



HELMUT SCHMIDT
UNIVERSITÄT

Universität der Bundeswehr Hamburg

Projektbezogenes Informationssicherheitskonzept

für die webbasierte Befragungs- & Prüfungssoftware

EvaSys & EvaExam

Stand: November 2022

Inhalt

1. Präambel	3
2. Projektidentifikation.....	3
2.1 Projektgegenstand	3
2.2 Projektziel.....	3
2.3 Funktionale und nicht-funktionale Anforderungen	3
2.4 Projektverantwortliche.....	4
2.5 Sicherheitseinstufung	4
2.6 Beziehungen und Abhängigkeiten.....	4
3. Aufgabe, Funktionale Struktur	4
3.1 Hauptaufgabe und Nebenaufgaben	4
3.2 Funktionale Struktur.....	5
3.3 Angaben zur Einsatzumgebung	6
3.4 Personal	6
3.5 Infrastrukturelle Randbedingungen	6
4. Informationsstruktur	6
4.1 Datenspeicherung	6
5. Systemstruktur	7
5.1 Hardware	7
5.2 Software	7
5.2.1 Clientseitig.....	7
5.2.2 Serverseitig	7
5.3 Netzwerk	7
6. Informationssicherheitsanforderungen, Risiken und Maßnahmen.....	8
6.1 Verfügbarkeit.....	8
6.2 Vertraulichkeit	8
6.3 Integrität.....	9
6.4 Serverseitige Maßnahmen	9
6.5 Clientseitige Maßnahmen	10
6.6 Nutzer	10
6.7 Verbleibende Risiken.....	10
7. Anlagen und Bezugsdokumente.....	10

1. Präambel

EvaSys ist eine auf Datenerfassungstechniken webbasierte Befragungs- & Prüfungssoftware mit Hilfe derer sich alle Phasen des Befragungs- und Prüfungsprozesses automatisieren lassen. Des Weiteren ermöglicht sie insbesondere eine schnelle und effektive Evaluation von Lehrveranstaltungen sowie Prüfungen.

Im Hochschulbereich wie auch im allgemeinen Bildungssektor bewährt EvaSys sich für Lehrevaluation und Bildungscontrolling-Maßnahmen von unterschiedlichem Umfang. Größtmögliche Automation und strukturierte Abläufe für die Formulargestaltung, Umfrageverwaltung sowie das Berichtswesen bilden die Grundlage für einen wirkungsvollen Evaluationsprozess.

EvaSys erlaubt dabei sowohl zentrale als auch dezentrale oder teilzentrale Evaluationsansätze und dient an der HSU UniBw Hamburg der zentralen Evaluation von Lehrveranstaltungen.

Dieses Informationssicherheitskonzept samt Anlagen unterwirft sich dem Informationssicherheitskonzept der HSU UniBw Hamburg.

2. Projektidentifikation

2.1 Projektgegenstand

Gegenstand dieses projektbezogenen Informationssicherheitskonzeptes ist der Einsatz der Lehrevaluationsplattform „EvaSys“ sowie „EvaExam“ der Firma evasys GmbH, Konrad-Zuse-Allee 13, 21337 Lüneburg, Deutschland.

2.2 Projektziel

Ziel ist es für alle Studierenden und Dozenten eine zeitgemäße, höchstmöglich verfügbare sowie Zeit und Ressourcen sparende Evaluationsplattform zur Verfügung zu stellen.

2.3 Funktionale und nicht-funktionale Anforderungen

Die wichtigsten funktionalen Anforderungen sind:

- Weltweiter sicherer Zugriff
- Evaluierung von online oder papiergebundenen Prüfungen sowie Umfragen
- Wahrung der Anonymität der Evaluierenden bei Umfragen

Die wichtigsten nicht-funktionalen Anforderungen sind:

- Die Forderungen des BDSG bzw. der DSGVO für die Auftragsverwaltung in Verbindung mit den Zentralen Dienstvorschriften A-2122/4 (Datenschutz) und A-960/1 (Informationssicherheit) müssen erfüllt sein.
- Das Projekt muss mit den vorhandenen Haushaltsmitteln und bis auf weiteres ohne zusätzliches Personal umsetzbar sein.

