-01T05:03:02Z (UTC)
- Anterior to 2015-01-01T05:09:02Z (UTC)

## 7.1.1.6 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<sup>60</sup> which respects the following format (case sensitive content): `http(s)://<INSTANCE_ADDRESS>:<INSTANCE_PORT_NB>/[v<WS_VERSION>]/<WS_TECH_NAME>`

Where:

---

<sup>55</sup> Simple Object Access Protocol

<sup>56</sup> HyperText Transfer Protocol

<sup>57</sup> Security Assertion Markup Language

<sup>58</sup> eXtended Markup Language

<sup>59</sup> Web Services Security

<sup>60</sup> Uniform Resource Identifier



- <INSTANCE\_ADDRESS> is the network address (DNS<sup>61</sup> name or IP address) of the host machine of the active updater instance or dispatcher instance of the 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 SOAP<sup>62</sup> 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 CC
  - **Charging Contract State Management**, used to manage the states of charging contracts which have been migrated to SAP CC
- 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
- Echo Services
- Restricted Services, which represent provided services and operations which can be used by other SAP applications, but not in an implementation project

---

<sup>61</sup> Domain Name Server

<sup>62</sup> Simple Object Access Protocol

- **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
- **Currencies Replication**, used to manage the synchronization of currencies with SAP S/4HANA Cloud
- **Billable Item Management**, used to manage the billable items creation in SAP S/4HANA Cloud

## i 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:

		Hosted By	
Web Service	Technical Name	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	/subscriberMappingTable-Management		■
Subscriber Range Table Management	/subscriberRangeTableManagement		■
Customer Master 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		■
Other Services			

Web Service	Technical Name	Hosted By	
		Dispatcher	Updater
Echo Services	/echo	■	
<b>Restricted Services</b>			
Data Export Management to SAP PSI	/IExporting		■
Transport of Catalog Data	/transport		■
Currencies Replication	/currency		■
Billable Item Management	/billableitem		■

## 7.1.2 REST over HTTP

SAP CC provides a Web Services technical interface based on REST<sup>63</sup> and HTTP<sup>64</sup> standards. This interface gives the possibility for external systems to consume Web Services and thus execute specific operations.

To communicate with the published web services, client applications send REST requests to the updater server instance using the HTTP protocol. In REST, resources are identified in a consistent way using a URI<sup>65</sup>. Actions are expressed using standard verbs like GET and POST. The REST design principle has the ability to establish the one to one mapping between CRUD (Create, Read, Update and Delete) operations and the methods of HTTP:

REST Operations	HTTP Methods
Create	POST
Read	GET
Update	PUT
Delete	DELETE

A REST request contains:

- an **envelope**, which defines an XML document as a REST request and represents its root
- a **header**, which contains application-specific related to the REST request
- a **body**, which contains the actual REST request intended for the ultimate endpoint of a request

### 7.1.2.1 Web Services 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:

<sup>63</sup> REpresentational State Transfer

<sup>64</sup> HyperText Transfer Protocol

<sup>65</sup> Uniform Resource Identifier

- **SAML Token**, when the SSO<sup>66</sup> mechanism is activated
- **Username Token**, which consists in sending the following information into the header of REST<sup>67</sup> messages:
  - A **username**, which must correspond to an existing user of SAP CC, granted 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.**

#### i Note

- The Username Token security profile is available for backward compatibility reasons
- The encryption of the HTTP<sup>68</sup> connections used during the execution of web services is automatically activated if the encryption is activated for the HCI<sup>69</sup> communications.

## 7.1.2.2 Channel Encryption

To use the communications relying on REST<sup>70</sup> messages with SAP CC updater instances, it is mandatory to use HTTPS<sup>71</sup>, which corresponds to the secured version of the HTTP<sup>72</sup> 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 XML requests and responses within SAP CC. For further information, refer to the [Securing SAP CC](#) procedure available in the [SAP CC 2020 Application Help](#) documentation.

