SQC Software & Systems Quality Conference in Düsseldorf April 2008

Static and Dynamic Analysis of an Internet Security System

Referent: Harry M. Sneed

Institut für Wirtschaftsinformatik I
University of Regensburg

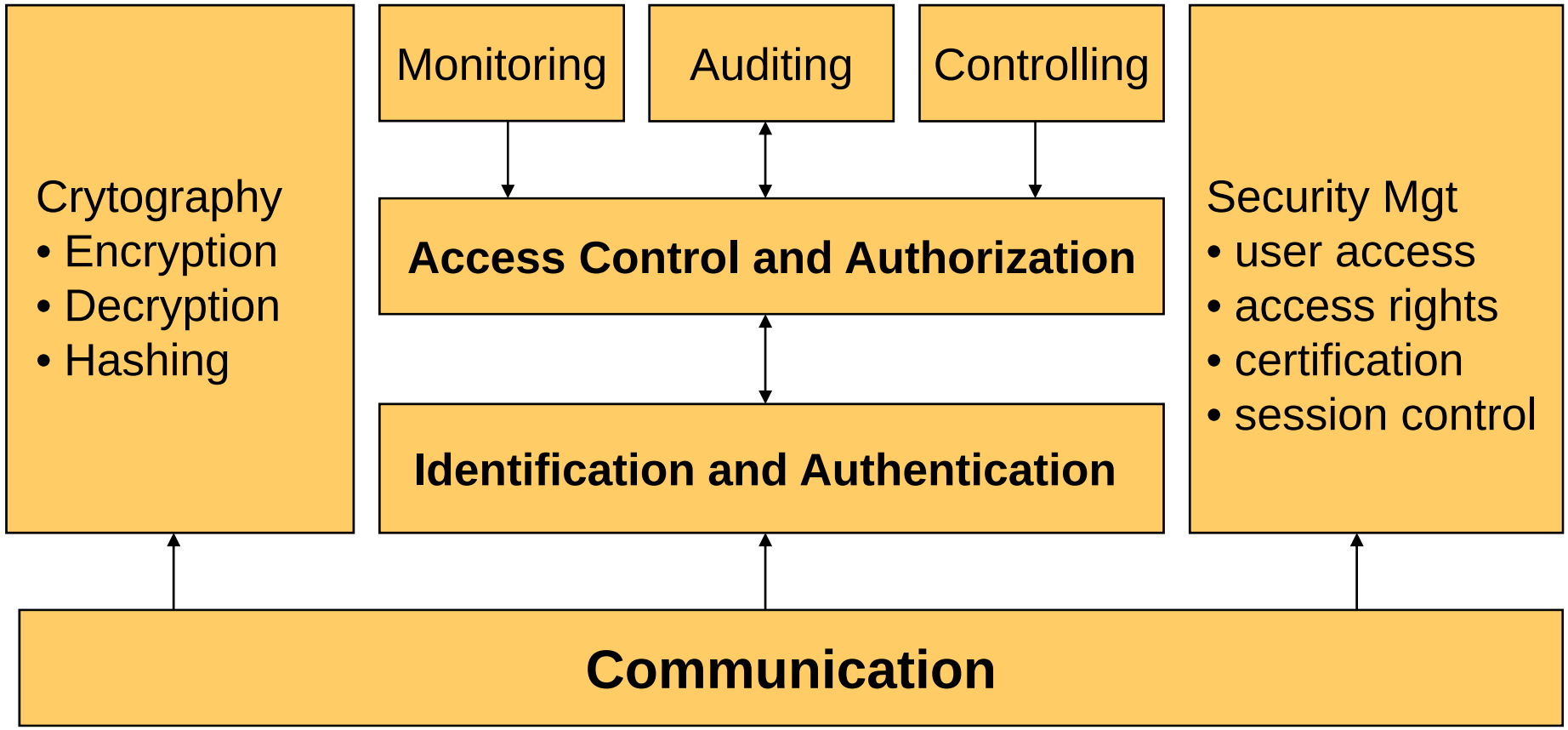
Presentation Structure

1. Description of the Security System assessed
2. Description of the Assessment Project
3. Description of the ISO-9126 standard
4. Results of the Static Analysis
5. Security Requirements Analysis
6. Security Test Plan
7. Security Test Cases
8. Results of the Dynamic Analysis
9. Defects uncovered
10. Final Assessment

