Certification Report

EAL 2 Evaluation of

SAMPAŞ A.Ş.
ÇAYBİS V 1.0

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

TABLE OF CONTENTS

Document Information

Date of Issue	***05.07.2014***
Version of Report	***1.0***
Author	***Kerem KEMANECİ***
Technical Responsible	***Mustafa YILMAZ***
Approved	***Mariye Umay AKKAYA***
Date Approved	***07.07.2014***
Certification Number	***21.0.01/14-020***
Sponsor and Developer	***Sampaş A.Ş.***
Evaluation Lab	***TÜBİTAK BİLGEM OKTEM***
TOE	***ÇAYBİS V1.0***
Pages	***16***

Document Change Log

Release	***Date***	***Pages Affected***	***Remarks/Change Reference***
0.1	***01.07.2014***	***All***	***Initial***
1.0	***05.07.2014***	***All***	***Final version***

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.

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 STCD 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) 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 TÜBİTAK BİLGEM OKTEM, which is a public 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 ÇAYBİS (Web Based Application Software, product version: 1.0) whose evaluation was completed on 19.06.2014 and whose evaluation technical report was drawn up by TÜBİTAK BİLGEM OKTEM (as CCTL), and with the Security Target document with version no Çaybis ST v1.9 of the relevant product.

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

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.

1. EXECUTIVE SUMMARY

Evaluated IT Product Name: ÇAYBİS V1.0 Web Based Application Software
Developer: Sampaş A.Ş.
Name of CCTL: TÜBİTAK BİLGEM OKTEM
Assurance Package: EAL 2
Completion Date of Evaluation: 19.06.2014

Çaybis is an online application system that enables ÇAYKUR to buy and sell fresh tea. This application is about how tea is processing from seedling time to processed tea. Farmers brings fresh teas to gathering places that CAYKUR checks teas and buys. Then these teas are transporting processing units.
Office Centre and 60 units, that is running agriculture and personnel program in client server mode locally. Personnel monitoring and the center of agricultural activity and Headquarters units based on this data in real-time monitoring and management decisions, should be taken immediately.
Being the central structure of software and web-based program development, maintenance, support and management processes will be carried out from a single center.

1.1 Major Security Features:

- Security Audit:
  - The TSF generates audit logs that consist of various auditable events
- User Data Protection:
  - Access privilege assignments protects user data from unauthorized access
- Identification and Authentication:
  - Authorized users can access their relevant resources or functions once they have been successfully identified and authenticated using their usernames and passwords.
- Security Management:
  - Assign/modify access privileges
  - unlocking password for users
- TOE Access:
  - The TOE is able to deny session establishment once the session has expired.

1.2 Threats

The threats identified in this section are addressed by the TOE.

T.UNAUTH: Users or attackers could gain unauthorized access to the TOE data by bypassing the identification and authentication requirements.

T.DISCLOSURE: Users could gain the valuable information (passwords and enterprise data) of authorized users and administrators by sniffing the traffic

T.INJECT: Users could inject a malicious code inserted into strings (through a SQL query) by inputting data from the forms available in the Web Portal.

T.DATA_ACCESS: An unauthorized person views restricted hosted content compromising the confidentiality and integrity of enterprise data.

T.WEB_ATTACK: An attacker may compromise the integrity, availability and confidentiality of enterprise information by performing web application attacks.

T.RECONFIG: An attacker attemps to reconfigure the TOE to gain access to protected enterprise data compromising integrity and confidentiality.

1.3 Organizational Security Policies

The TOE does not include any Organizational Security Policy.

1.4 Configuration Required by the TOE

Manage the full cycle of hardware and software product development including requirements gathering, design, development, implementation and maintenance. The TOE operates in a web server environment. In addition to requiring services from the environment to achieve its primary aim, the TOE also relies on the environment to maintain a secure posture so that the application cannot be compromised by factors out of the TSF Scope of Control.

Minimum Software Requirements	Details
Operating System	Windows Server 2008 R2 Enterprise
Web Server	IIS version 6.1
Browser	Google Chrome version 15.0
Database	Oracle 11G R2 x64/x86 Edition
Web installer package	Microsoft .Net Framework 4.0

Table 3: Software Requirements

Minimum Hardware Requirements	Details
Server	16 virtual CPU(8x2) or higher processor,16 GB or more RAM, running Win 2008 R2
Client	1.6 GHz or higher processor,2 GB or more RAM ,running Windows 7

1.5 Assumptions About the Operating Environment

A.APP: It is assumed that the TOE and third party applications that the TOE relies upon have been configured in accordance with the installation guides. They are securely configured in such a way that the applications provide protection for the TOE from any unauthorized users or processes.

