Certification Report

EAL 2+(ALC_FLR.1)

Evaluation of

Sisoft Sağlık Bilgi Sistemleri Ltd. Şti.
(Sisoft Healthcare Information Systems)

Sisoft WEBHBYS V2.0.0.3

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

TABLE OF CONTENTS

Document Information

Date of Issue	***04.09.2013***
Version of Report	***1.1***
Author	***Kerem KEMANECİ***
Technical Responsible	***Mustafa YILMAZ***
Approved	***Mariye Umay AKKAYA***
Date Approved	***04.09.2013***
Certification Report Number	***21.0.01/13-027***
Sponsor and Developer	***Sisoft Sağlık Bilgi Sistemleri Ltd. Şti.***
Evaluation Lab	***TÜBİTAK BİLGEM OKTEM***
TOE	***Sisoft WEBHBYS V2.0.0.3***
Pages	***22***

Document Change Log

Release	***Date***	***Pages Affected***	***Remarks/Change Reference***
V0.1	***15.08.2013***	***All***	***Initial***
V1.0	***03.09.2013***	***All***	***Final***
V1.1	***04.09.2013***	***All***	***Review Corrections***

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 Sisoft WEBHBYS (product version: V2.0.0.3) whose evaluation was completed on 19.07.2013

and whose evaluation technical report was drawn up by TÜBİTAK BİLGEM OKTEM (as CCTL), and with the Security Target document with version no 1.9 (16-JULY-13) 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: Sisoft WEBHBYS V2.0.0.3
Developer's Name: Sisoft Sağlık Bilgi Sistemleri Ltd. Şti. (Sisoft Healthcare Information Systems)
Name of CCTL: TÜBİTAK BİLGEM OKTEM
Assurance Package: EAL 2+ (ALC_FLR.1)
Completion Date of Evaluation: 19.07.2013

The Security Target v1.9 is the basis for this certification. It is not based on a certified Protection Profile.

For threats and assumptions see section 2.3*"Assumptions and Clarification of Scope"*.

1.1 Description Of TOE:

Sisoft WebHBYS v2.0.0.3 is a Healthcare Information Management System Software (HIMSS) which is used by hospitals. Sisoft WebHBYS product provides reuse of electronic registers of patients' examination, etude, medicine, material, operation, admission, reports and of all healthcare corporation/organization services with niceties, examining quickly every application of a patient. All personal informations of a patient (Name, Surname, Date/Place of Birth, Blood Group etc.) and all operation informations with contact information of a patient (Social Security, Referral, Corporation, Register No etc.) are being kept safely. (Speed taped in emergency service and primary operation realization feature are being provided.)

The TOE is a specialist software module designed to be used as a core security controlling module for a web-based application environment. The TOE provides core security functionality such as;

- ✓ identification,
- ✓ authentication,
- ✓ access control,
- ✓ secure communications
- ✓ application security management.

The TOE is a java module which is part of the Sisoft WebHBYS Healthcare information Management System is a web application hosted on a web server.

1.2 TOE Security Assurance Requirements:

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria. TOE meets the assurance requirements of Assurance Level EAL2 augmented by ALC_FLR.1. Detailed table of EAL2+(ALC_FLR.1) assurance package is shown below.

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_CMC.2 Use of a CM system
	ALC_DEL.1 Delivery procedures
	ALC_FLR.1 Flaw remediation
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security Problem Definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.2 Independent testing sample
	ATE_FUN.1 Functional testing
	ATE_COV.1 Evidence of coverage
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

1.3 TOE usage and major security functions

1.3.1 Rule-based application oriented access controls

Provide access to application-oriented access to external systems in environments where information is stored as encrypted. Managing the authority assigned to Sisoft WebHBYS application, rule-based application-oriented access controls can significantly mitigate the threats posed by malicious code due to software vulnerabilities.

1.3.2 Verification of Releases

SHA-2 checksum verification to ensure the integrity of releases are published values. These subprograms generate SHA-2 hashes of data. The SHA-2 algorithm ensures data integrity by generating a 128-bit cryptographic message digest value from given data confidence in the oracle.