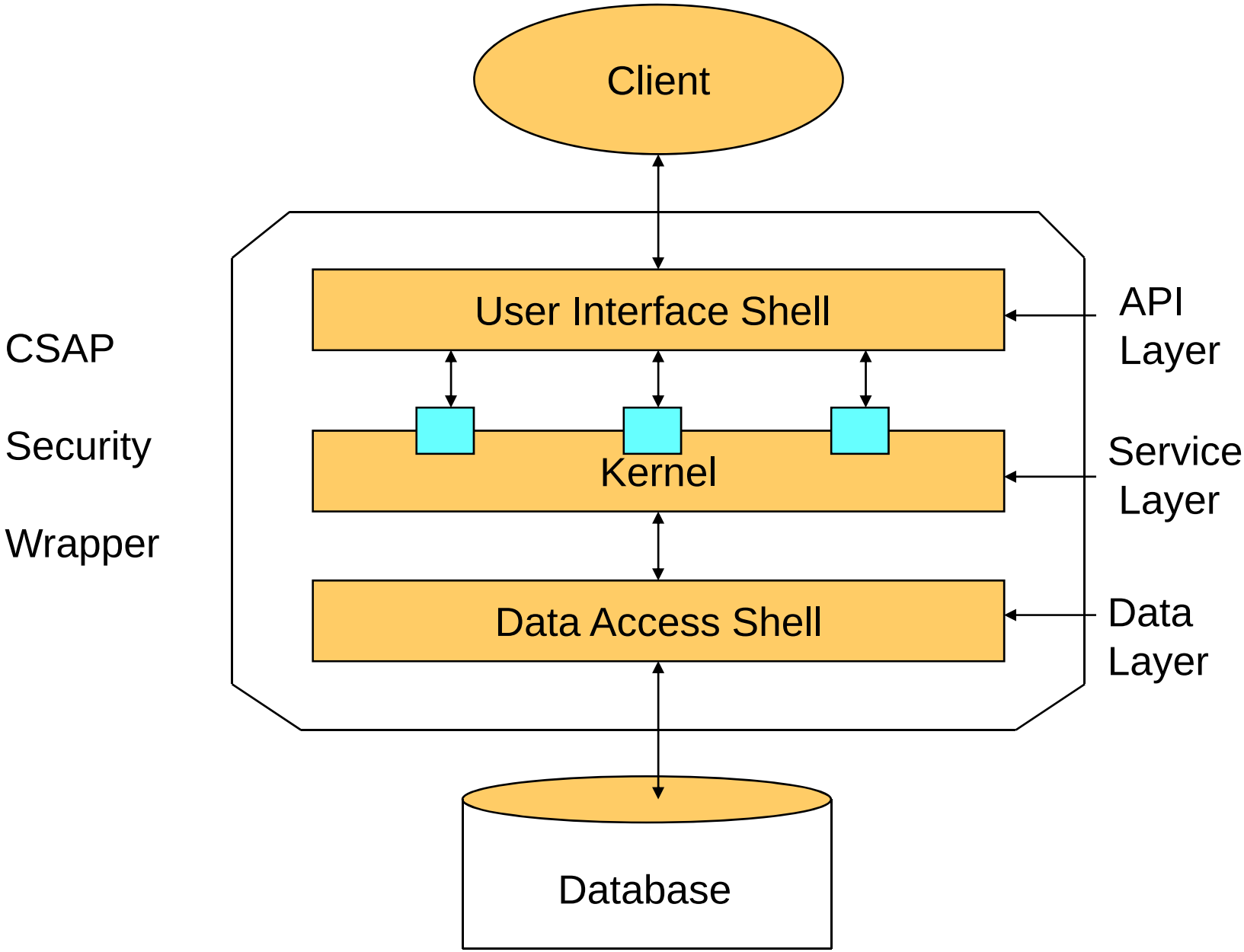
What is CSAP

- CSAP stands for Communication Security, Authentication and Privacy System
- CSAP is a security control system for eGov web applications developed at the University of Essen.
- CSAP defines roles and controls access to operations upon objects in an eGov network based on access rights.
- CSAP authenticates and authorizes users of an eGOV network and audits their sessions.
- CSAP is implemented as a security wrapper built around the three layers of a web application – User Interface, Kernel and Data Access Shell.
- CSAP has four main components – Authentication Service, Authorization Service, Auditing Service and Data Management

