



# Certification Report

**EAL2+ (ALC\_FLR.2) Evaluation of  
CRUNCHY DATA SOLUTIONS, INC  
CRUNCHY CERTIFIED POSTGRESQL 9.5**

issued by

**Turkish Standards Institution  
Common Criteria Certification Scheme**

*Certificate Number: 21.0.03/TSE-CCCS-33*


C.E

NK



	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	<b>Doküman No</b>	BTBD-03-01-FR-01	
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	30/07/2015	
		<b>Revizyon Tarihi</b>	29/04/2016	<b>No</b>

## TABLE OF CONTENTS

TABLE OF CONTENTS .....	2
DOCUMENT INFORMATION .....	3
DOCUMENT CHANGE LOG .....	3
DISCLAIMER .....	4
FOREWORD .....	5
RECOGNITION OF THE CERTIFICATE .....	6
1 EXECUTIVE SUMMARY .....	7
2 CERTIFICATION RESULTS .....	11
2.1 IDENTIFICATION OF TARGET OF EVALUATION .....	11
2.2 SECURITY POLICY .....	11
2.3 ASSUMPTIONS AND CLARIFICATION OF SCOPE .....	12
2.4 ARCHITECTURAL INFORMATION .....	13
2.5 DOCUMENTATION .....	16
2.6 IT PRODUCT TESTING .....	16
2.7 EVALUATED CONFIGURATION .....	16
2.8 RESULTS OF THE EVALUATION .....	17
2.9 EVALUATOR COMMENTS / RECOMMENDATIONS .....	17
3 SECURITY TARGET .....	18
4 GLOSSARY .....	19
5 BIBLIOGRAPHY .....	23

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	<b>Doküman No</b>	BTBD-03-01-FR-01	
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	30/07/2015	
		<b>Revizyon Tarihi</b>	29/04/2016	<b>No</b>


## DOCUMENT INFORMATION

<b>Date of Issue</b>	01.06.2016
<b>Approval Date</b>	09.06.2016
<b>Certification Report Number</b>	21.0.03/16-002
<b>Sponsor and Developer</b>	Crunchy Data Solutions, Inc
<b>Evaluation Facility</b>	CygnCom Solutions
<b>TOE Name</b>	Crunchy Certified Postgresql 9.5
<b>Pages</b>	23
<b>Prepared by</b>	Cem ERDİVAN 
<b>Reviewed by</b>	İbrahim Halil KIRMIZI 

This report has been prepared by the Certification Expert and reviewed by the Technical Responsible of which signatures are above.


## Document Change Log

Release	Date	Pages Affected	Remarks/Change Reference
1.0	01.06.2016	ALL	First Release

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	<b>Doküman No</b>	BTBD-03-01-FR-01	
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	30/07/2015	
		<b>Revizyon Tarihi</b>	29/04/2016	<b>No</b>

## **DISCLAIMER**

*This certification report and the IT product defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1, revision 4, using Common Methodology for IT Products Evaluation, version 3.1, revision 4. This certification report and the associated Common Criteria document apply only to the identified version and release of the product in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document, and no warranty is given for the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.*

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	<b>Doküman No</b>	BTBD-03-01-FR-01	
		<b>Yayın Tarihi</b>	30/07/2015	
	<b>CCCS CERTIFICATION REPORT</b>	<b>Revizyon Tarihi</b>	29/04/2016	<b>No</b>

## FOREWORD

The Certification Report is drawn up to submit the Certification Commission the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme. Certification Report covers all non-confidential security and technical information related with a Common Criteria evaluation which is made under the ITCD Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.


The Common Criteria Certification Scheme (CCSS) provides an evaluation and certification service to ensure the reliability of Information Security (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCTL = Common Criteria Testing Laboratory) under CCCS' supervision.

CCEF is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCEF has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by CygnaCom Solutions, which is a commercial CCTL.

A Common Criteria Certificate given to a product means that such product meets the security requirements defined in its security target document that has been approved by the CCCS. The Security Target document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the IT product should also review the security target document in order to understand any assumptions made in the course of evaluations, the environment where the IT product will run, security requirements of the IT product and the level of assurance provided by the product.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for CRUNCHY CERTIFIED POSTGRESQL 9.5 whose evaluation was completed on May 25, 2016 and whose evaluation technical report was drawn up by May 25, 2016 (as CCTL), and with the Security Target document with version no 1.6 of the relevant product.


The certification report, certificate of product evaluation and security target document are posted on the ITCD Certified Products List at [bilisim.tse.org.tr](http://bilisim.tse.org.tr) portal and the Common Criteria Portal (the official web site of the Common Criteria Project).

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	<b>Doküman No</b>	BTBD-03-01-FR-01	
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	30/07/2015	
		<b>Revizyon Tarihi</b>	29/04/2016	<b>No</b>

## **RECOGNITION OF THE CERTIFICATE**

*The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.*

*The CCRA has been signed by the Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on: <http://www.commoncriteriaportal.org>.*

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	<b>Doküman No</b>	BTBD-03-01-FR-01	
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	30/07/2015	
		<b>Revizyon Tarihi</b>	29/04/2016	<b>No</b>

## 1 - EXECUTIVE SUMMARY

This report constitutes the certification results by the certification body on the evaluation results applied with requirements of the Common Criteria for Information Security Evaluation.