2.4 Projektverantwortliche

Projektverantwortlich für EvaSys ist der Leiter der Dienststelle der HSU UniBw Hamburg. Als Betreiber an der HSU UniBw Hamburg gilt das Dezernat I.3 - IT-Management.

2.5 Sicherheitseinstufung

Das Projekt ist als nicht sicherheitsrelevant einzustufen.

2.6 Beziehungen und Abhängigkeiten

Die beteiligten Personen werden zur Nutzung der Anwendungen in die Nutzergruppen Administratoren, Sekundäradministratoren, Teiladministratoren, Verifikatoren, Dekane, Studiendekane, Prüfer, Dozenten, Berichtsteller und Datenerfassungskräfte unterteilt und erhalten Konten mit entsprechenden Berechtigungen und Einsichten. Die Pflichtangaben zum Anlegen eines Kontos bestehen lediglich aus den Angaben Nachname, Benutzername & Passwort.

Die Teilnehmer der Umfragen sowie Prüfungen erhalten kein Konto. Teilnehmer authentifizieren sich per TAN-Verfahren an Onlineumfragen und Prüfungen, die Verbindung selbst wird durch HTTPS unter Nutzung von TLS 1.2 in 128-Bit SSL sowohl bei Teilnehmern als auch Anwendern verschlüsselt. Onlinebasierte Prüfungen verlangen zusätzlich die Matrikelnummer der Teilnehmenden.

Bei papiergebundenen Umfragen oder Prüfungen wird die Teilnahme anhand der Bogensatznummerierung der Bögen, die mit der entsprechenden Transaktionsnummer verknüpft ist, ermittelt.

Weder EvaSys noch EvaExam nutzen LDAP, eine Abfrage von Nutzerdaten aus dem Active Directory des Domänencontrollers der HSU findet nicht statt.

Zur Benachrichtigung der Anwender und Teilnehmer wie zum Verschicken der Transaktionsnummern bei Online-Befragungen & Prüfungen oder zum Versenden der Ergebnisse und Feedbackberichte greifen die EvaSys-Systeme auf den lokalen Mailserver des Rechenzentrums der HSU zurück.

Anhand dieser Teilinformationen ist keine Identifikation einer Person möglich.

3. Aufgabe, Funktionale Struktur

3.1 Hauptaufgabe und Nebenaufgaben

Die Hauptaufgabe des EvaSys-Systems besteht in der Erstellung und Auswertung von Umfragen sowie Prüfungen.

Diese können entweder in Papierform oder digital erstellt und durchgeführt werden. Nach Beendigung der Umfrage oder Prüfung wertet das System die gescannten Fragebögen oder digital erfassten Daten vollautomatisiert aus und liefert so schnell, personal- und ressourcenschonend Ergebnisse. Hierbei können verschiedene Berichte und Auswertungen erzeugt und den Bedürfnissen der Dozenten angepasst werden.

Die Befragungs- oder Prüfungsbögen in Papierform werden nach Beendigung der Umfrage von dem Dozenten an den Präsidialbereich übergeben. Handschriftliche Kommentare werden vor dem Scannen durch die Datenerfassungskraft des Präsidialbereichs anonymisiert, der anschließend vom System erstellte Feedbackbericht wird nach der Erstellung an die zuständige Person übertragen.

Die Dateneinsicht zu Prüfungsergebnissen obliegt alleine dem Prüfer. Eine Dateneinsicht für Administratoren ist nur nach expliziter Erlaubnis des Prüfers möglich.

Für technische Mitarbeiter existiert das Nutzerkonto des technischen Administrators. Unter dieser Sonderrolle stehen dem Anwender lediglich technische Einstellungsmöglichkeiten zur Verfügung. Dieses ermöglicht die Konfiguration und technische Administration ohne etwaige Einsicht in Prüfungs- oder Umfrageunterlagen.

Die Nebenaufgaben des EvaSys-Systems bestehen zum einen aus der Möglichkeit der freien Gestaltung der Umfrage- und Prüfungsbögen, dem Bereitstellen einer intelligenten Fragen- und Fragebogenbibliothek sowie dem Qualitätsmanagement durch Analysefunktionen.