## 7.1.2.3 Channel Security

Communications performed over the REST<sup>73</sup> over HTTP<sup>74</sup> communication channel rely on the Apache CXF third-party software that addresses various security topics such as WS-SecurityPolicy or SAML<sup>75</sup>.

<sup>66</sup> Single Sign-On

<sup>67</sup> REpresentational State Transfer

<sup>68</sup> HyperText Transfer Protocol

<sup>69</sup> Http Communication Interface

<sup>70</sup> REpresentational State Transfer

<sup>71</sup> HyperText Transfer Protocol Secured

<sup>72</sup> HyperText Transfer Protocol

<sup>73</sup> REpresentational State Transfer

<sup>74</sup> HyperText Transfer Protocol

<sup>75</sup> Security Assertion Markup Language

Security relating to XML<sup>76</sup> parsing operations is only provided by the Woodstox StAX implementation, without any additional SAP CC-specific mechanism.

## 7.1.2.4 Known Limitations

The WSS<sup>77</sup> freshness time period mechanism (materialized by the `Created` element of the `UsernameToken` element) is optional. When a date is specified in the `Created` element, this date must be a valid date in the following range: **] D-5 minutes , D+1 minute [**, where D corresponds to the server's current date.

### ❖ Example

Considering an incoming request processed by SAP CC at 2015-01-01T05:08:02Z (UTC), the `Created` element of the `UsernameToken` element must correspond to a date:

- Posterior to 2015-01-01T05:03:02Z (UTC)
- Anterior to 2015-01-01T05:09:02Z (UTC)

## 7.1.2.5 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<sup>78</sup> 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<sup>79</sup> name or IP address) of the host machine of the active updater instance of the 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 a REST<sup>80</sup> Web Service that allows external systems to provision individual users in SAP Convergent Charging.

---

<sup>76</sup> eXtended Markup Language

<sup>77</sup> Web Services Security

<sup>78</sup> Uniform Resource Identifier

<sup>79</sup> Domain Name Server

<sup>80</sup> REpresentational State Transfer

## 7.1.3 XML over HTTP (HTTP Communication Interface - HCI)

SAP CC provides a proprietary communication interface "HTTP Communication Interface (HCI)" and based on XML<sup>81</sup> and HTTP<sup>82</sup> 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).

Most of the SAP CC user interfaces use the HCI technical interface. For example, [Core Tool](#), [BART Tool](#) and [Cockpit](#) communicate with their respective server systems.

### 7.1.3.1 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<sup>83</sup>
- The HTTP<sup>84</sup> protocol version

#### i Note

- 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` element 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 for more information 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.

---

<sup>81</sup> eXtended Markup Language

<sup>82</sup> HyperText Transfer Protocol

<sup>83</sup> Uniform Resource Identifier

<sup>84</sup> HyperText Transfer Protocol

## 7.1.3.2 HTTP Response

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

- The HTTP<sup>85</sup> 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<sup>86</sup> 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 `Body` part of a request. For further information about its content element, please refer in the dedicated [section \[page 46\]](#).

## 7.1.3.3 HCI Envelope

HCI<sup>87</sup> envelopes represent XML<sup>88</sup> messages carried over the HTTP<sup>89</sup> 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:

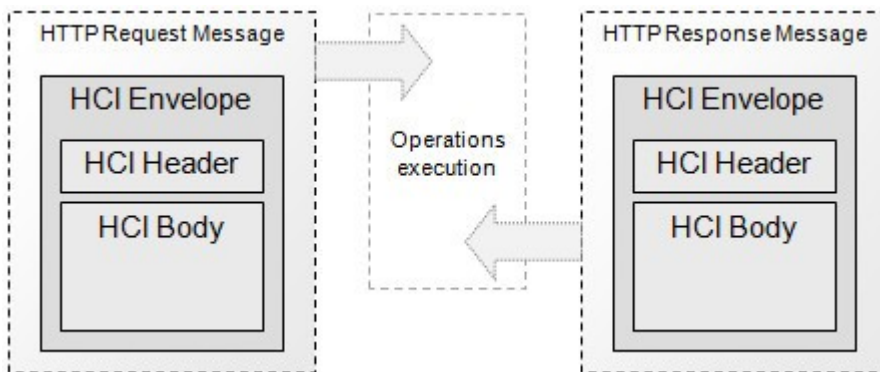
```
<xs:element name="envelope">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="header" minOccurs="1" maxOccurs="1"/>
      <xs:element ref="body" minOccurs="1" maxOccurs="1"/>
    </xs:sequence>
  </xs:complexType>
</xs:element></soapenv:Envelope>
```

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

---

<sup>85</sup> HyperText Transfer Protocol  
<sup>86</sup> Uniform Resource Identifier  
<sup>87</sup> Http Communication Interface  
<sup>88</sup> eXtended Markup Language  
<sup>89</sup> HyperText Transfer Protocol

- 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 SAP CC user, granted 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: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>

```

## 7.1.3.4 HCI Operation

A HCI<sup>90</sup> 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

### Note

- 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

The following XML<sup>91</sup> codes represent the HCI request and response related to a single HCI operation (creation of a subscriber account):

<sup>90</sup> Http Communication Interface

<sup>91</sup> eXtended Markup Language