**Evaluated IT product name:** Crunchy Certified Postgresql

**IT Product version:** 9.5

**Developer's Name:** Crunchy Data Solutions, Inc

**Name of CCTL:** CygnaCom Solutions

**Assurance Package:** EAL2+ (ALC\_FLR.2)

**Completion date of evaluation:** May 25, 2016

Crunchy Certified PostgreSQL 9.5 (also referred to as PostgreSQL) is an open source relational database management system. The TOE includes PostgreSQL and tools for clients, developers and administrators.

The TOE provides the following security functionality:

- Security Auditing,
- User Data Protection,
- Identification and Authentication (I&A),
- Security Management,
- Protection of the TSF and
- TOE Access and protection of the TSF.

The TOE is claiming conformance to the Base Protection Profile for Database Management Systems, Version 2.07, September 9, 2015.

PostgreSQL is a computerized repository that stores information and allows authorized users to retrieve and update that information. PostgreSQL may be operated as a single-user system, in which only one user may access the DBMS at a given time, or as a multi-user system, in which many users may access the DBMS simultaneously.

Crunchy Certified PostgreSQL 9.5 is a software-only TOE. The TOE is made up of the following software components:

- PostgreSQL 9.5 (in TOE)
- Client Connectors identified in Section 1.5.2 (in TOE)
- PostgreSQL Audit Extension 1.0.2 (in TOE)
- PostGIS Spatial Extensions 2.2.2 (in TOE)
- Crunchy MLS PostgreSQL 1.2.1 (not in TOE)

The components listed as “not in TOE” are prohibited in the scope of the evaluated configuration.


The TOE is installed using a RPM. The RPM provided contains the TOE's components and is installed by the Linux system administrator using RPM client utilities. The TOE has a separate set of RPM packages for each component, including the following:

- PostgreSQL Server RPM
- PostgreSQL JDBC Driver RPM
- PostgreSQL Audit RPM
- PostGIS RPM
- Crunchy MLS PostgreSQL RPM

### 1.1 PostgreSQL (in TOE)

PostgreSQL has the capability to limit DBMS access to authorized users, enforce DAC on objects under the control of the DBMS (based on user and optional group authorizations), and provide user accountability via the audit of user actions.

PostgreSQL is comprised of the DBMS server application that performs the following functions:

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	Doküman No	BTBD-03-01-FR-01	
	<b>CCCS CERTIFICATION REPORT</b>	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

- Controls users' accesses to user data and DBMS data;
- Interacts with, and possibly supplements portions of, the underlying operating system to retrieve and present the data that are under the DBMS's management;
- Indexes data values to their physical locations for quick retrievals based on a value or range of values;
- Executes pre-written programs (i.e., utilities) to perform common tasks like database backup, recovery, loading, and copying;
- Supports mechanisms that enable concurrent database access (e.g., locks);
- Assists recovery of user data and DBMS data (e.g., transaction log);
- Tracks operations that users perform;
- Implements a data model with which the DBMS data structures and organization can be conceptualized (e.g., hierarchical, object-oriented, relational data models) and DBMS objects defined; and
- Implements high-level language(s) or interfaces that allow authorized users to define database constructs; access and modify user or DBMS data; present user or DBMS data; and perform operations on those data.

PostgreSQL includes the following subcomponents:

- Server Utilities are a collection of command line utilities for managing the database. These utilities are only useful when run on the host system where the database server resides.
- Database Utilities allow for the creation and removal of databases, database user accounts and retrieving information about the installed version. These command line utilities can be run from a terminal emulation program on any host, independent of where the database server resides.
- Authentication Support. PostgreSQL provides support for multiple authentication mechanisms. Please see Section 1.5.10.3 Identification and Authentication for more information.
- PSQL: CLI to PostgreSQL

## 1.2 Client Connectors (in TOE)

Client Connectors are standardized programming interfaces allowing a software developer to connect a customer-specific application to PostgreSQL.


The TOE includes Client Connectors for the following enterprise programming environments:

- Java Database Connectivity (JDBC) is a Java database connectivity technology (Java Standard Edition platform) from Oracle Corporation. This technology is an Application Programming Interface (API) for the Java programming language that defines how a client may access a database. It provides methods for querying and updating data in a database. JDBC is oriented towards DBMS.
- Libpq, an API for client applications written in C, is the C application programmer's interface to PostgreSQL. libpq is a set of library functions that allow client programs to pass queries to the PostgreSQL backend server and to receive the results of these queries.

## 1.3 PostgreSQL Audit Extension (in TOE)

PostgreSQL Audit, an open source audit log generator, is included in the TOE. PostgreSQL Audit extends the logging capability supported by PostgreSQL by providing detailed logging classes, the ability to control logging at a per-object level, and including fully-qualified object names for logged statements in independent fields of the log output.