A.PROTECT: It is assumed that all hardware within the environment, including network and peripheral devices, has been approved for the transmitting of secured data. Each of these appliance configurations is securely managed by administrators to provide protection of secured data in terms of its confidentiality and integrity.

A.ADMIN: It is assumed that there are one or more competent individuals that are assigned to manage the TOE and its secured data. Such personnel are assumed not to be careless, willfully negligentor hostile.

A.NO_EVIL: TOE administrators and TOE users are assumed to be non-hostile and trusted to perform all their duties in a competent manner.

A.PHYS_SEC ÇAYBİS: Active Directory (LDAP)and Database will be hosted inside of a physically secure area.

A.TRANS_PROTECT: The IT environment will provide a secure channel so that all potentially valuable information (including credentials and enterprise data) is protected between the user and application server.

A.CAYBIS_DATA: The ÇAYBİS database is located within the enterprise network boundary and is configured so that only TOE administrators can directly access the interface of the database.

A.FIREWALL: The IT environment will implement gateway filtering, only allowing HTTPS traffic to pass through to ÇAYBİS.

2. CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Project Identifier	***TSE-CCCS-021***
TOE Name and Version	***ÇAYBİS V1.0***
Security Target Document Title	***Çaybis Security Target v1.9***
Security Target Document Version	***1.9***
Security Target Document Date	***19.06.2014***
Assurance Level	***EAL 2***
Criteria	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components,Version 3.1, Revision 4, September 2012
Methodology	• Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2012, Version 3.1, Revision 4
Protection Profile Conformance	***None***
Common Criteria Conformance	• Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components,Version 3.1, Revision 4, September 2012
Sponsor and Developer	***Sampaş A.Ş.***
Evaluation Facility	***TÜBİTAK BİLGEM OKTEM***
Certification Scheme	***Turkish Standards Institution*** ***Common Criteria Certification Scheme***

2.2 Security Policy

The TOE does not include any Organizational Security Policy.

2.3 Assumptions and Clarification of Scope

A.APP: It is assumed that the TOE and third party applications that the TOE relies upon have been configured in accordance with the installation guides. They are securely configured in such a way that the applications provide protection for the TOE from any unauthorized users or processes.

A.PROTECT: It is assumed that all hardware within the environment, including network and peripheral devices, has been approved for the transmitting of secured data. Each of these appliance configurations is securely managed by administrators to provide protection of secured data in terms of its confidentiality and integrity.

A.ADMIN: It is assumed that there are one or more competent individuals that are assigned to manage the TOE and its secured data. Such personnel are assumed not to be careless, willfully negligentor hostile.

A.NO_EVIL: TOE administrators and TOE users are assumed to be non-hostile and trusted to perform all their duties in a competent manner.

A.PHYS_SEC ÇAYBİS: Active Directory (LDAP)and Database will be hosted inside of a physically secure area.

A.TRANS_PROTECT: The IT environment will provide a secure channel so that all potentially valuable information (including credentials and enterprise data) is protected between the user and application server.