```

<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

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>

```

## 7.1.3.5 Channel Encryption

To increase the security level of communications relying on XML<sup>92</sup> messages, it is possible to use HTTPS<sup>93</sup>, which corresponds to the secured version of the HTTP<sup>94</sup> protocol. This protocol represents a combination of the HTTP with the SSL<sup>95</sup>/TLS<sup>96</sup> 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 CC 2020 Application Help](#) documentation.

<sup>92</sup> eXtended Markup Language

<sup>93</sup> HyperText Transfer Protocol Secured

<sup>94</sup> HyperText Transfer Protocol

<sup>95</sup> Secure Socket Layer

<sup>96</sup> Transport Layer Security

## 7.1.4 JSON over HTTP

JavaScript Object Notation (JSON) is a lightweight data interchange format that is based on a subset of the JavaScript programming language. Independent from any language, this text format is used by the [Cockpit](#) user interface for communications with the SAP Fiori user interfaces, based on the OData protocol used to consume RESTful API<sup>97</sup>s.

### i Note

Versions 2.0 of the OData protocol are supported by SAP Convergent Charging.

### 7.1.4.1 Channel Encryption

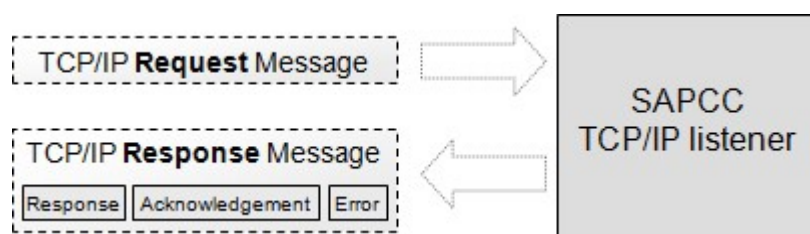
To increase the security level of communications relying on JSON messages, it is possible to use HTTPS<sup>98</sup>, which corresponds to the secured version of the HTTP<sup>99</sup> protocol. This protocol represents a combination of the HTTP with the SSL<sup>100</sup>/TLS<sup>101</sup> protocols used 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.

For further information, refer to the [Securing SAP CC](#) procedure available in the [SAP CC 2020 Application Help](#) documentation.

## 7.1.5 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<sup>102</sup> 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



<sup>97</sup> Application Programming Interface

<sup>98</sup> HyperText Transfer Protocol Secured

<sup>99</sup> HyperText Transfer Protocol

<sup>100</sup> Secure Socket Layer

<sup>101</sup> Transport Layer Security

<sup>102</sup> Transmission Control Protocol / Internet Protocol

### i Note

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.

## 7.1.5.1 Channel Encryption

As described above, communications relying on proprietary packets sent over TCP/IP<sup>103</sup> 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 CC 2020 Application Help](#) documentation.

### i 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.

## 7.1.5.2 Known Limitations

The size of the proprietary messages sent over TCP/IP<sup>104</sup> cannot exceed 1 MB.

## 7.1.6 RFC over TCP/IP

SAP CC uses the standard SAP interface named Remote Function Call (RFC) to communicate over TCP/IP<sup>105</sup> with the following SAP systems:

---

<sup>103</sup> Transmission Control Protocol / Internet Protocol

<sup>104</sup> Transmission Control Protocol / Internet Protocol

<sup>105</sup> Transmission Control Protocol / Internet Protocol

- SAP CRM
- SAP ERP

## 7.1.6.1 Channel Encryption

For security reasons, communications relying on RFC<sup>106</sup> over TCP/IP<sup>107</sup> are encrypted using the SAP Cryptographic Library.

### i Note

For general security information related to RFC over TCP/IP, refer to the [RFC/ICF Security Guide](https://help.sap.com) on <https://help.sap.com>.

## 7.1.6.2 Communication Destinations

SAP CC uses the following RFC<sup>108</sup> function modules, implemented by the different supported destinations:

- **BAPI\_CURRENCY\_GETLIST** is used to retrieve the list of currencies defined in the SAP ERP system.
- **CRM\_ISX\_PPACC\_ALERT\_HANDLER** is used to transmit the business notifications about prepaid accounts (balance amount alerts, account expiration alerts) to SAP CRM.
- **DDIF\_FIELDINFO\_GET** is used to retrieve the legible descriptions of the data fields that are defined in a billable item class.
- **FKK\_BIX\_BIT\_REVERSE\_CC** is 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 SAP 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 Convergent Invoicing. 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 SAP system landscape

<sup>106</sup> Remote Function Call

<sup>107</sup> Transmission Control Protocol / Internet Protocol

<sup>108</sup> Remote Function Call

- 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**
- **BAPI\_TRANSACTION\_COMMIT**, used to commit the changes related to the creation of billable items and consumption items (depends on the configuration of the bulkloader instances)
- **BAPI\_TRANSACTION\_ROLLBACK**, used to roll-back the changes related to the creation of billable items and consumption items (depends on the configuration of the bulkloader instances)

#### Note

- These destinations and functions can be configured using [Setup Tool](#) for the Core 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, refer to the [dedicated documentation](https://help.sap.com) on <https://help.sap.com>.

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