	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	Doküman No	BTBD-03-01-FR-01	
	<b>CCCS CERTIFICATION REPORT</b>	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

#### 1.4 PostGIS Spatial Extensions (in TOE)

PostGIS, an open source Geographic Information Server (GIS), is included in the TOE. PostGIS spatially enables PostgreSQL, allowing it to be used as a backend spatial database for geographic information systems. This is a non-security related component.

#### 1.5 Crunchy MLS PostgreSQL (not in TOE)

Crunchy MLS PostgreSQL is an optional component of Crunchy Certified PostgreSQL 9.5 that enhances PostgreSQL by allowing enhanced integration with Red Hat Enterprise Linux's SELinux capability. The Crunchy MLS PostgreSQL is prohibited in the evaluated configuration. The rationale for not including it in the scope of the evaluated configuration is it requires Red Hat Enterprise Linux's SELinux capability, which is not included in the evaluated configuration.

#### 1.6 Users

The users supported by the TOE are the same as those defined in the DBMS PP. The DBMS PP text is copied below:

*"A DBMS supports two major types of users:*

- *Users who interact with the DBMS to observe and/or modify data objects for which they have authorization to access; and*
- *The authorized administrators who implement and manage the various information-related policies of an organization (e.g., access, integrity, consistency, availability) for the databases that they install, configure, manage, and/or own."*

PostgreSQL supports the first major type of user defined in the DBMS PP through the use of Roles. A Role is used in PostgreSQL to define individual users, groups of users and sets of access privileges.

PostgreSQL supports the second major type of user defined in the DBMS PP, specifically authorized administrators, through:

- the Superuser, which is a role maintained by the TOE and
- the Cluster Owner, which is created during the installation of the TOE and is maintained by the operating system.

The Superuser administers the TOE through the TOE's user interfaces and is the focus of the SFR's described in this ST. The Cluster owner has the OS permissions to modify configuration files stored at the OS level and execute command line interfaces.


#### 1.7 Data

The data maintained by the TOE is the same as the definition of DBMS data in the DBMS PP as follows:

*"A DBMS stores, and controls access to, two types of data:*


- *The first type is the user data that the DBMS maintains and protects. User data may consist of the following:*
  - *The user data stored in or as database objects;*
  - *The definitions of user databases and database objects, commonly known as DBMS metadata; and*
  - *The user-developed queries, functions, or procedures that the DBMS maintains for users.*
- *The second type is the DBMS data (e.g., configuration parameters, user security attributes, transaction log, audit instructions, and records) that the DBMS maintains and may use to operate the DBMS."*

#### 1.8 Threats

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	Doküman No	BTBD-03-01-FR-01	
	<b>CCCS CERTIFICATION REPORT</b>	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

Threat	Definition
T.ACCESS_TSFDATA	A threat agent may read or modify TSF data using functions of the TOE without the proper authorization.
T.ACCESS_TSFFUNC	A threat agent may use or manage TSF bypassing the protection mechanisms of the TSF.
T.IA_MASQUERADE	A user or a process acting on behalf of a user may masquerade as an authorized entity in order to <u>gain unauthorized access to user data, TSF data, or TOE resources.</u>
T.IA_USER	A threat agent may gain access to user data, TSF data, or TOE resources with the <u>exception of public objects without being identified and authenticated.</u>
T.RESIDUAL_DATA	A user or a process acting on behalf of a user may gain unauthorized access to user or TSF data through <u>reallocation of TOE resources from one user or process to another.</u>
T.TSF_COMPROMISE	A user or a process acting on behalf of a user may cause configuration data to be inappropriately accessed (viewed, modified or deleted), or may compromise executable <u>code within the TSF.</u>
T.UNAUTHORIZED_ACCESS	A threat agent may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.

Table 1: Threats

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	Doküman No	BTBD-03-01-FR-01	
	<b>CCCS CERTIFICATION REPORT</b>	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

## 2 - CERTIFICATION RESULTS

### 2.1 Identification of Target of Evaluation


<b>Certificate Number</b>	21.0.03/TSE-CCCS-33
<b>TOE Name and Version</b>	Crunchy Certified PostgreSQL 9.5
<b>Security Target Document Title</b>	Crunchy Certified PostgreSQL 9.5 Security Target
<b>Security Target Document Version</b>	1.6
<b>Security Target Document Date</b>	May 9 2016
<b>Assurance Level</b>	EAL2+ (ALC_FLR.2)
<b>Criteria</b>	<ul style="list-style-type: none"> <li>Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012</li> <li>Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 4, September 2012</li> <li>Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 4, September 2012</li> </ul>
<b>Methodology</b>	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012
<b>Protection Profile Conformance</b>	Base Protection Profile for Database Management Systems (DBMS PP), Version 2.07, September 9, 2015
<b>Common Criteria Conformance</b>	<ul style="list-style-type: none"> <li>Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012</li> <li>Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012, extended</li> <li>Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 4, September 2012, conformant</li> </ul>
<b>Sponsor and Developer</b>	Crunchy Data Solutions, Inc
<b>Evaluation Facility</b>	CygnaCom Solutions
<b>Certification Scheme</b>	TSE CCCS

Table 2: Identification of TOE

### 2.2 Security Policy

The security policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	Doküman No	BTBD-03-01-FR-01	
	<b>CCCS CERTIFICATION REPORT</b>	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No


### 2.3 Assumptions and Clarification of Scope

Policy	Definition
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.ROLES	Administrative authority to TSF functionality shall be given to trusted personnel and be as restricted as possible supporting only the administrative duties the person has. This role shall be separate and distinct from other authorized users.
P.USER	Authority shall only be given to users who are trusted to perform the actions correctly.