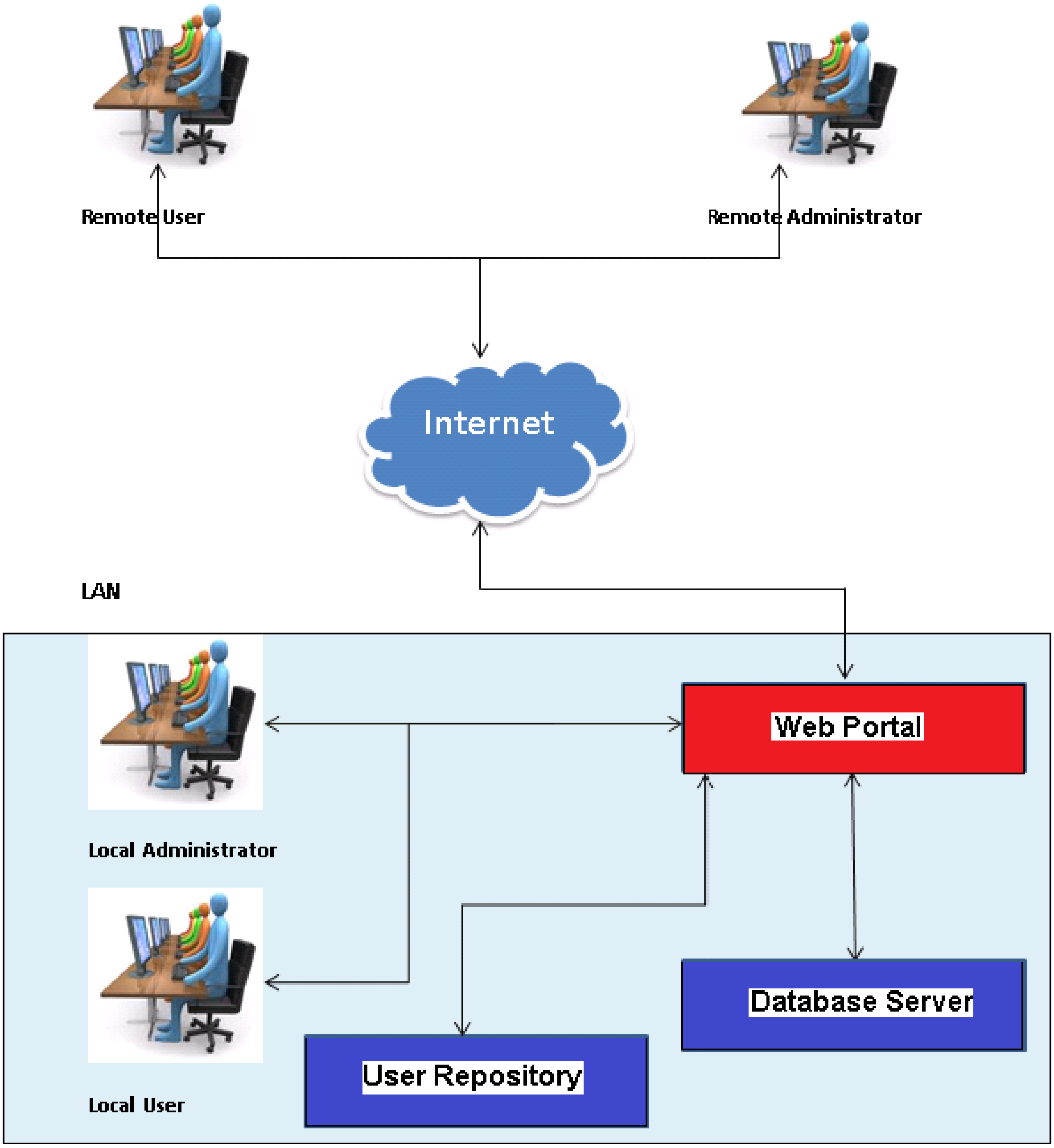
A.CAYBIS_DATA: The ÇAYBİS database is located within the enterprise network boundary and is configured so that only TOE administrators can directly access the interface of the database.

A.FIREWALL: The IT environment will implement gateway filtering, only allowing HTTPS traffic to pass through to ÇAYBİS.

2.4 Architectural Information

2.4.1 Physical Scope of the TOE

The TOE is the web application (web portal – indicated with red colour in the figure below) hosted on a web server. Web portal , database server and user repository (LDAP) are the components of the CAYBIS architecture. Process of authentication walks through on LDAP that will lock the user rights when user entered password incorrectly three times. Database server includes procedures.



Çaybis v1.0 physical scope

2.4.2 Logical Scope of the TOE

Logical scope under five main Security Functions headings ;

Security Function	TOE Scope Description
Security Audit	The most logical necessity is to see which user and which progress is in use. The TSF generates audit logs that consist of various auditable events. Date and time of events, usernames, and events taken by the authorized users are recorded. Authorized administrators have the capability to read and view all the recorded logs stated above through the web portal.
User Data Protection	Authorized administrators of the TOE can perform the following functions to the user or administrator accounts: 1. Access privilege assignments by user levels 2. Unlock passwords for authorized users 3. Change password for own administrator
Identification and Authentication	The unambiguous identification and authorised users and the correct association of security attributes with users and subjects is critical to the enforcement of the intended security policies.The families in this class deal with determining their authority to interact with the TOE, and with the correct association of security attributed for each authorised user. Identification and Authentication is required to ensure that users are associated with the proper security attributes(e.g. identity,group,roles,security or integrity levels). When a user issues a request to the TOE to access the modules defined,the TOE requires that the user(being User or Administrator) identify and authenticate themselves before performing any TSF mediated action on behalf of the user.The TOE checks the credentials presented by the user upon the login page against the authentication information in the database.Each users account only exists in the database that relates to the user organisation. Authorized users can access their relevant resources or functions once they have been successfully identified and authenticated using their usernames and passwords.

Security Management	At least one administrator is required to have full access rights to manage the TOE.Authorized administrators can assign access privileges to users by user levels based on the functions or resources that they are allowed to perform. Additional functionalities such as modifying access privileges and unlocking password for users are also accessible by authorized administrators.
TOE Access	Duration of the session can determined by the manager(in minutes). After inactivity of the specified period, the authorized users are then returned to the main page of the ÇAYBIS web portal. The TOE is able to deny session establishment once the session has expired. Re-authentication is required once the session ended.