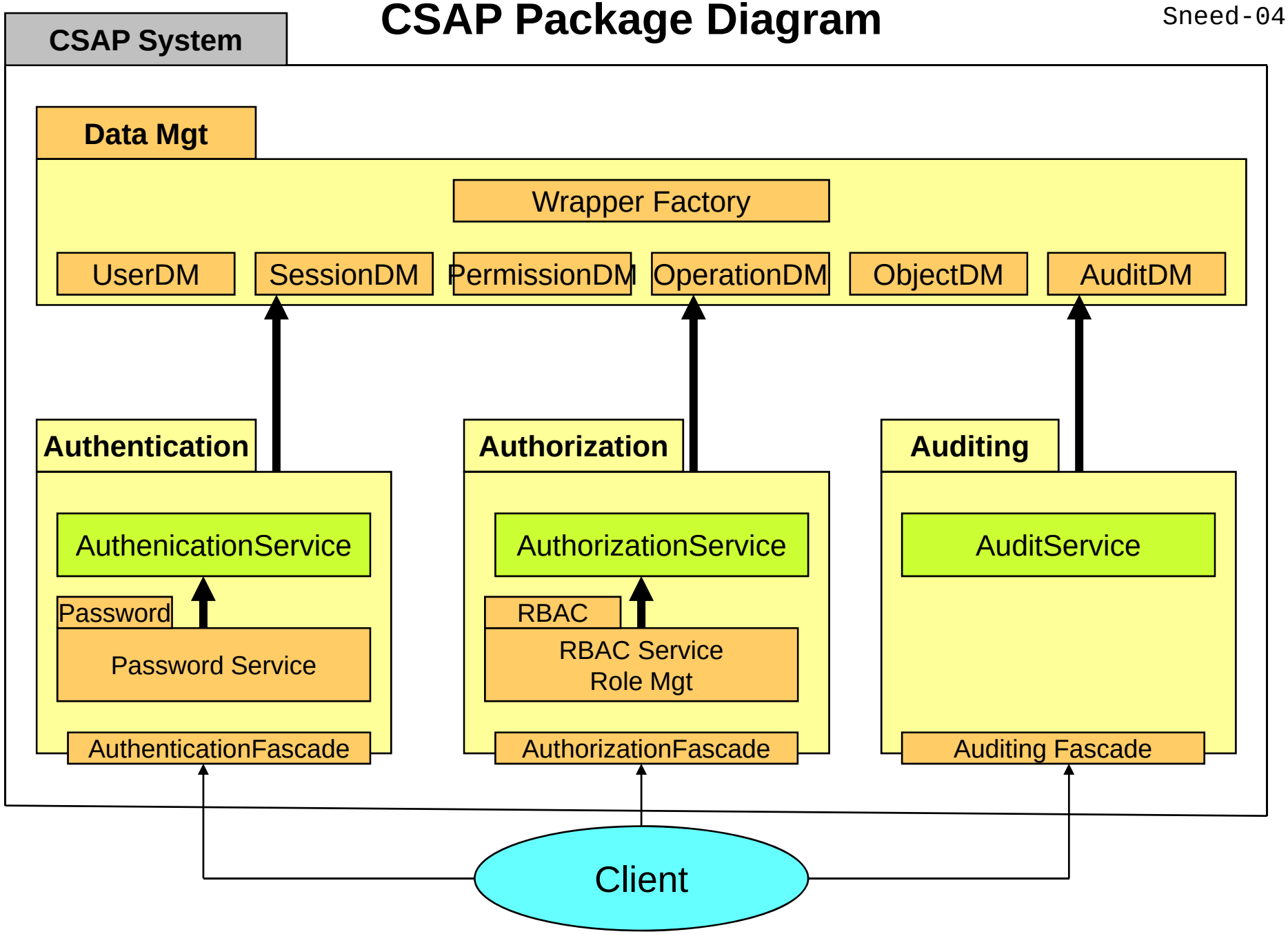
CSAP Security Architecture



CSAP Layered Architecture



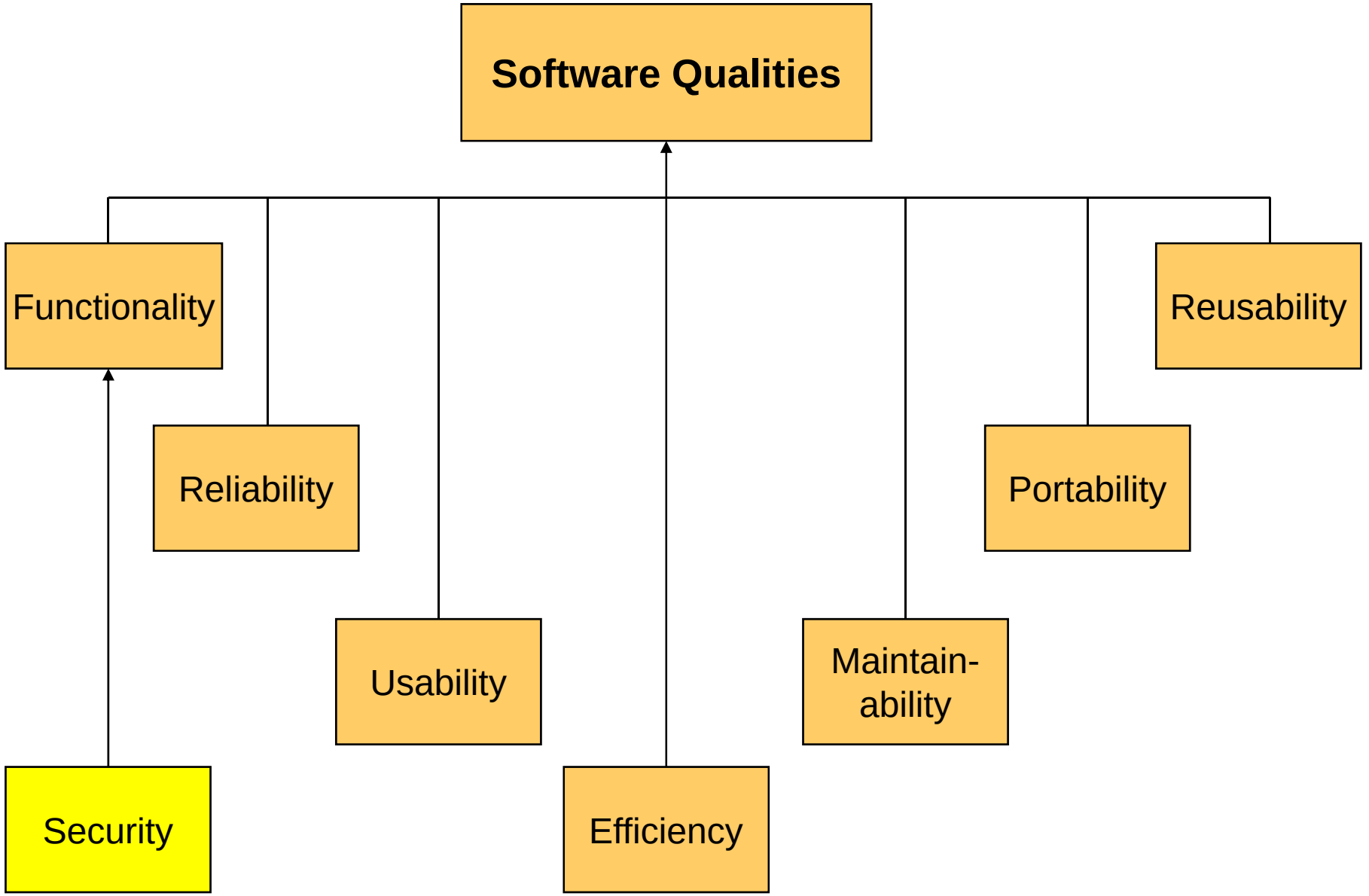
CSAP Package Diagram



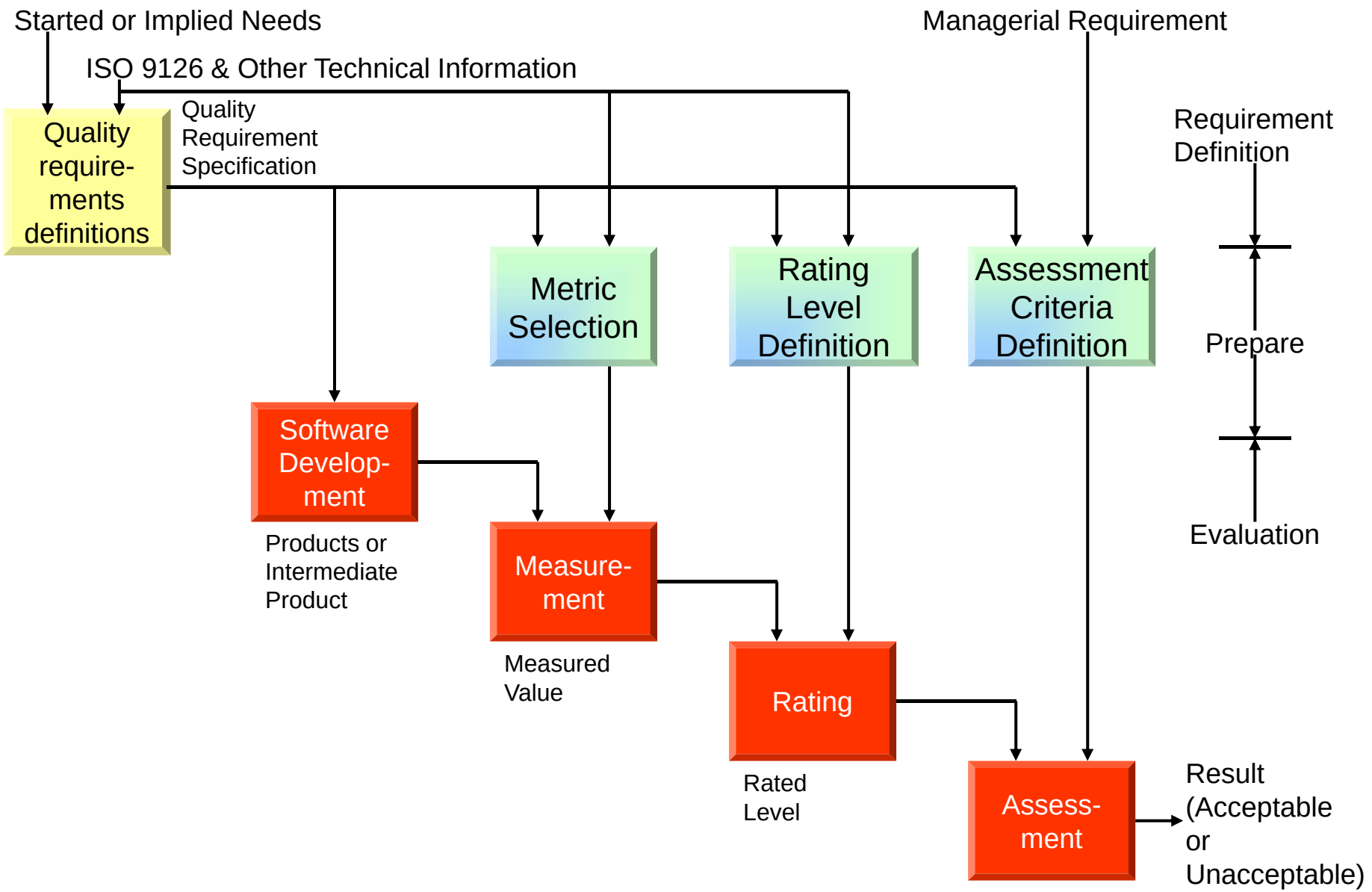
Purpose of Project

- Access_eGov is an EU sponsored project for networking local governments in Poland and Slovakia.
- The project partners are the universities of Krakow, Kosice and Regensburg as well as several local governments in Poland and Slovakia.
- The purpose of this project was to assess the CSAP system as to what extent it could be used to ensure the security of the Access_eGov network.
- It was decided to evaluate CSAP according to the quality criteria of the ISO-9126 standard.
- For this the assessment project was divided into two analysis subprojects:
  - a static analysis and
  - a dynamic analysis