Table 3: Organizational Security Policies

Assumption	Definition
<b>Physical aspects</b>	
A.PHYSICAL	It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.
<b>Personnel aspects</b>	
A.AUTHUSER	Authorized users possess the necessary authorization to access at least some of the information managed by the TOE.
A.MANAGE	The TOE security functionality is managed by one or more competent administrators. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.
A.TRAINEDUSER	Users are sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data.
<b>Procedural aspects</b>	
A.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration, and support of the DBMS.
A.PEER_FUNC_&_MGT	All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality and to be properly managed and operate under security policy constraints compatible with those of the TOE.
A.SUPPORT	Any information provided by a trusted entity in the IT environment and used to support the provision of time and date, information used in audit capture, user authentication, and authorization that is used by the TOE is correct and up to date.
<b>Connectivity aspects</b>	
A.CONNECT	All connections to and from remote trusted IT systems and between separate parts of the TSF not protected by the TSF itself are physically or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.

Table 4: Assumptions

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

## 2.4 Architectural Information

Figure 1 depicts a sample configuration of the TOE within its IT environment. Specifically, it shows a sample stand-alone system running the PostgreSQL server on Server 1.

User Applications (outside of the TOE) are shown running on each of Server 2 and Server 3. Each User Application has a Client Connection to the stand-alone PostgreSQL server running on Server 1. The sample stand-alone PostgreSQL server configuration reflected in Figure 1 contains the two Client Connectors supported by the TOE: JDBC, and libpq.

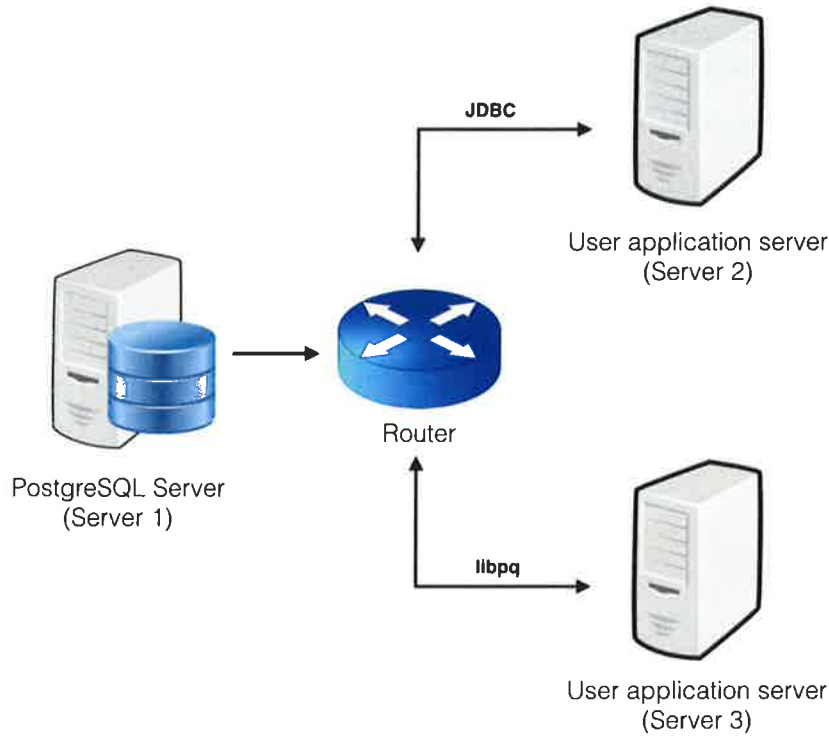


Figure 1: TOE Sample Configuration

### 2.4.1 Physical Scope of the TOE

Crunchy Certified PostgreSQL 9.5 is a software-only TOE. The physical scope of the TOE is an RPM.

#### 2.4.1.1 In Scope of Evaluation


The following Crunchy Certified PostgreSQL 9.5 components are in scope of evaluation:

- PostgreSQL
- Client Connectors
- PostgreSQL Audit Extension
- PostGIS Spatial Extensions

#### 2.4.1.2 Components and Capabilities that are Out of Scope

The following Crunchy Certified PostgreSQL 9.5 components are out of scope and thus not included in the TOE:

- Crunchy MLS PostgreSQL

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	<b>Doküman No</b>	BTBD-03-01-FR-01	
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	30/07/2015	
		<b>Revizyon Tarihi</b>	29/04/2016	<b>No</b>

The TOE relies on the operating system, which is part of the operational environment, to provide cryptographic support for communications, such as SSL encryption. Thus, cryptographic functionality is outside the scope of this evaluation. Specifically, support for secure communication channel and certificate-based authentication was not evaluated.