1.3.3 Update Policy

Version to update the license information are tracked by individual users, version of the update process details are recorded. Version updates is based on the feedbacks from our customers and the Republic of Turkey Ministry of Health. Each customer is determined by the license code number and password. In addition, ethernet and mac id is taken from customer application server.

1.3.4 SSL Option

The Sisoft WebHBYS application has the ability to work with SSL. Users have the option to log on with the application of qualified electronic signatures. Electronic data are used for the purpose of any change or modification. Qualified electronic certificates X.509 standards that meet this standard are produced and web browsers, smart cards and tokens that respect and are supported by Sisoft WebHBYS.

1.3.5 Authorization

Powers of access and operation by the user control is provided on the basis of the definitions. Sisoft WebHBYS contained in user and group definitions section for making authority, which authority will be determined user. This authorization can only be perform by administrator.

1.3.6 Authentication and Session Tracking

The activity does not present a specific period of time the application automatically terminated user sessions. If the user is authenticated, the server then verifies that the user has the privilege to access the requested page against a file. If the user has access, the Web server then serves the page. If the user is denied access, the server either requests the username/password combination again or presents an error message on the browser window. Sisoft WEBHBYS application user input incorrectly three times for 15 minutes in appreciation of his entry closes.

Security function	Description
Access control	The TOE manages access control within each organisation based on user IDs, user roles and access control lists. The TOE maintains access control lists for each object within an organisation. Each ACL maps users and roles to the operations that they are permitted to perform on the object.
Identification and authentication	The TOE requires that each user is successfully identified (user ID) and authenticated (password) before any interaction with protected resources is permitted.
Security Management	The TOE provides functions that allow management of the TOE and its security functions. The TOE restricts access to the management functions based on the role of the user.

1.4 Special Configuration Requirements

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 technology services.

The TOE requires the following from the environment to function:

Type	Description	
Operating System	Suse Enterprise Server 11 or MS Windows 2008 Ent Edt.	
Web Server	Oracle Weblogic 11g	
Database (RDBMS)	Oracle 11g R2	
VTYS Server	Processor	2 x Intel XEON Processor x5670 2.93 GHz 12MB Cache
	RAM	32 GB
	HDD	2 x 146 GB 10K 6Gbps SAS | 3 x 600 GB 10K 6Gbps SAS
	RAID Card	512 MB
	RAID Support	0 / 1 / 5 / 10
	Network	4 x gigabit LAN (10 /100 / 1000)
	Power Supply	2x 800W
APP Server	Processor	2 x Intel XEON Processor x5670 2.40 GHz 12MB Cache
	RAM	16 GB
	HDD	2 x 146 GB 10K 6Gbps SAS | 3 x 600 GB 10K 6Gbps SAS
	RAID Card	512 MB
	RAID Support	0 / 1 / 5 / 10
	Network	4 x gigabit LAN (10 /100 / 1000)
	Power Supply	2x 800W
Client	Processor	P4 CELERON 2.8 İŞLEMCİ
	RAM	512 MB DDR400 RAM
	HDD	40 GB RPM 7200 HDD
	Network	Ethernet (10 /100 / 1000)
	Power Supply	350W
	OEM	Klavye Mouse Barkode Writer and Reader

1.5 Evaluation result

According to Evaluation Technical Report for this product provides sufficient evidence that it meets the EAL 2 augmented with ALC_FLR.1 assurance requirements for the evaluated security functionality.The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4. CCS Certification Body declares that the

"Sisoft WEBHBYS v2.0.0.3" evaluation meets all the conditions of the Arrangement on the Recognotion of Common Criteria Certificates and that the product will be listed on the CCS Certified Product List (CPL) and the official Common Criteria Portal website.