Function	Implemented by		Used by
	SAP CRM	SAP ERP	Core Server
BAPI_CURRENCY_GETLIST		■	■
CRM_ISX_PPACC_ALERT_H ANDLER	■		■
DDIF_FIELDINFO_GET		■	■
FKK_BIX_BIT_REVERSE_CC		■	■
FKK_BIX_BIT_RE- VERSE_CHECK_CC		■	■
FKK_BIX_BIT- CAT_LIST_GET_SAPCC		■	■
FKK_BIX_BIT- CAT_STRUC_GET_API		■	■
FKK_BIX_CIT- CAT_CC_PROXY_GET		■	■
FKK_BIX_CIT- CAT_LIST_GET_SAPCC		■	■
FKK_BIX_RERATE_SESSION		■	■
FKK_PREP_MESSAGE		■	■
/1FC/<name of CIT Class>_CIT_CREATE_PROXY		■	■
/1FE/<name of BIT Class>_BIT_CREATE_API		■	■

## 7.1.7 Messages over UDP

Client applications and deployed server instances send UDP<sup>109</sup> 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.

### 7.1.7.1 UDP request

Discovery requests are sent to multicast UDP<sup>110</sup> 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 Core Server
  - **External**, which is provided by client applications
- The name of the concerned SAP CC system which needs to be contacted and analyzed

### 7.1.7.2 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

#### **i** Note

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

<sup>109</sup> User Datagram Protocol

<sup>110</sup> User Datagram Protocol

### 7.1.7.3 Channel Encryption

The Messages over UDP<sup>111</sup> 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<sup>112</sup>). **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

## 7.1.8 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<sup>113</sup> which:

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

#### i Note

SAP Convergent Charging uses the 2.0 implementation of JDBC<sup>114</sup> to interact with both Core Database and BART Database.

### 7.1.8.1 Channel Encryption

To increase the security level of communications relying on the JDBC<sup>115</sup> channel, it is possible to encrypt the connections to the different databases. For further information about the encryption of the databases connections, refer to the [Securing SAP CC](#) procedure available in the [SAP CC 2020 Application Help](#) documentation.

## 7.2 Network Security

As described in the [Technical System Landscape \[page 9\]](#) 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 SAP Convergent Charging:

- 
- <sup>111</sup> User Datagram Protocol
  - <sup>112</sup> Java platform, Standard Edition
  - <sup>113</sup> Application Programming Interface
  - <sup>114</sup> Java Database Connectivity
  - <sup>115</sup> Java Database Connectivity



Component	Description
<b>Core Server</b>	
updater instance	<p>The following ports must be configured for each deployed instance:</p> <ul style="list-style-type: none"> <li>• <b>HTTP</b><sup>116</sup>, used by client applications (including Cockpit) which communicate with the Core Server using HCI<sup>117</sup> operations</li> <li>• <b>Web Services</b> (called <code>WSPORT</code> in the instance map), used by client applications for master data distribution or replication purpose</li> </ul>
dispatcher instance	<p>The following ports must be configured for each deployed instance:</p> <ul style="list-style-type: none"> <li>• <b>HTTP</b>, used by client applications (including Cockpit) for administration purposes</li> <li>• <b>Messages</b>, used by client applications for business purposes (charging, rerating, and so on)</li> <li>• <b>Internal Messages</b>, used by the other deployed server instances for internal communication purposes (admin, multicast, and so on)</li> </ul>
Other instances	rater, guider, taxer, and bulkloader server instances are automatically configured by the dispatcher server instances.
SMD <sup>118</sup> web service	The SMD web service uses the HTTP port of the dispatcher server instance and thus does not need any specific configuration
<b>Cockpit</b>	
Cockpit back-end	<p>The following ports must be configured:</p> <ul style="list-style-type: none"> <li>• <b>JDBC</b><sup>119</sup>, used by Cockpit to connect to the Core Database</li> <li>• <b>HTTP</b>, used to connect to the dispatcher and updater instances of the Core Server</li> </ul>
<b>BART Server</b>	
BART Server	<p>The following ports must be configured:</p> <ul style="list-style-type: none"> <li>• <b>HTTP</b>, used by client applications for administration purposes</li> <li>• <b>Messages</b>, used by client applications for CDR<sup>120</sup> acquisition purposes</li> </ul>
<b>Diameter Server</b>	
Diameter Server	<p>The Diameter Server uses 2 different ports:</p> <ul style="list-style-type: none"> <li>• <b>HTTP Dispatcher</b>, which is used to communicate with the dispatcher instance of the Core Server. 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)</li> <li>• <b>Diameter</b>, which corresponds to the default 3868 port of the Diameter protocol. This port is not configurable</li> </ul>
<b>SAP CC databases</b>	

<sup>116</sup> HyperText Transfer Protocol

<sup>117</sup> Http Communication Interface

<sup>118</sup> SAP Manager Diagnostic

<sup>119</sup> Java Database Connectivity

<sup>120</sup> Call Detail Record or more generally Consumption Detail Record

Component	Description