Crunchy PostgreSQL provides synchronous streaming replication as a way to replicate changes to data on one database server to the other database servers within a cluster. The evaluated TOE architecture is a stand-alone system running a single PostgreSQL server. Thus, streaming replication functionality is outside the scope of this evaluation.

### 2.4.1.3 TOE Architecture

The TOE can support a network of workstations communicating with several distributed PostgreSQL servers simultaneously. For the purposes of evaluation, the PostgreSQL servers will all be within a single LAN as per Figure 1.

The TOE architecture is an Enclave in which users access the TOE via a LAN. Users in other Enclaves will access the LAN and the host computers and servers on it by way of one or more boundary protection mechanisms (e.g., a firewall) and then through a communications server or router to the LAN. Depending on the particular Enclave configuration and the DBMS access policy that it supports, all users (both inside and outside the Enclave) may then access an application server, which either connects the TOE user to the Enclave computer on which the TOE operates or manages the complete user/DBMS session.

No operating systems or platforms are included in the TOE.

In addition, the following components in the IT environment are out of scope:

- Authenticator servers, if configured; and
- Terminal emulator

### 2.4.2 Logical Scope of the TOE

#### 2.4.2.1 Security Audit

The TOE generates audit records for security relevant events using a standard logging facility that is controlled by a system configuration file. For security relevant events resulting from actions of users or groups, the TOE associates them with the user or group that caused such event.

The TOE provides the capability to select auditable events and determine the information to be included in the audit record based on settings in system configuration files.


#### 2.4.2.2 User Data Protection

The TOE provided DAC controls access to objects on all subjects, all DBMS-controlled objects, and all operations among them. The TOE enforces DAC to objects based on the identity of the subjects or groups to which the subjects and objects belong, with access operations implemented for DBMS-controlled objects and object identity.

The TOE allows authorized administrators to specify how the objects that they control are protected. The TOE provides the capability to grant privileges both on RDBMS objects (such as tables, columns, views, Triggers, Functions, Procedures, Tablespace and Schemas) and to Roles. The TOE also provides for the inheritance of privileges between Roles. Explicit delegation of privileges on a database object among users is also permitted.

Residual information protection is enforced within the TOE through the implementation of a “write before read” mechanism.

#### 2.4.2.3 Identification and Authentication

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	Doküman No	BTBD-03-01-FR-01	
	<b>CCCS CERTIFICATION REPORT</b>	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

The TOE requires that each user is identified and authenticated prior to allowing any actions on behalf of the user. Further, the TOE requires that users are identified and authenticated by some method before allowing them access to TSF resources.

The available methods (auth-method: parameter) for client authentication definition include:

- Password (password)
- Pluggable Authentication Modules (pam)
- Peer Authentication (peer)
- Lightweight Directory Access Protocol (ldap)
- Generic Security Services API (gssapi)
- RADIUS Authentication (radius)

Password authentication is provided wholly within the TOE and available in both “md5” and “password” method.

PAM, PEER, LDAP, GSSAPI and RADIUS authentication are provided with the support of an external authentication mechanism provided by the IT environment.

Note that the use of the “Trust”, “Ident”, “SSL” and “SSPI” authentication methods are prohibited in the evaluated configuration.

Note: The MD5 implementation is vendor developed to the RFC 1321 specification and is strictly used for password hashing. The MD5 cryptographic function implementation, or module, has not been FIPS certified. The correctness of the cryptographic module used by the TOE is by Vendor assertion; the correctness and conformance of this cryptographic module to the RFC 1321 standard is not to be part of this evaluation.

The TOE associates user security attributes with subjects acting on the behalf of that user through a series of Role security attributes. Only users with sufficient privileges may modify the Role security attributes associated with subjects acting on behalf of users.

#### **2.4.2.4 Security Management**

The TOE provides security management through the server command line utilities and database command line utilities.

The TOE restricts the ability to perform security management functions to the authorized administrator or users with proper privileges (specifically, the CREATEDB or CREATEROLE Roles). In PostgreSQL, the authorized administrator is referred to as the Superuser.

#### **2.4.2.5 Protection of the TSF**


The TOE provides protection of the TSF through support of secure initialization process, self-protection of the TSF from tampering, non-bypassability of the SFR-enforcing functionality, and separation of the security domains.

#### **2.4.2.6 TOE Access**

The TOE is able to restrict the maximum number of concurrent sessions that belong to the same user. The number of multiple concurrent sessions per user is determined by the “connection limit” role security attribute. The “connection limit” is checked during session establishment and is configurable by an authorized administrator.

The TOE provides users with the ability to view their own connection history based on information recorded in an audit log. Upon a session establishment attempt, the TSF stores the date and time of the session establishment attempt of the user and the incremental count of successive unsuccessful session establishment attempts by the user. The TOE allows the user to retrieve the date and time of the previous last successful session establishment, the last unsuccessful attempt to session establishment, and the number of unsuccessful attempts since the previous last successful session establishment.