Assurance Class	PASS/FAIL
ASE – Security Target	PASS
ADV - Development	PASS
AGD – Guidance Documents	PASS
ALC – Life Cycle Support	PASS
ATE - Tests	PASS
AVA – Vulnerability Analysis	PASS
RESULT	**PASS**

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Project Identifier	***TR-21.0.01/TSE-CCCS-015***
TOE Name and Version	***Sisoft WEBHBYS V2.0.0.3***
Security Target	***Sisoft WebHBYS of Security Target***
Security Target Version	***v1.9***
Security Target Date	***16-JULY-13***
Assurance Level	***EAL2 +(ALC_FLR.1)***
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 Criteria for Information Technology Security Evaluation, Evaluation Methodology Version 3.1 Revision 4, September 2012
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	***Sisoft Sağlık Bilgi Sistemleri Ltd. Şti.***
Evaluation Facility	***TÜBİTAK BİLGEM OKTEM***
Certification Scheme	***TSE-CCCS***

2.2 Security Policy

The TOE is a special software module designed to be used as a core security controlling module for a web-based application environment. The TOE provides core security functionality such as;

- ✓ identification,
- ✓ authentication,
- ✓ access control,
- ✓ secure communications
- ✓ application security management.

2.2.1 Identification&Authentication:

When a user issues a request to the TOE to access a protected resource, the TOE requires that the user (being an User, Administrator) identify and authenticate themselves before performing any 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.

2.2.2 Access Control:

The access control function permits a user to access a protected resource only if a user ID or role of the user has permission to perform the requested action on the resource. Access rules are stored in Access Control Lists.

2.2.3 Secure communications:

SSL provides secure data communication over the Internet encrypted. The TOE supports SSL protocol. Sets the SSL protocol for use with the product are made on the application server. SSL protocol allows communication confidential and integrity.

2.2.4 Application Security management:

The Sisoft WebHBYS contains various management functions to ensure efficient and secure management of the TOE: user management, permission management for functions and data management. The TOE maintains two roles within the TOE to ensure that the functions are restricted to only those users that need to have access to privileged functions. The roles maintained by the TOE are: User and Administrator. The functions above, and indeed, aspects of these functions, are restricted based on these roles.

None of Organizational Security Policy is adressed by the TOE.

2.3 Assumptions and Clarification of Scope

The consumers should know that TOE is a special Web Application Module which is part of Sisoft Web HBYS(Hastane Bilgi Yönetim Sistemi – Healthcare Information Management System) v.2.0.0.3, that brings secure web application management, identification, authentication, password security, secure connections.

The consumers who plans to use the product should consider the assumptions below:

2.3.1 ASSUMPTIONS:

2.3.1.1 A.ENVIRONMENT

The TOE environment will provide appropriate authentication and authorisation controls for all users and administrators in the under environment (including the Operating System, DataBase, and Web Server)

2.3.1.2 A.ADMIN

It is assumed that the administration who manages the TOE is not hostile and is competent.

2.3.1.3 A.PHYSICAL

It is assumed that the servers that host the web and database servers are hosted in a secure operating facility with restricted physical access with non- shared hardware.

2.3.1.4 A.DATABASE

It is assumed that the databases in the TOE environment have been correctly configured according to the principle of least privilege.

2.3.1.5 A.NETWORK

It is assumed there is appropriate network layer protection, that there is a firewall in place that only permits access through required ports for external users to access the web-server.

2.3.1.6 A.PATCH

It is assumed that the underlying operating system, web-server, application server and DBMSs and are patched and hardened to protect against known vulnerabilities and security configuration issues.

2.3.1.7 A.SSL_CONFIG

It is assumed that the web-server has SSL certificates installed and are valid (not revoked or expired), are sourced from a trusted entity.

2.3.1.8 A.MANAGEMENT

All management of the TOE will be performed through the management interfaces of the TOE and not through the under environment.

2.3.1.9 A.COMM

It is assumed that the web-server uses SSL when user data is traversing accross the internet from to the Sisoft WebHBYS application.

TOE is evaluated to meet all assurance requirements to provide security against Basic Level (EAL 2 augmented with ALC.FLR.1) attackers with the scope of the threats listed below:

2.3.2 THREATS:

2.3.2.1 T.ACCESS

An unauthorized user obtains or modifies stored user data that they are not authorised to access resulting in a loss of confidentiality or integrity of the data.