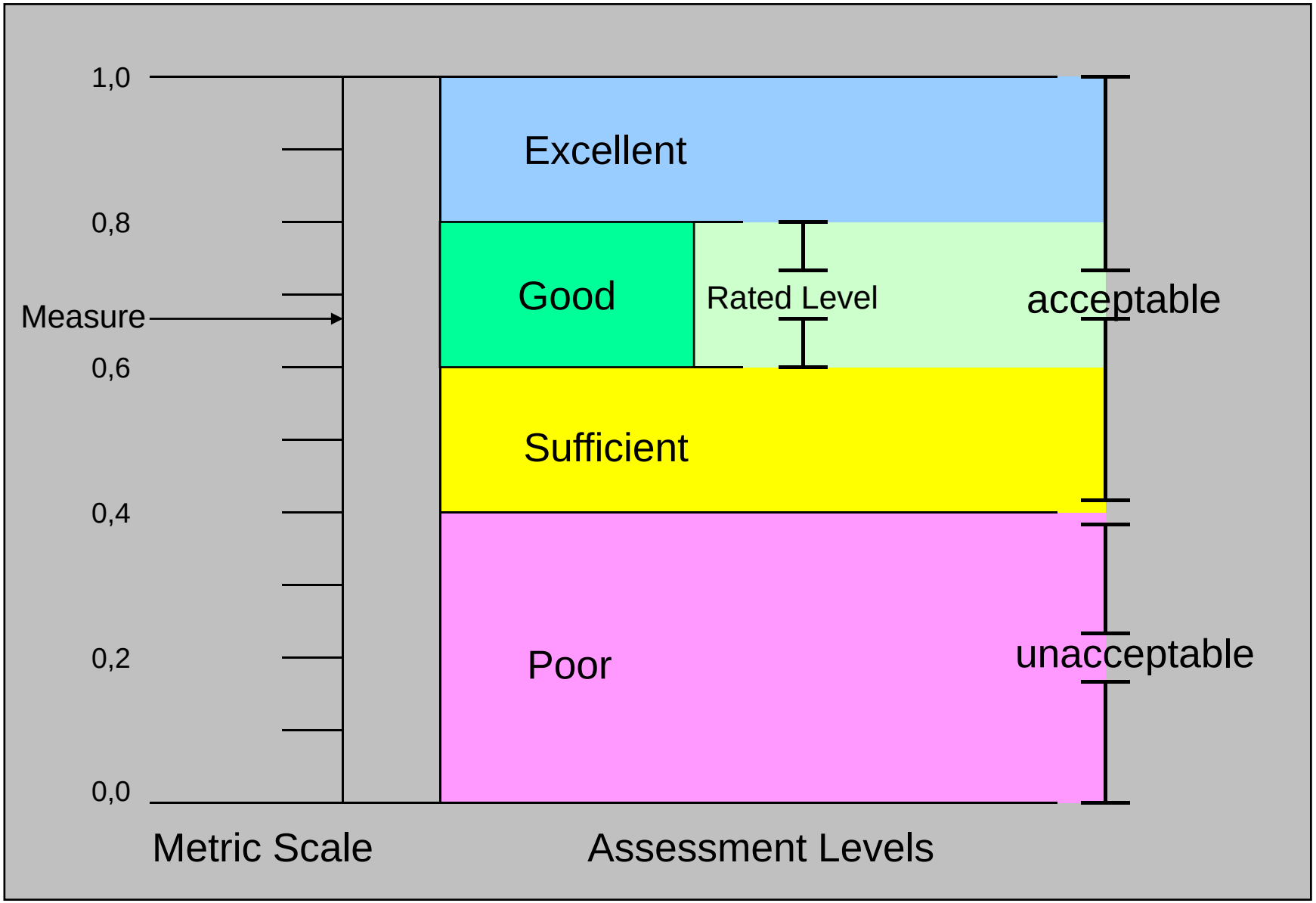
ISO-9126 Quality Characteristics



Product Assessment process according to ISO-9126



Product Assessment Scale of ISO-9126



Size, Complexity & Quality Measures

	source lines	Object - Points	Data - Points	Function Points	Programm Complexity	Programm Quality
csap	209	8	4	17	0,485	0,526
csap.auditing	172	34	41	23	0,562	0,457
csap.authentication	250	56	63	0	0,582	0,609
csap.authentication.passwd	114	23	25	3	0,526	0,453
csap.authorization	1157	260	243	35	0,563	0,532
csap.authorization.rbac	542	151	146	14	0,614	0,537
csap.common.config	284	53	81	19	0,611	0,417
csap.common.exceptions	204	39	60	5	0,374	0,541
csap.datamgt	117	37	20	0	0,51	0,475
csap.datamgt.adm	128	16	29	18	0,644	0,454
csap.datamgt.objdm	43	5	8	3	0,348	0,576
csap.datamgt.oprdm	43	5	8	3	0,348	0,576
csap.datamgt.pdm	79	12	16	3	0,593	0,467
csap.datamgt.rdm	319	62	66	8	0,601	0,531
csap.datamgt.sdm	107	16	13	3	0,571	0,497
csap.datamgt.udm	37	5	8	3	0,348	0,576
Mittelwerte	237,813	48,875	51,938	9,813	0,517	0,514

Coding Rule Violations

Package	major Rule Violations	media Rule Violations	minor Rule Violations	total Rule Violations	Number of Source Lines in all	Violations pro Lines of Code
csap	0	0	10	10	209	0,0478
csap.auditing	21	1	67	89	172	0,5174
csap.authentication	27	1	101	129	250	0,5160
csap.authentication.passwd	7	2	27	36	114	0,3158
csap.authorization	107	6	408	521	1157	0,4503
csap.authorization.rbac	62	5	253	320	542	0,5904
csap.common.config	46	2	97	145	284	0,5106
csap.common.exceptions	20	0	47	67	204	0,3284

System Size Assessment

C O D E Q U A N T I T Y M E T R I C S	
Number of Source Members analyzed	73
Number of Source Lines in all	5249
Number of Genuine Code Lines	2791
Number of Comment Lines	1832
Number of Major Rule Violations	289
Number of Medium Rule Violations	100
Number of Minor Rule Violations	1198
S T R U C T U R A L Q U A N T I T Y M E T R I C S	
Number of Modules	16
Number of Imports	63
Number of Classes declared	39
Number of Classes inherited	29
Number of Methods declared	256
Number of Methods inherited	40
Number of Interfaces implemented	27
Number of Interfaces declared	32
Number of Object-Points	1206
Number of Statements	2065