The TOE can deny session establishment based on user including user identity, time of day, day of the week, group identity, database name, Host IP address, and/or subnet address.

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	Doküman No	BTBD-03-01-FR-01	
	<b>CCCS CERTIFICATION REPORT</b>	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

## 2.5 Documentation

These documents listed below are provided to customer by the developer alongside the TOE:

Document Name	Version	Release Date
CRUNCHY CERTIFIED POSTGRESQL 9.5 SECURITY TARGET	1.6	May 9, 2016
SECURE INSTALLATION AND CONFIGURATION GUIDE	1.2	April 29, 2016

Table 5: Documentation-1

Also, the following product guidance documents are provided with the TOE. The documents are available to download from the TOE Vendor website.

Title	ID
The PostgreSQL Global Development Group; PostgreSQL 9.5 Documentation, Version 9.5	PG
The PostgreSQL JDBC Interface	JDBC
The PostgreSQL Global Development Group; PostgreSQL 9.5 Documentation, Chapter 31	libpq
PostgreSQL Audit Extension User Guide	pg_audit
PostGIS 2.2.2 Manual	PostGIS
Crunchy MLS PostgreSQL User Guide	mlspg

Table 6: Documentation-2

## 2.6 IT Product Testing

During the evaluation, all evaluation evidences of TOE were delivered and transferred completely to CCTL by the developers. All the delivered evaluation evidences which include software, documents, etc. are mapped to the assurance families Common Criteria and Common Methodology; so the connections between the assurance families and the evaluation evidences has been established. The evaluation results are available in the final Evaluation Technical Report v1.0 of Crunchy Certified PostgreSQL 9.5. It is concluded that the TOE supports EAL 2+ (ALC\_FLR.2).

IT Product Testing is mainly realized in two parts:


### 1-Developer Testing: (29 Tests)

- **TOE Test Coverage:** Developer has prepared TOE Test Document according to the TOE Functional Specification documentation.
- **TOE Test Depth:** Developer has prepared TOE Test Document according to the TOE Design documentation which includes TSF subsystems and its interactions.
- **TOE Functional Testing:** Developer has made functional tests according to the test documentation. Test plans, test scenarios, expected test results and actual test results are in the test documentation.

### 2- Evaluator Testing:

- **Independent Testing:** The evaluator conducted testing using all tests found in the developer test plan and procedures. All of them are related to TOE security functions. All functional tests were executed twice – once on RHEL 7.2 and once on RHEL 6.7. This ensured that all security functionality was tested on each claimed platform.
- **Penetration Testing:** Evaluator has done 3 penetration tests to find out if TOE's vulnerabilities can be used for malicious purposes:
  - Insecure Default Privileges
  - Denial of Service over Client Server Interface
  - Writing Arbitrary Data to Disk



	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

## 2.7 Evaluated Configuration

Hardware	Minimum Requirement
CPU	700 Mhz
RAM	256MB
Hard Disk	700Mb
Software	Minimum Requirement
Operating System	Red Hat Enterprise Linux 6.5
Kernel	2.6.32
GNU Make	3.8
GNU Readline	6.3
Tar	1.28
Gzip	1.2.4

Table 7: Evaluated Configuration

## 2.8 Results of the Evaluation


The verdict for the CC Part 3 assurance components (according to EAL2+ (ALC\_FLR.2) and the security target evaluation) is summarized in the following table:

Assurance Class	Component ID	Component Title	Verdict
Development	ADV ARC.1	Security architecture description	PASS
	ADV FSP.2	Security-enforcing functional specification	PASS
	ADV TDS.1	Basic design	PASS
Guidance documents	AGD OPE.1	Operational user guidance	PASS
	AGD PRE.1	Preparative procedures	PASS
Life-cycle support	ALC CMC.2	Use of a CM system	PASS
	ALC CMS.2	Parts of the TOE CM coverage	PASS
	ALC DEL.1	Delivery procedures	PASS
	ALC FLR.2	Flaw reporting procedures	PASS
Security Target evaluation	ASE CCL.1	Conformance claims	PASS
	ASE ECD.1	Extended components definition	PASS
	ASE INT.1	ST introduction	PASS
	ASE OBJ.2	Security objectives	PASS
	ASE REQ.2	Security requirements	PASS
	ASE SPD.1	Security problem definition	PASS
	ASE TSS.1	TOE summary specification	PASS
Tests	ATE COV.1	Evidence of coverage	PASS
	ATE FUN.1	Functional testing	PASS
	ATE IND.2	Independent testing - sample	PASS
Vulnerability assessment	AVA VAN.2	Vulnerability analysis	PASS

Table 8: Assurance Components

## 2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of "CRUNCHY CERTIFIED POSTGRESQL 9.5" product, result of the evaluation, or the ETR.