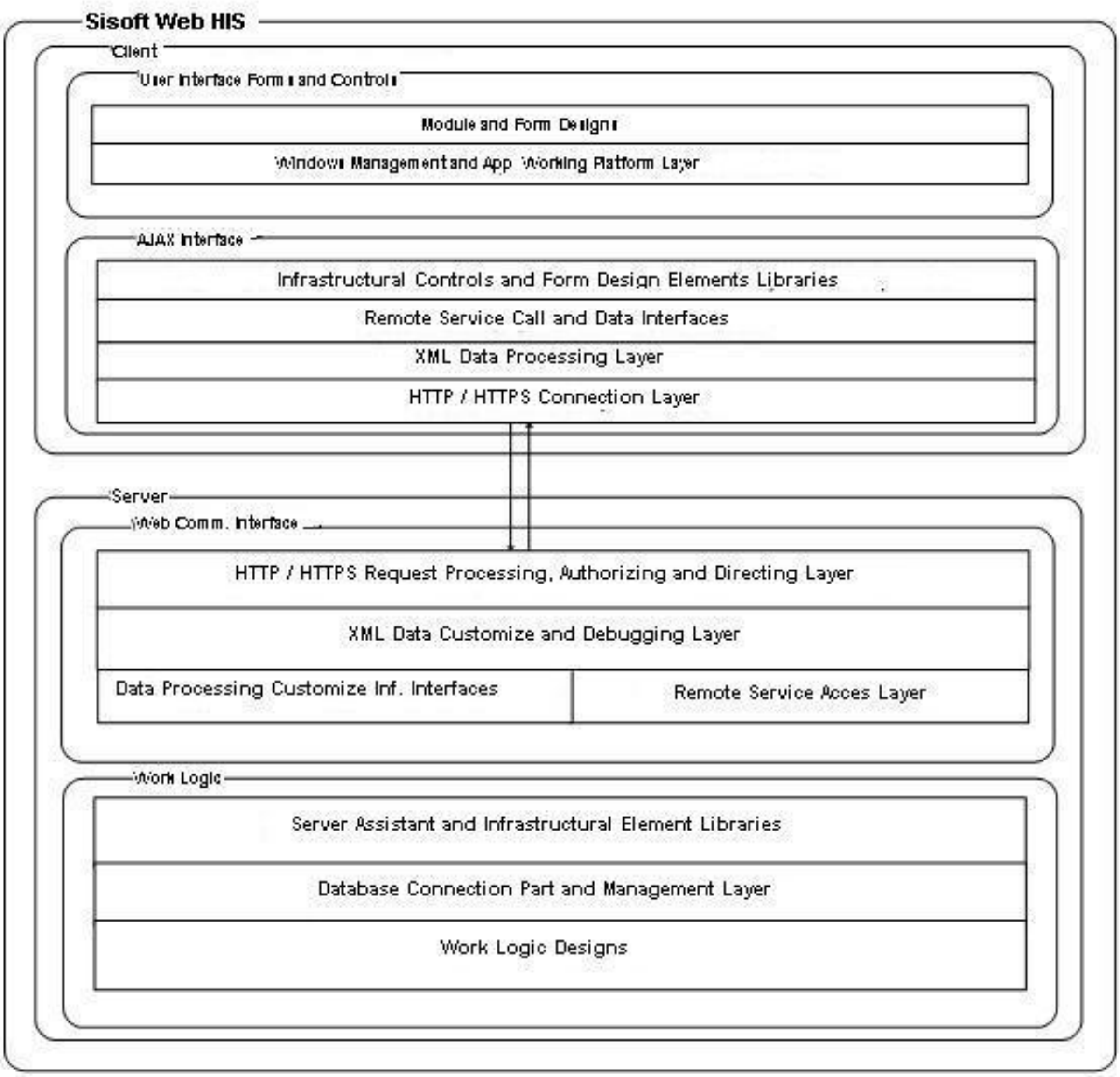
2.3.2.2 T.MANAGEMENT

An unauthorized user modifies management data that they are not authorisedto access resulting in a loss of integrity of the data that the TOE uses to enforce the security functions.

2.3.2.3 T.PASSWORD

An unauthorized user gains access to the passwords in the database and use them to authenticate to the TOE resulting in a loss of confidentiality or integrity of user or management data.