3.2 Funktionale Struktur

Die EvaSys-Anwendungen werden als Clouddienst durch die evasys GmbH betrieben und sind für die Administratoren, Prüfer und Evaluierenden über die Hosting Server in Frankfurt am Main weltweit erreichbar.

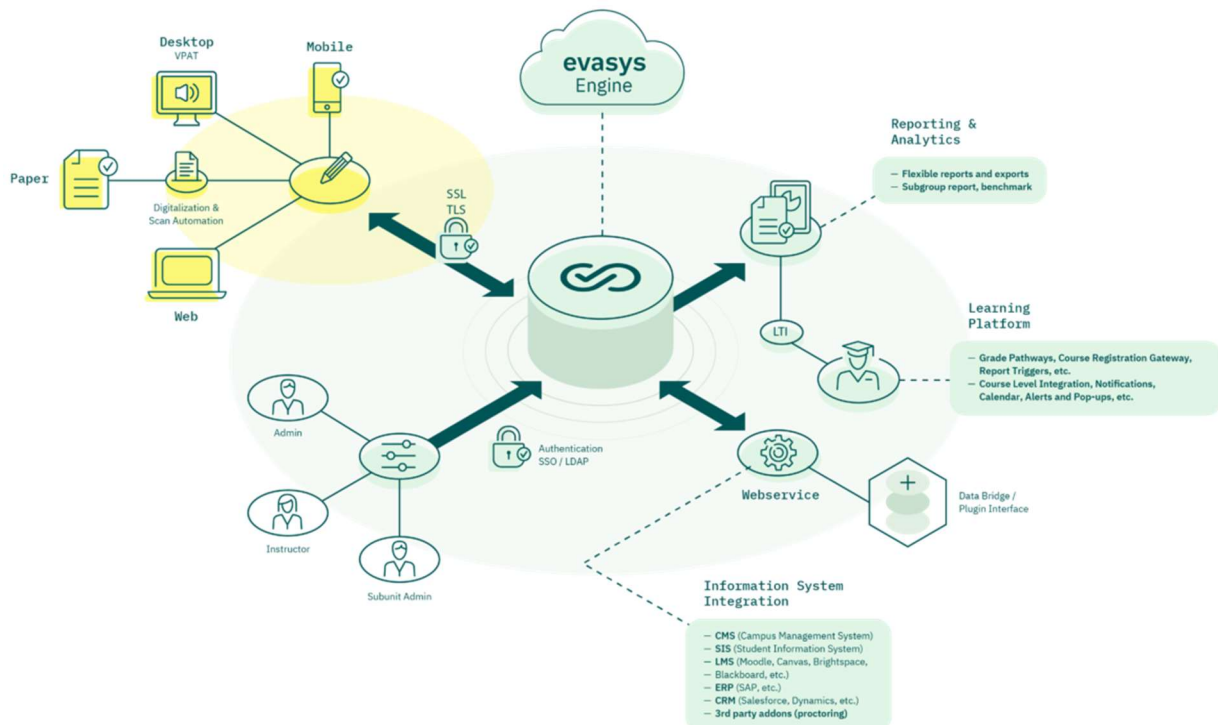


Abbildung 1 - Funktionale Struktur

Die Datenerfassung sowie -verarbeitung erfolgt dabei allein serverseitig durch digitalisierte, Papier gebundene Umfragen & Prüfungen, als auch über private oder dienstlich gelieferte Laptops &

Handys. Der Zugriff auf die Webservices erfolgt hierbei für alle Nutzergruppen über eine SSL verschlüsselte Verbindung (TLS v1.2).

3.3 Angaben zur Einsatzumgebung

- EvaSys & EvaExam werden als Clouddienst betrieben, die evasys GmbH nutzt hierfür Server aus der Rechenzentrumsregion Frankfurt am Main in Deutschland.
- Die evasys GmbH verpflichtet gemäß Artikel 28 DSGVO (1) nur Auftragsverarbeiter „...die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.“
- Die Transportverschlüsselung der Daten erfolgt durch HTTPS unter Nutzung von TLS 1.2
- Die Verschlüsselung der Daten auf den Servern erfolgt durch die Verwendung von Data Encryption at Rest, dem Verschlüsselungsstandard AES-256 sowie FIPS 140-2 konformer Ver- und Entschlüsselung.
- Clientseitig werden handelsübliche PCs, Laptops sowie Tablets und Smartphones verwendet.