Total Static Quality Assessment

| DEGREE OF MODULARITY ========> 0.721
| DEGREE OF PORTABILITY ========> 0.680
| DEGREE OF FLEXIBILITY ========> 0.424
| DEGREE OF TESTABILITY ========> 0.477
| DEGREE OF CONVERTIBILITY ========> 0.900
| DEGREE OF REUSABILITY ========> 0.449
| DEGREE OF CONFORMITY ========> 0.452
| DEGREE OF MAINTAINABILITY ========> 0.518
|
| WEIGHTED PROGRAM QUALITY ========> 0.517

Security Requirements of CSAP

RQ-08:	For every system usage, a new session must be created.
RQ-09:	For the duration of a session all of the user activities must be connected and treated as a single transaction from the viewpoint of security.
RQ-10:	To open a session the user must first be authenticated.
RQ-11:	Every new user must first be registered with the system.
RQ-12:	A user must select a predefined role.
RQ-13:	A user may only select a role for which he has an authentication.
RQ-14:	A user may only perform operations upon objects assigned to the role he has selected.
RQ-15:	A session can only be closed by the user himself with a legitimate Logout or by the system through a timeout..
RQ-16:	All actions performed by a user must be recorded and written in a logfile.
RQ-17:	The Administrator must have the possibility to access and change all Users, Objects, Operations, Permissions, Sessions und Rolls. He should be allowed to insert, update and delete them.
RQ-18:	The Administrator must be able to update the RBAC Modell, by defining and changing users, roles, objects and operations.

CSAP Test Plan according to ANSI-IEEE 829

4. Functions to be tested.

Use cases specified [Fisc02, 62 f]:

· Bei Benutzung des Systems muss eine Sitzung eröffnet werden, die alle Einzelaktivitäten des Benutzers für die Dauer der Sitzung miteinander verknüpft. **[Session Establishing]**

· Bei Eröffnung einer Sitzung muss sich der Benutzer zunächst autorisieren **[User Logon]**

· Ist der Benutzer dem System noch nicht bekannt, kann er sich vor der Anmeldung registrieren **[User Registration]**

· Nach erfolgter Authentifikation kann der Benutzer die Rollen auswählen, die er zur Durchführung seiner Tätigkeiten benötigt **[Role Selection].**

· Wenn ein Client auf die Module des Webocrat - Systems zugreift, muss vor dem Zugriff bestimmt werden, ob der Client für die aktive Sitzung durch die aktivierten Rollen berechtigt ist, die gewünschte Aktion auszuführen **[Permission Approval]**

· Eine Sitzung muss geschlossen werden **[Session Closing]**

o Die Sitzung kann durch den Benutzer geschlossen werden **[Logout]**

o Die Sitzung wird nach Ablauf einer definierten Zeitspanne durch das Modul selbst geschlossen **[Timeout]**

· Alle Aktionen innerhalb des CSAP-Moduls werden protokolliert und für Auswertungszwecke gespeichert. Das Auditing ist Teil jedes Anwendungsfalls. **[Auditing]**

· Über das Sicherheitsmanagement wird die Zuordnung von Berechtigungen und Benutzern zu Rollen und die Verwaltung und Einrichtung von Rollen, sowie die Organisation der Berechtigungen verwaltet. **[Security Management]**

CSAP Test Design with XML

```
<TestProcess type="Batch" id="CSAP_TEST_13" name="Objektzugriffstest / Permission Approval Test">
   <TestObjective>Test if a user can access those objects to which he has the access rights</TestObjective>
   <TestPrerequisite>In MySQL DB is filled with test data</TestPrerequisite>
   <TestPrerequisite>In MySQL DB the user roles are allocated </TestPrerequisite>
   <TestPrerequisite>In MySQL DB the roles are assigned objects with permission to access </TestPrerequisite>
   <TargetRequirement>RQ-06-The user may only excute those operations to which he is authorized to
access</TargetRequirement>
   <TargetUseCase>UC-02-Permission Approval</TargetUseCase>
   <TargetObject>MySQL Datenbank</TargetObject>
   <TargetObject>Authorization</TargetObject>
   <TargetObject>DataManager</TargetObject>
   <ProcessSteps>
      <sequence>
        <ProcessStep name="Generation of_MySQL_Dump_File">
            <ProcessStepAction>Generate MySQL Dump Files to record database content</ProcessStepAction>
        </ProcessStep>
        <ProcessStep name="Initialize DB_with_MySQL_Dump_File">
            <ProcessStepAction>Initialize DB with MySQL Dump File</ProcessStepAction>
        </ProcessStep>
        <ProcessStep name="Generate Java Test Classes">
            <ProcessStepAction>Generate Java Test Driver Classes</ProcessStepAction>
        </ProcessStep>
        <ProcessStep name=„Execute Java Test Driver">
            <ProcessStepAction>Execute Java Test Class</ProcessStepAction>
        </ProcessStep>
      </sequence>
    </ProcessSteps>
```