2.4 Architectural Information


Sisoft Web HIS
Client
User Interface Forms and Controls
Module and Form Designs
Windows Management and App. Working Platform Layer
AJAX Interface
Infrastructural Controls and Form Design Elements Libraries
Remote Service Call and Data Interfaces
XML Data Processing Layer
HTTP / HTTPS Connection Layer
Server
Web Comm. Interface
HTTP / HTTPS Request Processing, Authorizing and Directing Layer
XML Data Customize and Debugging Layer
Data Processing Customize Inf. Interfaces
Remote Service Acces Layer
Work Logic
Server Assistant and Infrastructural Element Libraries
Database Connection Part and Management Layer
Work Logic Designs

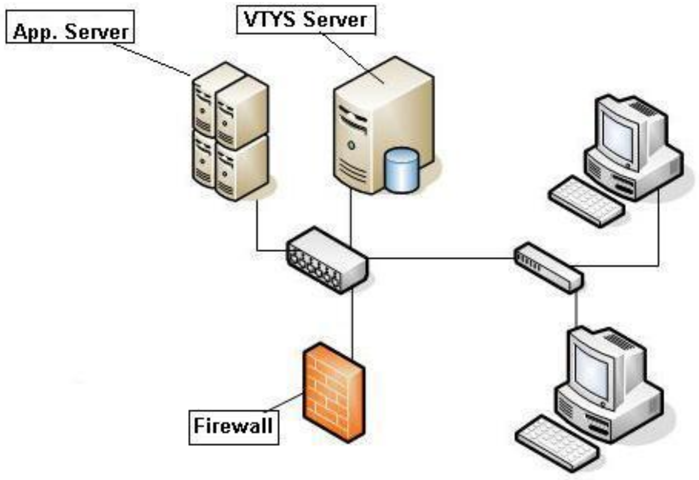
Communication Interface

Sisoft WEBHBYS (Healthcare Information System) architecture is formed with two primary structure such as server and client. The work type (logic) and code items in server part connect with user interfaces through XML Web Services.

Sisoft Healthcare Information Systems' Web-based Corporate Applications: It has highly strong and flexible architecture formed with infrastructures on server part such as load-balancing, authorizing, database connection management, etc... and web interface that connects XML Web Services that abstracts wholly work logic from user interfaces found on server part and powered by AJAX on WEB 2.0 standards and RIA (Rich Internet Applications) without needing any software set-up on updated Internet Browsers (E.g. Internet Explorer, Firefox, etc...)

There are some kind of structures that provides data connection between server and client and that provides the transformation of objective data to XML or XML to objective data. Starting from HTTP connection, authorizing, directing and data processing structures are composed in project core as infrastructural interfaces. Client is able to set-up synchronous and asynchronous connections through connection layer server. The results can be obtained by transmitting HTTP request to the server through those connections.

Securer and Broad Accessibility via HTTPS Protocol



HTTPS Protocol

Server Connection Layer transmits the request to a upper layer so as to provide the transformation XML to objective data following the analyze of HTTP request via various filters in a basis of an authorization by using HTTP session.

Then it's assigned to remote service access points so as to transmit upper design codes or other remote XML Web Services by using fundamental structures in Web Connection Interface. Now it's the role of work logic. The work logic forms a work type routine for all structural software library and a targeted processing in an easier, securer and quicker way in a common standard.

It's thought between a fundamental infrastructure parts for database connection repository and work logic forming in order to realize a high productivity database processing under control. Software code elements are found on topping layer in the system by leveling in the basis of modules.

It forms a multi-layered platform that can operate on Internet Browser without needing any set-up with a high level of accessibility and easier-to-use. It enables a high level of design and easier-to-use for code elements and XML Web Service Call and feedback process on application server. The Interface Design Library which is formed dynamically operates as integrated via AJAX by working with data processing and connection layer.

2.5 Documentation

Document list for customers:

Sisoft WEBHBYS v2.0.0.3 **Security Target Document v1.9** (Güvenlik Hedefi)
Sisoft WEBHBYS v2.0.0.3 **Kullanıcı Kılavuzu v2.1** (User Manual)
Sisoft WEBHBYS v2.0.0.3 **Teslim ve Kurulum Dökümanı v2.0** (Delivery and Installation Doc.)