3.4 Personal

Nutzer sind Mitarbeiter aus Lehre und Forschung, Studierende sowie zivile und militärische Mitarbeiter der HSU.

Administratoren sind Mitarbeiter des Dezernat I.3 und der Präsidialabteilung der HSU.

3.5 Infrastrukturelle Randbedingungen

Der Zugang zum Internet am Endgerät obliegt dem Nutzer, es handelt sich um Privatgeräte auf Seiten der User und durch das Dezernat I.3 bereitgestellte Endgeräte für die Administratoren.

4. Informationsstruktur

4.1 Datenspeicherung

Bei den von EvaSys & EvaExam ermittelten, bearbeiteten sowie übermittelten und gespeicherten Daten handelt es sich infolge der Anonymisierung nicht um personenbezogene Daten. Eine Datenübermittlung in Drittstaaten (Staaten außerhalb des Europäischen Wirtschaftsraums –EWR) findet wie im Datenschutzhinweise der Helmut-Schmidt-Universität/Universität der Bundeswehr Hamburg (HSU/UniBw H) nach Artikel 13 DSGVO gefordert ebenfalls nicht statt.

Folgende Daten werden erfasst und gespeichert:

- Gesamtheit der Strukturdaten
 - Name der Organisation
 - Teilbereiche (Fakultäten)
 - Nach- sowie Benutzername der angelegten Anwender
 - Email Adressen der angelegten Anwender sowie der Evaluierenden
- Sämtliche Befragungen mit Rohdaten sowie statistischen Kennwerten.

- Den Inhalt sowie die Auswertungsregeln aller Fragebögen.
- Betriebsdaten
 - Logbücher
 - Erhebungsperioden
 - TAN-Listen
- IP-Adressen
 - Jede HTTP/HTTPS-Anfrage an die EvaSys Systeme wird gespeichert
 - Bei einer erfolgreichen Anmeldung wird die entsprechende IP-Adresse geloggt und erst bei einer erneuten Anmeldung des Anwenders überschrieben.
 - Bei einem gescheiterten Anmeldeversuch in das Konto eines Anwenders, wird die IP-Adresse für mindestens 15 Minuten vorgehalten.

Fragebögen von papiergebundenen Umfragen werden am Ende einer jeden Evaluationsperiode, d.h. in der Mitte des auf die Lehrveranstaltung folgenden Trimesters vernichtet (geschreddert). Der digitale Scan der Fragebögen und alle mit einer Lehrveranstaltungsevaluation entstandenen Daten und Berichte werden über das laufende akademische Jahr und die beiden folgenden akademischen Jahre hinweg vorgehalten und im hierauf folgenden Januar vernichtet.

5. Systemstruktur

5.1 Hardware

Sämtliche verwendete Serverhardware ist Teil der oben genannten Cloudlösung und befindet sich nicht in den Räumlichkeiten der HSU.

5.2 Software

5.2.1 Clientseitig

Für die Teilnahme der User an Umfragen sowie Prüfungen ist keine gesonderte Software notwendig. Der Zugriff erfolgt über einen Standard-Browser wie Microsoft Edge, Chrome, Mozilla Firefox oder Safari.

5.2.2 Serverseitig

Die einzelnen Produkte, EvaSys sowie EvaExam, werden durch die evasys GmbH jeweils auf einer eigenen VM gehostet und von dieser betreut sowie gewartet. Jegliches Installieren oder Updaten der Software wird durch Mitarbeiter der evasys GmbH durchgeführt.

5.3 Netzwerk

Für den Übergang der DMZ der HSU wird die Firewall des RZ genutzt. Bei Nutzung privater Geräte außerhalb des Campus ist das Netzwerk der HSU nicht beteiligt.

6. Informationssicherheitsanforderungen, Risiken und Maßnahmen

6.1 Verfügbarkeit

Anforderung: Eine Verfügbarkeit der Server bei Dauerbetrieb (24/7) von >95%.

Risiken: Beeinträchtigung von Arbeits-, Lehr- und Lernprozessen bei Nichtverfügbarkeit.