CSAP Test Cases

Test Case	Req Nr	Priority	Tes Case Type	Test Case Purpose	Use Case	Test Objects
TC-01	RQ-01	1	Batch	Testen, ob bei Benutzung des System durch einen registrierten User eine Sitzung eröffnet wird	UC-01-01-User Logon; UC-01-03-Role Selection	MySQL Datenbank, Authentication, DataManager
TC-02	RQ-01	1	Batch	Testen, ob eine Session erzeugt wird. falls sich ein neuer User registriert und Rollen auswählt	UC-01-02-User Registration; UC-01-03-Role Selection	MySQL Datenbank, Authentication, DataManager, Registration
TC-03	RQ-02	1	Batch	Testen, ob bei Benutzung des System sich ein registrierter User authentifizieren muss	UC-01-01-User Logon	Authentication
TC-04	RQ-02	1	Batch	Testen, ob bei Benutzung des System sich ein neuer User authentifizieren muss	UC-01-02-User Registration	Authentication, Registration
TC-05	RQ-03	1	Batch	Testen, ob sich ein neuer Benutzer vor Anmeldung registrieren kann	UC-01-02-User Registration	MySQL Datenbank, Authentication, DataManager, Registration
TC-06	RQ-04	1	Batch	Testen, ob der Nutzer Rollen auswählen kann, die ihm zugeteilt sind	UC-01-03-Role Selection	MySQL Datenbank, Authorization, DataManager

Required Data Inputs

Test Case	Instance	Input Type	Input Data Name	Input Value
TC-04	1	Text	Name des neuen Benutzers zur Registrierung	newUser
TC-04	1	Text	Passwort des neuen Benutzers zur Registrierung	newPW
TC-04	1	Text	Name des Benutzers zur Authemtifikation	newUser
TC-04	1	Text	Passwort des Benutzers zur Authentifikation	newPW
TC-04	2	Text	Name des neuen Benutzers zur Registrierung	stefan
TC-04	2	Text	Passwort des neuen Benutzers zur Registrierung	passwort
TC-04	2	Text	Name des Benutzers zur Authemtifikation	stefan
TC-04	2	Text	Passwort des Benutzers zur Authentifikation	pw
TC-05	1	Text	Auswahl zur Registrierung	*nich festgelegt*
TC-06	1	Text	Name des Benutzers	test
TC-06	1	Text	Passwort des Benutzers	test
TC-06	1	Text	Auswahl der Rolle	test
TC-06	2	Text	Name des Benutzers	test
TC-06	2	Text	Passwort des Benutzers	test
TC-06	2	Text	Auswahl der Rolle	admin
TC-06	3	Text	Name des Benutzers	guest
TC-06	3	Text	Passwort des Benutzers	guest
TC-06	3	Text	Auswahl der Rolle	test

Expected Test Results

Test case	Instanc	Output Type	Output Name	Output Value
TC-01	1	SQL	Session_Table	neue Session ID
TC-01	2	SQL	Session_Table	neue Session ID
TC-01	3	SQL	Session_Table	neue Session ID
TC-01	4	SQL	Session_Table	keine neue Session ID
TC-01	5	SQL	Session_Table	neue Session ID
TC-02	1	SQL	Session_Table	neue Session ID
TC-02	1	SQL	User_Table	neue User ID
TC-02	2	SQL	Session_Table	keine neue Session ID
TC-02	2	SQL	User_Table	keine neue User ID
TC-03	1	GUI	Meldung	korrekte Authentifikation
TC-03	2	GUI	Meldung	korrekte Authentifikation
TC-03	3	GUI	Meldung	kein Zugang zu CSAP
TC-03	4	GUI	Meldung	v
TC-03	5	GUI	Meldung	keine Zugang zu CSAP
TC-03	6	GUI	Meldung	keine Zugang zu CSAP
TC-03	7	GUI	Meldung	keine Zugang zu CSAP
TC-03	8	GUI	Meldung	keine Zugang zu CSAP
TC-04	1	GUI	Meldung	korrekte Authentifikation
TC-04	2	GUI	Meldung	kein Zugang zu CSAP
TC-05	1	GUI	Meldung	Möglichkeit zur Authentifikation
TC-06	1	GUI	Meldung	Rolle
TC-06	2	GUI	Meldung	Access denied
TC-06	3	GUI	Meldung	Access denied

CSAP Method Instrumentation

```
public class PermissionService extends AbstractAuthorizationService
implements IPermissionService {
    /**
     * @throws RemoteException  */
    public PermissionService() throws RemoteException {
        super();
 /*001*/   Tracer.XTrace ("PermissionService",
"PermissionService_001");
    }
    public Vector enumerate(IUser admin, Map key) throws
RemoteException, PermissionException {
 /*002*/   Tracer.XTrace ("PermissionService", "enumerate_002");
        try {
            super.enumerate(admin, key);
            return pdm.enumerate(key);
        } catch (Exception e) {
            AuditService.error(this.getClass().getName() + ".get: " +
e.getMessage(), e);
        }
        return null;
    }
public IAbstractProduct get(IUser owner, Map data) throws
RemoteException {
 /*003*/   Tracer.XTrace ("PermissionService", "get_003");
```