2.6 ***IT Product Testing***

Sisoft WEBHBYS v2.0.0.3 is evaluated for EAL 2+(ALC_FLR.1). This level requires developer tests assessment, independent functional testing, penetration tests (vulnerability analaysis) conducted by evaluator laboratory.

2.6.1. Configuration Used For Tests:

Testing environment is same with suggested environment and application version(Sisoft WEBHBYS v2.0.0.3). See Certification report section **1.6. Special Configuration Requirements** for detailed configuration.

2.6.2. Developer Test Assessment:

Test Scenarios, expected results and obtained results are listed by Sisoft Company testers. For each test, expected results are same with obtained test results. Developer Tests are explained in Sisoft WEBHBYS v2.0.0.3 **Test Dökümanı v1.0** (Testing Document)

- The tester chosen different functionalities thus different interfaces seperately one by one. But tested every iterative step within each security funciton in one test scenario.
- Test document is specifying testing configuration, all tests are conducted according to suggested configuration. See section 1.6. This configuration is product's standard intallation configuration.
- Test results are given in a detailed and clearness as it requires.

2.6.3. Evaluator Tests:

The evaluator repeated all tests conducted by developer, according to Sisoft WEBHBYS v2.0.0.3 **Test Dökümanı v1.0** (Testing Document). Evaluator found that testing approach for each interface demonstrates the expected behaviour of that interface. There is correspondance between TSFI and developer tests and all security functions are covered. Test prerequisites, test steps and expected result(s) adequately test each interface.

2.6.4. Independent Testing:

Independent tests are conducted by the evaluator, the philosphy of independent tests are focusing the main security functions that could be very critical. After assessing developer tests, the evaluator creates more number of tests and goes into more details. Independent testing is a process, if a test is failed the developer is expected to fix the problem, after the update the same test is repeated. At the end of independent test process all test results are obtained as expected by test scenarios.

Total number of 14 independent tests were realized by evaluator. Expected test results are consistent with the obtained test results.

2.6.5. Penetration Tests:

Penetration tests are conducted by the evaluator against all exploitable vulnerabilities and residual vulnerabilities, detailing for each:

a) its source
b) the SFR(s) not met;
c) a description;
d) whether it is exploitable in its operational environment or not (i.e. exploitable or residual).
e) the amount of time, level of expertise, level of knowledge of the TOE, level of opportunity and the equipment required to perform the identified vulnerabilities, and the corresponding values using the tables 3 and 4 of Annex B.4 CEM v3.1 rev4.

Penetration tests are also independent tests those are conducted against vulnerabilities. Penetration testing work is also a kind of process if a test fails, evaluator is expected to fix the vulnerability. After update of the TOE test is reconducted. The final results are as expected and all penetration test results are successful.

Totally 13 penetration tests were conducted for Sisoft WebHBYS v2.0.0.2. Some vulnerabilities detected in this version and developer were informed about vulnerabilities. Then the developer released a new version (Sisoft WebHBYS v2.0.0.3) against faults detected. Those tests which failed were repeated by evaluator on Sisoft WebHBYS v2.0.0.3.

As a result no vulnerabilities were detected in the terms of given threats and assumtions specified in Security Target Document v1.9. In this terms Sisoft WebHBYS v2.0.0.3 is resistant against basic level attack potential attackers.

2.7 Evaluated Configuration

The suggested environment is given in section 1.6 of this report. All tests were conducted on this installed configuration. The evaluated version is Sisoft WebHBYS v2.0.0.3. The product supports SSL, SSL certificate ispresented in installated package by default. Its assumed that SSL is used. Subsystems of Sisoft WebHBYS v2.0.0.3:

- Access Control
- Security Management
- Calling Forms

Sisoft WebHBYS v2.0.0.3 Process Subsystem:

- Patient Book / Admittace
- Consulting Module

- Inpatient Follow-up Module
- Pay Desk Module
- Pharmacy Module
- Stock Follow-up Module
- Purchase Module
- Fixed Asset Module
- Accounting Module
- Billing Module
- Diet Module
- Blood Center Module
- Surgery Room Module
- Device Follow-up Module
- Emergency Action Module

2.8 Results of the Evaluation

All evaluator actions are satisfied for the evaluation level of EAL2+ (ALC_FLR.1) as defined by the Common Criteria and the Common Methodology. The overall verdict for the evaluation is PASS. The results are supported by the evidence in the ETR.