Maßnahmen des Cloud-Dienstleisters:

- Durch Virtualisierung ist die Wahrscheinlichkeit eines Hardwaredefekts minimiert und eine Skalierbarkeit der Rechenleistung bei Lastspitzen möglich.
- Backup und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
- Sicherung der Backups an zwei verschiedenen Sicherungsstandorten mit jeweils drei Replikaten.
- Regelmäßige Überprüfung der Backups auf Wiederherstellbarkeit.
- Monitoring des Hosting-Servers & dauerhafter DDoS-Schutz.
- Definierte Eskalationskette für den Fehler- oder Katastrophenfall zur schnellstmöglichen Wiederherstellung und Bereitstellung des Systems.
- Schutz der Server vor Stromausfällen mittels USV.
- Schutz der Räumlichkeiten vor Brandschäden durch eine eigene Betriebsfeuerwehr.
- Anbindung der Server mittels Glasfasernetz.
- Die evasys GmbH selbst garantiert eine durchschnittliche Server-Verfügbarkeit von >99%.

6.2 Vertraulichkeit

Anforderung: Vertraulichkeit der Zugangsdaten.

Risiken: Zugriff auf personenbezogene Daten durch Unbefugte, digitaler Identitätsraub, Abfluss von personenbezogenen Daten in die USA durch den Cloud-Dienstleister Microsoft Azure.

Maßnahmen der evasys GmbH:

- Daten sind während des Transports HTTPS-verschlüsselt unter Nutzung von TLS 1.2
- Die Verschlüsselung der Daten auf den Servern erfolgt durch die Verwendung von Data Encryption at Rest, dem Verschlüsselungsstandard AES-256 sowie FIPS 140-2 konformer Ver- und Entschlüsselung.
- Verwendung von Azure DDoS Protect Basic.
- Server-Passwörter sind nur der evasys GmbH bekannt und entsprechen der Passwortrichtlinie der Firma.
- Dokumentierte Schlüsselvergabe an Mitarbeiter der evasys GmbH.
- Durchgehende Eingangskontrolle während der Geschäftszeiten.
- Alarmanlage mit Alarmierung eines Wachdienstes außerhalb der Geschäftszeiten.
- Regelmäßige Überprüfung der technischen und organisatorischen Maßnahmen des Cloudanbieters durch die evasys GmbH.
- Regelmäßige Prüfung der Infrastruktur durch externe Pen-Tests.

Maßnahmen des Cloud-Dienstleisters:

- Elektronische Zutrittskontrolle mit Protokollierung
- Hochsicherheitszaun um das gesamte Rechenzentrum.

- Dokumentierte Schlüsselvergabe an Mitarbeiter.
- Begleitung und Kennzeichnung von Gästen.
- Dauerhafte (24/7) personelle Besetzung des Rechenzentrums.
- Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen.
- Serverstandort in Frankfurt am Main in Deutschland und DSGVO konform.
- Defekte Festplatten werden direkt im Rechenzentrum zerstört (geschreddert).

6.3 Integrität

Anforderung: Integrität des Datenbestandes.

Risiken: Unbefugte oder unbeabsichtigte Veränderung von Daten sowie unbefugter Zugriff auf diese.

Maßnahmen zur unbefugten Veränderung:

- Server-Passwörter sind limitiert auf befugtes und datenschutzrechtlich geschultes Personal der evasys GmbH.
- Die Anmeldedaten zur EvaSys Anwendung sind nur den Administratoren des Dezernat I.3 und limitierten Mitgliedern der Präsidialabteilung der HSU UniBw bekannt.
- Rechte- und Rollensystem innerhalb der EvaSys Anwendung zur Einschränkung von Änderungsmöglichkeiten und Zugriffsrechten.

Maßnahmen zur unbeabsichtigten Veränderung:

- Backup und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten für einen Zeitraum von 30 Tagen.
- Sicherung der Daten an zwei verschiedenen Sicherungsstandorten mit jeweils drei Replikaten.
- Die Datenwiederherstellung kann beauftragt werden und wird durch die evasys GmbH durchgeführt.
- Es ist eine Wiederherstellung des gesamten Systems oder einzelner Daten möglich.
- Live Support durch die evasys GmbH bei Problemen jeglicher Art.