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	<b>Doküman No</b>	BTBD-03-01-FR-01	
		<b>Yayın Tarihi</b>	30/07/2015	
	<b>CCCS CERTIFICATION REPORT</b>	<b>Revizyon Tarihi</b>	29/04/2016	<b>No</b>

### **3 - SECURITY TARGET**


The security target associated with this Certification Report is identified by the following terminology:

Title: Crunchy Certified PostgreSQL 9.5 Security Target

Version: 1.6

Date of Document: May 9, 2016

This Security Target describes the TOE, intended IT environment, security objectives, security requirements (for the TOE and IT environment), TOE security functions and all necessary rationale.

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	<b>Doküman No</b>	BTBD-03-01-FR-01	
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	30/07/2015	
		<b>Revizyon Tarihi</b>	29/04/2016	<b>No</b>

## 4 - GLOSSARY

### 4.1-Acronyms

API	Application Programming Interface
CLI	Command Line Interface
DBA	Database Administrator
DDL	Data Definition Language
DML	Data Manipulation Language
FDW	Foreign Data Wrapper
GSSAPI	Generic Security Services Application Programming Interface
LDAP	Lightweight Directory Access Protocol
PAM	Pluggable Authentication Modules
RDBMS	Relational DBMS
RPM	RPM Package Manager
SQL	Structured Query Language
SSL	Secure Socket Layer Protocol
SSPI	Security Services Provider Interface
WAL	Write-Ahead Logging

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

#### 4.2-Terminology

#### TOE TERMINOLOGY

**Access Privilege.** “Access Privilege” means an object security attribute.

**Accessor.** “Accessor” means subject accessing a database object.

**Authorized User.** “Authorized User” means an entity that has been properly identified and authenticated. These users are considered to be legitimate users of the TOE.

**Client Connectors.** “Client Connectors” means standardized programming interfaces allow a software developer to connect a customer-specific application to PostgreSQL.

**Cluster Owner.** “Cluster Owner” means a user created during the installation process that is given ownership permissions of the TOE. This user is maintained by the OS and can only access the TSF data stored at the OS level after being authenticated at the OS level.

**Database.** “Database” means one or more named schemas, which in turn contain tables.

**Foreign Data Wrapper.** “Foreign Data Wrapper” means a standardized approach in PostgreSQL for handling access to remote objects from SQL databases.

**Function.** “Fuction” means a predefined block of statements that can be invoked with SQL commands, trigger operators, in view definitions and indexes and return a value.

**pg\_hba.conf.** “pg\_hba.conf” means a configuration file in PostgreSQL that is stored in the database cluster’s data directory, modifiable only by the Cluster Owner at the operating system level.

**postgrespl.conf.** “postgrespl.conf” means a human readable operating system level configuration file that can be directly reviewed and modified by a Cluster Owner using an operating system text editor provided with the IT environment.

**PSQL.** “PSQL” means the terminal-based front-end to PostgreSQL enabling PostgreSQL users either type in queries interactively, issue them to PostgreSQL, and see the query results or input them from a file.

**Role.** “Role” means, in PostgreSQL, either defined individual users, groups of users or sets of access privileges.

**RPM Package Manager.** “RPM Package Manager” means a collection of software tools that automates the process of installing, upgrading, configuring, and removing software packages for a computer's operating system in a consistent manner.

**Schema.** “Schema” means a collection of database objects as well as logical structures of data.


**Security Definer.** “Security Definer” means a function in PostgreSQL that is used to specify that the applicable function is to be executed with the privileges of the role which owns the function.

**Security Invoker.** “Security Invoker” means a a function in PostgreSQL that is used to specify that that the applicable function is to be executed with the privileges of the user that calls it.

**Superuser.** “Superuser” means a PostgreSQL Role that has been assigned the ‘superuser’ Role attribute and as a consequence bypasses all permission checks in PostgreSQL except the login requirement. Importantly, the Superuse is represents the authorized administrator as defined in the DBMS PP.

**Tablespace.** “Tablespaces in PostgreSQL allow database administrators to define locations in the file system where the files representing database objects can be stored. Once created, a tablespace can be referred to by name when creating database objects. Tables, indexes, and entire databases can be assigned to particular tablespaces.

**Trigger.** “Trigger” means an attribute of a Table that is a predefined block of statements executed when a DELETE, INSERT,

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

TRUNCATE, or UPDATE command is executed on the Table.

**View.** “View” means a selection of rows and columns from a table or set of joined tables.

**Write-Ahead Logging.** “Write-Ahead Logging” means a method for ensuring data integrity by which changes to data files (where Tables and indexes reside) must be written only after those changes have been logged (i.e., after log records describing the changes have been flushed to permanent storage).

### DBMS PP TERMINOLOGY

**Access.** “Access” means interaction between an entity and an object that results in the flow or modification of data.

**Access Control.** “Access Control” means security service that controls the use of resources (hardware and software) and the disclosure and modification of data (stored or communicated).

**Accountability.** “Accountability” means a property that allows activities in an IT system to be traced to the entity responsible for the activity.

**Administrator.** “Administrator” means a user who has been specifically granted the authority to manage some portion or the entire TOE and whose actions may affect the TSP. Administrators may possess special privileges that provide capabilities to override portions of the TSP.

**Assurance.** “Assurance” means a measure of confidence that the security features of an IT system are sufficient to enforce its security policy.