As a result no vulnerabilities were detected in the terms of given threats and assumtions specified in Security Target Document v1.9 by the Developer. About TOE, in this terms no residual vulnerability was detected by evaluator, Sisoft WebHBYS v2.0.0.3 is resistant against 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
	ALC_FLR.1 Flaw remediation	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

- The TOE must be protected against insecure network connections and restricted physical access with non- shared hardware.
- The location of the TOE must be managed well (stable power, proper temperature etc.) Measures must be taken against non-hostile users.
- Appropriate network layer protection and a firewall in place must be provided that only permits access through required ports for external users to access the web-server.
- Appropriate authentication and authorisation controls must be provided for all users and administrators under environment (including the Operating System, DataBase, and Web Server).
- Operating system, web-server, application server and DBMS must be patched and hardened to protect against known vulnerabilities and security configuration issues.
- Web-server must be SSL certificates-installed and are valid (not revoked or expired), are sourced from a trusted entity.
- Responsible administrators must follow administrator guidence document for the conforming environment of the TOE and also installation and configuration of the TOE.
- All management of the TOE must be performed through the management interfaces of the TOE and not through the under environment.
- The web-server must use SSL when user data is traversing accross the internet from to the Sisoft WebHBYS application.

3 SECURITY TARGET

The Security Target associated with this Certification Report is identified by the following description of identity:

Title: Sisoft WEBHBYS v2.0.0.3 Security Target Document v1.9

Version: v1.9
Date: 16.07.2013

4 GLOSSARY

CCCS:	Common Criteria Certification Scheme (TSE)
CCTL:	Common Criteria Test Laboratory (OKTEM)
CCMB:	Common Criteria Management Board
CEM:	Common Evaluation Methodology
ETR:	Evaluation Technical Report
IT:	Information Technology
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
SHA:	Secure Hash Algorithm
HBYS	Hastane Bilgi Yönetim Sistemi
HIMS:	Healthcare Information Management System
HIS:	Hospital Information System
Evaluator:	TÜBİTAK BİLGEM OKTEM
Developer:	Sisoft Sağlık Bilgi Sistemleri
SSL	Secure Sockets Layer
HTTP	Hyper Text Transfer Protocol
HTTPS	Secure Hyper Text Transfer Protocol
RDBMS	Relational Database Management System
DBMS	Database Management System
TSE	Turkish Standards Institutions
TÜBİTAK	The Scientific and Technological Research Council of Turkey
BİLGEM	Informatics and Information Security Research Center

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 Criteria for Information Technology Security Evaluation, Evaluation Methodology Version 3.1 Revision 4, September 2012

[5]ETR - Sisoft WEBHBYS v2.0.0.3 Degerlendirme Teknik Raporu v1.0 - 14.08.2012

[6] Sisoft WEBHBYS Security Target 1.9 - 16.07.13

[7]YTBD-01-01TL-01 "CERTIFICATION REPORT PREPARATION INSTRUCTIONS"

[8] Sisoft WEBHBYS v2.0.0.3 Fonksiyonel Belirtim Dökümanı v2.1 (Functional Specification Doc.)

[9]Sisoft WEBHBYS v2.0.0.3 Konfigürasyon Yönetimi Dökümanı v2.3 (Configuration Management Doc.)

[10]Sisoft WEBHBYS v2.0.0.3 Kullanıcı Kılavuzu v2.1 (User Manual)

[11]Sisoft WEBHBYS v2.0.0.3 Tasarım ve Güvenli Mimari v1.1 (Design and Security Architecture)

[12]Sisoft WEBHBYS v2.0.0.3 Test Dökümanı v1.0 (Testing Document)

[13]Sisoft WEBHBYS v2.0.0.3 Teslim ve Kurulum Dökümanı v2.0 (Delivery and Installation Doc.)

6 ANNEXES

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