2.5 Documentation

Document list for customers:

- CAYBIS Fonksiyonel Belirtim Guvenli Mimari Tasarım Dokümanı V1.6 (Functional Specification and Secure Architecture Document)
- CAYBIS Konfigürasyon Dokümanı V1.1 (Configuration Document)
- CAYBIS Kullanıcı Dokümanı V1.3 (User Manual)
- CAYBIS Kurulum ve TeslimDokümanı V1.0 (Installation and Delivery Document)
- CAYBIS ST V1.9 (Security Target)
- CAYBIS TestDokümanı V1.1 (Test Documentation)

2.6 IT Product Testing

Developer Tests:
The developer's testing strategy was to define test cases that specified complete coverage of all security functions defined in the ST. The test cases were written by the developers to exercise the security functionality of the TOE.
Test scenarios, expected results and obtained results are listed by Sampaş A.Ş. testers. For each test, expected results are same with obtained test results.

Evaluator Tests:
The evaluator ran all of the developer tests to show completeness of the test coverage. The sample included tests to exercise each security function and TSFI. The purpose of running this sample of the tests was to gain confidence in the developer's functional test results. The evaluator compared the results of each test with the corresponding expected results provided by the developer as ATE_FUN.1 evidence.

Evaluator Defined Tests:
The evaluator's strategy in developing the evaluator-defined tests for the TOE was to supplement the developer's functional tests and the penetration tests.

The evaluator-defined tests were devised to augment the developer's functional tests in order to exercise functionality in greater depth than the developer tests provided. Evaluator defined 8 more functional tests and 9 penetration tests in this case.

Penetration Tests:
9 Evaluator defined - penetration tests were ran by evaluator. All results of the penetration testing were visually verified by the evaluator on same configuration provided in ST document. All penetration tests that were run by the evaluator passed.

2.7 Evaluated Configuration

The Evaluated configuration was consistent with the configuration specified in ST document(Çaybis ST V1.9). See Section 1.4 Configuration Required by the TOE

2.8 Results of the Evaluation

All evaluator actions are satisfied for the evaluation level of EAL 2 as defined by the Common Criteria and the Common Methodology. The overall verdict for the evaluation is PASS. The results are supported by evidence in the ETR. There is no residual vulnerability for this product. TOE is resistant against to "BASIC LEVEL" attack potential attackers.

Assurance class	**Assurance components**	**VERDICT**
ADV: Development	ADV_ARC.1 Security architecture description	PASS
	ADV_FSP.2 Security enforcing functional specification	PASS
	ADV_TDS.1 Basic design	PASS
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	PASS
	AGD_PRE.1 Preparative procedures	PASS
ALC: Life cycle support	ALC_CMS.2 Parts of the TOE CM coverage	PASS
	ALC_CMC.2 Use of a CM system	PASS
	ALC_DEL.1 Delivery procedures	PASS
ASE: 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 Derived security requirements	PASS
	ASE_SPD.1 Security Problem Definition	PASS
	ASE_TSS.1 TOE summary specification	PASS
ATE: Tests	ATE_IND.2 Independent testing sample	PASS
	ATE_FUN.1 Functional testing	PASS
	ATE_COV.1 Evidence of coverage	PASS
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis	PASS

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of Çaybis v1.0 Web Based Application Software product, result of the evaluation, or the ETR.

3 SECURITY TARGET

The ST associated with this Certification Report is identified by the following nomenclature:

Title:	Çaybis ST v1.9
Version:	1.9
Date:	19.06.2014

4 GLOSSARY

CCCS:	Common Criteria Certification Scheme (TSE)
CCTL:	Common Criteria Test Laboratory (OKTEM)
CCRA	Common Criteria Recognition Arrangement
CEM:	Common Evaluation Methodology
IIS	Internet Information Services
DNS	Domain Name System
ETR:	Evaluation Technical Report
IT:	Information Technology
ISP:	Internet Service Provider
LDAP:	Lightweight Directory Access Protocol
NTP:	Network Time Protocol
STCD:	Software Test and Certification Department
ST:	Security Target
TOE:	Target of Evaluation
TSF:	TOE Security Function
TSFI:	TSF Interface
SFR:	Security Functional Requirement
EAL:	Evaluation Assurance Level
Evaluator:	TÜBİTAK BİLGEM OKTEM
Developer:	Sampaş A.Ş.
RAM	Random Access Memory
HTTP	Hyper Text Transfer Protocol
HTTPS	Secure Hyper Text Transfer Protocol
TSE	Turkish Standards Institutions

5 BIBLIOGRAPHY

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012
2. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012
3. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components,Version 3.1, Revision 4, September 2012
4. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2012, Version 3.1, Revision 4

5. YTBD-01-01-TL-01 CERTIFICATION REPORT PREPARATION INSTRUCTIONS, Version 1.0

6 ANNEXES

There is no additional information which is inappropriate for reference in other sections.