6.4 Serverseitige Maßnahmen

Anforderung: Ständige Aktualität der Server sowie der EvaSys Anwendungen.

Risiken: Daten- und Zeitverlust durch verspätetes Einspielen von Updates oder Infektion mit Schadsoftware.

Maßnahmen:

- Verfügbare Upgrades und Updates der EvaSys Anwendungen werden Zeitnah installiert, das System ist somit stets aktuell.
- Mindestens alle 14 Tage erfolgt eine Prüfung auf eine Verfügbarkeit von Sicherheitsaktualisierungen für die Server und deren unverzügliche Installation.
- Die Aktualisierung der Sicherheitssoftware (Antiviren-Software) wird täglich geprüft. Unter keinen Umständen wird die Aktualisierung durch die evasys GmbH über mehr als 7 Tage ausgesetzt.

- Die Server-Datenträger werden regelmäßig (mindestens einmal im Monat) auf schädliche Software überprüft. Bei einer Infizierung wird eine Neuinstallation des Systems vorgenommen.
- Zur Absicherung der einzelnen VMs werden Netzwerksicherheitsgruppen gebildet. Hierbei werden alle nicht für das Produkt benötigten Dienste & Netzwerkports blockiert.

6.5 Clientseitige Maßnahmen

Anforderung: Standort, Geräte und gesundheitlich unabhängige Teilnahme an Umfragen und Prüfungen.

Risiken: Nutzung der Dienste mittels veralteter Software, bedingt durch private Hardware.
Diskriminierung von Menschen mit Behinderungen.

Maßnahmen:

- Regelmäßige Belehrung und Sensibilisierung der User.
- Zugriff der Administratoren des Dezernat I.3 und der Mitglieder der Präsidialabteilung erfolgt ausschließlich über durch das Dezernat I.3 der HSU bereitgestellte Hardware.
- Erstellte Umfragen können automatisch durch EvaSys auf Barrierefreiheit gemäß WCAG 2.1 AA geprüft werden um zu gewährleisten, dass Menschen mit Behinderungen und Menschen mit temporären Einschränkungen die Zugänglichkeit gewährleistet wird.

6.6 Nutzer

Die Nutzer der HSU werden jährlich gemäß Informationssicherheitsbelehrung nachweislich belehrt. Fehlbedienungen können nicht ausgeschlossen werden.

6.7 Verbleibende Risiken

Zu den Restrisiken zählen unter anderem die Möglichkeit der Einsicht in Daten einzelner Nutzer durch infizierte private Endgeräte und ein Abfluss von Daten in die USA durch den Cloud-Anbieter der evasys GmbH Microsoft.

Die Restrisiken werden als tolerierbar angesehen, die Vorteile der Verfügbarkeit überwiegen diese.

7. Anlagen und Bezugsdokumente

- A-960/1 Zentrale Dienstvorschrift Informationssicherheit in der Bundeswehr, Version 2
- A-2122/4 Zentrale Dienstvorschrift Datenschutz, Version 2
- Datenschutzerklärung der Helmut-Schmidt-Universität/Universität der Bundeswehr Hamburg (HSU/UniBw H) nach Artikel 13, 14 und 21 DSGVO – Juni 2020
- Datenschutzhinweise der Helmut-Schmidt-Universität/Universität der Bundeswehr Hamburg (HSU/UniBw H) nach Artikel 13 DSGVO für Lehrveranstaltungsevaluation – Dezember 2021
- EvaSys – Informationen zu Datenschutz und Anwendungssicherheit V8.2 – September 2021
- EvaExam – Informationen zu Datenschutz und Anwendungssicherheit V8.2 – September 2021
- EvaSys – Technikhandbuch V8.2 – September 2021

- EvaExam – Technikhandbuch V8.2– September 2021
- EvaSys – Nutzung von Produkten der evasys GmbH mittels Cloud-Technologie – November 2021
- EvaSys - Technische und organisatorische Maßnahmen für Live-Support und Hosting – Juni 2021
- EvaSys – Informationen zum Hosting-Dienstleister Microsoft AZURE – Februar 2021
- EvaSys – Factsheet Managed Hosting – Oktober 2021
- Abbildung 1 – Funktionale Struktur – Quelle: <https://evasys.de/evasys/>