Core Database	<p>Both Core Server instances and Cockpit application use a port to connect to the Core Database. This port can be configured to fit specific environment configurations, and is set by default to:</p> <ul style="list-style-type: none"> <li>• 3&lt;INSTANCE_NUMBER&gt;15 for a single-container SAP HANA system or between 3&lt;INSTANCE_NUMBER&gt;41 and 3&lt;INSTANCE_NUMBER&gt;98 for a multitenant SAP HANA system, considering that &lt;INSTANCE_NUMBER&gt; is the instance number of the SAP HANA database</li> <li>• 5000 for Sybase ASE databases</li> <li>• 4464 for DB2 databases</li> <li>• 1433 for Microsoft SQL Server databases</li> <li>• 1521 for Oracle databases</li> </ul>
Session Database	The rater instances of the Core Server use a port to connect to the Session Database. This port can be configured the same way than for the Core Database.
BART Database	BART Server uses a port to connect to the BART Database.
<b>SAP CC optional elements</b>	
Import/Export Connector	IEC <sup>122</sup> 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 <code>-port</code> argument in the command line.
<b>Other optional elements</b>	
SAP installer	<p>The installation of the different SAP Convergent Charging systems relies on a GUI<sup>123</sup> named SL Common GUI, that communicates with the SAP installer using the following defaults ports:</p> <ul style="list-style-type: none"> <li>• 4237 for HTTPS<sup>124</sup> connections with the SL Common GUI. This port can be specified at installer launch time using the <code>-SAPINST_HTTPS_PORT</code> argument in the command line</li> <li>• 4239 for managing the feedback evaluation form displayed at the end of the installation process. This port can be specified at installer launch time using the <code>-SAPINST_HTTP_PORT</code> argument in the command line</li> </ul>

### Note

Messages, internal messages and Diameter messages 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, SAP SE highly recommends that you implement typical network security rules such as:

- Firewall rules creation to control the traffic
- NAT<sup>125</sup> rules use to reduce ports exposure

<sup>121</sup> Real Application Cluster

<sup>122</sup> Import/Export Connector

<sup>123</sup> Graphical User Interface

<sup>124</sup> HyperText Transfer Protocol Secured

<sup>125</sup> Network Address Translation

- And so on

## 8 Data Storage Security

The SAP Convergent Charging solution does not implement any specific security mechanism to protect the Core Database and BART Database. The following typical standard rules have been applied to secure the connection with the RDBMS<sup>126</sup>:

- Every connection URL<sup>127</sup> used to connect to a given database requires a logon 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. SAP SE highly recommends you to create multiple user accounts in order 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 Database and BART Database are encrypted
- To ensure confidentiality, no feature or process provided by SAP Convergent Charging requires filling in person-related data. As a consequence, no specific mechanism has been implemented to filter and/or remove such data

---

<sup>126</sup> Relational Database Management System

<sup>127</sup> Uniform Resource Locator

## 9 Data Protection and Privacy

As SAP Convergent Charging does not provide any feature or process that requires to fill in sensitive data, no specific mechanism is available to ensure confidentiality and access control regarding such sensitive personal data. As a consequence, SAP SE recommends that you **do not store** any sensitive personal data (such as credit card number, bank account number, medical record number, biometric information, and so on) during the provisioning of master data related to end customers.

Furthermore, fulfilling the requirements of the Data Privacy Protection policy, SAP Convergent Charging ensures the physical and immediate deletion of the personal data that could exist in the Core Database, using dedicated functions. In case you created backups of the Core Database, you need to manually delete this personal data within these backups.

Moreover, no RAL (Read Access Logging) mechanism is provided by SAP Convergent Charging.

# 10 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 SAP Convergent Charging 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.

## i Note



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

# Important Disclaimers and Legal Information

## Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.

About the icons:

- Links with the icon  : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon  : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

## Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

## Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.

The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

## Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

## Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

© 2021 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see <https://www.sap.com/about/legal/trademark.html> for additional trademark information and notices.