CSAP Execution Trace


```
| PRODUCT: EGOV                                                                |
| DATE:   22.02.07                                          PAGE: 0047         |
|  Date       Time       Module name          Function executed                |
+------------------------------------------------------------------------------+
|  18.11.2006;20:13:10  ;AbstractMySqlWrapper;get_008                          |
|  18.11.2006;20:13:10  ;AbstractMySqlWrapper;getValidFields_003               |
|  18.11.2006;20:13:10  ;AbstractMySqlWrapper;createPreparedStatement_004      |
|  18.11.2006;20:13:10  ;AbstractMySqlWrapper;executeQuery_005                 |
|  18.11.2006;20:13:10  ;AbstractProduct     ;AbstractProduct_002              |
|  18.11.2006;20:13:10  ;Configurator        ;getService_005                   |
|  18.11.2006;20:13:10  ;AbstractProduct     ;setAttributes_010                |
|  18.11.2006;20:13:10  ;AbstractProduct     ;checkAttributes_009              |
|  18.11.2006;20:13:10  ;RBACService         ;Role_029                         |
|  18.11.2006;20:13:10  ;AbstractProduct     ;getOwner_008                     |
|  18.11.2006;20:13:10  ;RBACService         ;get_003                          |
|  18.11.2006;20:13:10  ;AbstractService     ;get_003                          |
|  18.11.2006;20:13:10  ;AbstractProduct     ;getOwner_008                     |
|  18.11.2006;20:13:10  ;AbstractMySqlWrapper;get_008                          |
|  18.11.2006;20:13:10  ;AbstractMySqlWrapper;getValidFields_003               |
|  18.11.2006;20:13:10  ;AbstractMySqlWrapper;createPreparedStatement_004      |
|  18.11.2006;20:13:10  ;AuditService        ;debug_008                        |
|  18.11.2006;20:13:10  ;AbstractMySqlWrapper;executeQuery_005                 |
|  18.11.2006;20:13:10  ;AbstractProduct     ;AbstractProduct_002              |
|  18.11.2006;20:13:10  ;AbstractProduct     ;initService_003                  |
|  18.11.2006;20:13:10  ;Configurator        ;getService_005                   |
|  18.11.2006;20:13:10  ;AbstractProduct     ;setAttributes_010                |
|  18.11.2006;20:13:10  ;AbstractProduct     ;checkAttributes_009              |
|  18.11.2006;20:13:10  ;RBACService         ;Role_029                         |
|  18.11.2006;20:13:10  ;AbstractProduct     ;getName_006                      |
```

CSAP Test Coverage

```
+-------------------------------------------------------------------+
|               T E S T   C O V E R A G E   R E P O R T             |
|                                                                   |
| PRODUCT: EGOV                                                     |
| SYSTEM : TEST                                                     |
| DATE:   22.02.07                                 PAGE: 0005       |
|                                                                   |
| Module Name          Function executed                Executions  |
+-------------------------------------------------------------------+
| AbstractService      get_003                             822      |
| AbstractService      add_004                             350      |
| AbstractService      update_005                           34      |
| AbstractService      delete_006                           78      |
| AbstractService      addCallback_007                       0   *  |
| AbstractService      removeCallback_008                    0   *  |
| AbstractService      getCallback_009                       0   *  |
+-------------------------------------------------------------------+
|                                                                   |
|                      Number of Test Probes inserted =        251  |
|                      Number of Test Probes executed =        164  |
|                      Number of Test Probes missed   =         87  |
|                      Coverage Ratio for this system =      0.653  |
+-------------------------------------------------------------------+
```

Recorded Errors by Test Case

Test Case	Error Description	Error Category
TC_05	The use case „Registration“ can not be executed because the a required class is missing.	3
TC_07 _ TC_12	The log file is missing info necessary for tracing. It is not recorded which user actions have been executed.	2
TC_20	Die Function "AuthorizationFac ade .checkAccess“ denies access to all test cases.	2
TC_22	Individual users can gain access to all objects via the AuthorizationFacade.getObject Method even though they are not the owner.	5

10 Recorded Errors

Error	Category
Function for Registration is missing (3).	Medium
Function for Session Closing is missing	Medium
Access to objects given to non-owners.	Fatal
RBAC Access Errors.	Fatal
Logging Omissions (2).	Minor
Erroneous CheckAccess Method.	Severe
Access Function missing for RBAC Service.	Medium

CSAP Test Metric Report

Metric Definition	Metric Type	Metric Value
Number of Test Cases specified	Absolute Count	23
Number of Test Cases executed	Absolute Count	23
Number of Code Modules	Absolute Count	26
Number of Code Statements	Absolute Count	2594
Number of Methods&Procedures coded	Absolute Count	253
Number of Methods&Procedures tested	Absolute Count	157
Number of Defects predicted	Absolute Count	12
Number of Defects in total	Absolute Count	10
Number of Critical Defects (8)	Absolute Count	2
Number of Severe Defects (4)	Absolute Count	1
Number of Major Defects (2)	Absolute Count	1
Number of Medium Defects (1)	Absolute Count	3
Number of Minor Defects (0.5)	Absolute Count	3
Number of Weighted Defects	Weighted Count	28
Defect Density Rate	Relational Scale	0.0054
Weighted Defect Density Rate	Relational Scale	0.0116
Case Coverage Rate	Relational Scale	1.000
Code Coverage Rate	Relational Scale	0.621
Test Coverage Rate	Relational Scale	0.621
Defect Coverage Rate	Relational Scale	0.933
Remaining Error Probability	Relational Scale	0.007
Weighted Error Probability	Relational Scale	0.016
System Trust Coefficient	Relational Scale	0.248
Test Effectiveness Coefficient	Relational Scale	0.962

Final Assessment of CSAP

Quality Characteristic	Quality Metric	Rating
Functionality	0,525	Sufficient
Reliability	0,370	Poor
Usability	0,650	Good
Efficiency	0,737	Good
Maintainability	0,518	Sufficient
Reusability	0,449	Sufficient
Portability	0,680	Good