**Attack.** “Attack” means an intentional act attempting to violate the security policy of an IT system.

**Authentication.** “Authentication” means a security measure that verifies a claimed identity.

**Authentication Data.** “Authentication Data” means information used to verify a claimed identity.

**Authorization.** “Authorization” means permission, granted by an entity authorized to do so, to perform functions and access data.

**Authorized Administrator.** “Authorized Administrator” means the authorized person in contact with the TOE who is responsible for maintaining its operational capability.

**Authorized User.** “Authorized User” means an authenticated user who may, in accordance with the TSP, perform an operation.

**Availability.** “Availability” means timely (according to a defined metric), reliable access to IT resources.

**Compromise.** “Compromise” means a violation of a security policy.


**Confidentiality.** “Confidentiality” means a security policy pertaining to the disclosure of data.

**Configuration Data.** “Configuration Data” means data that is used in configuring the TOE.

**Conformant Product.** “Conformant Product” means a TOE that satisfied all the functional security requirements in Section 7.1 of the DBMS PP and satisfies all the TOE security assurance requirements in Section 7.2 of the DBMS PP.

**Database Management System (DBMS).** “Database Management System (DBMS)” means a suite of programs that typically manage large structured sets of persistent data, offering ad hoc query facilities to many users. They are widely used in business applications.

**Discretionary Access Control (DAC).** “Discretionary Access Control (DAC)” means a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. Those controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	<b>Doküman No</b>	BTBD-03-01-FR-01	
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	30/07/2015	
		<b>Revizyon Tarihi</b>	29/04/2016	<b>No</b>

**Enclave.** Enclave means a collection of entities under the control of a single authority and having a homogeneous security policy. They may be logical, or may be based on physical location and proximity.

**Entity.** “Entity” means a subject, object, user or another IT device, which interacts with TOE objects, data, or resources.

**Executable Code Within the TSF.** “Executable Code Within the TSF” the software that makes up the TSF which is in a form that can be run by the computer.

**External IT Entity.** “External IT Entity” means any trusted Information Technology (IT) product or system, outside of the TOE, which may, in accordance with the TSP, perform an operation.

**Identity.** “Identity” means a representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

**Integrity.** “Integrity” means a security policy pertaining to the corruption of data and TSF mechanisms.

**Named Object.** “Named Object” means an object that exhibits all of the following characteristics:

- The object may be used to transfer information between subjects of differing user and/or group identities within the TSF.
- Subjects in the TOE must be able to require a specific instance of the object.
- The name used to refer to a specific instance of the object must exist in a context that potentially allows subjects with different user and/or group identities to require the same instance of the object.

**Object.** “Object” means an entity within the TSC that contains or receives information and upon which subjects perform operations.

**Operating Environment.** “Operating Environment” means the total environment in which a TOE operates. It includes the physical facility and any physical, procedural, administrative and personnel controls.

**Public Object.** “Public Object” means an object for which the TSF unconditionally permits all entities “read” access. Only the TSF or authorized administrators may create, delete, or modify the public objects.

**Row Security Policy.** “Row Security Policy” means a policy determining access to the table for selecting rows or adding rows when row security is enabled.

**Secure State.** “Secure State” means a condition in which all TOE security policies are enforced.

**Security Attributes.** “Security Attributes” means TSF data associated with subjects, objects, and users that are used for the enforcement of the TSP.

**Security Level.** “Security Level” means the combination of a hierarchical classification and a set of non-hierarchical categories that represent the sensitivity of the information.

**Sensitive Information.** “Sensitive Information” means information that, as determined by a competent authority, must be protected because its unauthorized disclosure, alteration, loss, or destruction will at least cause perceivable damage to someone or something.

**Subject.** “Subject” means an entity within the TSC that causes operation to be performed.


**Threat.** “Threat” means capabilities, intentions and attack methods of adversaries, or any circumstance or event, with the potential to violate the TOE security policy.

**TOE Resources.** “TOE Resources” means anything useable or consumable in the TOE.

**Unauthorized User.** “Unauthorized User” means a user who may obtain access only to system provided public objects if any exist.

**User.** “User” means any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

**Vulnerability.** “Vulnerability” means a weakness that can be exploited to violate the TOE security policy.

	<b>BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT</b>	<b>Doküman No</b>	BTBD-03-01-FR-01	
	<b>CCCS CERTIFICATION REPORT</b>	<b>Yayın Tarihi</b>	30/07/2015	
		<b>Revizyon Tarihi</b>	29/04/2016	<b>No</b>

## 5 - BIBLIOGRAPHY

- [1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012
- [2] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012
- [3] BTBD-03-01-TL-01 Certification Report Preparation Instructions, Rel. Date: February 8, 2016
- [4] ETR v1.0 of Crunchy Certified PostgreSQL 9.5, Rel. Date: June 1, 2016
- [5] Crunchy Certified PostgreSQL 9.5 Security Target v1.6 [ST]
- [6] Secure Install and Configuration Guide v1.2 [INSTALL]
- [7] PostgreSQL 9.5.2 Documentation [ADMIN]

